Oracle<sup>®</sup> Retail Store Inventory Management Installation Guide Release 16.0.3 F28523-02

October 2020



Copyright © 2020, Oracle. All rights reserved.

Contributors: Nathan Young, Shreyas S Manipura

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**<sup>™</sup> 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, reengineering 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

Se	end Us Your Comments	ix
Pr	eface	xi
	Audience	xi
	Customer Support	xi
	Review Patch Documentation	xi
	Improved Process for Oracle Retail Documentation Corrections	xii
	Oracle Retail Documentation on the Oracle Help Center docs.oracle.com	xii
	Conventions	xii
1	Preinstallation Tasks	1
	Implementation Capacity Planning	1
	Check Supported Database Server Requirements	
	Check Supported Application Server Requirements	3
	Check Single Sign-On Requirements	4
	Check Directory Server Requirements	
	Check Third-Party Software Dependencies	4
	Check Client PC and Web Browser Requirements	4
	Supported Oracle Retail Products	5
	UNIX User Account Privileges to Install the Software	
	SIM Installation Overview	5
2	RAC and Clustering	7
3	Database Installation Tasks	9
	Expand the SIM Database Schema Installer Distribution	9
	Required Database Character Set	
	Required Tablespaces	0
	Required Tablespaces	9
	Create the SIM Database User	
	1 I	10
	Create the SIM Database User	10 12
	Create the SIM Database User Run the SIM Database Schema Installer	10 12 12
	Create the SIM Database User Run the SIM Database Schema Installer Grant Privileges for the Roles	10 12 12 13
	Create the SIM Database User Run the SIM Database Schema Installer Grant Privileges for the Roles Create Synonyms for Additional users	10 12 12 13 13
	Create the SIM Database User Run the SIM Database Schema Installer Grant Privileges for the Roles Create Synonyms for Additional users Resolving Errors Encountered During Database Schema Installation	10 12 13 13 14
	Create the SIM Database User Run the SIM Database Schema Installer Grant Privileges for the Roles Create Synonyms for Additional users Resolving Errors Encountered During Database Schema Installation Data Seeding	10 12 12 13 13 14 14
	Create the SIM Database User Run the SIM Database Schema Installer Grant Privileges for the Roles Create Synonyms for Additional users Resolving Errors Encountered During Database Schema Installation Data Seeding Prerequisite	10 12 12 13 13 14 14 14
	Create the SIM Database User Run the SIM Database Schema Installer Grant Privileges for the Roles Create Synonyms for Additional users Resolving Errors Encountered During Database Schema Installation Data Seeding Prerequisite Data Seeding Setup	
	Create the SIM Database User Run the SIM Database Schema Installer Grant Privileges for the Roles Create Synonyms for Additional users Resolving Errors Encountered During Database Schema Installation Data Seeding Prerequisite Data Seeding Setup Export Seed Data	10 12 12 13 13 14 14 14 15 15
4	Create the SIM Database User Run the SIM Database Schema Installer Grant Privileges for the Roles Create Synonyms for Additional users Resolving Errors Encountered During Database Schema Installation Data Seeding Prerequisite Data Seeding Setup Export Seed Data Ftp Export Data Files	
4	Create the SIM Database User Run the SIM Database Schema Installer Grant Privileges for the Roles Create Synonyms for Additional users Resolving Errors Encountered During Database Schema Installation Data Seeding Prerequisite Data Seeding Setup Export Seed Data Ftp Export Data Files Import Seed Data	10 12 12 13 13 13 14 14 14 14 15 15 15 15
4	Create the SIM Database User Run the SIM Database Schema Installer Grant Privileges for the Roles Create Synonyms for Additional users Resolving Errors Encountered During Database Schema Installation Data Seeding Prerequisite Data Seeding Setup Export Seed Data Ftp Export Data Files Import Seed Data <b>Database Installation Tasks – Upgrade</b>	

	Set Environment Variables	18
	Run the Upgrade Scripts	18
	Compile Invalid Objects	18
	Check Logs	18
	Grant Privileges for the Roles	18
	Create Synonyms for Additional Users	18
5	Application Installation Tasks	20
	Middleware Infrastructure and Weblogic Server12c (12.2.1.4.0) Installation	20
	Install RCU Database Schemas	25
	Create a New ADF Domain (with managed server and EM)	33
	Start the Node Manager	46
	Start the AdminServer (admin console)	46
	Start the Managed Server	47
	Configuration of OID LDAP Provider in Weblogic Domain:	
	Verify OID Authenticator	53
	Clustered Installations - Pre-Installation Steps	53
	Expand the SIM Application Distribution	54
	Loading SIM LDIFs into the OID	55
	Set the Environment Variables for the SIM Installer	55
	Clustered Installations - Post-Installation Steps	56
	SIM Database Authentication Provider set up (to be done after the application	
	deploy)	
	Review and/or Configure Oracle Single Sign-On	
	Create the SIM SSO provider in the SIMDomain	
	SIM Batch Scripts	
	Resolving Errors Encountered During Application Installation	
	Web Help Files	
	Starting and Stopping the Wavelink Server	
6	Test the SIM Application	65
Α	Appendix: SIM Database Schema Installer Screens	67
В	Appendix: SIM Application WebLogic Server Installer Screens	73
С	Appendix: Common Installation Errors	139
	EJB Deployment Errors during Installation to WebLogic	139
	Output Freezes during Text Mode Installation to WebLogic	139
	Database Installer Hangs on Startup	140
	Warning: Could not create system preferences directory	140
	Warning: Couldn't find X Input Context	140
	ConcurrentModificationException in Installer GUI	141
	A Second Login Screen Appears After Single Sign-On Login	141
	Error Connecting to Database URL	
	GUI screens fail to open when running Installer	

D Appendix: Setting up SIM Reports/Tickets in BI Publisher       14         BiPublisher 12c - BI Server Component Installation Tasks       14         BiPublisher 12c only - Installation Process Overview       14         Post install steps for BiPublisher 12C       14         Installing the SIM BI Publisher Templates       14         Configuring the SIM JDBC connection       14         Verify Oracle BI Publisher Set Up for SIM Reports       15         Configuring SIM for CUPS printers using BIPublisher 12c       15         E Appendix: Single Sign-On for WebLogic       15         What Do I Need for Single Sign-On?       15         Can Oracle Access Manager Work with Other SSO Implementations?       15         What Single Sign-On is not       15         How Oracle Single Sign-On Works       15         Installation Overview       15         User Management       15
BiPublisher 12c only - Installation Process Overview       14         Post install steps for BiPublisher 12C
Post install steps for BiPublisher 12C
Installing the SIM BI Publisher Templates
Configuring the SIM JDBC connection14Verify Oracle BI Publisher Set Up for SIM Reports15Configuring SIM for CUPS printers using BIPublisher 12c15E Appendix: Single Sign-On for WebLogic15What Do I Need for Single Sign-On?15Can Oracle Access Manager Work with Other SSO Implementations?15Oracle Single Sign-On Terms and Definitions15What Single Sign-On is not15How Oracle Single Sign-On Works15Installation Overview15
Verify Oracle BI Publisher Set Up for SIM Reports       15         Configuring SIM for CUPS printers using BIPublisher 12c       15         E Appendix: Single Sign-On for WebLogic       15         What Do I Need for Single Sign-On?       15         Can Oracle Access Manager Work with Other SSO Implementations?       15         Oracle Single Sign-On Terms and Definitions       15         What Single Sign-On is not       15         How Oracle Single Sign-On Works       15         Installation Overview       15
Configuring SIM for CUPS printers using BIPublisher 12c15E Appendix: Single Sign-On for WebLogic15What Do I Need for Single Sign-On?15Can Oracle Access Manager Work with Other SSO Implementations?15Oracle Single Sign-on Terms and Definitions15What Single Sign-On is not15How Oracle Single Sign-On Works15Installation Overview15
E Appendix: Single Sign-On for WebLogic       15         What Do I Need for Single Sign-On?       15         Can Oracle Access Manager Work with Other SSO Implementations?       15         Oracle Single Sign-on Terms and Definitions       15         What Single Sign-On is not.       15         How Oracle Single Sign-On Works       15         Installation Overview       15
What Do I Need for Single Sign-On?15Can Oracle Access Manager Work with Other SSO Implementations?15Oracle Single Sign-on Terms and Definitions15What Single Sign-On is not15How Oracle Single Sign-On Works15Installation Overview15
Can Oracle Access Manager Work with Other SSO Implementations?
Oracle Single Sign-on Terms and Definitions
What Single Sign-On is not15How Oracle Single Sign-On Works15Installation Overview15
How Oracle Single Sign-On Works
Installation Overview15
User Management15
F Appendix: Setting Up Password Stores with wallets/credential stores
About Database Password Stores and Oracle Wallet16
Setting Up Password Stores for Database User Accounts16
Setting up Wallets for Database User Accounts16
For RMS, RWMS, RPM Batch using sqlplus or sqlldr, RETL, RMS, RWMS, and
ARI
Setting up RETL Wallets
For Java Applications (SIM, ReIM, RPM, RIB, AIP, Alloc, ReSA, RETL)
How does the Wallet Relate to the Application?
How does the Wallet Relate to Java Batch Program use?
Database Credential Store Administration
Managing Credentials with WSLT/OPSS Scripts
listCred
updateCred
deleteCred17
deleteCred

н	Appendix: Database Parameter File	191
L	Appendix: Installation Order	193
	Enterprise Installation Order	.193

## **Send Us Your Comments**

Oracle Retail Store Inventory Management, Installation Guide, Release 16.0.3

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

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

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

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

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

Send your comments to us using the electronic mail address: retail-doc\_us@oracle.com Please give your name, address, electronic mail address, and telephone number (optional).

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

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

## Preface

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

### Audience

This Installation Guide is written for the following audiences:

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

### **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, 16.0) or a later patch release (for example, 16.0.3). 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 Help Center 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 Help Center at the following URL:

https://docs.oracle.com/en/industries/retail/index.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 Help Center docs.oracle.com

Oracle Retail product documentation is available on the following web site: https://docs.oracle.com/en/industries/retail/index.html

(Data Model documents are not available through docs.oracle.com. 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
```

**Note:** In the images or examples below, user details / company name / address / email / telephone number represent a fictitious sample. Any similarity to actual persons, living or dead is purely coincidental and not intended in any manner.

# 1 Preinstallation Tasks

This chapter discusses the tasks to complete before installation.

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

### Implementation Capacity Planning

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

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

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

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

### **Check Supported Database Server Requirements**

General Requirements for a database server running SIM include:

Supported on:	Versions Supported:	
Database Server OS	OS certified with Oracle Database 12cR1 and 19c Enterprise Edition. Options are:	
	<ul> <li>Oracle Linux 6 and 7 for x86-64 (Actual hardware or Oracle virtual machine).</li> </ul>	
	<ul> <li>Red Hat Enterprise Linux 6 and 7 for x86-64 (Actual hardware or Oracle virtual machine).</li> </ul>	
	<ul> <li>AIX 7.1 (Actual hardware or LPARs)</li> </ul>	
	• Solaris 11.x SPARC (Actual hardware or logical domains)	
Database Server 12cR1	Oracle Database Enterprise Edition 12cR1 (12.1.0.2) with the following specifications:	
	Components:	
	Oracle Partitioning	
	<ul> <li>Examples CD</li> </ul>	
	One-offs:	
	<ul> <li>20846438: ORA-600 [KKPAPXFORMFKK2KEY_1] WITH LIST PARTITION</li> </ul>	
	<ul> <li>19623450: MISSING JAVA CLASSES AFTER UPGRADE TO JDK 7</li> </ul>	
	<ul> <li>20406840: PROC 12.1.0.2 THROWS ORA-600 [17998]</li> <li>WHEN PRECOMPILING BY 'OTHER' USER</li> </ul>	
	<ul> <li>20925154: ORA-39126: WORKER UNEXPECTED FATAL ERROR IN KUPW\$WORKER GATHER_PARSE_ITEMS JAVA</li> </ul>	
	<ul> <li>19672263: Patch 19672263: GTT SESSION LEVEL STATISTICS RETURNS ORA-20006</li> </ul>	
	RAC only:	
	<ul> <li>21260431: APPSST 12C : GETTING ORA-4031 AFTER 12C UPGRADE</li> </ul>	
	<ul> <li>21373473: INSTANCE TERMINATED AS LMD0 AND LMD2 HUNG FOR MORE THAN 70 SECS</li> </ul>	
	Other components:	
	<ul> <li>Perl interpreter 5.0 or later</li> </ul>	
	<ul> <li>X-Windows interface</li> </ul>	
	• JDK 1.7	
Database Server 19c	Oracle Database Enterprise Edition 19c (19.3.0.0) with the following components:	
	Components:	
	DB HOME	
	Examples CD	
	Other components:	
	<ul> <li>Perl interpreter 5.0 or later</li> </ul>	
	<ul> <li>X-Windows interface</li> </ul>	
	• 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**

The SIM application must be deployed on Oracle WebLogic 12c (12.2.1.4) with ADF.

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

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

Supported on:	Versions Supported:	
Application Server OS	<ul> <li>OS certified with Oracle Fusion Middleware 12.2.1.4</li> <li>Options are: <ul> <li>Oracle Linux 6 and 7 for x86-64 (Actual hardware or Oracle virtual machine).</li> <li>Red Hat Enterprise Linux 6 and 7 for x86-64 (Actual hardware or Oracle virtual machine).</li> <li>AIX 7.2 (Actual hardware or LPARs)</li> <li>Solaris 11.x SPARC (Actual hardware or logical domains)</li> </ul> </li> </ul>	
Application Server	<ul> <li>Oracle Fusion Middleware 12.2.1.4</li> <li>Components: <ul> <li>FMW 12.2.1.4 Infrastructure (WLS and ADF included)</li> <li>Oracle Identity Management 12.2.1.4</li> <li>Oracle Enterprise Manager 12.2.1.4</li> </ul> </li> <li>Note: Oracle Internet Directory (OID) is the supported LDAP directory for Oracle Retail products. For alternate LDAP directories, refer to Oracle WebLogic documentation set.</li> <li>JDK 1.8+ 64 bit</li> <li>Optional (required for running reports)</li> </ul>	
	<ul> <li>BI Publisher 12.2.1.4 for legacy reports</li> <li>Note: OBIEE 12.2.1.4 release does not support standalone BI Publisher installation with new installation (Doc ID 2472158.1), so install OBIEE 12.2.1.3 and upgrade it to 12.2.1.4.</li> <li>Please refer OBIEE 12.2.1.4 Installation guide for compatible FMW infrastructure version - Oracle Business Intelligence Publisher 12.2.1.4.0</li> <li>Optional (required for SSO)</li> <li>Oracle WebTier 12c (12.2.1.4) Oracle Access Manager (12.1.2.4)</li> </ul>	

### **Check Single Sign-On Requirements**

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

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

### **Check Directory Server Requirements**

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

• Oracle Identity Management 12.2.1.4

### **Check Third-Party Software Dependencies**

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

### **Check Client PC and Web Browser Requirements**

Requirement	Versions	
Operating system	Windows 10 <b>Note</b> : Oracle Retail assumes that the retailer has ensured its Operating System has been patched with all applicable Windows updates.	
Oracle (Sun) Java Runtime Java 8+ Environment (JRE)		
Browser	Microsoft Edge 44+ Microsoft Internet Explorer 11 Mozilla Firefox ESR 60+ Chrome 73+ The browser is used to launch the Java WebStart client.	

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

### Supported Oracle Retail Products

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

 Retail Integration Bus (RIB) 16.0.3 and all subsequent patches and hot fixes – Required

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

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

- Retail Merchandising System (RMS) 16.0.3 Optional
- Oracle Retail Price Management 16.0.3 Optional
- Oracle Retail Xstore Suite 17.0.2 Optional

**Note:** If integrating with Xstore Point of Service, SSL must be enabled for the SIM Webservices.

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

### UNIX User Account Privileges to Install the Software

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

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

#### SIM Installation Overview

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

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

# **RAC and Clustering**

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

- Standalone WebLogic and Database installations
- Real Application Cluster Database and WebLogic Clustering

The Oracle Retail products have been validated against a 12.1.0.2 and/or a 19.3.0.0 RAC database. When using a RAC database, all JDBC connections should be configured to use THIN connections rather than OCI connections. 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 and/or a 19.3.0.0 Oracle Internet Directory database with the WebLogic 12.2.1.4.0 cluster. It is suggested that a Web Tier 11.1.1.9 installation be configured to reflect all application server installations if SSO will be utilized.

#### **References for Configuration:**

- Oracle Fusion Middleware High Availability Guide, 12c Part Number E95492-01
- Oracle Real Application Clusters Administration and Deployment Guide 19c (19.3) E95728-06

This chapter describes the tasks required for a full database installation.

**Note:** If the SIM 16.0.x software is already installed, please see **"Database Installation Tasks – Upgrade"** for information on Upgrading to SIM 16.0.3.

### Expand the SIM Database Schema Installer Distribution

- 1. Log in to the UNIX server as a user which has sufficient access to run sqlplus from the Oracle Database installation.
- **2.** Create a new staging directory for the SIM database schema installer distribution (sim16-db.zip). There should be a minimum of 50 MB disk space available for the database schema installation files. This location is referred to as INSTALL\_DIR for the remainder of this chapter.
- **3.** Copy sim16-db.zip to <INSTALL\_DIR> and extract its contents. This creates a /sim/dbschema subdirectory under INSTALL\_DIR.

### **Required Database Character Set**

SIM 16.0.3 databases should be created with the AL32UTF8 database character set. This will ensure support for characters of all languages supported by SIM and ensure proper integration with other Oracle Retail applications.

### **Required Tablespaces**

Before you run the SIM database schema installer, make sure that the required tablespaces have been created in the database As of Release 15, SIM has its own dedicated tablespaces. They are: SIM\_DATA, SIM\_INDEX, SIM\_LOB\_DATA, SIM\_LOB\_INDEX, SIM\_ENCRYPTED\_DATA, and SIM\_ENCRYPTED\_INDEX. The SIM\_ENCRYPTED\_DATA and SIM\_ENCRYPTED\_INDEX tablespaces hold data which may include Personally Identifiable Information data (PII Data). If you hold the Advanced Security Option license, you can choose to create these two tablespaces with TDE tablespace encryption to protect the PII data. If you do not hold an Advanced Security Option license, you can create the tablespaces as normal tablespaces, but with no encryption. The tablespace names must always be SIM\_ENCRYPTED\_DATA and SIM\_ENCRYPTED\_INDEX regardless of whether TDE encryption is used, because the table and index creation scripts look for these specific names.

1. Modify the paths of the script <INSTALL\_DIR>/sim/dbschema/dbutils /create\_tablespaces.sql. The table below shows the default initial sizes:

TABLESPACE_NAME	Size
SIM_ENCRYPTED_INDEX	12G
SIM_ENCRYPTED_DATA	10G
SIM_INDEX	10G

TABLESPACE_NAME	Size
SIM_DATA	8G
SIM_LOB_DATA	2G
SIM_LOB_INDEX	2G
USERS	2G

- 2. Once the script has been modified, execute it in SQL\*Plus as sys.
  - For Example: SQL> @ create\_tablespaces.sql
- 3. Review create\_tablespaces.log for errors and correct as needed.
- 4. If you do not wish to use TDE tablespace encryption, follow below steps; or for TDE encryption skip to step 5.
  - **a.** Modify the paths of the script <INSTALL\_DIR>/sim/dbschema/dbutils /create\_encrypted\_tablespaces\_no\_TDE.sql as per your environment.
  - **b.** Run the script using SQL\*Plus as sys.
  - **c.** Review Create\_encrypted\_tablespaces\_no\_TDE.log for errors and correct as needed.
- 5. If you hold an Advanced Security Option license and wish to use TDE tablespace encryption
  - **a.** Modify the paths of the script <INSTALL\_DIR>/sim/dbschema/dbutils /create\_encrypted\_tablespaces\_TDE.sql as per your environment.
  - **b.** Run the script using SQL\*Plus as sys.
  - c. Review Create\_encrypted\_tablespaces\_TDE.log for errors and correct as needed.
  - **d.** Refer to Appendix: Tablespace Creation for details about how to create tablespaces in an encrypted format.

### Create the SIM Database User

The user in the database which will own the SIM tables (master schema) must be created prior to running the SIM database schema installer.

In addition to SIM database Schema owner, 6 required database users are also need to be created as application data source users, the data source user is granted to appropriate SIM database roles based on user responsibilities.

SIM database master schema and Data source users

Schema	Database Role granted
master schema , <master_user> Example: sim01</master_user>	SIM database schema owner
Admin user, < master_schema >_ADM	Roles granted: SIM_ADMIN,
Example: sim01_adm	SIM_BUSINESS_VIEWER.
Security user, <master_schema>_SEC</master_schema>	Roles granted: SIM_SECURITY,
Example: sim01_sec	SIM_ADMIN_VIEWER
Business viewer, <master_schema>_BSV</master_schema>	Roles granted: SIM_BUSINESS_VIEWER,
Example: sim01_bsv	SIM_ADMIN_VIEWER

Schema	Database Role granted
Business user, <schema_owner>_BSI</schema_owner>	Roles granted: SIM_BUSINESS
MPS user, <schema_owner>_MPS Example: sim01_mps</schema_owner>	Roles granted: SIM_MPS (user granted to Message Processing Staging Role)
RIB user, <schema_owner>_RIB Example: sim01_rib</schema_owner>	Roles granted: SIM_RIB (user granted to Retail Integration Bus Role)

- 1. Change the directory to <INSTALL\_DIR>/sim/dbschema/dbutils/
- Create a directory "log" for user creation spool files mkdir log
- 3. Create SIM database roles: SQL> @create\_roles.sql
- 4. Create SIM database master schema owner:

**Note:** The below user creation scripts take three arguments on the command line in sqlplus: username, password, and temporary tablespace.

SQL> @create\_user\_sim\_owner.sql

Example username: sim01

5. Create additional db users as application data source users:

In addition to SIM database Schema owner, SIM application uses 6 data source users to access to the appropriate database objects based on user responsibilities.

Run following create data source user scripts to create required data source users, the script also grants the user to appropriate SIM database roles based on user responsibilities.

SQL> @create\_user\_sim\_admin.sql

Example username: sim01\_adm

SQL> @create\_user\_sim\_rib.sql Example username: sim01\_rib

SQL>@create\_user\_sim\_business.sql Example username: sim01\_bsi

SQL> @create\_user\_sim\_business\_viewer.sql Example username: sim01\_bsv

SQL> @create\_user\_sim\_mps.sql Example username: sim01\_mps SQL> @create\_user\_sim\_security.sql

Example username: sim01\_sec

**Note:** The grant\_privs\_<role\_name>.sql scripts and create\_synonym.sql scripts are provided to grant database users to the proper privileges.

### Run the SIM Database Schema Installer

This installer installs the SIM database schema, compile SIM objects, inserts SIM control data.

- 1. Set the following environment variables:
  - Set the ORACLE\_HOME to point to an installation that contains sqlplus. It is recommended that this be the ORACLE\_HOME of the SIM database.
  - Set the PATH to: \$ORACLE\_HOME/bin:\$PATH
  - Set the ORACLE\_SID to the name of your database
  - Set the NLS\_LANG for proper locale and character encoding

#### Example: NLS\_LANG=AMERICAN\_AMERICA.AL32UTF8

- **2.** 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.
- Run the install.sh script in <INSTALL\_DIR>/ sim/dbschema path. This launches the installer. After installation is completed, a detailed installation log file is created: <INSTALL\_DIR>/ sim/dbschema/logs/sim-install-db.<timestamp>.log.

**Note:** Appendix A contains details on every screen and field in the database schema installer.

**4.** When the installer finishes it prints the values of the database SID and database schema user. Note these values as they are needed later when you run the SIM application installer.

#### Grant Privileges for the Roles

SIM database objects are owned by SIM database master schema owner, and database object privileges are granted to database users via database roles.

SIM database installer grants SIM object privileges to SIM pre-defined database roles.

**Note:** The grant\_sim\_role\_privs.sql can be used to grant SIM owned object privileges to SIM database roles as follow:

Change the directory to <INSTALL\_DIR>/sim/dbschema/dbscripts/util

SQL> @grant\_sim\_role\_privs.sql <master schema owner>

### Create Synonyms for Additional users

In addition to SIM database schema owner, six required data source users are also created as part of SIM database creation, the data source users are granted to the proper database roles based on the data source user responsibilities.

Change the directory to <INSTALL\_DIR>/sim/dbschema/dbscripts. Run Create synonyms scripts as SIM database owner:

```
SQL>@util/create_synonym_list.sql <schema_owner>
<list_of_synonym_schema>
For example:
SQL> @util/create_synonym_list.sql sim01
sim01_bsi,sim01_bsv,sim01_adm,sim01_sec,sim01_mps
```

**Note:** Alternatively, the synonym can be created individually by executing the create\_synonym.sql for each user, the script will prompt enter the schema owner and synonym user:

For example:

To create synonym for user "sim01app"

@create\_synonym.sql;

Enter schema owner: sim01

Enter synonym schema: sim01app

### **Resolving Errors Encountered During Database Schema Installation**

If the database schema installer encounters any errors, it halts execution immediately and prints to the screen which SQL script it was running when the error occurred. It also writes the path to this script to the .dberrors file. When this happens, you must run that particular script using sqlplus. After you are able to complete execution of the script, delete the .dberrors file and run the installer again. You can run the installer in silent mode so that you do not have to retype the settings for your environment. See Appendix D of this document for instructions on silent mode.

See Appendix F of this document for a list of common installation errors.

Subsequent executions of the installer will skip the SQL scripts which have already been executed in previous installer runs. This is possible because the installer maintains a **.dbhistory** file with a listing of the SQL scripts that have been run. If you have dropped the SIM schema and want to start with a clean install, you can delete the .dbhistory file so that the installer runs through all of the scripts again. It is recommended that you allow the installer to skip the files that it has already run.

### **Data Seeding**

After full fresh install SIM database schema and SIM application installation tasks completed.

**Note:** Data seeding is only applicable for full SIM install.

The data seeding process seeds store foundation data from RMS into SIM, there are three steps:

- 1. Export seed data from RMS
- 2. Move seeded data files via SFTP (if needed) to location that SIM needs to run from
- 3. Import seed data into SIM

#### Prerequisite

A full SIM database install has been completed.

#### Data Seeding Setup

The SIM database installer extracts the data seeding scripts from the sim-database-dataseeding.zip to the following location:

STAGING\_DIR/sim/dbschema/data\_seeding

This folder is referred to as DATA\_SEEDING\_DIR for the remainder of this chapter.

Verify the directory and the file permissions:

The recommended permissions for data seeding directories are 775 (rwxrwxr-x).

Set the following environment variables:

- Set ORACLE\_SID to the name of SIM database.
   Example:
   export ORACLE\_SID=<SIM\_DB\_NAME>
- Set the ORACLE\_HOME. It is recommended that this be the ORACLE\_HOME of the SIM database.

Example: export ORACLE HOME=/u00/oracle/product/19.3.0.0

Set JAVA\_HOME

Example: export JAVA\_HOME= /path/javal.7+\_64bit Set NLS\_LANG Example:

- export NLS\_LANG=AMERICAN\_AMERICA.AL32UTF8
- Set the PATH to: \$ORACLE\_HOME/bin:

Example:

export PATH=\$ORACLE\_HOME/bin:\$JAVA\_HOME/bin:\$PATH

#### **Export Seed Data**

#### **Export Foundation Data**

startDataSeedCli.sh -a 2 -s <rmsDBServer> -p <port> -d <rmsDB>

#### **Export Store Data**

startDataSeedCli.sh -a 3 -s <rmsDBServer > -p <port> -d <rmsDB>

#### **Check Export logs**

The data seeding process writes master log files into <DATA\_SEEDING\_DIR>/log directory.

Please check following the master log files:

- export\_foundation.log
- export\_store.log
- data\_seed\_common.log

The master log files may have references to sub-process log files:

- <DATA\_SEEDING\_DIR>/export/foundation/log
- <DATA\_SEEDING\_DIR>/export/store/log

#### Zip Export Data Files

Zip the data directories to be uploaded to SIM data seeding import location.

#### Ftp Export Data Files

Move foundation & store data via SFTP (if needed) to location that SIM needs to run from.

This is implementation dependent step.

#### Import Seed Data

Login as SIM db schema owner (or SIM DBA), and perform following steps:

- 1. Put unzipped the data files under DATA\_SEEDING\_DIR.
- 2. Run Set Up. startDataSeedCli.sh -a 1 -s <simDBServer> -p <port> -d <simDB>
- 3. Run Import Foundation Data. startDataSeedCli.sh -a 4 -s <simDBServer> -p <port> -d <simDB>
- 4. Run Import Store Data. startDataSeedCli.sh -a 5 -s <simDBServer> -p <port> -d <simDB>
- 5. Run Cleanup. startDataSeedCli.sh -a 6 -s <simDBServer> -p <port> -d <simDB>
- 6. Check data seeding logs:

The data seeding process writes master log files into  $\mbox{DATA}SEEDINGDIR\mbox{DIR}\mbox{log}$  directory.

Please check following the master log files:

- import\_foundtion.log
- import\_store.log
- data\_seed\_common.log

The master log files may have references to sub-process log files:

- <DATA\_SEEDING\_DIR>/import/foundation/log
- <DATA\_SEEDING\_DIR>/import/store/log
- 7. Verify the seeding results files.

The verification files are located at directory <DATA\_SEEDING\_DIR>/verify/out:

- verify\_foundation\_data.out
- verify\_store\_data.out
- disabled\_constraints.out
- 8. Check disabled database constraints:

After inspecting the result files, resolve the problematic data. A database administrator will need to manually enable the disabled constraints which are reported.

9. Remove data files:

After data seeding is finished and you are convinced that your data was correctly seeded, you can remove all data seeding files from <DATA\_SEEDING\_DIR>

## **Database Installation Tasks – Upgrade**

If SIM 16.0.2 is already installed, it is possible to do a patch install from 16.0.2 to 16.0.3. The upgrade scripts are developed based on the following assumptions:

- These scripts are provided as helper or guidance scripts.
- Industry-standard best practices are followed for schemas, data, upgrades, and migrations.
- Client customization to the base schema is not addressed by these scripts.
- Invalid data might cause referential constraints in invalid state. The bad data must to be handled manually and any invalid constraints must be resolved manually.
- The upgrade drops the database objects such as tables, views, constraints, packages and sequences that do not exist in the new schema. If these objects must be retained, the scripts must be modified accordingly.
- Due to the schema changes (for example, data types in columns), scripts perform validation. If the data type conversion causes errors, the data type change is not applied and is only logged. Manual intervention is required.
- System data is inserted as part of the upgrade scripts. There will be some system data that already exists and overlaps with the new system data. The overlap might cause errors due to unique key constraint.

### Expand the SIM Database Schema Installer Distribution

- 1. Log in to the UNIX server as a user which has sufficient access to run sqlplus from the Oracle Database installation.
- 2. Create a new staging directory for the SIM database schema distribution (sim16-db.zip). There should be a minimum of 50 MB disk space available for the database schema installation files. This location is referred to as INSTALL\_DIR for the remainder of this chapter.
- 3. Copy sim16-db.zip to <INSTALL\_DIR> and extract its contents.
- 4. Change the directory to <INSTALL\_DIR>sim/dbschema
- 5. Create a directory sim-database-delta, and copy sim-database-delta.zip to simdatabase-delta directory
- 6. Change the directory to <INSTALL\_DIR>/sim/dbschema/sim-database-delta, unzip sim-database-delta.zip

### **Required Database Character Set**

SIM 16.0.3 databases should be created with the AL32UTF8 database character set. This will ensure support for characters of all languages supported by SIM and ensure proper integration with other Oracle Retail applications.

### Run the SIM Database Schema Upgrade

#### Set Environment Variables

- Set the ORACLE\_HOME to point to SQLPLUS executable
- Set the PATH to: \$ORACLE\_HOME/bin:\$PATH
- Set the ORACLE\_SID to the name of your database
- Set the NLS\_LANG for proper locale and character encoding Example: NLS\_LANG=AMERICAN\_AMERICA.AL32UTF8

#### Run the Upgrade Scripts

Login database as SIM schema owner, run following script: @run\_all.sql;

#### **Compile Invalid Objects**

Login database as SIM schema owner, run following script: @util/inv\_obj\_comp.sql;

#### **Check Logs**

Check upgrade.log and invalid\_object.log files after completion; verify if there is any disabled constraint prior to proceed to next step.

#### Grant Privileges for the Roles

SIM database objects are owned by SIM database schema owner, and SIM database object privileges are granted to database users via database roles.

Login SQL\*Plus as Schema owner,

SQL> @util/grant\_sim\_role\_privs.sql <SIM db schema owner>

For example:

SQL> @util/grant\_sim\_role\_privs.sql sim01

**Note**: After running the grant role privileges, remove the generated scripts from the generated\_script directory.

#### Create Synonyms for Additional Users

In addition to SIM database schema owner, six required data source users are also created as part of SIM database creation, the data source users are granted to the proper database roles based on the data source user responsibilities.

Run Create synonyms scripts as SIM database owner:

```
SQL>@util/create_synonym_list.sql <schema_owner>
<list_of_synonym_schema>
For example:
SQL> @create_synonym_list.sql sim01
sim01_bsi,sim01_bsv,sim01_adm,sim01_sec,sim01_mps
```

**Note:** Alternatively, the synonym can be created individually by executing the create\_synonym.sql for each user, the script will prompt enter the schema owner and synonym user:

For example:

To create synonym for user "sim01app"

@create\_synonym.sql;

Enter schema owner: sim01

Enter synonym schema: sim01app

## **Application Installation Tasks**

Before proceeding, you must install Oracle WebLogic Server 12c with ADF and any patches listed in the Chapter 1 of this document. The Oracle Retail Store Inventory Management application is deployed to a WebLogic Managed server within the WebLogic installation. It is assumed Oracle Database has already been configured and loaded with the appropriate Store Inventory Management schemas for your installation. Installing a separate domain is mandated. It can be called "SIMDomain" (or something similar) and will be used to install the managed servers. The ADF libraries should be extended to this domain and the Enterprise Manager application should be deployed.

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

### 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:

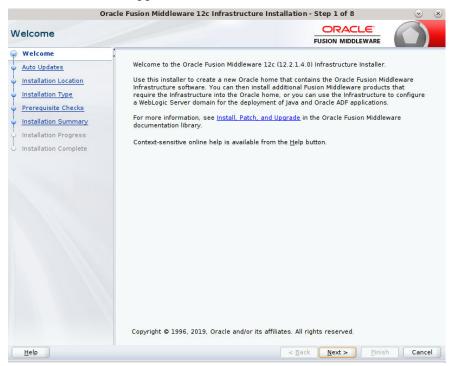
```
$export ORACLE_HOME=/u00/webadmin/products/wls_retail
$export JAVA_HOME=/u00/webadmin/products/jdk_java
(This should point to the Java which is installed on your server)
$export PATH=$JAVA_HOME/bin:$PATH
```

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.

0	racle Fusion Middleware 12c Infrastruc	cture Installation - Step 2 of 8 🛛 😒 🙁
Auto Updates		
Welcome Auto Updates Installation Location Installation Type Prerequisite Checks Installation Progress Installation Complete	Skip Auto Updates  Select patches from girectory Location:  Search My Oracle Support for Updates Username: Password:  Proxy Settings Search	Brgwse
Help	(here	< Back Next > Finish Cancel

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

Oracle home =<Path to the ORACLE\_HOME>

#### Example:

/u00/webadmin/products/wls\_retail

Orac	le Fusion Middleware 12c Infrastructure Installation	- Step 3 of 8	$\odot$ $\otimes$
Installation Location			
Y <u>Welcome</u>	<u>O</u> racle Home:		
Auto Updates	/scratch/u00/webadmin/products/wls_retail		▼ Browse
Installation Location	Feature Sets Installed At Selected Oracle Home: View		
Installation Type			
Prerequisite Checks			
Installation Summary			
Installation Progress			
Unstallation Complete			
	Oracle Home may only contain alphanumeric, underscore ( must begin with an alphanumeric character.	), hyphen (-) or dot(.) ch	aracters and it
	( constant		
Help	< <u>B</u> ack	<u>N</u> ext > <u>Finis</u>	h Cancel

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

Installation Type		
Welcome Auto Updates Installation Location Installation Type Prerequisite Checks Installation Summary Installation Progress Installation Complete		
	WebLogic Evaluation Database 12.2.1.4.0 Open Source Components Fusion Middleware Maven Support 12.2.1.4.0 JRF and Enterprise Manager WLS for FWW 12.2.1.4.0 Oracle Automatic Diagnostic Repository Feature Set Group FMW Platform Generic 12.2.1.4.0	

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

- 7. Click Next
- 8. Click Install.

Oracle Fusion Middleware 12c Infrastructure Installation - Step 6 of 8 🛛 😒			
Installation Summary			
φ <u>Welcome</u>	🔄 🖂 Install Oracle Fusion Middleware 12c Infrastructure		
Auto Updates	Installation Location		
Installation Location	Oracle Home Location: /scratch/u00/webadmin/products/wls_retail		
and the second	Log File Location: /tmp/OraInstall2020-02-27_02-18-05AM/install2020-02-27_02-18-05AM		
Installation Type	log		
Prerequisite Checks	Disk Space		
Installation Summary	Required: 2127 MB		
installation Summary	Available: 7223 MB		
Installation Progress	Feature Sets to Install		
Installation Complete	Administration Console Additional Language Help Files 12.2.1.4.0 CIE WLS Config 12.2.1.4.0		
	Enterprise manager 12.2.1.4.0		
	Third party IDBC Drivers 12.2.1.4.0		
	WebLogic Evaluation Database 12.2.1.4.0		
	EMW Platform Generic 12, 2, 1, 4, 0		
	OPatch 13 9 4 2 1		
	Toplink Developer 12.2.1.4.0		
	WLS for FMW 12.2.1.4.0		
	Core Application Server 12.2.1.4.0		
	Coherence Product Files 12.2.1.4.0		
	Web 2.0 HTTP Pub-Sub Server 12.2.1.4.0		
	WebLogic SCA 12.2.1.4.0		
	WebLogic Client Jars 12.2.1.4.0		
	Fusion Middleware Maven Support 12.2.1.4.0		
	Save Response File		
	Select Install to accept the above options and start the installation.		
	To change the above options before starting the installation, select the option to change in the left pane or use the Back button.		
Help	< Back Next > Install Cance		

Ora	le Fusion Middleware 12c Infrastructure Insta	llation - Step 7 of 8	<ul> <li>Image: Image: Ima</li></ul>
Installation Progress			
Y Welcome			
Auto Updates	100	1%	
Installation Location     Installation Type     Prerequisite Checks     Installation Summary     Installation Progress     Installation Complete	<ul> <li>Prepare</li> <li>Copy</li> <li>Generating Libraries</li> <li>Performing String Substitutions</li> <li>Linking</li> <li>Setup</li> <li>Saving the inventory</li> <li>Post install scripts</li> </ul>		
Help	View Messages	uccessful Tasks Hardware and Sof Engineered to Work To < Back Next > Einish	

#### 10. Click Finish.

Or	acle Fusion Middleware 12c Infrastructure Installation - Step 8 of 8 🛛 📀 🛞		
Installation Complete			
♀ Welcome	😑 Install Oracle Fusion Middleware 12c Infrastructure		
Auto Updates	Installation Location		
Installation Location	Oracle Home Location: /scratch/u00/webadmin/products/wls_retail		
	Log File Location: /tmp/OraInstall2020-02-27_02-18-05AM/install2020-02-27_02-18-05AM		
Ý Installation Type	.log ⊒ Feature Sets Installed Successfully		
Prerequisite Checks	Feature Sets Installed Successfully Administration Console Additional Language Help Files 12.2.1.4.0		
Installation Summary	CIE WLS Config 12.2.1.4.0		
Installation Progress	Enterprise manager 12.2.1.4.0		
	Third party JDBC Drivers 12.2.1.4.0		
Installation Complete	WebLogic Evaluation Database 12.2.1.4.0		
	FMW Platform Generic 12.2.1.4.0		
	OPatch 13.9.4.2.1 Toplink Developer 12.2.1.4.0		
	WLS for FMW 12.2.1.4.0		
	Core Application Server 12.2.1.4.0 Coherence Product Files 12.2.1.4.0 Web 2.0 HTTP Pub-Sub Server 12.2.1.4.0		
	WebLogic SCA 12.2.1.4.0		
	WebLogic Client Jars 12.2.1.4.0		
	Fusion Middleware Maven Support 12.2.1.4.0		
	Next Step(s):		
See the online help for next steps after installation.			
	Oracle Fusion Middleware 12c Infrastructure installation completed successfully		
Help	< <u>B</u> ack <u>N</u> ext > <u>F</u> inish Cancel		

## Install RCU Database Schemas

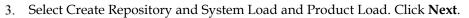
The RCU database schemas are required for the installation of configuration of domain and retail application.

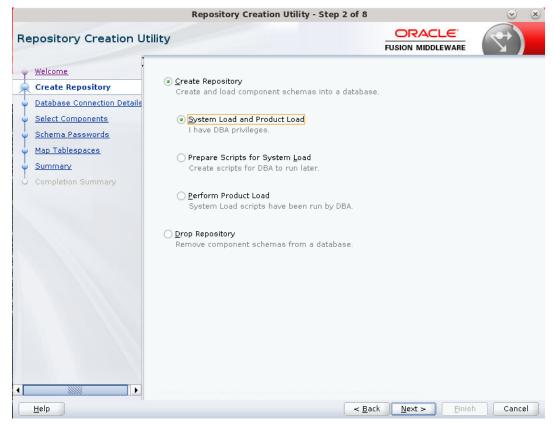
**Note:** Need user which have sys admin privileges to install the RCU database schemas.

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

- Navigate to the directory into which RCU is installed. For example: <ORACLE\_HOME>/oracle\_common/bin/ Run "./rcu"
- 2. Click Next.

	Repository Creation Utility - Step 1 o	f 8	⊗ ⊗
Repository Creation U	tility		7
🥥 Welcome	Welcome to Repository Creation Utility 12.2.1.4.0 for	Oracle Fusion Middleware.	
Repository	The Repository Creation Utility enables you to create a for	and drop database schemas tha	t are required
Database Connection Details	Oracle Fusion Middleware products.		
<ul> <li><u>Select Components</u></li> <li><u>Schema Passwords</u></li> </ul>			
Wap Tablespaces			
y <u>Summary</u>			
Completion Summary			
•	Copyright © 1996,2019, Oracle and/or its affiliates. Al	ll rights reserved.	
Help		< <u>B</u> ack Next > Finish	Cancel





- 4. Enter database connection details:
  - Database Type: Oracle Database
  - Host Name: dbhostname.us.oracle.com
  - Port: 1521
  - Service Name: dbservicename
  - Username: sys
  - Password: <syspassword>
  - Role: SYSDBA

	Repository Crea	tion Utility - Step 3 of 8			
Repository Creation Ut				7)	
Welcome Create Repository	<u>D</u> atabase Type:	Oracle Database			•
🙀 Database Connection Def	Connection String Format:	Onnection Parameters	O Connection S	String	
Select Components	Conne <u>c</u> t String				
Map Tablespaces	Host Na <u>m</u> e:	dbhostname.us.oracle.com			
Summary	Port	1521			
Completion Summary	Service Name:	pborcl			
	<u>U</u> sername:	sys as SYSDBA			
	Password:				
	<u>R</u> ole:	SYSDBA			-
	•				
Help		< <u>B</u> a	k <u>N</u> ext >	Einish	Cancel

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

pository Crea							
	ation Ut	ility					\$)
Welcome	:	Database Type:	Oracle Database				
Create Repository			Ofacie Database				
Database Connec	ction Del	Connection String Format:	Onnection Param	eters 🔿 Con	nection S <u>t</u> rin	ig	
Select Components	2						
Schema Passwords	<u>s</u>	Conne <u>c</u> t String					
Map Tablespaces		Repository Creation U	Jtility - Checking Pr	rerequisites	🕑 🗵	1	
Summary	Checking (	Global Prerequisites					
Completion Summa	🛷 Obtai	izing repository configuration n properties of the specifie k requirement for specified	d database	00:00.8060	(ms)		
	Operation	completed. Click OK to continu	ue to next name				
	Operation	completed. Click OK to contini	ue to next page.		<u>o</u> k		, i
	Operation	completed. Click OK to contini	ue to next page.		<u>O</u> K		

- Click the Create a new prefix option, the prefix name for your schemas should be unique to your application environment. Example: ReIM, ALLOC, ReSA, and so on.
- 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.

Percent of the provided of the		Repository Creati	on Utility - Step 4 o	f 8		<ul> <li>Section 1</li> </ul>
Welcome       and manage the schemas later.         Create Repository       Database Connection Details         Select Components       Select existing prefix:         Schema Passwords       Alpha numeric only. Cannot start with a number. No special         Map Tablespaces       Summary         Completion Summary       Component         Schema Passwords       Schema Owner         Summary       Component         Schema Summary       Common Infrastructure Services *         Oracle Platform Security Services       APPNAME_IAU         Oracle Platform Security Services       APPNAME_IAU         Maudit Services       APPNAME_IAU         Audit Services       APPNAME_IAU         Audit Services       APPNAME_IAU         Audit Services       APPNAME_IAU         Matadata Services       APPNAME_IAU         Weblogic Services *       APPNAME_WLS         * Mandatory component. Mandatory components cannot be deselected.	Repository Creation U	Itility				7
Select Components Schema Passwords Map Tablespaces Summary Completion Summary Completion Summary  * Mandatory component. Mandatory components cannot be deselected.  * Mandatory component. Mandatory components cannot be deselected.  * Mandatory component. Mandatory components cannot be deselected.				session, so	you can easily loca	ate, reference,
Select Components Schema Passwords Map Tablespaces Summary Completion Summary Completion Summary Completion Summary Completion Summary Completion Summary Completion Summary As Common Infrastructure Services * APPNAME STB Corracle Platform Security Services APPNAME_OPSS User Messaging Service UMA Caudit Services Append APPNAME_IAU_APPEND Audit Services Viewer APPNAME_IAU_VIEWER Metadata Services * APPNAME_MDS Weblogic Services * APPNAME_WLS * Mandatory component. Mandatory components cannot be deselected.	Database Connection Details	<ul> <li>Select existing prefix:</li> </ul>	AIP			-
Schema Passwords Map Tablespaces Summary Completion Summary Completio	Select Components					
Map Tablespaces         Summary         Completion Summary         Component         Schema Owner         Completion Summary         Component         Schema Owner         Component         Component         Schema Owner         Component         Component         Schema Owner         Component         Component         Schema Owner         Component         Schema Owner         Component         Component         Schema Owner         Component         Schema Owner         AppNAME_IAU         Audit Services         AppNAME_IAU         Metadata Services         AppNAME_MDS         Weeblogic Services *         APPNAME_WLS         * Mandatory component. Mandatory components cannot be deselected.	· ·	Oreate new prefix:				
Summary       Component       Schema Owner         © Oracle AS Repository Components       Image: Component Schemas       Image: Component Schemas         Image: Component Schemas       Image: Component Schemas       Image: Component Schemas         Image: Component Schemas       Image: Component Schemas       Image: Component Schemas         Image: Component Schemas       Image: Component Schemas       Image: Component Schemas         Image: Component Schemas       Image: Component Schemas       Image: Component Schemas         Image: Component Schemas       Image: Component Schemas       Image: Component Schemas         Image: Component Schemas       Image: Component Schemas       Image: Component Schemas         Image: Component Schemas       Image: Component Schemas       Image: Component Schemas         Image: Component Schemas       Image: Component Schemas       Image: Component Schemas         Image: Component Schemas       Image: Component Schemas       Image: Component Schemas         Image: Component Schemas       Image: Component Schemas       Image: Component Schemas         Image: Component Schemas       Image: Component Schemas       Image: Component Schemas         Image: Component Schemas       Image: Component Schemas       Image: Component Schemas         Image: Component Schemas       Image: Component Schemas       Image: Component Schemas			Alpha numeric only. (	annot start (	with a number. No	special
Summary     Completion Summary     Completion Summary     Common Schemas     Gracle AS Repository Components     Gracle AS Common Schemas     Gracle Platform Security Services     APPNAME_STB     Oracle Platform Security Services     APPNAME_OPSS     User Messaging Service     UMS     Audit Services Append     AppNAME_IAU     Audit Services Viewer     APPNAME_IAU VIEWER     Metadata Services     APPNAME_MDS     Weblogic Services *     APPNAME_WLS     * Mandatory component. Mandatory components cannot be deselected.	Map Tablespaces					
Completion Summary  Common Schemas  Common Schemas  Common Infrastructure Services * APPNAME_STB  Oracle Platform Security Services  APPNAME_OPSS User Messaging Service  APPNAME_IAU  APPNAME_IAU APPEND  Audit Services Append  APPNAME_IAU VIEWER  Metadata Services  APPNAME_MDS  Weblogic Services * APPNAME_WLS  * Mandatory component. Mandatory components cannot be deselected.   Metadata Services  * Mandatory component. Mandatory components cannot be deselected.	🖕 <u>Summary</u>		. Cara a a a a a a a		Schema Owner	r
Common Infrastructure Services * APPNAME_STB Oracle Platform Security Services APPNAME_OPSS USer Messaging Service UMS Audit Services Append APPNAME_IAU Audit Services Append APPNAME_IAU_APPEND Audit Services Viewer APPNAME_IAU_VIEWER Metadata Services APPNAME_MDS Weblogic Services * APPNAME_WLS  * Mandatory component. Mandatory components cannot be deselected.	Completion Summary					
Oracle Platform Security Services APPNAME_OPSS     User Messaging Service     UMS     Audit Services Append APPNAME_IAU     Audit Services Viewer     APPNAME_IAU_VIEWER     Metadata Services     APPNAME_MDS     Weblogic Services *     APPNAME_WLS     * Mandatory component. Mandatory components cannot be deselected.	e completion commany				APPNAME STR	
User Messaging Service     UMS     Adudit Services     APPNAME_IAU     Audit Services Append     AppNAME_IAU VIEWER     APPNAME_IAU VIEWER     Metadata Services     APPNAME_MDS     Weblogic Services *     APPNAME_WLS      * Mandatory component: Mandatory components cannot be deselected.						S
Addit Services Append     APPNAME IAU APPEND     Audit Services Viewer     APPNAME IAU VIEWER     Metadata Services     APPNAME MDS     Weblogic Services *     APPNAME_WLS      * Mandatory component. Mandatory components cannot be deselected.						
			<b>.</b>		APPNAME IAU	
Metadata Services     APPNAME_MDS     Weblogic Services *     APPNAME_WLS      * Mandatory component. Mandatory components cannot be deselected.		Audit Services	Append		APPNAME IAU	APPEND
Weblogic Services * APPNAME_WLS      * Mandatory component. Mandatory components cannot be deselected.		Audit Services	Viewer		APPNAME_IAU_	VIEWER
Mandatory component. Mandatory components cannot be deselected.		Metadata Servi	ces		APPNAME_MDS	
		Weblogic Servic	ces *		APPNAME_WLS	
		* Mandatory component. M.	andatory components c	annot be des	selected.	
	Help			< Back	Next > Finis	h Cancel

#### 9. Click Next.

Velcome		Specify a unique prefix for all so and manage the schemas later.		ession, so you can	easily locate, ref
Create Repository					
atabase Connectio	on Details	<ul> <li>Select existing prefix:</li> </ul>	AIP		
Select Componen		01			
Schema Password		Repository Creation Util	ity - Checking Prere	quisites 🕑	×
	Chacking	Component Prerequisites			. No special
unione and the second second		mon Infrastructure Services		00:00.100(ms)	wner
Summary		cle Platform Security Services		00:00.100(ms)	
Completion Summ		it Services		00:00.101(ms)	-
		it Services Append	1	00:00.101(ms)	STB
	🛷 Aud	it Services Viewer	1	00:00.101(ms)	OPSS
	💜 Meta	adata Services	1	00:00.100(ms)	
	🖋 Web	logic Services	1	00:00.101(ms)	AU IAU APPEN
					IAU_APPEN
					MDS
		n completed. Click OK to continue 1			WLS
				<u>_</u>	К
		* Mandatory component. Ma	andatory components ca	nnot be deselected	

10. Enter password of your choice.

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

	Repository C	Creation Utility - Step 5 of 8		<ul> <li>S</li> </ul>
Repository Creation U	tility			7
Welcome Create Repository Database Connection Details Select Components Schema Passwords Map Tablespaces Summary Completion Summary	Use same passwords     Password:     Alp     No     Confirm Password:	ha numeric only Cannot start with a special characters except: \$. # 		
Help		< <u>B</u> ack	. <u>N</u> ext > <u>Finis</u>	Cancel

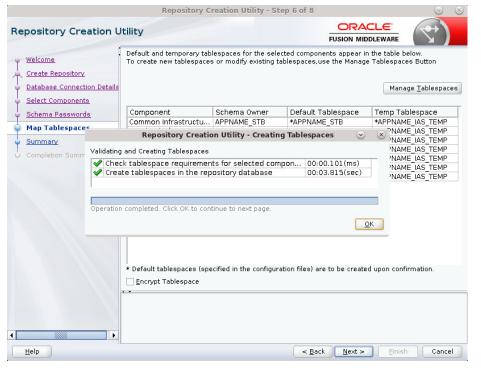
			FUSION MID	
Welcome	<ul> <li>Default and temporary tab</li> <li>To create new tablespaces</li> </ul>			
	To create new tablespaces	s or mouny existing tab	nespaces, use the Manage	e rabiespaces button
Create Repository				
Database Connection Details				Manage Tablespa
Select Components				
	Component	Schema Owner	Default Tablespace	Temp Tablespace
Schema Passwords	Common Infrastructu		*APPNAME_STB	*APPNAME IAS TEMP
Map Tablespaces	Oracle Platform Secu	APPNAME OPSS	*APPNAME IAS OPSS	*APPNAME IAS TEMP
Summary	Audit Services	APPNAME IAU	*APPNAME IAU	*APPNAME IAS TEMP
A CONTRACTOR OF A CONTRACTOR OFTA CONTRACTOR O	Audit Services Append	APPNAME IAU AP	*APPNAME IAU	*APPNAME IAS TEMP
Completion Summary	Audit Services Viewer	APPNAME IAU VIE	*APPNAME IAU	*APPNAME IAS TEMP
	Metadata Services	APPNAME MDS	*APPNAME MDS	*APPNAME IAS TEMP
	Weblogic Services	APPNAME WLS	*APPNAME WLS	*APPNAME IAS TEMP
	* Default tablespaces (spe	cified in the configurat	ion files) are to be create	d upon confirmation.

11. Provide the password and Click 'Next'.

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

	Repository C	reation Utility - St	ep 6 of 8	$\otimes$
Repository Creation U	tility			
Welcome Create Repository Database Connection Details Select Components	Default and temporary tab To create new tablespaced			
Schema Passwords	Component	Schema Owner	Default Tablespace	Temp Tablespace
	Common Infrastructu	APPNAME_STB	*APPNAME_STB	*APPNAME_IAS_TEMP
Map Tablespaces     Summary     Completion Summary	Auc Auc Auc Auc Met Wet Click C	Repository Creation Utility - Confirmation 😒 🙁		
1	* Default tablespaces (spe <u>Encrypt</u> Tablespace	rcified in the configura	ation files) are to be crea	ted upon confirmation.
Help			< <u>B</u> ack <u>N</u> ext	> Einish Cancel

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.

	Repository Creation	Utility - Step 7 of 8		$\odot$
Repository Creation U	Itility			
Welcome	Database details:			
Create Repository	Host Name	msp00ayz.us.oracle	e.com	
Database Connection Details	Port	1521		
Select Components	Service Name	PKOLSP05APP		
Schema Passwords	Connected As	sys as SYSDBA		
Map Tablespaces	Operation	System and Data Lo	oad concurrently	
	Prefix for (prefixable) Schema Own	ers APPNAME		
Summary				
Completion Summary	Component	Schema Owner	Tablespace Type	Tablespace Name
	Common Infrastructure Services	APPNAME_STB	Default Temp Additional	APPNAME_STB APPNAME_IAS_TEMP [None]
	Oracle Platform Security Services	APPNAME_OPSS	Default Temp Additional	APPNAME_IAS_OPSS APPNAME_IAS_TEMP [None]
	Audit Services	APPNAME_IAU	Default Temp Additional	APPNAME_IAU APPNAME_IAS_TEMP [None]
	Audit Services Append	APPNAME_IAU_APPEND	Default Temp Additional	APPNAME_IAU APPNAME_IAS_TEMP [None]
	Audit Services Viewer	APPNAME_IAU_VIEWER	Default Temp Additional	APPNAME_IAU APPNAME_IAS_TEMP [None]
	Save <u>R</u> esponse File			
Help		< <u>B</u> a	ick Next >	Create Cance

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

	Reposito	ry Creation U	tility - Step 8	of 8	$\odot$
epository Creation L	tility				
y Welcome	Database details:				
Create Repository	Host Name	msp00ayz.us.	oracle.com		
Database Connection Details	Port	1521			
Select Components	Service Name	PKOLSP05APF			
	Connected As	sys as SYSDE	BA		
) Schema Passwords	Operation	System and D	ata Load concu	rrently	
Map Tablespaces	Execution Time	1 minute 49			
) Summary					
Completion Summary	RCU Logfile	/tmp/RCU202	0-02-27_05-16_3	26381587/logs/rcu.log	l
	Component Log Directory	/tmp/RCU202	<b>0-0</b> 2-27_ <b>0</b> 5-16_3	26381587 <b>/</b> logs	
	View Log rcu.log				
	Prefix for (prefixable) Schema Owners	APPNAME			
	Compo	inent	Status	Time	Logfile(Click to view
	Common Infrastructu	re Services	Success	00:10.306(sec)	stb.log
	Oracle Platform Secu	rity Services	Success	00:18.719(sec)	opss.log
	Audit Services		Success	00:13.603(sec)	iau.log
				00:09.459(sec)	iau append.log
	Audit Services Appen	d	Success	00.05.455(300)	idd_append.iog
	Audit Services Viewer		Success Success	00:09.430(sec)	iau_viewer.log
	Audit Services Viewer Metadata Services			00:09.430(sec) 00:16.420(sec)	iau_viewer.log mds.log
	Audit Services Viewer		Success	00:09.430(sec)	iau_viewer.log
	Audit Services Viewer Metadata Services		Success Success	00:09.430(sec) 00:16.420(sec)	iau_viewer.log mds.log

#### 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_HOMEis 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.
```

	Fusion Middle	ware Configuration Wizard -	Page 1 of 8	$\odot$ $\otimes$
Configuration Type				
🙊 Create Domain	:			
Templates				
Administrator Account				
Domain Mode and JDK				
Advanced Configuration				
Configuration Summary				
Configuration Progress	What do you want	t to do?		
End Of Configuration		domain		
	O <u>U</u> pdate an exis	sting domain		
	Domain Location:		omains/wls_retail/APPNAMEDoma	ain B <u>r</u> owse
Help			< <u>B</u> ack <u>N</u> ext > <u>F</u> inis	h Cancel

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.

	Fusion Middleware Configuration Wizard - Page 2 of 12	S (S)
Templates		
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	<ul> <li>         Create Domain Using Product Templates:     </li> <li>Filter Templates: Type here         Include all gelected templates Include all previously and Available Templates     </li> <li>         Available Templates     </li> <li>         Ø Oracle Enterprise Manager [em]         Oracle Enterprise Manager [em]         Oracle User Messaging Service Basic [oracle_common]         Oracle User Messaging Service [oracle_common]         Oracle IRF SOAP/JMS Web Services [oracle_common]     </li> <li>         Oracle WSM Policy Manager [oracle_common]</li> <li>         Oracle JRF [oracle_common]</li> <li>Oracle JRF [oracle_common]</li> <li>Oracle Restricted JRF [oracle_common]</li> <li>Ø Oracle Domain Using Custom Template:</li> <li>Template location: [scratch/u00/webadmin/products/wls_retail</li> </ul>	pplied templates
Help	< <u>B</u> ack <u>N</u> ext > <u>Finish</u>	Cancel

Application location: Application directory location. Example: /u00/webadmin/config/applications/wls\_retail/APPNAMEDomain

#### 7. Click Next.

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	Application Location		24	ORACLE	
	Templates         Application Location         Administrator Account         Domain Mode and JDK         Database Configuration Type         Component Datasources         JDBC Test         Advanced Configuration         Configuration Summary         Configuration Progress	Domain name: Domain location:	/scratch/u00/webadmin/conf	ig/domains/wls_retail	in Browse

- 8. Provide the WebLogic administrator credentials and click **Next**:
  - Username: weblogic
  - Password: <Password>

	Fusion Middlewa	are Configuration Wizard - Page 4 of 12	S (S
Administrator Account			
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 Password Confirm Password Must be the same a	weblogic	characters with
Help		< Back Next > Einis	Cancel

	Fusion Middleware Configuration Wizard - Page 5 of 12	<ul> <li>×</li> </ul>
Domain Mode and JDK		
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 <u>D</u> evelopment         Utilize boot.properties for username and password, and poll for application <u>Production</u> Require the entry of a username and password, and do not poll for applica <b>jDK</b> <u>O</u> racle HotSpot 1.8.0_221 /scratch/u00/webadmin/products/jdk_java             Other JDK Location:	
Help	< Back Next > Finis	h Cancel

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

10. Select RCU Data.

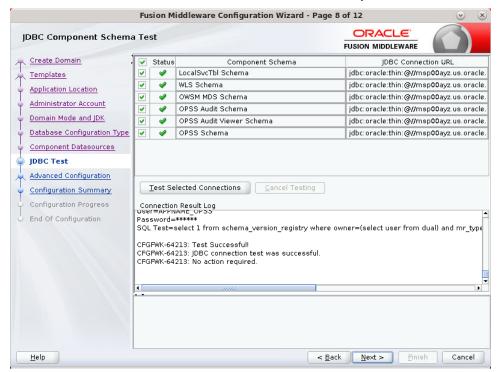
- Vendor: Oracle
- DBMS/Service: dbservicename
- Host Name: dbhostname.us.oracle.com
- Port: 1521
- Schema Owner: APPNAME\_STB (Example: ALLOC\_STB, ReSA\_STB, and so on.)
- Password: <Password>. This password which was used for RCU schema creation.

	Fusion Middleware Configuration Wizard -	Page 6 of 12	$\odot$ $\otimes$
Database Configuration	Гуре		
Create Domain Templates Application Location Administrator Account Domain Mode and JDK Database Configuration Ty Component Datasources JDBC Test Advanced Configuration Configuration Summary Configuration Progress End Of Configuration	Specify AutoConfiguration Options Using:	ry Creation Utility. The Wizard use d for components in this domain. racle's Driver (Thin) for Service co String L Issword:	s this connection
Help		< Back Next > Einish	Cancel

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

#### 12. Click Next.

	Fu	ision Middleware Co	nfiguration \	Wizard - Page 7	of 12		$\odot$	$\otimes$
JDBC Component Schema	a				-			
Templates Application Location		ndor: Connection <u>P</u> arameters		river:				-
<u>Administrator Account</u> <u>Domain Mode and JDK</u>		st Name:	P	ort:				
Database Configuration Type     Omponent Datasources		hema Owner:		chema Password:				
<u>IDBC Test</u> <u>Advanced Configuration</u> <u>Configuration Summary</u>	Oracle RAC configuration for component schemas: <ul> <li>Convert to GridLink</li> <li>Convert to RAC multi data source</li> <li>Don't convert</li> </ul> Edits to the data above will affect all checked rows in the table below.							
Configuration Progress		Component Schema	DBMS/Service	Host Name	Port	Schema Ow	Schema Pa	ssw
O End Of Configuration		LocalSvcTbl Schema	PKOLSP05APF	msp00ayz.us.or	1521	APPNAME_STE		
		WLS Schema	PKOLSP05APF	msp00ayz.us.or	1521	APPNAME_WL	•••••	
		OWSM MDS Schema	PKOLSP05APF	msp00ayz.us.or	1521	APPNAME_MD	•••••	
		OPSS Audit Schema	PKOLSP05APF	msp00ayz.us.or	1521	APPNAME_IAU		
		OPSS Audit Viewer St	PKOLSP05APF	msp00ayz.us.or	1521	APPNAME_IAU		
		OPSS Schema	PKOLSP05APF	msp00ayz.us.or	1521	APPNAME_OP:		
Help				< <u>B</u> ack	Nex	t > Einist	Canc	el



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

- 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

	Fusion Middleware Configuration Wizard - Page 10 of 23	
Administration Server		
Create Domain Templates Application Location Administrator Account Domain Mode and IDK Database Configuration Type Component Datasources IDBC Test Advanced Configuration Administration Server Node Manager Managed Servers Clusters Server Templates Coherence Clusters Machines Machines Partitions Deployments Targeting Services Targeting	Server Name AdminServer Listen Address APPhostname.us.oracle.com Listen Port 7001 Enable SSL SSL Listen Port Server Groups Unspecified The name must not be null or empty and may not contain any : , = * ? % /_cloned.	v
Help	< Back Next > Enish	Cancel

17. Configure Node Manager:

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

	Fusion Middleware Con	nfiguration Wizard - I	Page 11 of 23	S (S
Node Manager				
Create Domain  Templates Application Location Administrator Account Domain Mode and JDK Database Configuration Tyr Component Datasources JDBC Test Advanced Configuration Advanced Configuration Advanced Configuration Advanced Servers Clusters Server Templates Coherence Clusters Machines Virtual Targets Partitions Deployments Targeting Configuration Sargeting Configuration Co	Manual Node Manager Node Manager Credenti Username: Password: Confirm Password:	ocation  (config/domains/wls_re Setup  ials  weblogic	tail/APPNAMEDomain/nodemanage	
Help			< Back Next > Finish	Cancel

- 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

	Fusion Middlewar	e Configuration Wiza	rd - Page 12	2 of 23		🕑 🗵
Managed Servers						
Templates	. 🛉 Add 🖹 🤇	C <u>l</u> one 🔀 <u>D</u> elete			🔊 Dis <u>c</u> a	rd Changes
Application Location     Administrator Account	Server Name	Listen Address	Listen Port	Enable SSL	SSL Listen Port	Server Groups
Domain Mode and JDK	appsever-name	APPhostname.us 🔻	7003		Disabled	JRF-MAN-S
Database Configuration Typ     Component Datasources						
JDBC Test						
Advanced Configuration Administration Server						
Node Manager						
Managed Servers						
<u>Clusters</u> <u>Server Templates</u>						
Coherence Clusters						
Virtual Targets						
Partitions						
<ul> <li>Deployments Targeting</li> </ul>						
Services Targeting	-					
Help	۱ <u>ــــــــــــــــــــــــــــــــــــ</u>		< <u>B</u> ack	<u>N</u> ext >	Einish	Cancel

#### 19. Skip Configure Clusters and click Next.

	Fusion Middlewa	re Configuration V	Vizard - Page 13	3 of 23	~ ×
Clusters					
Templates	👍 Add 🗙	Delete		<b>ii)</b> 1	Dis <u>c</u> ard Changes
Application Location Administrator Account Domain Mode and JDK Database Configuration Tyr Component Datasources JDBC Test Advanced Configuration Administration Server Node Manager Managed Servers Clusters Server Templates Coherence Clusters Machines	Cluster Name	Cluster Address	Frontend Host	Frontend HTTP Port	Frontend HTTPS Port
Virtual Targets     Partitions     Deployments Targeting     Services Targeting					
Help			< <u>B</u> ack	<u>N</u> ext > <u>F</u> in	ish Cancel

	Fusion Middleware Conf	iguration Wizard - Pa	ge 14 of 23	$\odot$ (
Server Templates				
Create Domain	Add X Delete		<b>i</b>	Dis <u>c</u> ard Changes
Application Location	Name	Listen Port	SSL Listen Port	Enable SSL
Administrator Account	wsm-cache-server-temp	7100	8100	
<ul> <li>Domain Mode and JDK</li> <li>Database Configuration Typ</li> </ul>	wsmpm-server-template	7100	8100	
Component Datasources				
JDBC Test				
Advanced Configuration				
Administration Server				
Node Manager				
Managed Servers				
<u>Clusters</u>				
Server Templates				
Coherence Clusters				
Machines				
Virtual Targets				
Partitions				
Deployments Targeting				
Services Targeting				
Services Targeting			< Back Next > Fin	sh Cancel

20. Do not change anything and click **Next**.



	Fusion Middleware Configuration Wi	izard - Page 15 of 23	⊗ ⊗
Coherence Clusters			
Create Domain	<b>_</b> .	Dir	scard Changes
Templates			
Application Location	Cluster Name	Cluster Listen P	ort
Administrator Account	defaultCoherenceCluster	7574	
Domain Mode and JDK			
Database Configuration Typ			
Component Datasources			
JDBC Test			
Advanced Configuration			
Administration Server			
Vode Manager			
Managed Servers			
Clusters			
Server Templates			
Coherence Clusters			
Machines			
Virtual Targets			
Partitions			
Deployments Targeting			
Services Targeting			
Configuration Summani			
Help		< Back Next > Finis	Cancel

22. 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.

	Fusion Middleware	e Configui	ration Wiza	ard - Pag	e 16 of 24	1	🕑 🙁
Machines							
Create Domain     Templates     Application Location	Machine Unix Mac	hine Delete				🔊 Dis <u>c</u> ard	Changes
Administrator Account     Domain Mode and JDK	Name	Enable	Post Bind GID	Enable	Post Bind UID	Node Manager Listen Address	Node Manager
Database Configuration Typ     Component Datasources	apphost		nobody		nobody	APPhost.us.oracl 💌	5556
JDBC Test							
Advanced Configuration Administration Server							
<u>Node Manager</u> Managed Servers							
Clusters							
<u>Server Templates</u> <u>Coherence Clusters</u>							
Machines     Assign Servers to Machines							
<u>Virtual Targets</u>							
Partitions     Deployments Targeting							
Help				<	Back	Next > Finish	Cancel

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

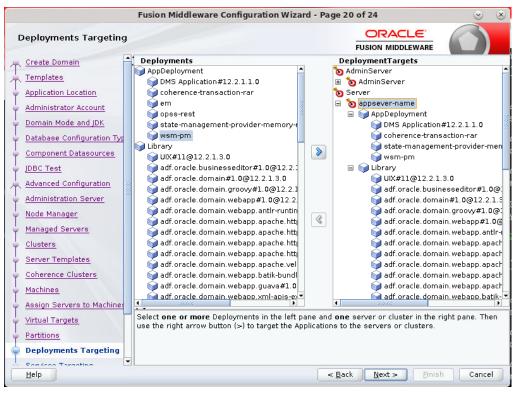
	Fusion Middleware Configuration Wizar	d - Pa	ge 17 of 24	
Assign Servers to Machin	nes			
💻 Create Domain	Servers		Machines	
Templates			o UnixMachine	
Application Location			apphost AdminServer	
Administrator Account			🍑 appsever-name	
Domain Mode and JDK				
<ul> <li><u>Database Configuration Typ</u></li> </ul>				
<u>Component Datasources</u>		۶		
JDBC Test				
Advanced Configuration				
Administration Server				
Vode Manager		8		
Managed Servers		1		
Clusters				
Server Templates				
Coherence Clusters				
Machines				
Assign Servers to Machi		1	1.5	
Virtual Targets	Select one or more servers in the left pane ar arrow button (>) to assign the server or server			se the right
Partitions				
Deployments Targeting				
Sonicos Tarastina		-		-
Help		1	Back <u>N</u> ext > Finish	Cancel

1 0	Fusion Middleward	- Can Farmatian 14	Canad Dama	10-634		0 0
	Fusion Middleware	e Configuration w	rizard - Page	18 01 24		<ul> <li>×</li> </ul>
Virtual Targets						
Create Domain Templates	: 👍 Add 🗙 🛛	<u>)</u> elete			🗐 Dis <u>c</u> ard (	hanges
Application Location     Administrator Account	Name	Target	Host Names	URI Prefix	Explicit Port	Port Offset
Domain Mode and JDK     Database Configuration Typ						
<u>Component Datasources</u> <u>IDBC Test</u> <u>Advanced Configuration</u>						
Administration Server						
<ul> <li>Managed Servers</li> <li>Clusters</li> </ul>						
<ul> <li><u>Server Templates</u></li> <li><u>Coherence Clusters</u></li> </ul>						
<ul> <li>Machines</li> <li>Assign Servers to Machines</li> </ul>						
Son icon Toractina			< <u>B</u> a	ack Next >	Einish	Cancel

24. Skip Virtual Targets. Click Next.

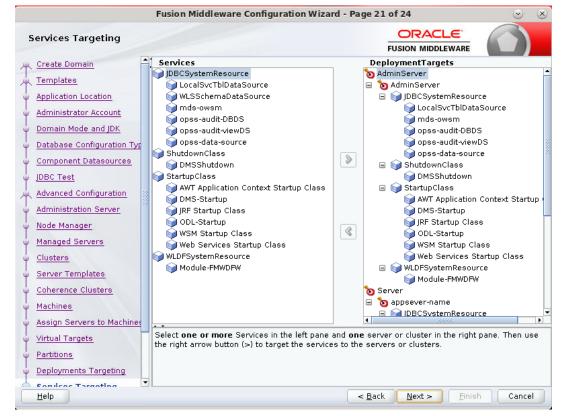
25. Skip Partitions. Click Next.

Fusion Middleware Config	juration Wizard - Page 19 of 24 🛛 😒 🔇
Partitions	
Create Domain	🗐 Dis <u>c</u> ard Changes
	Name
Application Location	Name
Administrator Account	
Domain Mode and JDK	
Database Configuration Typ	
<u>Component Datasources</u>	
IDBC Test	
K Advanced Configuration	
Administration Server	
Node Manager	
Managed Servers	
Clusters	
Server Templates	
Coherence Clusters	
Machines	
Assign Servers to Machines	
Virtual Targets	
Partitions	
Deployments Targeting	
Convices Taxasting	
Help	< Back Next > Finish Cancel

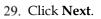


26. Target the "wsm-pm" deployment to APPNAME\_AdminServer:

27. .Click Next.



	Fusion Middleware Configuration Wizard - P	age 22 of 24 🛛 😒 🤅
Configuration Summary		
Create Domain Templates Application Location Administrator Account Domain Mode and JDK Database Configuration Typ Component Datasources JDBC Test Advanced Configuration Administration Server Node Manager Managed Servers Clusters Server Templates Coherence Clusters Machines Assign Servers to Machines Virtual Targets Partitions Deployments Targeting	View:       Deployment	ain Creation, go back to the relevant page by



.

1	usion Middleware Configuration Wizard - Pag	ge 23 of 24	S
Configuration Progress			
🔍 Create Domain			
L Templates	100%		
Application Location	Copy Unprocessed Artifacts		
	<ul> <li>OPSS Processing</li> </ul>		
	OWSM Processing		
	<ul> <li>Security Processing</li> <li>Artifacts Generation</li> </ul>		
O Database Contiduration IVE I	<ul> <li>String Substitution</li> </ul>		
	Post Processing		
y JDBC Test			
🕺 Advanced Configuration			
Q Administration Server			
V Node Manager			
Managed Servers			
Clusters			
Server Templates			
Coherence Clusters			
V Machines			
Assign Servers to Machines	·		
Virtual Targets			
Partitions			
Contraction Deployments Targeting			
Consiston Toracting			
Help	<	: <u>B</u> ack <u>N</u> ext > <u>F</u> inis	h Cancel

Fu	usion Middleware Configuration Wizard - Page 24 of 24	_ ×
End Of Configuration		
Create Domain  Templates  Application Location  Administrator Account  Domain Mode and JDK  Database Configuration Typ  Component Datasources  JDBC Test  Advanced Configuration  Administration Server  Advanced Configuration  Administration Server  Managed Servers  Clusters  Server Templates  Coherence Clusters  Machines  Assign Servers to Machinet  Virtual Targets  Deployments Targeting  T	Oracle Weblogic Server Configuration Succeeded New Domain APPNAMEDomain Creation Succeeded Domain Location /scratch/u00/webadmin/config/domains/wls_retail2/APPNAMEDomain Admin Server URL http://apphost.us.oracle.com:7001/console	
Help	< <u>B</u> ack <u>N</u> ext > <u>Finis</u>	Cancel

30. When the process completes, click Finish.

## Start the Node Manager

 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:
- 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.

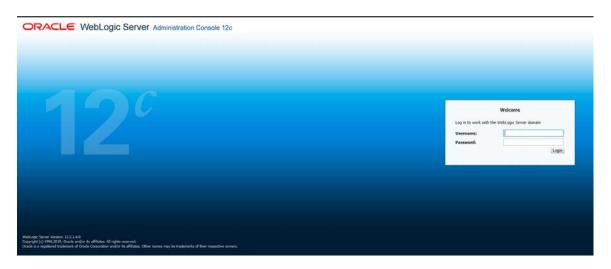
Save the boot.properties file and start WebLogic server.

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

nohup ./startWebLogic.sh &

Example: nohup /u00/webadmin/config/domains/wls\_retail1/APPdomain/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 the 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**.

Change Catary         Image Catary         Image Catary         Image Ca	PNAMEDomain
View Configuration     Persuages       Configuration     A regard the beliefs of an elected severs.	
Robust Cardigansian Cardingansian Cardinata Ca	
Domain Structure	
APROVINCES - Constraints - Con	
Internity         Contrast           - Contrast         - Contrast           Contrast         - Contrast	
- Notifies Element Energies Element State	totes   Nest
- Yourd Transfer We Henders	
- Concurrent Templates apprante-server apphos 745K COMPLETED	
Li-Secourse Monsenant applicat PUMCHG	
How do La State / Recurrer Soupport / StateState / Recurrer Soupport / StateState / Source (152-012)	ious   Next
Attraction for the second and t	
• Restart 52.	
Start Managed Servers In Admin mode	
Start Receiped Servers in a cluster     Orderset Servers in a cluster	

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

- 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.

Change Center	D Home Log Clut Preferences and Record Help		Welcome, weblogic Connected to: APPNAPIEDoma	
view changes and restarts	Home effortency of Sarone of Contrary of Enderstand Sciences of Carsen Contrary of Hack	kipus chorney of Encircle Connegy of Encircle Connegy of Encircle Connegy of Encircle Connegy of Encircle Radius connegy of Encircle Radius connegy of Encircle Radius connegling		
click the cack a astrouton to mooth, add or	Settings for myrcales			
telete items in this domain.	Configuration Users and Groups Roles and Policies Credential Nappings Prov	Aders Higration		
Roleane Cerkpreter	Autoentication Presiver Validation Autoritation Adjudication Rule Higgs	ing Auditing Crederbal Reging Certification Fath		
Senen				
B Cluters - Charace Cluters - Resource Group - Resource Group Templates - Machines - Vythair Hods	Authentikation Providers Cick the Zwik & Editorizon in the Clarge Center to wohide all the bottom on this pay [1998] Center: [1998] Center: [1998]	¢	Showing 2 to 3 of 3. Annabou i Red	
8: Clutters - Coherence Clutters - Resource Groups - Resource Groups - Nethines	Citik the Lock & Celiffortion in the Change Center to schede all the bottom on this pay	ye. Description	Showing 1 to 3 of 5 Herebool ; Next	
P: Catares - Cohenera Clusters - Resourc Group Timplates - Resourc Group Timplates - Matheme - Vitaul Hotal - Vitaul Hotal - Vitaul Tangels - Vitaul Tangels - Concurrent Templates	Cityl the Look & Coldbotton in the Clange Center to activity all the bottons on this pay [Tenne   Center   [Houston]		10000	
B Claters - Coherence Claters - Resource Drogs - Republic Coop Timpbets - Resource Croop Timpbets - Virtual Toppes - Virtual Toppes - Concurrent Teoplets - Ensurum Netwoomment - Ensurum Netwoomment	Clot the Lock & Zoldhutton in the Clarine Center to actuate all the buttors on this pay [1988] [Center] [Center] [Interpret]	Description	Version	
Collations     Collations     Collations     Collations     Collations     Collations     Collation     Colla	Cick the Ank & Editions in the Clarge Setter to achieve all the buttors on this pay Termin Commit (Internet) Name Trad Service Mently Asserter	Descognices · Truct Service Service Asservice Provider	Version 50	
P: Catares - Cohenera Clusters - Resourc Group Timplates - Resourc Group Timplates - Matheme - Vitaul Hotal - Vitaul Hotal - Vitaul Tangels - Vitaul Tangels - Concurrent Templates	Citik the set if a Collinear in the Charge Center to schild all the betters on this pay [Well: Control: [Wenter: Control: Control: Control: [Wenter: Control: Control: Cont	Dissolution     True Series Series Associate Associate     True Series Series Associate     Analogue Associate Associate     Analogue Associate Associate	Version 50 20	

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

ORACLE WebLogic Server A		
Change Center	😰 Hene Log Cut Preteienas 🔝 Accord Hele	Welcone, weblogic Converted for APPNAMEDoenal
View changes and restarts	new standing of terms standing of terminant standing of terminant of Halline septements of terminal of termination standing terminations.	
No pending changes exist. Click the Release Configuration button to allow others to edit the domain.	Cerete a New Auflandsation Provider	
Look & East		
Relates Configuration	Oreste a new Authentication Provider The following properties will be used to identify your rear Authentication Provider.	
Domain Structure	* Indicates resured fields	
APPROVEDEDMAN A BF Durais Partitions BF Classes BF Classes BF Classes Colosence Clastes	The rates of the authentication provide. *Researc DEAuthentic atio	
- Resource Groups	This is the type of authentication provider you wish to create.	
- Resource Oroup Templates - Hactaries - Virtual Rosts	Types CrucketnemetDisectoryAuthenticator •	
- Virtual Bargers - Work Hanagers - Concurrent Templates - Kessuste Management	OK Gener	
Now do L. III	1	
Nanage security providers     Configure Authentication and Mentity     Assertion providers		

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

hange Center	1 Home Log Out Preferences 🔤 Record Help	Q	Welcome, weblogic Connected to: APPNAMEDon
iew changes and restarts	Home >Summary of Servers >Summary of Environment >Summary of Servers >	Summary of Hachines suppliest sSummary of Servers sSummary of Security Realins simplication sProviders	
nding changes exist. They must be activated	Settings for myrealm		
ake effect.	Configuration Users and Groups Rates and Policies Credential Mappings Prevalers Migration		
Undo All Changes	Authentication Password Validation Authorization Adjudicati	ton Role Napping Auditing Credential Mapping Certification Path	
-Domain Partitions Environment —Servers ⊕-Chaters —Coherence Clusters —Resource Groups —Resource Groups —Resource Group Templates	Customize this table     Authentication Previders     Mew, [Dikto]   Recider,		Showing 1 to 4 of 4 - Previous ( Not
Binkroment Skrives - Cubers - Cobernice Clusters - Resource Circup Templates - Resource Circup Templates - Resource Circup Templates - Notifies - Virtual Hoods	Authentication Providers	Description	Showing 1 to 4 of 4 invalved ( too
Indicament - Schreis - Coherence Clusters - Coherence Clusters - Resource Circup Templates - "Rechines - "Virtual Targets	Authentication Providers	Description Truit Service Jacobia Provider	
Indiormed Sectors - Coherens - Coherens - Coherens - Resource Cruces - Resource Cruce Templates - Virball Nots - Virball Trayts - Virball Strayts - Vorket Emplates - Virball Strayts	Authentication Providers           Mex.         Data           Mex.         Data           Name         Name		Version
Environment -Servers Bi-Clatters - Coherence Clutters - Resource Croup Templates - Hechices - Virnual Toupts - Virnual Toupts - Virnual Toupts - Concurrent Templates - Environt Nessenernt	Authentication Providers           New:         Deskin         Manne           Instance         Trust Service Lider/Dr. Asseter	Trust Service Identity Assertion Provider	Version 1.0
Builtsoment Stroves - Clusters - Coherence Clusters - Resource Croups - Reduces - Reduces - Vitual Targets - Vitual Targets - Work Managers	Astheathcatton Providers           New:         Data           Image:         Name           That Sovice Jointly Assets         Desktiful/articleator           Desktiful/articleator         Desktiful/articleator	Trust Service Identity Assertion Provider WebLogic Authentication Provider	Version 1.0 1.0
Indiament Servers Clusters Clusters Clusters Resource Crusters Resource Crusters Resource Cruster Servers Resource Crusters Virtual Tragets Virtual Tragets Concurrent Tragetes Concurrent Tragetes Concurrent Tragetes	Activatication Previders           Name         Reaction           Image: Second Second Acceler         Image: Second Second Acceler           Image: Second Second Acceler         Image: Second Second Acceler	Trist Service Safetity Assettion Provider Webuagic Activerication Provider Webuagic Udentity Assertion provider	Version 20 20 20

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

ORACLE WebLogic Server Ad	ministration Console 12c	
Change Center	🙆 Home Log Out Preferences 📐	Record Help
View changes and restarts	Home >Summary of Servers >Summar	ry of Environment >Summary of Servers >Summary of Machines >apphost >Summary of Servers >Summary of Security Realms >myrealm >Providers >OIDAuthenticate
Pending changes exist. They must be activated to take effect.	Settings for OIDAuthenticator	
Activate Changes	Configuration Performance	
Undo All Changes	Common Provider Specific	
Undo All Changes		
Domain Structure	Save	
APPNAMEDomain ▲ ⊡- Domain Partitions ⊡- Environment	This page displays basic informati	ion about this Oracle Internet Directory Authentication provider. You can also use this page to set the JAAS Control Flag to control how this provider is use
E Clusters	個 Name:	OIDAuthenticator
Coherence Clusters Resource Groups	Bescription:	Provider that performs LDAP authentication using Oracle Internet Directory
Resource Group Templates		
····Machines	🚯 Version:	1.0
Virtual Targets Work Managers	街 Control Flag:	SUFFICIENT V
Concurrent Templates	Save	
How do I		
Configure the Oracle Internet Directory     Authentication provider		
<ul> <li>Configure Authentication and Identity Assertion providers</li> </ul>		
<ul> <li>Set the JAAS control flag</li> </ul>		
Configure the Password Validation provider		
<ul> <li>Manage security providers</li> </ul>		

- 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.

ORACLE WebLogic Server Ad	ministration Console 12c
Change Center	🔒 Home Log Out Preferences 🔤 Record Help
View changes and restarts	Home >Summary of Servers >Summary of Machines >apphoat >Summary of Servers >Summary of Security Realms >myrealm >Providers >OIDAuthenticator >Providers >DefaultAuthenticator
Pending changes exist. They must be activated to take effect.	Settings for DefaultAuthenticator
Activate Changes	Configuration Performance Migration
Undo All Changes	Common Provider Specific
Domain Structure	Save
APPNAMEDomain	This page displays basic information about this WebLogic Authentication provider. You can also use this page to set the JAAS Control Flag to control how this provider is used in the login sequences of the second
Servers Clusters	de Name: DefaultAuthenticator
Resource Groups	d Description: WebLogic Authentication Provider
	<b>Æ</b> Version: 1.0
Virtual Targets Work Managers	E Control Flag:
Concurrent Templates	Save
How do I	
Configure Authentication and Identity     Assertion providers	
Configure the Password Validation provider	
<ul> <li>Set the JAAS control flag</li> </ul>	
Manage security providers	

- 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.'

ange Center	😥 Home Log Out: Preferences 🐼 Record: Help	Q.	Welcome, weblogic Connected to: APPNAMEDoes							
rw changes and restarts	Home -Summary of Servers -Summary of Security Realine Integration -Providery -OD	DAuffweitisator								
pending changes exist. Click the Release	Settings for 000Authenticator									
Configuration button to allow others to edit the domain.	Configuration Ferformance									
Lack & Edit	Common Provider Specific	Comm Provider Security								
Release Configuration	[Free]									
main Structure	(Seve.)									
Therebonan	Use this page to define the provider specific configuration for this Grade Inte	ernet Cirectory Authentication provider,								
Domain Partitions Environment	Connectia									
PriServers	Connection									
Ousters     Coherence Ousters	Host:	idmhost.us.oracle.com	The host name or IP address of the LDAP server. Nore Info							
Resource Groups Resource Group Templates	Port	3060	The port number on which the LDAP server is listening. Here Info							
Machines		14444								
	Principalt	crimorcladmin	The Distinguished Name (DN) of the LDAP user that WebLogic Server should use to connect to the LDAP server. None Info							
- Work Managers Concurrent Templates	Credential		The predential (usually a persiverit) used to connect to the USAP server. More brits							
Resource Management	Creating		ние снаратели (цашину и различата) коно о соккест то се съку натиет. Нов сисо-							
w do L	Confirm Credential:									
Configure the Oracle Internet Directory Authentication provider										
Configure Authentication and Identity	SSLEnabled		Specifies whether the SSL protocol should be used when convecting to the LDAP server. More bits							
Assertion providers	Users									
Herage security providers	User Base DN:	crimusers, dc mus, dc moracle, dc	The base distinguished name (DR) of the tree in the LDRP directory that contains users. Hore \$10							
stem Status										
alth of Running Servers	de All Users Filter:	(& ic n=*)(object class=person)	An LDAF search filter for finding all users beneath the base user distinguished name (DN), Note: If you change the user name attribute to a type other than on, you must Suplicate that change in the User From Name Filter and User Name Attribute attribute. Here Sife.							
Failed (0) Critical (0)										
Overloaded (0)	Cuser From Name Filter:	(& cri=%u)(objectclass=persc	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. Now \$rfo							
Warning (0) OK (1)	User Search Scope:	subtree *	Specifies how deep in the LDAP directory tree the LDAP Authentication provider should search for users. More Sec.							
	J User Name Attribute:	ćn	The attribute of an LDAP user object class that specifies the same of the case. The user name attribute specified must match the							
			one specified in the All Users Filter and User Troin Name Filter attributes. Name Enfo							
	de User Object Class:	penon	The LDAP object class that stores users. Nore Info							
	Vise 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. Hore							

#### 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,c	The bas
卷 All Groups Filter:	(&(cn=*)(((objectclass=groupc	An LDAF be modi More Inf
ச Group From Name Filter:	(((&(cn=%g)(objectclass=grou	An LDAF necessa
Group Search Scope:	subtree v	Specifie
Group Membership Searching:	unlimited <b>v</b>	Specifie off. Mk
Max Group Membership Search Level:	0	Specifie tolimite positive
Ignore Duplicate Membership		Determi Info

#### 13. Check Propagate Cause For Login Exception

— General	
Connection Pool Size:	6
Connect Timeout:	0
Connection Retry Limit:	1
Parallel Connect Delay:	0
Results Time Limit:	0
Ceep Alive Enabled	
🗹 Follow Referrals	
📄 🍓 Bind Anonymously On Referrals	
🕑 街 Propagate Cause For Login Exception	

14. Click Save.

15. Click the Providers tab.

ORACLE	WebLogic	Server	Administration	Console 12c

hange Center		-	Preferences 📐 Rei			Q				
ew changes and restarts	Home >	apphost >Sur	mmary of Servers >Sur	nmary of Security Re	alms >myrealm >Pr	oviders >OIDAuthe	nticator >Prov	iders >DefaultAuthentica	ator >OIDAuthenticator >F	Providers
Pending changes exist. They must be activated Settings for myrealm to take effect.										
Activate Changes	Configu	ration Us	ers and Groups R	oles and Policies	Credential Map	oings Provider	s Migratio	n		
	Auther	itication	Password Validatio	n Authorization	Adjudication	Role Mapping	Auditing	Credential Mapping	Certification Path	
Undo All Changes										
omain Structure										
PNAMEDomain A		hentication ervers or DE		Logic Server to est	ablish trust by va	idating a user. Yo	u must have	one Authentication pr	ovider in a security real	m, and you can confi
Domain Partitions										
Environment										
Servers	Custo	mize this t	table							
Clusters	Authe	ntication P	Providers							
Coherence Clusters										
Resource Groups Resource Group Templates	New	Delete	Reorder							
Machines										
Virtual Hosts	· ·	lame					Description	1		
Virtual Targets	П	nuct Convice	Identity Asserter				Trust Consiso	Identity Acception Pro	vider	
Work Managers							Trust Service Identity Assertion Provider			
Concurrent Templates		efaultAuthe	enticator				WebLogic Authentication Provider			
	Resource Management DefaultIdentityAsserter						WebLogic Identity Assertion provider			
		IDAuthentio	cator			1	Provider that	performs LDAP auther	ntication using Oracle Ir	nternet Directory
configure Authentication and Identity		IDAuthentio	Reorder				Provider that	performs LDAP auther	ntication using Oracle Ir	iternet Directory
w do I  Configure Authentication and Identity Assertion providers		IDAuthentio				1	Provider that	performs LDAP auther	ntication using Oracle Ir	nternet Directory
w do I Configure Authentication and Identity Assertion providers Configure the Password Validation provider		IDAuthentio					Provider that	performs LDAP auther	ntication using Oracle Ir	nternet Directory
		IDAuthentio					Provider that	performs LDAP auther	ntication using Oracle Ir	iternet Directory

#### 16. Click Reorder.

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

ORACLE WebLogic Server Administration Console 12c

Change Center	🕜 Home Log Out Preferences 🔤 Record Help
View changes and restarts	Home >apphost >Summary of Servers >Summary of Security Realms >myrealm >Providers >OIDAuthenticator >Providers >DefaultAuthenticator >OIDAuthenticator >DefaultAuthenticator >OIDAuthenticator >Providers >DefaultAuthenticator >OIDAuthenticator >Providers >DefaultAuthenticator >OIDAuthenticator >Providers >DefaultAuthenticator >OIDAuthenticator >Providers >DefaultAuthenticator >OIDAuthenticator >DefaultAuthenticator >OIDAuthenticator >Providers >DefaultAuthenticator >OIDAuthenticator >DefaultAuthenticator >DefaultAuthenticat
Pending changes exist. They must be activated to take effect.	Reorder Authentication Providers
Activate Changes	OK Cancel
Undo All Changes	Reorder Authentication Providers
Domain Structure	You can reorder your Authentication Providers using the list below. By reordering Authentication Providers, you can alter the authentication
APPNAMEDomain APPNAMEDomain APPNAMEDomain Partitions  Demvinoment Servers  De-Clusters Coherence Clusters Resource Groups Resource Groups Work Managers Work Managers Work Managers Concurrent Templates Resource Management	Select authenticator(s) in the list and use arrows to move them up and down in the list.
How do I	OK Cancel
<ul><li>Re-order Authentication providers</li><li>Set the JAAS control flag</li></ul>	

18. Click OK.

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

Change Center	2 Huma Log Out Preferences 22 Forced Help	<u>A</u>
Wew changes and restarts		strades scillubercate strades objective scillubercate strades
Click the Lock & Bill Switten to modify, add or delete items in this domain.	Messages # All charges have been activated. However 2 tierrs must be restarted	for the changes to take effect.
Lock & for	Settings for myrealm	
Namese Configuration	Configuration Users and Groups Roles and Policies Credential R	tegorige Peoviders Hippiton
Densele Structure	Authentication Personal Validation Authentiation Adjustments	on Rule Magang Auditing Credential Magang Certification Firth
Concentration     Concentration	LDAP servers or DDPS. © Continues the table Authentication Prevalers Clot the Each & Addroids in the Change Center to actuate all the by [Terms] [Dense]	validating a user. You muit have one Authentication poolder in a security realin, and you can configurer multiple Authentication poolders in a security realin. If
Benaria Benarment	Asse	Description
How do L	CCDAuthentication	Provider that performs LDAP authentication using Cracle Internet Directory
<ul> <li>Configure Authentication and Literativy Assertion providers</li> </ul>	Triat Service Identity Asserter	Trust Service Identity Asserbon Provider
Configure the Passeord Validation provider	El Defaublutterbotor	Heltungs Authentication Provider
<ul> <li>Manage security providers</li> </ul>	EF DefaultiontryAuerter	WebLogic Identity Assertion provider
Set the SAKS control flag     Re-order Authentication providers	(New) (Dense) (Newsel)	
System Status		
Health of Running Servers		
Putled (0) Critical (0) C-estuaded (0) Warring (0) DK (0)		

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

## Verify OID Authenticator

- 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.

ORACLE WebLogit Server A					
Change Canter	R time up bit Palances and failed large	4	Websee, weblage: Cartering to APPlettere		
Were changes and evaluate	there character diseases regrade interval frage the	44 ·			
Citrà-the unci à dél'humor to maitris, edit or delata merca in this derivan.	furthings for represents				
Lon Silve	Colligation   Links and Disease   Roles and Traces   Dester	of Tearran Developer ( Plantan			
Radiante Carriagneeder	Authentication   Passent Voldation   Automation   Auto-	halon   Not Report   Autors   Enderliel Report   Technice Pub			
Depart Streetan Artikart Suriau B. Useran Artition B. Suriau Artition B. Suriau Suriau Suriau Suriau B. Suriau B. Surguentitio B. Surguentitio	Al Advertigator protein vilous industri Second Vasialisian Conferences Second Bio Conference Marchae Autoritation Resolution Calification and a Additional on the Theoph Desire in Advanced	al bu shishing a yan. Yu nuti ban sa kubartumur posite na yacati sadin, sal yu ya curigan hubuk kubartumur posite y Inclution o filo yapi	- Institution of the entrance of independent answing and according to come off-entrance and an entrance of the entrance of independent answing and according to the entrance of the entrance of the entrance of the entrance of the entrance of the entrance of the entrance of the entrance of the entrance of the entranc		
- Independent	their Stared (Starler		(Denning 1.1) A of A. Prentum ( See		
	-	Incryles			
		Provider that performs (200P authentication using Charles Intenter) Streetury	4		
medit	That Service (dentry Assertar	Truit Service Sterbly Asserbur Pointie	Li L		
	<ul> <li>Selauturbereuros</li> </ul>	Teducquit Authoritouttus Providei	14		
<ul> <li>Seffger identication and Methy Insertion provides</li> </ul>	C (Multipleterini	field page (see the Assertion provider	34		
Configure the transmit relation around     Principal and around the     South for the Local state of the     Normalian addressing provides	The Trans Period		Strong Use of A Strainer, Start		
fystes Status	1				
realit of Funning Servers					
Aviet (0) Colored (2) Diselected (2) Westing (2) On (2)					

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

hange Genter	3.3	Distance (angling Performance (B) source ( tests )		Weikaning weiklegte Contactual in APPROVED and					
Area changes and exchants		Sine clipitus d'accès fuite centre et bisai d'actes dant antibian							
to hitse Land of 2007 hadron to resultify, and or	1.5	arthings for supervalue							
alate terro o filo doran.	1.0	Configuration   Marce and Groups   Auto-and Policies   Contacted Heapings							
Salarang Carlignman		Rem Orașe							
Harding Harding Soughter Soughter Second Second Second Second	110	This page digited offerentige allocal soft over that have configured in this second in Conference (Marcel (Allocal Colling) Marcel (Marcel (Allocal Colling)							
<ul> <li>Intergenetitity</li> </ul>		(bes. [limi]		(Arrows ) to 21 of 211 Provide ) from					
- Depute		C Barren de	Description	President					
		INC. NUTY, INCOMENCE AND ADDR	A user for the "bit fields insertion Taxes" role.	CEALSwitzein					
		Addada_Maintee	A use for the locards handle (people) rise.	00Adwitter					
		410004PL/Artikle_Monign_crim	A user for the 'Accounts Haudia Harage' role.	ODeuterisata					
	-	Automation	Addression	COLUMN THE REAL PROPERTY AND A DESCRIPTION OF A DESCRIPTI					
te de la		All Adversed and	A user for the factory extremator' risk.	ODkutherisiana					
Partners were and proved		AUX, MIRCER	a user for the 'billionitie Henger' (de.	ODA/Rentation					
Deate uses	111	ALL DATE	A case for the Minister role.	GEMulterituitor					
Partitly upons	1.1	ALLOCATOR, ADMIN	4 user for the Millioniton Application Administration of Isla	(EA/hertian)					
Delete cases		Autorities, steward	A user for the Albuston Data Nevand rule	(EAdwitistor					
	- 1	ANAUTICAL, SUPPLICED, JOH	4 user for the "Analytical Eagler case" rule.	05Adheritate					
alarse Blad set	1	the line		Basing ( to () of (11, Persona ) had					
atth of Russing Servers									
Taskal (1) Orthogi (1) Orthogi (1) Tasking (1) Orthogi	1								

## **Clustered Installations – Pre-Installation Steps**

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

If SIM is being installed into a clustered environment, the "Cluster Address" field must be set prior to installation. This is set in:

Clusters -> sim-cluster (or name of your cluster) -> configuration (tab) -> general (tab) Set the address to your cluster in the "Cluster Address" field, for example,

apphost1:7143,apphost2:7143

	minary c	of Clusters > <b>si</b>	ini-cluster								
ttings fo	r sim-c	luster									
Configura	ation	Monitoring	Control	Deployments	Services	Notes					
General	JTA	Messaging	Servers	Replication	Migration	Singleton	Services	Scheduling	Overload	Health Monitoring	
нттр	Coheren	ce									
Save											
This page	e allows	you to define	the genera	l settings for thi	s cluster.						
lame:				sim	-cluster		The na	ame of this con	figuration. W	ebLogic Server	
					uses an MBean to			n MBean to imp	mplement and persist the		
							config	uration. More	Info		
🖲 Dofau	ht Load	Algorithm:			und-robin	•	Define	s the algorithm	to be used f	or load-balancing	
Delad		Agontinii		10		•	betwee	en replicated se	rvices if none	e is specified for a	
										algorithm cycles	
								t-based load ba		instances in order. oves on the	
							round	robin algorithn	n by taking in	to account a	
								signed weight f ing, requests a		er. In random load	
								n. More Info.			
-											
🗄 Clusto	er Addr	ess:		ora	apphost7143	Borappt				of the URL a client d that is used for	
							genera	ating EJB handl	es and entity	EJB failover	
										ither a DNS host	
							name	that maps to m	iumple th add	resses or a	

## **Expand the SIM Application Distribution**

To expand the SIM application distribution, do the following.

 Log in to the UNIX server as the user who owns the Web Logic installation. Create a new staging directory for the SIM application distribution (sim16-application.zip). There should be approximately 1 GB of disk space available for the application media and installation files.

This location is referred to as INSTALL\_DIR for the remainder of this chapter.

2. Copy sim16-application.zip to <INSTALL\_DIR> and extract its contents.

## Loading SIM LDIFs into the OID

The SIM installation media contains a zip file with a group of template LDIF files. They are in the SIM distribution you previously expanded:

<INSTALL\_DIR>/sim/application/sim16/ldap/sim-ldap.zip

The LDIF files included are just templates and must be modified to fit the structure and conventions of the OID setup for your environment. Once the LDIFs are updated for your configuration they can be loaded into LDAP using the ldapadd tool that is included in the OID installation.

For example, to load the SIM Object classes (this is done on the OID host):

# export ORACLE\_HOME=/u00/webadmin/products/wls\_idm/Oracle\_IDM

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

#ldapadd -v -c -h <OID\_HOST> -p 3060 -w <ORCLADMIN PASSWORD> -D cn=orcladmin -f sim\_objectclasses.ldif

The order of the LDIF install should be:

- 1. sim\_objectclasses.ldif
- 2. sim\_add\_company.ldif
- 3. sim\_add\_containers.ldif
- 4. sim\_data\_groups.ldif
- 5. sim\_data\_roles.ldif
- 6. sim\_data\_stores.ldif
- 7. sim\_data\_user\_groups.ldif
- 8. sim\_data\_users.ldif
- 9. sim\_data\_users\_roles.ldif

**Note:** Users that are needed for integration with SIM (for example, for XStore or RIB) need to be a member of these groups :

- SIM\_SECURE\_USERS

- SIM\_INTEGRATION\_USERS

## Set the Environment Variables for the SIM Installer

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

```
ORACLE_HOME=/u00/webadmin/products/wls_retail
WEBLOGIC_DOMAIN_HOME=/u00/webadmin/config/domains/wls_retail/SIMDomain
JAVA_HOME=/u00/webadmin/product/jdk_java
PATH=$JAVA_HOME/bin:$PATH
export ORACLE_HOME WEBLOGIC_DOMAIN_HOME JAVA_HOME PATH
```

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

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

An example of this would be:

```
export ANT_OPTS="-Djavax.net.ssl.keyStore=/u00/webadmin/product/wls_retail
/wlserver/server/lib/apphost.keystore -Djavax.net.ssl.keyStoreType=jks -
Djavax.net.ssl.keyStorePassword=retail123 -Djavax.net.ssl.trustStore=/
u00/webadmin/product/wls_retail /wlserver/server/lib/apphost.keystore -
Djavax.net.ssl.trustStoreType=jks -
Djavax.net.ssl.trustStorePassword=retail123"
Run the SIM Application Installer
```

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

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

<INSTALL\_DIR>/sim/application/logs/sim-install-app.<timestamp>.log.

**Note:** The manual install option in the installer is not functional for this release.

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

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

## Clustered Installations – Post-Installation Steps

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

If you are installing the SIM application into a clustered WebLogic server environment the installer will automatically set the cluster to use a consensus migration basis. It is recommended to use database migration basis for clusters with only 2 nodes or if this is to be used in a production system.

The database cluster migration configuration setup is described in the "Whole Server Migration" section of the following Oracle document:

Oracle® Fusion Middleware Administering Clusters for Oracle WebLogic Server (E55168-02)

Please refer to that document on how to perform this procedure. In addition, note that since the installer sets this to consensus, this will need to be done every time that SIM is installed.

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

**Note:** This procedure is only needed if you plan on using database authentication for the SIM application. This should be skipped if LDAP is going to be used for authentication.

- 1. Shut down all the servers of the WebLogic Domain created.
- 2. Once you extract the SIM installer to <INSTALL\_DIR> copy the sim-security.zip present in <INSTALL\_DIR>/sim/application/sim16 to the <WEBLOGIC\_DOMAIN\_HOME>/lib and extract it contents in the folder.
- 3. Start the domain admin server.
- 4. Log into the WebLogic console.
- 5. Navigate to: security realms -> myrealm (default realm) -> providers.

OSC OSC									
Change Center	Home Log Out	Preferences 🔤 R	ecord Help	Q	We	elcome, weblogic Conne	cted to: SIMDomai		
View changes and restarts	Home >Summary o	f Security Realms >my	realm > <b>Providers</b>						
Click the Lock & Edit button to modify, add or delete items in this domain.	Settings for myrealm								
Lock & Edit	Configuration U	sers and Groups R	toles and Policies	Credential Mappings	Providers	Migration			
Release Configuration	Authentication	Password Validation	Authorization	Adjudication Ro	le Mapping A	Auditing Credential Mapp	ing		
Domain Structure	Certification Path	Keystores							
SIMDomain       An Authentication provider alows WebLogic Server to establish trust by validating a user. You must have on a security realm, and you can configure multiple Authentication providers in a security realm. Jand you can configure multiple Authentication providers in a security realm. There are designed to access different tabas society are designed to access different tabas you to work with users and groups from previous releases of WebLogic Server.         Image: Services       Image: Services         Image: Services       Image: Services <th>cation providers</th>							cation providers		
	Click the Lock & Edit button in the Change Center to activate all the buttons on this page.								
	New Delete	Reorder				Showing 1 to 3 of 3	Previous   Next		
How do I	Name		D	escription			Version		
Configure Authentication and Identity	Trust Servic	e Identity Asserter	Т	rust Service Identity	Assertion Provid	ler	1.0		
Assertion providers	DefaultAuth	enticator	v	VebLogic Authenticat	ion Provider		1.0		
Configure the Password Validation provider	DefaultIdent	tityAsserter	v	VebLogic Identity Ass	ertion provider		1.0		

- 6. Click Lock & Edit in the change center.
- 7. Click New provider.
- 8. Select the provider type from the list: SimWlsDbAuthenticator.
- 9. Set the provider name (Default: SimWlsDbAuthenticator).

Change Center	😰 Home Log Out Preferences 🖾 Record Help	9	Welcome, weblogic Connected to: APPDomain
View changes and restarts	Home >Summary of Security Realms > mynailm > Providers	- Internet	
Pending changes exist. They must be activated to take effect.	Create a New Authentication Provider		
Adivate Changes	OK Cancel		
Undo Al Changes	Create a new Authentication Provider		
Domain Structure	The following properties will be used to identify your new Authenticate * Indicates required fields	son Provider.	
Environment     Deployments     Security Realms     Intercoperability	The name of the authentication provider. * Name: simWisDbAuthenticator		
® Cagnostica	This is the type of authentication provider you with to create. Type: SimWisDbAuthenticator		
	Cit. Cancel		
How do L.			
Nanage security providers			
Configure Authentication and Identity     Assertion providers			
System Status			
Health of Running Servers			
Paled (0) Critical (0) Overloaded (0)			
Warning (0) OK (7)			

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

UIVALLE WebLogic Server	* Administration Console		
Change Center	A Home Log Out Preferences	Record Help	Welcome, weblogic Connected to: APPDomain
View changes and restarts	Home >Summary of Security Real	ma xmynain xProviden xSummary of Security Rains xmynain xProviden xSimWisDbAatheeticator	
Click the Lock & Edit button to modify, add or delete items in this domain.	Settings for SimWhObAuthenticator		
Look & Edt	Configuration		
Release Configuration	Common Provider Specific		
Domain Structure	Cick the Lock & Editbutton in	the Change Center to modify the settings on this page.	
Vertices of Vertices # Sin-ourset - Security man - Security Instance - Security Instance # Onegoversor	fam .		
	This page allows you to define the general configuration of this provider.		
	🛃 Name:	SmillsObAuthenticator	
	de Description:	Authentication provider for SIM database security.	
	de Version:	1.0	
	Control Flag:	SUFFICIENT +	
	Save		
Now do L. S	Cick the Lock & Editbutton in the Change Center to nodify the settings on this page.		
No task help found.			
System Status iii	1		
Health of Running Servers			
Faled (0)			
Critical (0) Overloaded (0)			
Warning (0)			
	1		

- 14. Click the Provider Specific tab.
- 15. The SIM Data Source Name defaults to SimSecurityDataSource which is what the SIM installer creates. It should be left to the default value. The Group Name defaults to 'sim\_secure\_users'. If this was changed during the SIM installation then it also needs to be changed here.

View changes and restarts	Home >Summary of Security Realms >myrealm >Providers >SimWisDbA	Authenticator	
Click the Lock & Edit button to modify, add or delete items in this domain.	Settings for SimWIsDbAuthenticator		
Lock & Edit Release Configuration	Configuration Common Provider Specific		
Domain Structure	Click the Lock & Edit button in the Change Center to modify the sett	ings on this page.	
SIMDomain	Save		
Domain Partitions     Environment	This page allows you to configure additional attributes for this security provider.		
Deployments     Services     Security Realms	🚰 Group Name:	sim_secure_users	
⊕-Interoperability ⊕-Diagnostics	街 Principal Provider:	oracle.retail.sim.security	
	🥵 Credential Store Map:	oracle.retail.sim	
	Encryption Provider:	oracle.retail.sim.security	
How do I 🖃 No task help found.	Credential Store Provider:	oracle.retail.sim.security	
System Status	🚝 Dao Factory:	oracle.retail.sim.security	
Health of Running Servers	👸 Encryption Key Alias:	internal-password-key	
Failed (0) Critical (0) Overloaded (0)	👸 Refresh Rate Config:	3600	
Warning (0) OK (2)	👸 Data Source Name:	SimSecurityDataSource	
	Save		

16. Click Save.

\_

- 17. Back on the provider tab, click Reorder.
- 18. Move the SimWlsDbAuthenticator to the top of the list.

OSC OSC				
Change Center	🏦 Home Log Out Preferences 🔤 Record Help			
View changes and restarts	Home >Summary of Security Realms >myrealm >Providers >SimWisSbAuthenticator >Providers			
Pending changes exist. They must be Reorder Authentication Providers activated to take effect.				
Activate Changes	OK Cancel			
Undo All Changes	Reorder Authentication Providers			
You can reorder your Authentication Providers using the list below. By reordering Authentication Providers, you can alter the authentication sequence.				
SIMDomain Environment	Select authenticator(s) in the list and use arrows to move them up and down in the list.			
Deployments Services	E Authentication Providers:			
Security Realms	Available:			
Interoperability     Diagnostics	SimWlsSbAuthenticator			
Dignosics	Trust Service Identity Asser			
	DefaultIdentityAsserter			
	X			
How do I				
How do 1	OK Cancel			

- 19. Click Ok.
- 20. Click Activate Changes.
- 21. Shutdown the SIMDomain (The adminserver and the managed servers).
- 22. Start the admin and managed servers for the domain.

## Review and/or Configure Oracle Single Sign-On

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

### Create the SIM SSO provider in the SIMDomain

- 1. Shut down all the servers of the WebLogic Domain created.
- Once you copy the contents to <INSTALL\_DIR> copy the sim-security.zip present in <INSTALL\_DIR>/sim/application/sim16 to the <WEBLOGIC\_DOMAIN\_HOME>/lib and extract it contents in the folder.
- 3. Start the domain admin server.
- 4. Log into the WebLogic console
- 5. Navigate to: security realms -> myrealm (default realm) -> providers.
- 6. Click Lock & Edit in the change center.
- 7. Click New.
- 8. Select the provider type from the list: SimWlsSsoAuthenticator.
- 9. Set the provider name (Default: SimSsoAuthenticator).
- 10. Click OK.
- 11. Click on the newly created 'SimSsoAuthenticator'.
- 12. Under Common tab, set the Control Flag to SUFFICIENT and click Save.
- 13. Click Provider Specific tab.
- 14. Check that the GroupName is set to the name of the group used for SIM secure users (sim\_secure\_users by default).
- 15. All other values under the Provider Specific tab can be left as the default value.
- 16. Click Save.
- 17. On the provider list, click Reorder.
- 18. Move the SimWlsSsoAuthenticator to the top of the list.
- 19. Click Ok.
- 20. Click Activate Changes in the control center.
- 21. Shutdown the domain.
- 22. Start the admin and managed servers for the domain.

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

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

For example, in mod\_wl\_ohs.conf set:

```
<Location /sim-client >
WebLogicCluster apphost1:apphost2
SetHandler weblogic-handler
```

#### </Location>

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

Resource URL: /sim-client/launch Protection Level: Protected Authentication Policy: Protected Resource Policy Authorization Policy: Protected Resource Policy

Resource URL: /sim-client/.../\* Protection Level: Excluded

Resource URL: /favicon.ico Protection Level: Excluded

In the OAM you need to add a response to the Protected Resource Policy:

- 1. Under Access Manager click Application Domains.
- 2. Search and click on the domain used for your SIM deployment.
- 3. Click Authorization Policies.
- 4. Click Protected Resource Policy.
- 5. Click Responses.
- 6. Click Add and enter the following values:
  - Type: Header
  - Name: OAM\_REMOTE\_USER\_GROUPS
  - Value: \$user.groups

It will look similar to the following:

	Application Security	Sederation	<b>.</b>	
unch Pad Application Domain x APP x APP	: Protected Resource ×			Ľ
Access Manager >				
Protected Resource Policy Authoriza	ation Policy		Duplicate	Apply
Identity Assertion This will cause an assertion to be generated for the	e user, optionally containing any Ass	erted Attribute set below.		
Responses + Add / Edit X Del	ete			
Responses + Add / Edit X Del Name	ete Type	Value		
		Value Suser.gr	oups	

# SIM Batch Scripts

The SIM batch programs are installed into the WEBLOGIC\_DOMAIN\_HOME location that was specified during application installation.

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

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

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

# **Resolving Errors Encountered During Application Installation**

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

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

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

# Web Help Files

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

# Starting and Stopping the Wavelink Server

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

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

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

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

# cd /u00/webadmin/config/domains/wls\_retail/SIMDomain/retail/sim16/wireless/bin

- # ./wavelink-shutdown.sh
- # ./wavelink-startup.sh

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

For the handheld to interact correctly with SIM, it is required to install the appropriate Wavelink studio client. The Wavelink studio client and its installation instructions can be found at

http://www.wavelink.com/download/downloads.aspx.

The Oracle Retail Wireless Foundation Server is bundled with the SIM server. It has a single session free license. For multiple sessions additional licenses need to be obtained.

Contact your Oracle sales representative or client partner for Wavelink Studio Client and Oracle Retail Wireless Foundation Server license information.

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

# **Test the SIM Application**

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

Example:

WLS: http://apphost:7143/sim-client/launch

# <u>A</u>

# Appendix: SIM Database Schema Installer Screens

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

Screen: Data Source Details

SIM Schema Installer - Oracle Retail		
ORACLE		
Data Source Details		
Please provide information on a pre-existing database user for this SIM installation. The installer will authenticate as this user and create the SIM database objects.		
SIM Schema Owner	sim01	
SIM Schema Password	•••••	
SIM Oracle SID	dbname	
Temporary tablespace name	ТЕМР	
😣 Cancel) 🔇 Back 🕢 Next 🔷 Install		

Field Title	SIM Schema Owner
Field Description	The pre-existing database user for this installation.
Example	sim01
Field Title	Sim Schema Password
Field Description	The SIM Schema Owner's password.

Field Title	SIM Oracle SID
Field Description	The name of the database or pluggable db service name where the SIM schema will be installed.
Example	dbname
Field Title	Temporary tablespace name
Field Description	Temporary tablespace provided to the create_user_sim_owner.sql script at the time that the SIM database user was created.
Example	TEMP

SIM Schema Installer - Oracle Retail _ ×		
ORACLE		
Data Source Users Details		
Provide details about the pre-existing SIM data source users. Enter the same user names and passwords that were previously created.		
SIM Database Admin User Name	sim01_admin	
SIM Database Admin User Password	•••••	
SIM Database Business User Name	sim01_business	
SIM Database Business User Password	•••••	
SIM Database Business Viewer User Name	sim01_business_viewer	
SIM Database Business Viewer User Password	•••••	
SIM Database MPS User Name	sim01_mps	
SIM Database MPS User Password	•••••	
Cancel Cancel Next Install		

#### Screen: Data Source Users Details

Field Title	SIM Database Admin User Name
Field Description	The pre-existing database admin user for this installation.
Example	Sim01_admin
Field Title	SIM Database Admin User Password
Field Description	The SIM database admin user's password.
Field Title	SIM Database Business User Name
Field Description	The pre-existing database business user for this installation.
Example	Sim01_business

Field Title	SIM Database Business User Password
Field Description	The SIM database business user's password.
Field Title	SIM Database Business Viewer User Name
Field Description	The pre-existing database business viewer user for this installation.
Example	Sim01_business_viewer
Field Title	SIM Database Business Viewer User Password
Field Description	The SIM database business viewer user's password.
Field Title	SIM Database MPS User Name
Field Description	The pre-existing database MPS user for this installation.
Example	Sim01_mps
Field Title	SIM Database MPS User Password
Field Description	The SIM database MPS user's password.
Field Title	SIM Database RIB User Name
Field Description	The pre-existing database RIB user for this installation.
Example	Sim01_rib
Field Title	SIM Database RIB User Password
Field Description	The SIM database RIB user's password.

Field Title	SIM Database Security User Name	
Field Description	The pre-existing database security user for this installation.	
Example	Sim01_security	
Field Title	SIM Database Security User Password	
Field Description	The SIM database security user's password.	

#### Screen: Installation Summary

SIM Schema Installer - Oracle Retail _ ×		
ORACLE		
Installation Summary		
Summary of Installation.		
SIM Schema Owner	sim 01	
Oracle SID	dbname	
Temporary Tablespace	TEMP	
SIM Database Admin User Name	sim01_admin	
SIM Database Business User Name	sim01_business	
SIM Database Business Viewer User Name	sim01_business_viewer	
SIM Database MPS User Name	sim01_mps	
SIM Database RIB User Name	sim 01_rib	
SIM Database Security User Name	sim01_security	
Cancel Cancel Next Install		

# Appendix: SIM Application WebLogic Server Installer Screens

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

#### Screen: Installation Type

Store Inventory Management Installer - Oracle Retail _ x
ORACLE
Installation Type
The SIM application can be installed on two types of servers Standalone server or Cluster servers. The default Installation is Standalone server, alternatively you can choose cluster installation
Which Installation method will you use?
<ul> <li>Standalone server</li> </ul>
O Cluster servers
Cancel Cancel Next Install

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

#### Screen: Cluster load-balancer Address

This screen will be displayed, if Cluster Servers option is selected in "Installation Type" screen.

Store Inventory Management Installer - Oracle Retail _ x			
ORACLE	and the		
cluster load-balancer /	Address		
Please enter the Cluster address/load-balancer DNS server name			
Load-Balancer/Cluster DNS Add	ress	clusteraddress	
Cancel Cancel Next Install			

Field Title	Load-Balancer/Cluster DNS Address	
Field Description	This contains Virtual Host name of the load balancer that will be used if SIM is to be deployed to a clustered environment. Note, this screen will not appear in case you select Standalone server in previous screen.	

## Screen: Security Details

Store Inventory Management Installer - Oracle Retail _ x
ORACLE
Security Details
Provide security details for the SIM 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 SIM?
Yes
O No
😣 Cancel 🔇 Back 🕢 Next 🤜 Install

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

Store Inventory Management Installer - Oracle Retail _ x		
ORACLE		
Turn off the application	ı server's non-SSL port	
If turned off, all clients connecting	g to the application server must use a secured connection.	
	application server's non-SSL port will be inactive. A value of "No" ver's non-SSL port will still be active.	
Disable non-SSL port?	Yes	
	○ No	
	Cancel 🔇 Back 🕢 Next 🐟 Install	

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

Field Title	Disable non SSL port?	
Field Description	Selecting Yes will make that the application server's non – SSL port inactive and a Selecting No will keep application server's non-SSL port active.	

	Store Inventory Mar	nagement Installer - Oracle Retail _	×
ORA	ACLE		
Enable	tunneling for client se	rver communications	
lf enabled, f	PC client communication will be	tunneled through HTTP to the application server.	
	Yes" indicates that the applicati plications server will not suppor	ion server will support tunneling. A value of "No" indicates rt tunneling.	
Enable clien	it tunneling?	• Yes	
		O No	
Cancel Cancel Next Install			

Screen: Enable Tunneling for Client Server Communications

Field Title	Enable Tunneling for Client Server Communications?	
Field	Selecting Yes indicates that the application server will support tunneling.	
Description	Selecting No indicates that the application server will not support tunneling.	

Screen: Application Server Details

Store Inventory Managemer	nt Installer - Oracle Retail 🛛 💶 🗙	
ORACLE	Contraction of the second seco	
Application Server Details		
Note:if SSL is enabled, this value MUST match the DNS	name used in the SSL certificate.	
Weblogic Server Hostname hostname		
Note: if SSL is enabled, this value MUST match SSL Port.		
Weblogic Server Port	7001	
Weblogic Admin User Name	weblogic	
Weblogic Admin User Password	•••••	
Cancel Cancel Next Install		

Field Title	VebLogic Server Hostname	
Field Description	The hostname of the server where the WebLogic server is installed.	
Example	hostname	
Notes	Used by installer scripts to install the application and to create default inputs for client codebase and JNDI provider URL.	

Field Title	WebLogic Server Port	
Field Description	Listen port for the WebLogic Admin server.	
Example	7001	

Field Title	WebLogic Admin User Name
Field Description	The WebLogic user which will be used to install the SIM application.
Example	weblogic
Notes	Used by installer scripts to install the application

Field Title	WebLogic Admin User Password	
Field Description	The password of the WebLogic Admin User used above.	
Notes	Used by installer scripts to install the application	

## Screen: Application Deployment Details

Store Inventory Managemer	nt Installer - Oracle Retail _ ×	
ORACLE		
Application Deployment Details		
Provide the following details for the SIM application be examples.	ing installed. The default values shown below are	
Client Context Root	sim-client	
Mobile Server Context Root	sim-mobile	
You can deploy to a single managed server or a cluster of servers. You can deploy to the AdminServer for testing purposes, but this is not recommended for production deployments.		
Weblogic server/cluster	sim-server	
Cancel Cancel Next Install		

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

Field Title	Mobile Server Context Root
Field Description	This is the managed server name for mobile deployment.
Example	sim-mobile

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

0	Store Inventory M	lanagement Installer - Oracle Retail _ >	ĸ
OR/	ACLE	and the second s	
Choo	se Apps to Integrate w	vith SIM	
Choose	which applications you would	like to integrate with SIM.	
Configur	e RIB for SIM?		
Configur	e RPM for SIM?		
Configur	e RMS for SIM?	$\checkmark$	
Configur	e Manifest for SIM?		
Configur	e OMS for SIM?	<b>V</b>	
	😡 Car	ncel 🔇 Back 📀 Next 🐟 Install	

# $\label{eq:screen: Choose Apps to Integrate with SIM$

Field Title	Configure RIB for SIM?
Field Description	Select this option if you will be using RIB with SIM. Note, if you select this option then RIB Integration Details screen will be enabled and appropriate details have to be entered in RIB Integration Details screen.

Field Title	Configure RPM for SIM?
Field Description	Select this option if you will be using RPM with SIM. Note, if you select this option then RPM Integration Details screen will be enabled and appropriate details have to be entered in RPM Integration Details screen.

Field Title	Configure RMS for SIM?
Field Description	Select this option if you will be using RMS with SIM. Note, if you select this option then RMS Integration Details screen will be enabled and appropriate details have to be entered in RMS Integration Details screen.

Field Title	Configure Manifest for SIM? <b>Note</b> : Refer to the <i>Oracle Retail Store Inventory Management Operations Guide</i> for more information.
Field Description	Manifest integration is configured if an external Shipment Management System is to be used in conjunction with SIM. (Optional). Note, if you select this option then the Manifest Integration Details screen will be enabled and appropriate details will be entered in the subsequent Manifest Integration Details screen.

Field Title	Configure OMS for SIM? <b>Note</b> : Refer to the <i>Oracle Retail Store Inventory Management Operations Guide</i> for more information.
Field Description	OMS integration is configured if an external Shipment Management System is to be used in conjunction with SIM. (Optional). Note, if you select this option then OMS Integration Details screen will be enabled and appropriate details will be entered in the subsequent OMS Integration Details screen.

## Screen: RIB Integration Details

This screen will be displayed if the Configure RIB for SIM option is checked on the Choose Apps to Integrate with SIM screen.

Store Inventory Mana	gement Installer - Oracle Retail	0
ORACLE		
RIB Integration Details		
Configure SIM for RIB integration using web services	i i i i i i i i i i i i i i i i i i i	
Are you integrating RIB using web services?	Yes	
	O No	
Cancel	Back 🕢 Next 💿 Install	

Field Title	Are you integrating RIB using web services?
Field Description	This field provides an option for integrating RIB using web services on integration with SIM. Select "Yes" if you are integrating RIB using web services. Select "No" if you are not integrating RIB using web services

## Screen: RIB Integration Inject WebService Details

This page will appear if you selected "Yes" in the previous screen.

🖸 🛛 Store Inventory Management Installer - Oracle Retail 🚬 🗙		
ORACLE		
RIB Integration Inject WebService Details		
SIM Inject User Name (RIB to SIM)	simribuser	
SIM Inject User Password	•••••	
Select the Policy for securing RIB inject web service		
	Policy A	
Cancel Sack	🖉 Next) 🔷 Install	

Field Title	SIM Inject User Name
Field Description	The SIM inject user (RIB to SIM) is the user that the installer will setup for RIB to use for injection to SIM.
	This same user/pass should be used in the RIB-SIM installation for the credentials to call SIM for injection.
	Note that this user ONLY exists in the SIM server, you do NOT need to create this user in the RIB-SIM server.
Example	simribuser

Field Title	SIM Inject User Password
Field Description	Password for the SIM inject user.

Field Title	Select the Policy for securing RIB inject web service	
Field Description	Select the Policy for securing RIB inject web service. Please refer to the <i>Oracle Retail Store Inventory Management Security Guide</i> to learn more about Policy A and Policy B.	

0	Store Inventory Management Installer - Oracle Retail _ ×
C	DRACLE
	RIB Integration Publish WebService Policy
Select the web service security policy for RIB publish integration	
	Policy A
	😣 Cancel 🔇 Back 🕢 Next 🖘 Install

## Screen: RIB Integration Publish WebService Policy

Field Title	Select the web service security policy for integration with RIB.	
Field Description	Select the web service security policy for integration with RIB. Please refer to the <i>Oracle Retail Store Inventory Management Security Guide</i> to learn more about Policy A and Policy B.	

## Screen: RIB Integration Publish Policy A Details

This screen will appear if you selected "Policy A" in the previous screen.

Store Inventory Management Installer - Oracle Retail _ ×		
ORACLE	Walk was a start of the	
RIB Integration Publish Policy A Details		
Note: If RIB uses SSL, use https as the protocol. Otherwise use http.		
RIB Publish WSDL URL /ApplicationMessagePublishingService?WSDL		
RIB Publish User Name (SIM to RIB) ribuser		
RIB Publish User Password	•••••	
Cancel Cack Next Install		

Field Title	RIB Publish WSDL URL
Field Description	This is the provider URL for RIB Publish WSDL
Example	https://hostname:portno/ApplicationMessagePublishingServiceBean/Applic ationMessagePublishingService?WSDL

Field Title	RIB Publish User Name (SIM to RIB)
Field Description	The SIM publish user (SIM to RIB) is the user that SIM will be configured to use when publishing messages from SIM.
	This user does NOT exist in the SIM server and will NOT be created by the installer.
	This user should exist in the RIB-SIM server and should be created as part of the RIB-SIM install.
Example	ribuser

Field Title	RIB Publish User Password
Field Description	This is the password used for the above RIB Publish username
Example	https://hostname:portno/ApplicationMessagePublishingServiceBean/Applic ationMessagePublishingService?WSDL

## Screen: RPM Web service Policy

This screen will be displayed if the Configure RPM for SIM option is checked on the Choose Apps to Integrate with SIM screen.

Store Inventory Management	Installer - Oracle Retail _ ×
ORACLE	
RPM WebService Policy	
Select the web service security policy for integration wit	h RPM
	Policy A
Cancel Sack	📀 Next 🔿 Install

Field Title	Select the web service security policy for integration with RPM.	
Field Description	Select the web service security policy for integration with RPM. Please refer to the <i>Oracle Retail Store Inventory Management Security Guide</i> to learn more about Policy A and Policy B.	

#### Screen: RPM Integration Policy A Details

This screen will be displayed if the Configure RPM for SIM option is checked on the Choose Apps to Integrate with SIM screen and "Policy A" is selected in the previous screen.

Store Inventory Management Installer - Oracle Retail _ x		
ORACLE		
RPM Integration Policy A Details		
Note: If RPM uses SSL, use https as the protocol. Otherwise use http.		
RPM Price Change WSDL URL	kyService/PriceChangeAppServiceProxy?wsdl	
Note: If RPM uses SSL, use https as the protocol. Otherwise use http.		
RPM Price Inquiry WSDL URL	xyService/PriceInquiryAppServiceProxy?wsdl	
RPM User Name	rpmuser	
RPM User Password	•••••	
😣 Cancel 🔇 Back 🕢 Next 🔷 Install		

**Note:** If the user chooses to integrate SIM with RPM then RPM installation is a pre-requisite to installing SIM.

Field Title	RPM Price Change WSDL URL	
Field Description	This is the provider URL for RPM Price change WSDL.	
Example	https://hostname:portno/rpm-PriceChange- AppServiceDecorator/ProxyService/PriceChangeAppServiceProxy?wsdl	

Field Title	RPM Price Inquiry WSDL URL	
Field Description	This is the provider URL for RPM Price Inquiry WSDL.	
Example	https://hostname:portno/rpm-PriceInquiry- AppServiceDecorator/ProxyService/PriceInquiryAppServiceProxy?wsdl	

Field Title	RPM User Name
Field Description	This is the username used while integrating SIM with RPM
Example	rpmuser

Field Title	RPM Password
Field Description	This is the password used while integrating SIM with RPM

#### Screen: RMS Web service Policy

This screen will be displayed if the Configure RMS for SIM option is checked on the Choose Apps to Integrate with SIM screen.

Store Inventory Management Installer - Oracle Retail _ x		
ORACLE		
RMS WebService Policy		
Select the web service security policy for inte	gration with RMS	
	Policy A	
😣 Cancel 🔇 Back 📀 Next 🤜 Install		

Field Title	Select the web service security policy for Integration with RMS.
Field Description	Select the type of web service security policy for integration with RMS. Please refer to the <i>Oracle Retail Store Inventory Management Security Guide</i> to learn more about Policy A and Policy B.
Example	None, PolicyA, PolicyB.

#### Screen: RMS Integration Policy A Details

This screen will be displayed if the Configure RMS for SIM option is checked on the Choose Apps to Integrate with SIM screen and if you select "Policy A" in the previous screen.

Store Inventory Management Installer - Oracle Retail _ ×			
ORACLE	State of the second		
RMS Integration Policy A Details			
Note: If RMS uses SSL, use https as the protocol. Otherwise use http.			
RMS Store Order WSDL URL	xyService/StoreOrderAppServiceProxy?wsdl		
RMS User Name	rmsuser		
RMS User Password	•••••		
😣 Cancel 🔇 Back 🕢 Next 🖘 Install			

**Note:** If the user chooses to integrate SIM with RMS then RMS installation is pre-requisite to install SIM.

Field Title	RMS Store Order WSDL URL	
Field Description	This is the provider URL for RMS Store Order WSDL.	
Example	https://hostname:portno/rms-StoreOrder- AppServiceDecorator/ProxyService/StoreOrderAppServiceProxy?wsdl	

Field Title	RMS User Name
Field Description	This is the username used while integrating SIM with RMS
Example	rmsuser

Field Title	RMS User Password
Field Description	This is the password used while integrating SIM with RMS

## Screen: Manifest Web service Policy

This screen will be displayed if the Configure Manifest for SIM option is checked on the Choose Apps to Integrate with SIM screen.

Store Inventory Management Installer - Oracle Retail _ ×		
ORACLE		
Manifest WebService Policy		
Select the web service security policy for Manifest integ	ration	
	Policy A	
😪 Cancel 🔇 Back 📀 Next 🖘 Install		

Field Title	Select the web service security policy for Manifest Integration
Field Description	Select the type of web service security policy for Manifest Integration. Please refer to the <i>Oracle Retail Store Inventory Management Security Guide</i> to learn more about Policy A and Policy B.
Example	None, PolicyA, PolicyB

#### Screen: Manifest Integration Policy A Details

This screen will be displayed if the Configure Manifest for SIM option is checked on the Choose Apps to Integrate with SIM screen and if "Policy A" was selected in the previous screen

Store Inventory Management	Installer - Oracle Retail 🛛 🔔 🗙			
ORACLE				
Manifest Integration Policy A Details				
Note: If Manifest uses SSL, use https as the protocol. Oth	nerwise use http.			
Manifest WSDL URL	estBean/StoreShipmentManifestService?WSDL			
Manifest User Name	manifestuser			
Manifest User Password	•••••			
😣 Cancel 🔇 Back 🕢 Next 🔷 Install				

Field Title	Manifest WSDL URL
Field Description	<ul><li>This is the provider URL for Manifest WSDL, when SIM is integrated with the manifest system.</li><li>Note: Refer to the <i>Oracle Retail Store Inventory Management Operations Guide</i> for more information.</li></ul>
Example	https://hostname:portno/StoreShipmentManifestBean/StoreShipmentManifest Service?WSDL

Field Title	Manifest User Name
Field Description	This is the username used while integrating SIM with Manifest
Example	manifestuser

Field Title	Manifest User Password
Field Description	This is the password used while integrating SIM with Manifest

#### Screen: OMS Web service Policy

This screen will be displayed, if Configure OMS for SIM option is checked on the Choose Apps to Integrate with SIM screen.

Store Inventory Management	Installer - Oracle Retail _ ×
ORACLE	
OMS WebService Policy	
Select the web service security policy for integration wit	h OMS
	Policy A
L	
Cancel Cancel	🕢 Next 🔍 Install

**Note:** This screen will appear when user chooses to integrate SIM with OMS.

Field Title	Select the web service security policy for integration with OMS
Field Description	Selects the type of web service security policy for integration with OMS. Please refer to the <i>Oracle Retail Store Inventory Management Security Guide</i> to learn more about Policy A and Policy B.
Destination	None, PolicyA, PolicyB

# Screen: OMS Integration Policy A Details

This screen will be displayed if the Configure OMS for SIM option is checked on the Choose Apps to Integrate with SIM screen and if "Policy A" is selected in the previous screen.

Store Inventory Management	Installer - Oracle Retail _ ×
ORACLE	
OMS Integration Policy A Details	
Note: If OMS uses SSL, use https as the protocol. Otherw	ise use http.
OMS WSDL URL	ervice/CustomerOrderAppServiceProxy?wsdl
OMS User Name	omsuser
OMS User Password	•••••
😣 Cancel 🔇 Back	Next Install

Field Title	OMS WSDL URL
Field Description	This is the provider URL for the OMS WSDL. <b>Note</b> : Refer to the <i>Oracle Retail Store Inventory Management Operations Guide</i> for more information.
Example	https://hostname:portno/oms-CustomerOrder- AppServiceDecorator/ProxyService/CustomerOrderAppServiceProxy?wsdl

Field Title	OMS User Name
Field Description	This is the username used while integrating SIM with OMS
Example	omsuser

Field Title	OMS User Password
Field Description	This is the password used while integrating SIM with OMS

Store Inventory Management Installer - Oracle Retail _ ×
ORACLE
JDBC Security Details
Note: Enabling Secure JDBC requires that security certificates have been configured and installed for this WebLogic domain.
Enable Secure JDBC connection
Yes
○ No
Cancel Cancel Next Install

# Screen: JDBC Security Details

Field Title	Enable Secure JDBC connection
Field Description	Select Yes if you have a secured database already set up, otherwise select No.

#### Screen: Data Source Details

Store Inventory Management	Installer - Oracle Retail _ ×	
ORACLE	and the second s	
Data Source Details		
Provide details about the SIM data source. Enter the same user name and password that was used in the Database installer.		
See Install Guide for JDBC URL format		
SIM JDBC URL	jdbc:oracle:thin:@dbhost:1521/dbname	
SIM Database Schema Owner User Name	sim 01	
SIM Database Schema Owner User Password	•••••	
SIM Database Admin User Name	sim01_adm	
SIM Database Admin User Password	•••••	
SIM Database Business User Name	sim01_business	
SIM Database Business User Password	•••••	
😡 Cancel 🔇 Back 🕢 Next 🗇 Install		

Field Title	SIM JDBC URL
Field Description	URL used by the SIM application to access the SIM database schema.
Destination	WebLogic admin server
Example	Standard Thin Connection: jdbc:oracle:thin:@myhost:1521:mysimsid If it is a pluggable db then use the URL as shown belowjdbc:oracle:thin:@myhost:1521/ <service name=""> RAC connection: jdbc:oracle:thin:@(DESCRIPTION =(ADDRESS_LIST =(ADDRESS = (PROTOCOL = TCP)(HOST = myhost1)(PORT = 1521))(ADDRESS = (PROTOCOL = TCP)(HOST = myhost2)(PORT = 1521))(LOAD_BALANCE = yes))(CONNECT_DATA =(SERVICE_NAME = mysimsid)))</service>

Field Title	SIM Database Schema Owner User Name	
Field Description	The schema owner name.	
Destination	WebLogic admin server	
Notes	The schema owner name should match the name you provided when you ran the SIM database schema installer.	

Field Title	SIM Database Schema Owner User Password
Field Description	The password for the SIM schema owner.

Field Title	SIM Database Admin User Name
Field Description	The database admin user name.

Field Title	SIM Database Admin User Password
Field Description	The password for the database admin user.

Field Title	SIM Database Business User Name
Field Description	The database business user name.

Field Title	SIM Database Business User Password
Field Description	The password for the database business user.

Field Title	SIM Database MPS User Name
Field Description	The database MPS user name.

Field Title	SIM Database MPS User Password
Field Description	The password for the database MPS user.

Field Title	SIM Database Security User Name
Field Description	The database security user name.

Field Title	SIM Database Security User Password
Field Description	The password for the database Security user.

#### Screen: Secure Data Source Details

This screen is displayed if a Secure JDBC connection is enabled.

Store Inventory Management Installer - Oracle Retail _ x		
ORACLE		
Secure Data Source Details		
Provide the details for the SIM secure data source		
Identity Keystore	/home/hostname.keystore	
Identity KeyStore Type	JKS	
Identity KeyStore Password	•••••	
Identity truststore	/home/hostname.keystore	
Identity TrustStore Type	JKS	
Identity TrustStore Password	•••••	
😣 Cancel 🔇 Back 🕢 Next 🖘 Install		

Field Title	Identity Keystore
Field	Path to the identity keystore, for example,
Description	/home/hostname.keystore

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

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

Field Title	Identity TrustStore
Field	Path to the identity truststore, for example,
Description	/home/hostname.keystore

Field Title	Identity TrustStore Type
Field Description	Keystore type for example, JKS

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

Screen:	LDAP	Server	Details
---------	------	--------	---------

Store Inventory Management	nt Installer - Oracle Retail 🛛 💶 🗙	
ORACLE		
LDAP Server Details		
SIM requires the use of an LDAP directory for storage the details for your LDAP directory.	of its user, role, and store entries. Please provide	
Note: If the Idap server is configured to use SSL, use lo	laps as the protocol. Otherwise use Idap.	
LDAP Server URL	[dap[s]://[LDAP Host]:[LDAP Port]	
Enter the search base DN. This is a directory entry un	der which SIM will search for user and store entries	
LDAP Search Base DN	dc=us,dc=oracle,dc=com	
Enter the search user DN. SIM will authenticate to the L	DAP directory as this entry.	
LDAP User DN		
LDAP User Password		
Cancel Cancel Next Install		

Field Title	LDAP server URL
Field Description	URL for your LDAP directory server.
Example	Non-secured ldap: ldap://myhost:3060/ Secured ldap: ldaps://myhost:2484/

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

Field Title	LDAP User DN
Field Description	Distinguished name of the user that SIM uses to authenticate to the LDAP directory.

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

#### Screen: Mail Session Details

Store Inventory Management	nt Installer - Oracle Retail 🛛 💶 🗙	
ORACLE		
Mail Session Details		
SIM Mail SMTP Host	[SMTP Host]	
Enable SSL for mail session connection	• Yes	
	○ No	
SIM will send emails using this port.		
SIM Mail SMTP Port	25	
SIM Mail User Name	username	
SIM Mail User password	•••••	
Enable authentication for mail session connection	• Yes	
	O No	
Note: Enabling STARTTLS requires that an appropriate trust store must configured		
Enable STARTTLS	• Yes	
	○ No	
Cancel Cancel Next Install		

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

Field Title	Enable SSL for Mail session connection
Field	Select Yes for secure connection.
Description	Select No for plain connection.

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

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

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

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

Field Title	Enable STARTTLS
Field Description	StartTLS is an email command used to upgrade security of unprotected connections. This is a technical parameter and should be configured according to how the email server is setup.

Screen:	Wireless	Server	Details

Store Inventory Management	nt Installer - Oracle Retail 🛛 💶 🗙	
ORACLE		
Wireless Server Details		
Note: this must be a valid user.		
Wireless Server User Name	sim.wireless	
Wireless Server User Password	•••••	
Enter wireless port number. SIM's wireless server will devices on this port.	listen for incoming messages from wireless	
SIM Wireless Server Port	40002	
Enable SSL for Wireless Server	• Yes	
	○ No	
😣 Cancel) 🔇 Back 🕢 Next 🔷 Install		

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

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

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

Field Title	Enable SSL for Wireless Server
Field Description	Yes or No depending on SSL configuration.

Store Inventory Management	Installer - Oracle Retail _ ×		
ORACLE			
Wireless Server SSL Details			
Wireless Server KeyStore Type	ЈКЅ		
Wireless Server KeyStore Name	/home/hostname.keystore		
Wireless Server KeyStore Password	•••••		
Wireless Server Key Name	wirelesskey		
Wireless Server Key Password	•••••		
Cancel Cancel Next Install			

Screen: Wireless Server SSL Details

Field Title	Wireless Server Keystore Type
Field Description	Keystore type i.e: JKS

Field Title	Wireless Server Keystore Name
Field	Path to the wireless server keystore, for example,
Description	/home/hostname.keystore

Field Title	Wireless Server Keystore Password
Field Description	Password used to access the wireless server keystore defined above.

Field Title	Wireless Server Key Name
Field Description	The wireless server key alias name

Field Title	Wireless Server Key Password
Field Description	Password used to access the wireless server key alias name defined above.

Screen:	Batch	Server	Details

Store Inventory Management Installer - Oracle Retail _ x	
ORACLE	
Batch Server Details	
batti server Details	
Note: this must be a valid user.	
Batch User Name	sim.batch
Batch User Password	•••••
Cancel Cancel Next Install	

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

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

#### Screen: Server User Details

Store Inventory Management Installer - Oracle Retail _ ×		
ORACLE		
SIM Server User Details		
Note: this must be a valid user.		
SIM Server User Name	sim.server	
SIM Server User Password	•••••	
Cancel Cancel Next Install		

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

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

Store Inventory Management Installer - Oracle Retail _ ×		
ORACLE		
SIM Admin User Details		
Note: this must be a valid user.		
SIM Admin User Name	sim.admin	
SIM Admin User Password	•••••	
Cancel 🔇 Back	Next Next	

Screen: SIM Admin User Details

Field Title	SIM Admin User
Field Description	User name for SIM Internal Administrator
Example	sim.admin

Field Title	SIM Admin User Password
Field Description	Password for SIM Internal Administrator

.

Store Inventory Management	nt Installer - Oracle Retail _ ×
ORACLE	Service and the service of the servi
Internal Security Installation User Deta	ails
· · · · · · · · · · · · · · · · · · ·	
SIM Internal Security Installation User Name	simsecuser
SIM Internal Security Installation User Password	•••••
😣 Cancel 🔇 Back	Next 🔷 Install

# Screen: Internal Security Installation User Details

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

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

🖸 s	tore Inventory Management Installer - Oracle Retail	×
ORAC	LE	le-
SIM WebS	ervice Provider Policy	
Select the Polic	y for securing SIM integration web services	
	Policy A	
	😡 Cancel 🔇 Back 🕢 Next 🖘 Install	

# Screen: SIM Webservice Provider Policy

Field Title	Select the policy for securing SIM web service providers
Field Description	Select the type of web service policy for SIM. Please refer to the <i>Oracle Retail Store Inventory Management Security Guide</i> to learn more about Policy A and Policy B.
Example	None, PolicyA, PolicyB

# Screen: Printing Details

Store Inventory Managem	ent Installer - Oracle Retail _ ×
ORACLE	College and the second se
Printing Details	
Are you using BI Publisher for SIM reporting?	
Configure SIM reporting for BI Publisher	
Are you using SIM ticket printing?	
Configure SIM ticket printing	🔿 None
	Il Publisher
	<ul> <li>External WebService</li> </ul>
Cancel 🔇 Ba	ick Next Install

Field Title	Configure SIM reporting for BI publisher
Field Description	Select this option if you will be using BI Publisher for SIM reporting. Note, if you select this option then the "Report BIP Details" screen will be enabled and appropriate details will have to be entered in the subsequent "Report BIP Details" Details screen.

Field Title	Configure SIM ticket Printing
Field Description	Choose the ticket printing option.

Field Title	Configure SIM ticket Printing "None"
Field Description	Select this option if you will not be using ticket printing feature.

Field Title	Configure SIM ticket Printing "BI Publisher"
Field Description	Select this option if you will be using an out of box BI Publisher ticketing implementation.
	Note, if you select this option then the "Ticket Printing BIP Details" screen will be enabled and appropriate details will have to be entered in the subsequent "Ticket Printing BIP Details" Details screen.

Field Title	Configure SIM ticket Printing "External Web Service"
Field Description	Select this option if you will provide web service provider. See the "Item Ticket Printing" Section in SIM Implementation Guide for details.
	Note, if you select this option then the "External Ticket Printing Service Details" screen will be enabled and appropriate details will have to be entered in the subsequent "External Ticket Printing Service Details" screen.

#### Screen: Reporting BIP Details 1

This screen will be displayed if you select the Configure SIM reporting for BI Publisher option on the Printing Details screen.

Store Inventory Management Installer - Oracle Retail _ x		
ORACLE		
Reporting BIP Details 1		
Configure SIM reporting for BI Publisher		
BI Publisher Host	hostname	
Bl Publisher Port	port	
BI Publisher Context Root	xmlpserver	
Note: enabling SSL requires that security certificates h	nave been configured.	
Enable SSL for reporting O http		
	• https	
😣 Cancel 🔇 Back 📀 Next 🖘 Install		

Field Title	BI Publisher Host
Field Description	Host name where BI Publisher is installed.
Destination	Updates the BI Publisher related default values in SIM database.
Example	redevlv0074.us.example.com

Field Title	BI Publisher Port
Field Description	Port where BI Publisher is configured.
Destination	Updates the BI Publisher related default values in SIM database.
Example	7003

Field Title	BI Publisher Context Root
Field Description	Context root where BI Publisher is installed.
Destination	Updates the BI Publisher related default values in SIM database.
Example	Xmlpserver

Field Title	Enable SSL for reporting
Field Description	The Protocol to be used for configuring reporting.

#### Screen: Reporting BIP Details 2

This screen will be displayed if you select the Configure SIM reporting for BI Publisher option on the Printing Details screen.

Store Inventory Management Installer - Oracle Retail _ x		
ORACLE		
Reporting BIP Details 2		
Note: All reports are being configured using the template base path. Please refer to the Implementation Guide for more details Note: If BI Publisher uses SSL, use https as the protocol. Otherwise use http.		
Reporting URL	https:// hostname: port/ xmlpserver	
This path resides inside of BI Publisher to hold report	templates	
Report Template Base Path	/Base/SIM/16	
Reporting User Name	retail.user	
Reporting User Password	•••••	
😣 Cancel 🔇 Back 🔗 Next 🐟 Install		

Field Title	Reporting URL
Field Description	Confirmation field of address configured from values provided on previous screen.
Destination	Updates the reporting tool related default values in SIM database.
Example	http://hostname:18005/xmlpserver/

Field Title	Report Template Base Path
Field Description	The root directory in which your SIM report templates are located.
Example	/Base/SIM /u00/webadmin/product/10.3.X/WLS/user_projects/domains/bifoundation_ domain/config/bipublisher/repository/Reports/Guest/SIM

Field Title	Reporting Username
Field Description	From the Oracle Retail Store Inventory Management Implementation Guide: <bip_reports_user> or <sso_user></sso_user></bip_reports_user>
Destination	This user MUST exist as a BI Publisher user.
Example	retail.user

Field Title	Reporting user Password	
Field Description	From the Oracle Retail Store Inventory Management Implementation Guide: <bip_reports_user_password> or <sso_password></sso_password></bip_reports_user_password>	
Destination	Updates security wallet info	

# Screen: Ticket Printing BIP Details 1

This screen will be displayed if you select the Configure SIM ticket printing option on the Printing Details screen.

Store Inventory Management Installer - Oracle Retail _ ×			
ORACLE			
Ticket Printing BIP Details 1			
Configure SIM ticket printing for BI Publisher			
Bl Publisher Host	hostname		
Bl Publisher Port	port		
BI Publisher Context Root	xmlpserver		
Note: enabling SSL requires that security certificates I	nave been configured.		
Enable SSL for ticket printing	🔿 http		
https			
😣 Cancel 🔇 Back 🕢 Next 🔷 Install			

Field Title	BI Publisher Host	
Field Description	Host name where BI Publisher is installed.	
Destination	Updates the BI Publisher related default values in SIM database.	
Example	hostname	

Field Title	BI Publisher Port
Field Description	Port where BI Publisher is configured.
Destination	Updates the BI Publisher related default values in SIM database.
Example	7003

Field Title	BI Publisher Context Root
Field Description	Context root where BI Publisher is installed.
Destination	Updates the BI Publisher related default values in SIM database.
Example	Xmlpserver

Field Title	Enable SSL for ticket printing
Field Description	The Protocol to be used for ticket printing.

# Screen: Ticket Printing BIP Details 2

This screen will be displayed if you select the Configure SIM ticket printing option on the Printing Details screen.

Store Inventory Management Installer - Oracle Retail _ x			
ORACLE			
Ticket Printing BIP Details 2			
Note: All reports are being configured using the template base path. Please refer to the Implementation Guide for more details			
Note: If BI Publisher uses SSL, use https as the protocol. Otherwise use http.			
Ticket Printing URL https://hostname: port/xmlpserver			
This path resides inside of BI Publisher to hold report	templates		
Ticket Template Base Path	/Base/SIM/16		
Ticket Printing User Name retail.user			
Ticket Printing User Password			
Cancel Cancel Next Install			

Field Title	Ticket Printing URL	
Field Description	<b>n</b> Confirmation field of address configured from values provided on previous screen.	
Destination	n Updates the ticket printing BIP related default values in SIM database.	
Example	http://hostname:18006/xmlpserver	

Field Title	Ticket Template Base Path	
Field Description	The root directory in which your SIM ticket templates are located. <b>Note:</b> See Appendix: Setting up SIM Reports/Tickets in BI Publisher for instructions for migrating SIM reports/tickets to BI Publisher	
Example       /Base/SIM         An example from this install guide is:       /u00/webadmin/product/10.3.X/WLS/user_projects/domains/bifo         domain/config/bipublisher/repository/Reports/Guest/SIM		

Field Title	Ticket Printing Username	
Field Description	<pre>From the Oracle Retail Store Inventory Management Implementation Guide: <bip_ticketprinting_user> or <sso_user></sso_user></bip_ticketprinting_user></pre>	
<b>Destination</b> This user MUST exist as a BI Publisher user.		
Example retail.user		

Field Title	Ticket Printing user Password	
Field         From the Oracle Retail Store Inventory Management           Description         Implementation Guide: <bip_ticketprinting_user_password> or <sso_password></sso_password></bip_ticketprinting_user_password>		
Destination	Updates security wallet info	

# Screen: External Ticket Printing WebService Policy

This screen will be displayed if you select the External Webservice option on the Printing Details screen.

Store Inventory Management Installer - Oracle Retail _ x			
OR/	ACLE		
Extern	External Ticket Printing WebService Policy		
Select the	web service security policy for external ticket printing		
	Policy A		
Cancel Cack Next Install			

Field Title	Select the web service security policy for external ticket printing <b>Note</b> : The user should refer the <i>Oracle Retail Store Inventory Management Operations</i> <i>Guide</i> to know what OMS to choose.
Field Description	Selects the type of web service security policy for external ticket printing. Please refer to the <i>Oracle Retail Store Inventory Management Security Guide</i> to learn more about Policy A and Policy B.
Destination	None, PolicyA, PolicyB <b>Note</b> : If web services are to be secured using either Policy A or Policy B, then user should have some basic knowledge about the same. A user can refer to security guide to know more about Policy A and Policy B

# Screen: External Ticket Printing Service Details

This screen will be displayed if you select the External Webservice option on the Printing Details screen.

Store Inventory Management Installer - Oracle Retail _ x				
ORACLE				
External Ticket Printing service details				
External Ticket Printing WSDL URL	<pre>vService/ticketprintingAppServiceProxy?wsdl</pre>			
Cancel Sack	📀 Next 🔿 Install			

Field Title	External Ticket Printing WSDL URL
Field Description	This is the External Ticket Printing WSDL URL.
Example	http://hostname:18007/ticket-printing- AppServiceDecorator/ProxyService/ticketprintingAppServiceProxy?wsdl

# Screen: Data Export Details

Store Inventory Management Installer - Oracle Retail _ x				
ORACLE	Contraction of the second seco			
Data Export Details				
Please configure the relevant data export details. Note: File exports for a cluster should use a shared location.				
Inventory Export Path	/path/to/SIMDomain/retail/inventory/export/expo			
Stock Count Export Path	/path/to/SIMDomain/retail/stock-count/export			
Cancel G Back	R Next Install			

Field Title	Inventory Export Path
Field Description	Directory in which export the store inventory data in the export file on application server. The directory must exist.
	If directory is not specified, the installation will create a default location at
	<sim application="" domain="" server="">/<retail_dir>/inventory/export</retail_dir></sim>
	The directory and file into which you export the data should be protected with
	operating system security.
	Read, Write, and Create New File permissions to the export data directory for SIM application server user.
	Note:
	Ftp user permission for moving data to secure ftp site:
	Read, Write permissions to the export data directory for user who is responsible to move export data files to secure ftp sites for importer applications.
Example	<sim application="" domain="" server="">/retail/inventory/export</sim>

Field Title	Stock Count Export Path						
Field Description	Directory in which export the store inventory data in the export file on application server. The directory must exist.						
	If directory is not specified, the installation will create a default location at						
	<sim application="" domain="" server="">/<retail_dir>/inventory/export</retail_dir></sim>						
	The directory and file into which you export the data should be protected with operating system security.						
	Read, Write, and Create New File permissions to the export data directory for SIM application server user.						
	Note:						
	Ftp user permission for moving data to secure ftp site:						
	Read, Write permissions to the export data directory for user who is responsible to move export data files to secure ftp sites for importer applications.						
Example	<pre><sim application="" domain="" server="">/retail/inventory/export</sim></pre>						

### Screen: Enable SSO in SIM

Store Inventory Management Installer - Oracle Retail _ x
ORACLE
Enable SSO in SIM
Oracle Single Sign-On must be installed separately. You should only check the box below if you have already set up and configured Oracle SSO.
Use Oracle Single Sign On for user identification and authentication?
Enable Single Sign On in SIM?
😣 Cancel 🔇 Back 🕢 Next 🐟 Install

Field Title	box. Leaving the box unchecked will configure SIM to use its own LDAP			
Field Description	authenticate users. If SSO is being used in your environment then click the check			

•	Store Inventory Manageme	nt Installer - Oracle Retail _ ×
ORA	ACLE	
Single	Sign On Details	
Please enter	r the Oracle Single Sign-On web tier server	r details.
SSO Server	Host	[SSO Host]
SSO Server		[SSO Port]
	😣 Cancel 🔇 Back	Next Next

# Screen: Single Sign-On Details

Field Title     SSO Server Host       Field     This is the host used to access the Single Sign-On web tier.	SSO Server Host
	This is the host used to access the Single Sign-On web tier.
Example	WEBTIERSERVER.us.com

Field Title	SSO Server Port
Field Description	This is the HTTP port used to access the Single Sign-On web tier.
Example	18888

# Screen: Manual Deployment Option

	Store Inventory Manageme	nt Installer - Oracle Retail 🛛 💶 🗙
		A Stranger and the standard
Manua	l Deployment Option	
application deploy usin	into the server. If you do not have filesyst	erver files. Then it can proceed with installing the tem access to the application server, or you wish to have the installer skip the final installation phase. se after this installer has completed.
Install files t	to app server?	• Yes. I have write access to the application serv
		O No. Configure but do not install the application.
	😣 Cancel 🔇 Bac	k 🕢 Next 🔍 Install

Field Title	Install files to app server?
Field Description	The installer will configure the application and application server files. Then, it can proceed with installing the application into the server. If a user does not have filesystem access to application server, or wishes to deploy using a different method, he can choose to have the installer skip the final installation phase.
Example	Select Yes, I have write access to the application server.

# Screen: Installation Summary

Store Inventory Manageme	ent Installer - Oracle Retail _ ×
ORACLE	
Installation Summary	
Summary of Installation	
Enable SSL for SIM	true
Weblogic Server Hostname	apphostname
Weblogic Admin Port	7001
Weblogic Admin User Name	weblogic
Client Context Root	sim-client
Mobile Server Context Root	sim-mobile
Weblogic server/cluster	sim-server
Configure RIB for SIM	true
Configure RPM for SIM	true 🗾
😣 Cancel 🔇 Bac	k 🕢 Next 🤜 Install

Field Title	Summary of Installation	
Field Description	Field       Lists the values entered in the previous install screens.         Description       Verify each value and if they are correct click next, else use back button to go	
Example	Verify each value and if they are correct click next, else use back button to go back and change the value. Selecting Cancel will Cancel the installation.	

# **Appendix: Common Installation Errors**

This section provides some common errors encountered during installation.

# EJB Deployment Errors during Installation to WebLogic

### Symptom

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

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

### Solution

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

# Output Freezes during Text Mode Installation to WebLogic

### Symptom

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

### Solution

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

# Database Installer Hangs on Startup

#### Symptom

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

Running pre-install checks Running thsping to get listener port

#### Solution

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

# Warning: Could not create system preferences directory

#### Symptom

The following text appears in the installer Errors tab:

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

#### Solution

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

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

# Warning: Couldn't find X Input Context

#### Symptom

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

Couldn't find X Input Context

#### Solution

This message is harmless and can be ignored.

# ConcurrentModificationException in Installer GUI

#### Symptom

#### Solution

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

# A Second Login Screen Appears After Single Sign-On Login

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

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

#### Symptom

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

#### Solution

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

# Error Connecting to Database URL

#### Symptom

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

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

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

#### Solution

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

Error connecting to database URL <url> as user <user> java.lang.Exception: UnsatisfiedLinkError encountered when using the Oracle driver.

Please check that the library path is set up properly or switch to the JDBC thin client.

It may mean that the installer is using the incorrect library path variables for the platform you are installing on. Open the file

<STAGING\_DIR>/rms/dbschema/common/preinstall.sh and toggle the variable, use32bit, to True if it is set to False or vice versa. This setting is dependent on the JRE that is being used.

# GUI screens fail to open when running Installer

#### Symptom

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

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

#### Solution

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

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

#### Symptom

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

In SIM Database, in the CONFIG\_SYSTEM table, the value for SECURITY\_AUTHENTICATION\_METHOD should be set to 1 for LDAP authentication. Check in LDAP to be sure the password is set to the correct value.

# Appendix: Setting up SIM Reports/Tickets in BI Publisher

SIM 16.0.3 reports and ticket printing supports BiPublisher 12.2.1.3 for new installs or 12.2.1.4 for upgrades. At the time of creating this install guide BiPublisher is not supporting a BIP only install for new installs of 12.2.1.4 you must install BiPublisher 12.2.1.3.

# BiPublisher 12c - BI Server Component Installation Tasks

Oracle BI Publisher is used as the main RMS, RWMS, REIM, and SIM reporting engine and can be used in conjunction with external printing solutions like label printing. This section describes the installation of Oracle BI Publisher as a server application within WebLogic 12c. One deployment of BI Publisher can be used for any of the RMS, RWMS, REIM, and SIM reports.

### **BiPublisher 12c only - Installation Process Overview**

Oracle BiPublisher must be installed in a standalone setup, it cannot be incorporated with OBIEE Analytics as this would prevent Guest access to the BiPublisher reports.

The BiPublisher install steps are documented here: http://docs.oracle.com/middleware/12213/bip/index.html

**Note:** BIP standalone was not part of the featureset in 12.2.1.4.0. It is currently scheduled for a future release (Doc ID 2472158.1). BIP standalone is supported only when it is upgraded to 12.2.1.4 version.

**Note**: To make report rendering work in BIP 12.2.1.4 using Guest access, below WebLogic patches must to be applied in the same order after shutting down all the domains running on that Oracle home- 28186730 (Update OPatch to 13.9.4.2.x), 30499026 (OBI Bundle patch for 12.2.1.4) and 27545920 (Guest report access error).

Once BiPublisher is installed follow the post install steps below to configure the reports.

### Post install steps for BiPublisher 12C

1. Test your BIPublisher installation, Get the xmlpserver url from your Installation Screen and launch xmlpserver. Login with the credentials you entered in your Oracle BI EE configuration (weblogic / password). Example URL:http://[obiee\_host]:[obiee server\_port]/xmlpserver

ORACLE' BI Publisher B	interprise	
	Sign In Please enter username and password Username weblogic Password Accessibility Mode Sign In Sign In Composition (United States)	

2. After sign on, select "Administration".

DRACLE' BI Publisher Enterprise	Search All		*		٩	Administration	Help 🔻	Sign Oi	ut e
Iministration		Home	Catalog	New	Ŧ	Open v	Signed in As	retaiLuse	er v
Data Sources	System Maintenance								
JDBC Connection JNDI Connection Tile LUAP Connection OLAP Connection Web Service Connection HTTP Connection	Sarver Configuration Scheduler Configuration Scheduler Digenotics Report Verver Configuration Manage Cache								
Security Center	Runtime Configuration								
Security Configuration Liters Holes and Portmessons Digital Signature	Properties Foot Mappings Currency Formats								
Delivery	Integration								
Delivery Configuration Printer Far Far WebDAV WHIP FTF Context Server CUPS Server CUPS Server	Oracle BI Presentation Services								

3. On the System Maintenance Section, click **Server Configuration**.

ORACLE' BI Publisher Enterprise	Search All			<	Administrati	Help 🔫	Sign Out
Administration		Home	Catalog	New *	Open 🔻	Signed In As	retail.user
Administration > Server Configuration							0
System Maintenance							
Server Configuration Scheduler Configuration Scheduler Diagnostics Report Viewer Configuration Man	age Cache						
TIP Any changes will only take effect after the application is restarted.						A	oply Cancel
Catalog							
Catalog Type Oracle 81 Publisher - File System							
Gatalog Type - Oracle BF Publisher - File System Path - /scratch/u00/webadmin/config/domains/wle_obieve/BDPublisherDomain/bidsta/components/bipublis	he/repository						
	her/repository-						
Path /scratch/unit/webadmin/config/domains/win_obiee/EBPublisherDomain/bidsta/components/bipublish	her/repository						
Path /scratch/unti/webadmm/cenflg/domains/wile_obee/85Publishe/Domain/bidata/components/bipublishe/ General Properties System Temporary Directory	ke/repolitory						
Path /srztch/uth/wbdmin/cenfig/domain/wite_oblex/BibliobarDomain/bidzti/components/byobles General Properties System Temporary Directory Peoport Sculable Threahaid Caching	ke/repository						
Path /scratch/uth/webdmin/cenfig/domain/wile_oblee/EPublisherComain/bidat2(components/buoble General Properties System Temporary Directory Report Scieble Threshold Caching Cache Expiration (nimulas)	her/repository						
Path /srztch/uth/wbdmin/cenfig/domain/wite_oblex/BibliobarDomain/bidzti/components/byobles General Properties System Temporary Directory Peoport Sculable Threahaid Caching	ket (repositor)						

- 4. On this screen In the Server Configuration Folder section, enter the path to your repository.
  - This is the path you entered in the Configuration Section and Catalog Section:
     Example: \$<OBIEE\_DOMAIN\_HOME>/bidata/components/bipublisher/repository
- 5. Click **Apply**.
- 6. Click Administration link at top of screen.

ORACLE <sup>®</sup> BI Publisher Enterprise	Search All	*		् Administration	Help v	Sign Out
Administration	Home	Catalog	New v	Open v	Signed In As	retailuser v
Data Sources JUBC Connection JUNIC Connection File LIAP Connection OLAP Connection Web Service Connection HTTP Connection	System Maintenance Soner Configuration Scheduler Configuration Scheduler Diagnonico Report Vener Configuration Manage Cache					
Security Center Security Configuration Users Roles and Permissions Digtal Synchure	Runtime Configuration Properties Font Mappings Currency Formatis					
Delivery Delivery Configuration Printer Fax Eau WebDay WEDDay HTTP FTP Content Server CUPS Server	Integration Oracle BI Presentation Services					

7. Click on the Security Configuration link under the Security Center to setup a super user and apply the BI Publisher security model.

			Search All				् Administration	n Help =	Sign Out
Administration				Home	Catalog	New +	Open 👻	Signed In As	retail.user
Administration > Security Configuration									
Security Center									
Security Configuration Users Roles and Permissions Digital Signature	1.4								
TIP Any changes will only take effect after the application is restarted.								Ap	ply Cancel
Local Superviser		 							
Local superviser can log in to the system independent from the selected security model $\mathscr B$ Enable Local Superviser									
Superuser name	retail.user								
Password									
Guest Access		 			_	_			-
📽 Allow Guett Access									
Guest Folder Name	Guest								
Authentication									

- 8. Enable a Superuser by checking the "Enable Local Superuser" box and by entering name and password on the corresponding fields on this screen.
- 9. Mark "Allow Guest Access" check box. Enter "Guest" as Guest Folder Name.
- 10. Click Apply.
- 11. Scroll down the screen and locate the Authorization section:

		Search All				°, Admin	nistration	ныр т	Sign Out
Administration			Home	Catalog	New	v 0p	en v	Signed In As	retail.user
Single Sign-On Type	Oracle Single Sign On								
Single Sign-Off URL									
How to get username	HTTP Header								
User Name Parameter									
How to get user locale	HTTP Header								
User Locale Parameter									
Enter the value for URL, Administrator Username, Administrator Password, Distinguishe	f Name for Users and other required information below								
URL									
Administrator Usemame	(Example: Idep///komame.port.)								
Administrator Password									
Distinguished Name for Users									
	(Example: Invitient.dovecample.dovcom )								
JNDI Context Factory Class									
Attribute used for Login Username	(Default Value: con.aux.)vd.ldap.LdapCo.Factory.)								
	(Defect Value or )								
Attribute used for user matching with authorization system									
	(Reargie: ardpart)								

- 12. Select BI Publisher Security from the Security Model list.
- 13. The default user name for the BI Publisher Security Model is Administrator.
- 14. On the password text field, enter a value that you can remember. It is going to be the password for Login to xmlpserver.
- 15. Click Apply.
  - Leave BI Publisher up while completing the next section.
- 16. Post install step: Create role Bipub\_default\_role.
  - **a.** From the xmlpserver Administration screen, scroll down to Security Center and click Roles and Permissions.

ORACLE <sup>®</sup> BI Publisher Enterprise	Search All	*	9	Administration	Help v	Sign Out
Administration	Но	ne Catalog	New +	Open v	Signed In As	retail.user v
Data Sources JDBC Connector	System Maintenance Server Configuration					
WNI Contection File 104P Connection CL4P Connection Web Service Connection HTTP Connection	Scheduler Configuration Scheduler Diparation Report Viewer Configuration Manage Cache					
Security Center	Runtime Configuration					
Skouth Configuration Lister Roles and Permissions Digtal Signature	Properties Frank Mappings Currency Formats					
Delivery	Integration					
Dellers/Configuration Printer Fax Email WeDAV HTTP FTP Content Server CUPS Server	Oracle 81 Presentation Services					

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

ORACLE' BI Publisher Enterprise				Search All			1	Administration	Help 🐨	Sign Out	
Administration					Home	Catalog	New <i>x</i>	Open v	Signed In As	retail.use	т. <del>у</del>
Administration > Roles and Permissions > Create Role											0
Create Role											
			1						1	Apply Ca	incel
	* Name Description	Bipub_default_role									

- c. Create the Bipub\_default\_role. Enter in Create Role Section name of the role.
- d. When the information has been entered press Apply changes.
- 17. Post install step: Assign BiPub system roles to the newly created Bipub\_default\_role.
  - **a.** To assign BiPub system roles to the newly create Bipub\_default\_role, go to Security Center section and navigate to the Roles and Permissions screen:

DRACLE NI	Publisher Enterprise				Search	All	*		٩,	Administration	Help w	Sign Out	
Administration						Home	Catalog	New	¥	Open v	Signed In As	retail.user	v
dministration > Roles and Pe	emissions												0
Security Center													
Security Configuration	Users Roles and Permiss	ons Digital Signa	ature										_
Number of rows displayed p	per page 10 👻												
Role Name	Sea	ch											
Create Role													
Role Name	Description			Add Data Sources	Add Roles	Delete							
Ripub_default_role				R	72	8							

b. On the Roles and Permissions screen you should see the new role created:
 "Bipub\_default\_role". Add multiple roles to the Bipub\_Default\_Role by pressing the corresponding green icon on the Add Roles column.

BI Publisher Excel Analyzer, BI Publisher Online Analyzer, BI Publisher Scheduler.

ORACLE' BI Publisher Enterprise				Search All			9,	Administration	Help +	Sign (	Out ***
Administration					Home	Catalog	New +	Open +	Signed In A	s retail.u	iser v
Administration > Roles and Permissions > Add Roles: Bpub_defauR_role Add Roles: Bipub_defauR_role										Apply	Cancel
	Available Roles	Nove S	Included Roles	300							
	BI Publisher Administrator BI Publisher Template Designer	Nove All	BL Publisher Excel Analyzer BL Publisher Online Analyzer	0000							

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

18. Post install step: create Guest (XMLP\_GUEST) user.

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

ORACLE' BI Publis	her Enterprise			Search All		Ψ.		٩,	Administratio	n Help	۰.	Sign Out	
Administration					Home	Catalog	New	τ.	Open +	Signed	in As	retail.user	. *
dministration > Users													0
Security Center													
Security Configuration Users	Roles and Permissions Digital Signati	ire	 								_		
Security Configuration Users Number of rown displayed per page Username		ire											
Number of rows displayed per page Username	10 👻	ire											
Number of rows displayed per page Usemane Create User	10 👻	Del											
Number of rows displayed per page Username	10 • Search												

- **b.** Select the "Create User" button to create the "xmlp\_guest" user and save the changes
- 19. Post install step: Adding the Bipub\_default\_role to XMLP\_GUEST user.
  - **a.** Open the Users section:
  - **b.** For xmlp\_guest user, press on the "Assign Roles" icon to navigate to the next screen:



**c.** On the Assign Roles screen, select the BiPub\_default\_role from the Available Roles panel to the "Assigned Roles" panel and press the Apply button to save your changes.

## Installing the SIM BI Publisher Templates

In this section we will outline how the SIM report templates are installed into the appropriate BI server repositories.

```
Example: $<OBIEE_DOMAIN_HOME>/bidata/components/bipublisher/repository
```

Report files are included in the SIM installation media and have to be copied into a newly created directory within BI Publisher repository Guest Reports directory.

- Create the directory to hold the reports under <BI\_REPOSITORY> mkdir <BI\_REPOSITORY>/Reports/Guest/SIM
- 2. Change directory to the <INSTALL\_DIR>/sim16/reports/ in the SIM installation media extracted previously. This directory contains a sim-reports.zip file which contains all the SIM reports.
- Copy the sim-reports.zip above to your repository and extract them cp sim-reports.xip <BI\_REPOSITORY>/Reports/Guest/SIM cd <BI\_REPOSITORY>/Reports/Guest/SIM unzip sim-reports.zip

## Configuring the SIM JDBC connection

Follow the below steps to configure a JDBC connection for the SIM Data Source, which is required for SIM reports.

- 1. If not still logged into BIPublisher:
  - Login with the credentials you entered in your Oracle BI EE configuration. (weblogic / password)
- 2. If the server was restarted:
  - Login as the super user that was created in prior security setup steps.

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

ORACLE' EN PUBLI Home	and Complete			Search Home Catalog Ner	C Administration Help v Sign Out ····
Create	Recent				
Report	Reports				
Report Job					
More + Browse/Manage	sabstr Open Eds More +	saffi Open Edit More +	Snresadb Open Eldt More +	dtypurge Open Edit More +	inbpoship Open Edit More +
Catalog Folders	Others				
Report Job History	satsstr Edit		Edit	Edit	
	dtypurpe Edit				
	Favorites Manage				

3. Click the Administration link at top of screen

			Search		Q Ad	ministration	Help v	Sign Out
dministration		Home	Catalog	New	•	Open v	Signed In As	retaiLuser
Data Sources JDBC Connection JNDC Connection File CAP Connection CAP Connection Web Server Connection HTTP Connection	System Maintenance Servit Configuration Scientific Configuration Scientific Configuration Report Vinew Configuration Manager Cardo							
Security Center Security Configuration Users Roles and Permissions Digital Signature	Runtime Configuration Proportes Point Mappings Currency Formats							
Delivery Delivery configuration Protect Fast Ensat Ensat ViveTP VitTP FTP Control Server CUIPS Server	Integration Oracle Bi Preservation Services							

4. Select the JDBC Connection hyperlink in the Data Sources lists.

DRACLE' NI	abusner Enterprise		Search All				Q. Admin	histration	Help v	Sign Out
dministration				Home	Catalog	Nex 7	Op	en +	Signed In As	retail.user
ministration > JDBC										
lata Sources										
	P OLAP Web Services HTTP									
JOBC JNDI File LDA	P OLAP Web Services HTTP									
Add Data Source	P OLAP Web Services HTTP Connection String	Delete								
JOBC JNDI File LDA		Delete								

#### 5. Click the Add Data Source button.

ORACLE' BI Publisher Enterprise			Search All			9	Administratic	m Help v	Sign O	ut 😁
Administration				Home	Catalog	New +	Open +	Signed In As	retail.us	er 🔹
Administration > 3DBC > Add Data Source										0
Add Data Source								1-2		-
								Ap	ply Can	.cel
General										-
of TIP Flease make sure to install the required JDBC driver classes. of TIP With Oracle Fusion Middleware Security Model, select the Use System User che * Data Source Name.	ckbox to use the BI System U	ser for your BI Server Database Connect	an.							
* Driver Type	Oracle 12c									
	oracle.jdbc.OracleDriver (Dampin work.jdbcDrockDriver) jdbcroraclerthin:@[host]:[p	ort]-[ad]								
Use System User										
* Username	retailuser									
Password										
Pre Process Function										
Post Process Function										
	Use Proxy Authentication Test Connection									
Backup Data Source										

- 6. Enter the appropriate details for the SIM data source. Click Test Connection to test the connection on the screen once the data is entered.
  - Data Source Name: BIP-SIM-DATASOURCE
    - Must be this name due to code dependencies.
  - Driver type is ORACLE 12C
  - Database driver class should be oracle.jdbc.OracleDriver.
  - Connection string is similar to this example:
    - Pluggable: jdbc:oracle:thin:@dbhostname:1521/servicename
    - Non- Pluggable dbc:oracle:thin:@dbhostname:1521:SID

- Enter the username and password for the SIM application user's data source. Click Test Connection to test the connection on the screen once the data is entered.
- 7. Scroll to the bottom of the screen and check the Allow Guest Access check box. Click **Apply**.

		Search All		v	Q,	Administration	Help =	Sign Out
Administration		Home	e	Catalog New	٣	Open 🔻	Signed In As	retail.user
Use Backup Data Source Connection String	0							
Username Password	Test Connection							
Security Allow Guest Access Allowed User Avalabi BI Core BI Core	Roles		8					

8. Restart WebLogic Server.

### Verify Oracle BI Publisher Set Up for SIM Reports

Verify that Oracle BI Publisher has been set up correctly as follows:

- 1. Click the Administration tab. Click Server Configuration under System Maintenance. The Catalog path variable should be set as part of the BI Publisher install, REPORTS\_DIR.
- **2.** Click Catalog link at the top of the screen and then click the Guest folder on the left so that it is highlighted. You should see the SIM reports are now in the catalog:

ORACL	E' Bl Publisher	Enterprise					5	Search All		*	c	Administration	n Help *	Sign Out	
Catalog									Home	Catalog	New w	Open w	Signed In As	retail.user	v
+* 2 2	<b>6 Д В</b>	× 2 -	Location Share	ed Folders/Guest		•									9
Folders Im My Folder	ints	RWMS Expand	Last Modified 7/14/16 1 More w Last Modified 7/14/16 More w ast Modified 7/14/16 10 More w	6 10:20 AM Create	ed By										
Tasks		ł.													
Eipand Detece Copy Paste Premissions	관, Upload 쇼, Download 및 Cut 대) Rename 때 Properties 단한 Expert XLIFF														

## Configuring SIM for CUPS printers using BIPublisher 12c

Prerequisite: CUPS printer has to be set up on the host that the BIPublisher application is installed on.

1. Login to BI Publisher using the Super user that was created earlier and Click the Administration link at the top of the screen. Click on the CUPS Server under the Delivery section.

	Search All	Ψ	9,	Administration		
Administration	Home	Catalog	New *	Open 🔻		
Data Sources	System Maintenance					
JDBC Connection JNDI Connection File LDAP Connection OLAP Connection Web Service Connection HTTP Connection	Server Configuration Scheduler Configuration Scheduler Diagnostics Report Viewer Configuratio Manage Cache	'n				
Security Center	Runtime Configuration					
Security Configuration Users Roles and Permissions Digital Signature	Properties Font Mappings Currency Formats					
Delivery	Integration					
Delivery Configuration Printer Fax Email WebDAV HTTP FTP Content Server CUPS Server	Oracle BI Presentation Ser	vices				

#### **2.** Click Add Server.

	Search All		Ŧ	0,	Administration
Administration		Home	Catalog	New 🔻	Open 🔻
Administration > CUPS Server > Add Server					
Add Server					
* Server Name					
* Host					
* Port					

- 3. Enter in values and click **Apply**:
  - Server Name: SIMCUP
    - Can be any name
  - Host: localhost
  - Port: 631
    - 631 is default port that is used as an example This may be different on the host.

**4.** After adding, refresh the servers and printers.

						Search	All		w	۰ ۹			Administration		
dministration								Home	Catalog	New	*	Open	٠	Siç	
ministration > CUPS Se elivery Delivery Configuration	N873	x Email	WebDAV	нттр	FTP	Content Server	CUPS Server								
Details	Server N	ame		Host			Po	rt		Refresh P	rinters		I	)elet	
	tion Show SIMCUP			localho			63			6				1	

# 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 Release 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 Oracle Identity Management (12.2.1.4), 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 are 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 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 12c Agent (WebGate)

Oracle WebGates are policy enforcement agents that 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 WebTier 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 of Failure.
- 10. Credential collector redirects to WebGate and authorization processing begins.
- 11. WebGate prompts OAM to look up policies, compare them to the user's identity, and determine the user's level of authorization.
- 12. OAM logs policy decision and checks the session cookie.
- 13. OAM Server evaluates authorization policies and cache the result.

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

# Installation Overview

Installing an Oracle Retail supported Single Sign-On installation using OAM 11g 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 must be installed and configured.
- 3. 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 Guide 12c.* 

#### **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 and is designed for both administrators and users and 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: 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-username>

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:

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 and RWMS

#### 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/rms16/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/rms16/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\_rms0luser.

```
ifile = /u00/oracle/product/19.3.0.0/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 = xxxxx.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/rms16/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 ths alias that was setup in the wallet's thsnames.ora file.

mkstore -wrl . -createCredential <tns\_alias> <username> <password>

**Example:** mkstore -wrl . -createCredential dvols29\_rms0luser rms0luser 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/rms16/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 19.0.0.0.0 - Production on Fri Feb 28 09:40:53 2020 Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Last Successful login time: Fri Feb 28 2020 09:21:25 -08:00

Connected to: Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production Version 19.3.0.0.0

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\_rms0luser 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\_rms0luser 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/RPMDomain/retail/rpm/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>/retailpublic-security-api/bin for administering wallet entries.
- Example:
- /u00/webadmin/config/domains/wls\_retail/RPMDomain/retail/rpm/retailpublic-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/rpm/application/rpm/Build/orpatch/deploy/retail-publicsecurity-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/RPMDomain/retail/rpm/retail-publicsecurity-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/RPMDomain/retail/rpm/retail-publicsecurity-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/RPMDomain/retail/rpm/config

```
Retail Public Security API Utility
```

Below are the credentials found in the wallet at the location/u00/webadmin/config/domains/wls\_retail/RPMDomain/retail/rpm/con fig

-----

```
Application level key partition name:rpm
```

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:rms16mock

User Name Alias: REIMBAT-ALIAS User Name: rpmbat

#### 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/mock16\_testing/rpm16/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 = rpm to retrieve the password for application use.

Reim.properties code sample:

csm.wallet.partition.name=rpm

## 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 install guides.

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

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

Webl	ogic											
		Home		1		<b>U</b> p (21)		( C	-	<b>U</b> p (9)		
		Control		,	105				TROW			
(6) (5)				-11		Status	Target	Name	Status	Host	CPU Usage	
Met		Port Usage		- 12	oyments			🖃 🎦 WebLogic Domain			(%)	
				- 00	ications			APPOomain				
		Application Deploymen		,			Cluster-reim	AdminServer	~			
						Û	rem-12115		Û	msp12115.us.ora	0.12	
		Web Services				Û	rem-12116	Cluster-reim	-			
		ADF Domain Configura		(p			Cluster-reim		Û	msp12115.us.ora		
			bon	h		G	reim-12115	areim-12116	Û	msp12116.us.ora		
		Security		>	Credentials	0	rem-12116	🖂 🏩 Cluster-rpm				
		Metadata Repositories					Cluster-rpm	a rpm-12115	G	msp12115.us.ora		
		JDBC Data Sources			Security Provider Configuration	1	rpm-12115	mpm-12116	Û	msp12116.us.ora		
		System MBean Browse	e		and the second second second	0	rpm-12116	E A Cluster est				
				-	Application Policies	1.1	Cluster-rpm	👸 rsl-12115	0	msp12115.us.ora		
3		WebLogic Server Admit	nistration Console		Application Roles	1	rpm-12115	👸 rsl-12116	Ŷ	msp12116.us.ora		
		-				0	rpm-12116	🖂 🧸 Cluster-sim				
		General Information			System Policies		Cluster-rsl	👸 sin-12115	G	msp12115.us.ora		
-	-		Crsl-r	me	1.		rsl-12115	👸 sim-12116	Ŷ	msp12116.us.ora		
			Orsie		Audit Policy	1	rsl-12116	🗉 🚞 Metadata Repositories				
			🖂 🤉 sim die	nt	Audit Store	-	Cluster-sm	o mds-owen		msp12115.us.ora		
			C1sm-		Power prove	分	sim-12115	🖻 Farm Resource Center			0	
			n sim-	dient		1	sm-12116	Before You Begin				
			E S sim hel				Cluster-sim	Introduction to Orade Fusion Mide	Seware			
			Pisim-			1	sm-12115	Understanding Key Oracle Fusion				
			() sm-			ů.	sim-12116	Overview of Oracle Fusion Middleware Administration Tools				
								Typical Administration Tasks				

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.

Application Deployments     Application Deployments     Application Deployments     Application Deployment     Application Deployment     Application Deployments     Application Deployments	Credentials A credential force is the repository of security data that certify the authority of entities used by Java 2, J2EE, and ACP applications. Applications can use the Credential Store, a single, consolidated service provider to store and manage their credentials securely.  Credential Store Provider  Score Web.opc Domain Provider CB_ORACLE									
Metadata Repositories	💠 Create Map 💠 Create Key   🥜 Edit	ap 🖕 Create Key   🥜 Edit 💥 Delete   Gredential Key		۲						
	Credential	Type	Description							
	🖂 🧰 orade.retai.sm									
	Ø bip-user	Password			11					
	P rpm-user	Password								
	😵 rib-user	Password								
	😵 rsi-ms-user	Password								
	Server-user	Password			0					
	Ø datasource-user	Password								
	😵 ldap-user	Password								
	Sso-token-key	Generic								
	Erpm									
	V LDAP-ALIAS	Password			1.0					
	😵 user.signature.salt	Password								
	OB-ALIAS	Password								

The Create Map add above is to create a new map with keys under it. A map would usually be an application such as rpm. The keys will usually represent alias to various users (database user, WebLogic user, LDAP user, and so on). 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:

E 🔐 Farm, APPDomain E 🎦 Application Deployments	WebLogic Domain 🕳						Page Refreshed Oct 25, 2013 12:41:37 PM ED		
WebLogic Domain	Credentials A credential store is the repositor provider to store and manage the	y of security data that ce in credentials securely.	entry the authority of	entites used by Java 2, J	22E, and ADF applic	ations. Applications can use the Creder	ital Store, a single, consolidated service		
E A Cluster-rem	Credential Store Provide	r							
田 篇 Cluster epm 田 篇 Cluster eni 田 篇 Cluster eni	Score WebLog: Doman Provider DB_CRACLE								
II Metadata Repositories	💠 Create Map 🔺 Create I	Key / Edit 💥	Delete Cred	ential Key Name		0			
	Credential	1	Type	Description					
	♦ bo-user ♦ rsi-rpm-user	Edit Key					1		
	P rib-user P rai-ma-user	Select Map	rpm DB-ALIAS						
	Server-user		Password		You	can enter a different user name for aut	hentication.		
	datasource-user	* User Name	ms01app						
		* Password							
	🕈 🗇 sso-token-key	<ul> <li>Confirm Password</li> </ul>							
	CDAP-ALIAS	Description							
	V LDAP-ALLAS V user.signature.se								
	0 06-ALIAS								
	0.00 0.00					K Cancel			
					10	K Cance			

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

/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 WLST:

/u00/webadmin/product/wls\_apps/oracle\_common/common/bin> sh wlst.sh

Initializing WebLogic Scripting Tool (WLST)...

Welcome to WebLogic Server Administration Scripting Shell

wls:/offline> connect('weblogic','password123','xxxxx.us.oracle.com:17001') Connecting to t3://xxxxx.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 : rms0lapp, Description : null, expiry Date : null]
PASSWORD:retail
\*The above means for map rpm in APPDomain, alias DB-ALIAS points to database user
rms0lapp 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  ${\tt myMap}$  and key name  ${\tt myKey:}$ 

deleteCred.py -map myMap -key myKey

#### modifyBootStrapCredential

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

This script is available in interactive mode only.

#### Interactive Mode Syntax

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

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

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

Example of Use:

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

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

Any output regarding the audit service can be disregarded.

### addBootStrapCredential

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

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

This script is available in interactive mode only.

#### Interactive Mode Syntax

addBootStrapCredential(jpsConfigFile="pathName", map="mapName", key="keyName", username="usrName", password="usrPass")

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

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

Example of Use:

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

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

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
RMS batch	DB	<rms batch="" dir<br="" install="">(RETAIL_HOME)&gt;/.wallet</rms>	n/a	<database SID&gt;_<data base schema owner&gt;</data </database 	<rms schema owner&gt;</rms 	Compile, execution	Installer	n/a	Alias hard-coded by installer
RMWS forms	DB	<forms install<br="">dir&gt;/base/.wallet</forms>	n/a	<database SID&gt;_<data base schema owner&gt;</data </database 	<rwms schema owner&gt;</rwms 	Compile forms, execute batch	Installer	n/a	Alias hard-coded by installer
RPM batch plsql and sqlldr	DB	<rpm batch="" install<br="">dir&gt;/.wallet</rpm>	n/a	<rms schema owner alias&gt;</rms 	<rms schema owner&gt;</rms 	Execute batch	Manual	rms-alias	RPM plsql and sqlldr batches
RWMS auto- login	JAVA	<forms install<br="">dir&gt;/base/.javawallet</forms>							
			<rwms Installation name&gt;</rwms 	<rwms database user alias&gt;</rwms 	<rwms schema owner&gt;</rwms 	RWMS forms app to avoid dblogin screen	Installer	rwms16inst	
			<rwms Installation name&gt;</rwms 	BI_ALIAS	<bi Publisher administrat ive user&gt;</bi 	RWMS forms app to connect to BI Publisher	Installer	n/a	Alias hard-coded by installer
AIP app	JAVA	<weblogic domain<br="">home&gt;/retail/<deployed aip app name&gt;/config</deployed </weblogic>							Each alias must be unique

# 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
			aip	<aip weblogic user alias&gt;</aip 	<aip weblogic user name&gt;</aip 	App use	Installer	aip- weblogic- alias	
			aip	<aip database schema user alias&gt;</aip 	<aip database schema user name&gt;</aip 	App use	Installer	aip01user- alias	
			aip	<rib-aip weblogic user alias&gt;</rib-aip 	<rib-aip weblogic user name&gt;</rib-aip 	App use	Installer	rib-aip- weblogic- alias	
RPM app	DB credenti al store		Map=rpm or what you called the app at install time.	Many for app use					<weblogic domain<br="">home&gt;/config/fmwc onfig/jps-config.xml has info on the credential store. This directory also has the domain cwallet.sso file.</weblogic>
RPM app	JAVA	<weblogic domain<br="">home&gt;/retail/<deployed rpm app name&gt;/config</deployed </weblogic>							Each alias must be unique
			rpm	<rpm weblogic user alias&gt;</rpm 	<rpm weblogic user name&gt;</rpm 	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<br="">user name&gt; is the alias. Yes, here alias name = user name</rpm>	<rpm batch<br="">user name&gt;</rpm>	App, batch use	Installer	RETAIL.US ER	
	JAVA	<retail_home>/orpatch/co nfig/javaapp_rpm</retail_home>							Each alias must be unique
			retail_install er	<rpm weblogic user alias&gt;</rpm 	<rpm weblogic user name&gt;</rpm 	App use	Installer	weblogic- alias	
			retail_install er	<rms shema<br="">user alias&gt;</rms>	<rms shema user name&gt;</rms 	App, batch use	Installer	rms01user- alias	
			retail_install er	<reim batch<br="">user alias&gt;</reim>	<reim batch<br="">user name&gt;</reim>	App, batch use	Installer	reimbat- alias	
			retail_install er	<ldap- ALIAS&gt;</ldap- 	cn=rpm.ad min,cn=Use rs,dc=us,dc =oracle,dc= com	LDAP user use	Installer	LDAP_ALI AS	
ReIM app	JAVA	<weblogic domain<br="">home&gt;/retail/<deployed reim app name&gt;/config</deployed </weblogic>							Each alias must be unique
			<installed app name, ex: reim&gt;</installed 	<reim weblogic user alias&gt;</reim 	<reim weblogic user name&gt;</reim 	App use	Installer	weblogic- alias	
			<installed app name, ex: reim&gt;</installed 	<rms shema<br="">user alias&gt;</rms>	<rms shema user name&gt;</rms 	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&gt;</installed 	<reim webservice validation user alias&gt;</reim 	<reim webservice validation user name&gt;</reim 	App use	Installer	reimwebser vice-alias	
			<installed app name, ex: reim&gt;</installed 	<reim batch<br="">user alias&gt;</reim>	<reim batch<br="">user name&gt;</reim>	App, batch use	Installer	reimbat- alias	
			<installed app name, ex: reim&gt;</installed 	<ldap- ALIAS&gt;</ldap- 	cn=REIM.A DMIN,cn= Users,dc=u s,dc=oracle, dc=com	LDAP user use	Installer	LDAP_ALI AS	
	JAVA	<retail_home>/orpatch/co nfig/javaapp_reim</retail_home>							Each alias must be unique
			retail_install er	<reim weblogic user alias&gt;</reim 	<reim weblogic user name&gt;</reim 	App use	Installer	weblogic- alias	
			retail_install er	<rms shema<br="">user alias&gt;</rms>	<rms shema user name&gt;</rms 	App, batch use	Installer	rms01user- alias	
			retail_install er	<reim webservice validation user alias&gt;</reim 	<reim webservice validation user name&gt;</reim 	App use	Installer	reimwebser vice-alias	
			retail_install er	<reim batch<br="">user alias&gt;</reim>	<reim batch<br="">user name&gt;</reim>	App, batch use	Installer	reimbat- alias	
			retail_install er	<ldap- ALIAS&gt;</ldap- 	cn=REIM.A DMIN,cn= Users,dc=u s,dc=oracle, dc=com	LDAP user use	Installer	LDAP_ALI AS	

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
RESA app	DB credenti al store		Map=resaor what you called the app at install time	Many for login and policies					<weblogic domain<br="">home&gt;/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.</weblogic>
RESA app	JAVA	<weblogic domain<br="">home&gt;/retail/<deployed resa app name&gt;/config</deployed </weblogic>							Each alias must be unique
			<installed app name&gt;</installed 	<resa weblogic user alias&gt;</resa 	<resa weblogic user name&gt;</resa 	App use	Installer	wlsalias	
			<installed app name&gt;</installed 	<resa schema db user alias&gt;</resa 	<rmsdb shema user name&gt;</rmsdb 	App use	Installer	Resadb-alias	
			<installed app name&gt;</installed 	<resa schema user alias&gt;</resa 	<rmsdb shema user name&gt;&gt;</rmsdb 	App use	Installer	resa-alias	
	JAVA	<retail_home>/orpatch/co nfig/javaapp_resa</retail_home>							Each alias must be unique

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
			retail_install er	<resa weblogic user alias&gt;</resa 	<resa weblogic user name&gt;</resa 	App use	Installer	wlsalias	
			retail_install er	<resa schema db user alias&gt;</resa 	<rmsdb shema user name&gt;</rmsdb 	App use	Installer	Resadb-alias	
	JAVA	<retail_ home&gt;/orpatch/config/ja vaapp_rasrm</retail_ 							Each alias must be unique
			retail_install er	<alloc weblogic user alias&gt;</alloc 	<alloc weblogic user name&gt;</alloc 	App use	Installer	weblogic- alias	
Alloc app	DB credenti al store		Map=alloc or what you called the app at install time	Many for login and policies					<pre><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.</weblogic></pre>
Alloc app	JAVA	<weblogic domain<br="">home&gt;/retail/config</weblogic>							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&gt;</installed 	<alloc weblogic user alias&gt;</alloc 	<alloc weblogic user name&gt;</alloc 	App use	Installer	weblogic- alias	
			<installed app name&gt;</installed 	<rms schema user alias&gt;</rms 	<rms schema user name&gt;</rms 	App use	Installer	dsallocAlias	
			<installed app name&gt;</installed 	<alloc batch<br="">user alias&gt;</alloc>	<system_ ADMINIST RATOR&gt;</system_ 	Batch use	Installer	alloc14	
	JAVA	<retail_ home&gt;/orpatch/config/ja vaapp_alloc</retail_ 							Each alias must be unique
			retail_install er	<alloc weblogic user alias&gt;</alloc 	<alloc weblogic user name&gt;</alloc 	App use	Installer	weblogic- alias	
			retail_install er	<rms schema user alias&gt;</rms 	<rms schema user name&gt;</rms 	App use	Installer	dsallocAlias	
			retail_install er	<alloc batch<br="">user alias&gt;</alloc>	<system_ ADMINIST RATOR&gt;</system_ 	Batch use	Installer	alloc14	
	JAVA	<retail_ home&gt;/orpatch/config/ja vaapp_rasrm</retail_ 							Each alias must be unique
			retail_install er	<alloc weblogic user alias&gt;</alloc 	<alloc weblogic user name&gt;</alloc 	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 credenti al store		Map=oracle. retail.sim	Aliases required for SIM app use					<pre><weblogic domain="" home="">/config/fmwc onfig/jps-config.xml has info on the credential store. This directory also has the domain cwallet.sso file.</weblogic></pre>
	JAVA	<weblogic domain<br="">home&gt;/retail/<deployed sim app name&gt;/batch/resources/c onf</deployed </weblogic>	oracle.retail. sim	<sim batch<br="">user alias&gt;</sim>	<sim batch<br="">user name&gt;</sim>	App use	Installer	BATCH- ALIAS	
	JAVA	<weblogic domain<br="">home&gt;/retail/<deployed sim app name&gt;/wireless/resources /conf</deployed </weblogic>	oracle.retail. sim	<sim wireless user alias&gt;</sim 	<sim wireless user name&gt;</sim 	App use	Installer	WIRELESS- ALIAS	
RETL	JAVA	<retl home&gt;/etc/security</retl 	n/a	<target application user alias&gt;</target 	<target application db userid&gt;</target 	App use	Manual	retl_java_rm s01user	User may vary depending on RETL flow's target application
RETL	DB	<retl home="">/.wallet</retl>	n/a	<target application user alias&gt;</target 	<target application db userid&gt;</target 	App use	Manual	<db>_<user &gt;</user </db>	User may vary depending on RETL flow's target application
RIB	JAVA	<ribhome DIR&gt;/deployment- home/conf/security</ribhome 							<app> is one of aip, rfm, rms, rpm, sim, rwms, tafr</app>
JMS			jms<1-5>	<jms user<br="">alias&gt; for jms&lt;1-5&gt;</jms>	<jms user<br="">name&gt; for jms&lt;1-5&gt;</jms>	Integra- tion 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</app>	<rib-app weblogic user alias&gt;</rib-app 	<rib-app weblogic user name&gt;</rib-app 	Integra- tion use	Installer	weblogic- alias	
Admin GUI			rib- <app>#web- app-user- alias</app>	<rib-app admin gui user alias&gt;</rib-app 	<rib-app admin gui user name&gt;</rib-app 	Integra- tion use	Installer	admin-gui- alias	
Application			rib- <app>#user- alias</app>	<app weblogic user alias&gt;</app 	<app weblogic user name&gt;</app 	Integra- tion use	Installer	app-user- alias	Valid only for aip, rpm, sim
DB			rib- <app>#app- db-user-alias</app>	<rib-app database schema user alias&gt;</rib-app 	<rib-app database schema user name&gt;</rib-app 	Integra- tion use	Installer	db-user- alias	Valid only for rfm, rms, rwms, tafr
Error Hospital			rib- <app>#hosp -user-alias</app>	<rib-app error hospital database schema user alias&gt;</rib-app 	<rib-app error hospital database schema user name&gt;</rib-app 	Integra- tion use	Installer	hosp-user- alias	
RFI	Java	<rfi-home>/retail- financial-integration- solution/service-based- integration/conf/security</rfi-home>							
			<installed app name&gt;</installed 	rfiAppServe rAdminServ erUserAlias	<rfi weblogic user name&gt;</rfi 	App use	Installer	rfiAppServe rAdminServ erUserAlias	
			<installed app name&gt;</installed 	rfiAdminUi UserAlias	<orfi admin user&gt;</orfi 	App use	Installer	rfiAdminUi UserAlias	

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
			<installed app name&gt;</installed 	rfiDataSourc eUserAlias	<orfi schema user name&gt;</orfi 	App use	Installer	rfiDataSourc eUserAlias	
			<installed app name&gt;</installed 	ebsDataSour ceUserAlias	<ebs schema user name&gt;</ebs 	App use	Installer	ebsDataSour ceUserAlias	
			<installed app name&gt;</installed 	smtpMailFr omAddress Alias	<from email address&gt;</from 	App use	Installer	smtpMailFr omAddress Alias	

# **Appendix: Tablespace Creation**

# Non-Encrypted Tablespace Creation

Standard SIM tablespaces are created using the create\_tablespaces.sql script located in <INSTALL\_DIR>/sim/dbschema/dbutils /.

- 1. Update the paths of the script in <INSTALL\_DIR>/sim/dbschema/dbutils /create\_tablespaces.sql as pertain to your environment.
- 2. The table below shows the default initial sizes.

TABLESPACE_NAME	Size
SIM_ENCRYPTED_INDEX	12G
SIM_ENCRYPTED_DATA	10G
SIM_INDEX	10G
SIM_DATA	8G
SIM_LOB_DATA	2G
SIM_LOB_INDEX	2G
USERS	2G

- 3. Once the paths of script has been modified, execute it in SQL\*Plus as sys.
- 4. Review create\_tablespaces.log for errors and correct as needed.

## **Encrypted Tablespace Creation**

If you do not have an Advanced Security Option license, create the sim\_encrypted\_data and sim\_encrypted\_index tablespaces as normal tablespaces but without the encryption.

- 1. Modify the paths of the script <INSTALL\_DIR>/sim/dbschema/dbutils /create\_encrypted\_tablespaces\_no\_TDE.sql
- 2. Run the script using SQL\*Plus as sys
- 3. Review create\_encrypted\_tablespaces\_no\_TDE.log for errors and correct as needed With an Advanced Security license, tablespaces can be created in an encrypted format. The steps are:

### **Configure a Wallet**

1. Create a sqlnet.ora in \$TNS\_ADMIN directory of the database server similar to the below entry:

```
ENCRYPTION_WALLET_LOCATION =
  (SOURCE = (METHOD = FILE)
   (METHOD_DATA =
    (DIRECTORY = /u00/oracle/admin/ORACLE_SID/wallet)))
```

2. Create the wallet directory:

mkdir -p /u00/oracle/admin/<ORACLE\_SID>/wallet

3. As a user with the 'alter system' privilege, create the wallet as follows:

Non-container databases:

- a. ADMINISTER KEY MANAGEMENT CREATE KEYSTORE '/u00/oracle/admin/dbName/wallet' IDENTIFIED BY "pwd#";
- b. ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY "pwd#";
- **c.** ADMINISTER KEY MANAGEMENT SET KEY IDENTIFIED BY "pwd#" WITH BACKUP;
- **d.** ADMINISTER KEY MANAGEMENT CREATE AUTO\_LOGIN KEYSTORE FROM KEYSTORE '/u00/oracle/admin/dbName/wallet' identified by pwd#;
- a. Container databases:
- b. ADMINISTER KEY MANAGEMENT CREATE KEYSTORE '/u00/oracle/admin/dbName/wallet' IDENTIFIED BY "pwd#";
- c. ADMINISTER KEY MANAGEMENT CREATE AUTO\_LOGIN KEYSTORE FROM KEYSTORE '/u00/oracle/admin/dbName/wallet' identified by "pwd#";
- **d.** ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY "pwd#" Container=ALL;
- e. ADMINISTER KEY MANAGEMENT SET KEY IDENTIFIED BY "pwd#" WITH BACKUP USING 'TDE\_ENCRYPTION' Container=all;
- 4. Confirm if the wallet is created and open (the TDE master encryption key has been created and inserted automatically):

```
SQL>
select substr(wrl_type, 1, 10) wrl_type, substr(wrl_parameter, 1, 45) param,
substr(status, 1, 10) status, substr(wallet_type, 1, 15) w_type
from v$encryption_wallet;
```

WRL_TYPE	PARAM	STATUS	W_TYPE
FILE	/u00/oracle/admin/ORACLE_SID/wallet	OPEN	AUTOLOGIN

An auto-open wallet is created. You are ready to create the encrypted tablespaces as shown in the following section.

#### **Encryption at Tablespace Level**

Once the wallet is configured, determine an encryption algorithm to be used for the encrypted tablespace and then create them. The sample scripts use the default algorithm AES128:

- Modify the paths of the script <INSTALL\_DIR>/sim/dbschema/dbutils /create\_encrypted\_ tablespaces\_TDE.sql.
- 2. Run the script using SQL\*Plus as sys.
- 3. Review Create\_encrypted\_tablespaces\_TDE.log for errors and correct as needed. Once the tablespaces have been created, the SIM schema installation can be run.

**Note:** After encryption at the tablespace level, it is absolutely crucial to backup the contents in the wallet directory; otherwise, if they are lost you will not be able to access the tablespaces.

# **Appendix: Database Parameter File**

```
******
# Copyright (c) 2014 by Oracle Corporation
# Oracle 19.x.x Parameter file
# NOTES: Before using this script:
       1. Change <datafile_path>, <admin_path>, <utl_file_path>, <diag_path>
#
and <hostname>
#
         values as appropriate.
#
       2. Replace the word SID with the database name.
       3. Size parameters as necessary for development, test, and production
#
environments.
# -----
*.audit_file_dest=full_path_of_audit_dir
*.audit trail='db'
*.compatible='19.0.0.0'
*.control_files='full_path_of_controlfile_1','full_path_of_controlfile_2'
****
# Memory Settings:
# xxxM = Some reasonable starting value for your environment.
****
*.db block size=xxxM
*.db_cache_size=xxxM
*.java_pool_size=xxxM
*.memory_target=xxxM
*.pga_aggregate_target=xxxM
*.shared_pool_size=xxxM
*.streams pool size=xxxM
*.db block_size=8192
*.db domain=''
*.db_name='dbName'
*.diagnostic dest='full path of diag dir'
*.enable_pluggable_database=true|false
*.fast_start_mttr_target=900
*.nls_calendar='GREGORIAN'
*.nls_date_format='DD-MON-RR'
*.nls_language='AMERICAN'
*.nls_numeric_characters='.,'
*.nls sort=BINARY
*.open_cursors=900
*.os authent prefix=''
*.plsql optimize level=2
*.processes=2000
*.query_rewrite_enabled='true'
*.remote_dependencies_mode='SIGNATURE'
*.remote_login_passwordfile='EXCLUSIVE'
*.remote_os_authent=true
*.sec case sensitive logon=false
*.undo tablespace='UNDOTBS1'
```

# **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 Warehouse Management System (RWMS)
- 5. Oracle Retail Invoice Matching (ReIM)
- 6. Oracle Retail Price Management (RPM)
- 7. Oracle Retail Allocation
- 8. Oracle Retail Mobile Merchandising (ORMM)
- 9. Oracle Retail Customer Engagement (ORCE)
- 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 Predictive Application Server Batch Script Architecture (RPAS BSA)
- 17. Oracle Retail Demand Forecasting (RDF)
- Oracle Retail Category Management Planning and Optimization/Macro Space Optimization (CMPO/MSO)
- 19. Oracle Retail Replenishment Optimization (RO)
- 20. Oracle Retail Regular Price Optimization (RPO)
- 21. Oracle Retail Merchandise Financial Planning (MFP)
- 22. Oracle Retail Size Profile Optimization (SPO)
- 23. Oracle Retail Assortment Planning (AP)
- 24. Oracle Retail Item Planning (IP)
- 25. Oracle Retail Item Planning Configured for COE (IP COE)
- 26. Oracle Retail Advanced Inventory Planning (AIP)
- 27. Oracle Retail Integration Bus (RIB)
- 28. Oracle Retail Service Backbone (RSB)

- 29. Oracle Retail Financial Integration (ORFI)
- 30. Oracle Retail Bulk Data Integration (BDI)
- 31. Oracle Retail Integration Console (RIC)
- 32. Oracle Commerce Retail Extension Module (ORXM)
- 33. Oracle Retail Data Extractor for Merchandising
- 34. Oracle Retail Clearance Optimization Engine (COE)
- 35. Oracle Retail Analytic Parameter Calculator for Regular Price Optimization (APC-RPO)
- Oracle Retail Insights, including Retail Merchandising Insights (previously Retail Merchandising Analytics) and Retail Customer Insights (previously Retail Customer Analytics)
- 37. Oracle Retail Order Broker