Oracle® Retail Store Inventory Management

Installation Guide

Release 13.2.9

E73366-02

September 2017

Oracle® Retail Store Inventory Management Installation Guide, Release 13.2.9

Primary Author: Donna Linde

Contributors: Nathan Young

Value-Added Reseller (VAR) Language

Oracle Retail VAR Applications

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

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

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

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

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

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

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

Contents

Send Us Your Comments ix

Preface xi

Audience.. xi
Related Documents xi
Customer Support.. xi
Review Patch Documentation.. xi
Improved Process for Oracle Retail Documentation Corrections................................ xii
Oracle Retail Documentation on the Oracle Technology Network xii
Conventions.. xii

1 Preinstallation Tasks 1

Implementation Capacity Planning.. 1
Upgrading SIM.. 1
Requesting Infrastructure Software 1
Check Supported Database Server Requirements 2
Check Supported Application Server Requirements.. 4
Check Single Sign-On Requirements 6
Check Directory Server Requirements... 7
Check Third-Party Software Dependencies... 7
Check Client PC and Web Browser Requirements 7
Supported Oracle Retail Products 8
UNIX User Account Privileges to Install the Software.. 8
SIM Installation Overview 8
Customer Profiles... 9

2 RAC and Clustering 11

3 Database Patch Installation Tasks 13

Upgrading to the Latest Version 13
Expand the SIM Database Patch.. 13
Patching the Database.. 13

4 Application Installation.. 15

Application Server Deployment Options 15

5 Installing the SIM Application on Oracle Application Server (OAS) 17

Oracle Configuration Manager.. 17
Create a New OC4J Instance and Group for SIM... 17
Configure Apache for JNLP Files 19
Set the LANG Environment Variable... 19
Expand the SIM Application Distribution... 19
Run the SIM Application Installer.. 20
Review and/or Configure Oracle Single Sign-On 20
SIM Batch Scripts 21

Adding Users to Application Server for Web Services 21

Resolving Errors Encountered During Application Installation 24

Web Help Files 24

Starting and Stopping SIM 24

Starting and Stopping the Wavelink Server 25

6 Installing the SIM Application on WebLogic 27

Oracle Configuration Manager 27

Install Managed Server in WebLogic 27

Install NodeManager 31

Start the Managed Server 38

Set the LANG Environment Variable 41

Expand the SIM Application Distribution 41

SIM Custom Security Providers 41

SIM Database Authentication Provider Set up 41

SIM SSO Authentication Provider set up (if SSO is configured) 44

Run the SIM Application Installer 45

Clustered Installations – Post-Installation Steps 46

Review and/or Configure Oracle Single Sign-On 46

SIM Batch Scripts 47

Configure Web Service Security in SIM 47

Resolving Errors Encountered During Application Installation 51

Web Help Files 51

Starting and Stopping the Wavelink Server 51

Set the SSO_TIMEOUT Parameter 52

7 Test the SIM Application 53

A Appendix: SIM Application Oracle Application Server (OAS) Installer Screens 55

B Appendix: SIM Application WebLogic Server Installer Screens 85

C Appendix: Installer Silent Mode 115

D Appendix: Common Installation Errors 117

EJB Deployment Errors during Installation to WebLogic 117

XML Processing Errors while configuring sim-client.ear or sim-server.ear 118

Output Freezes during Text Mode Installation to OAS and WebLogic 118

Database Installer Hangs on Startup 119

Unreadable Buttons in the Installer 119

Message: Unable to get a deployment manager 119

Warning: Could not create system preferences directory 120

Warning: Couldn't find X Input Context 120

ConcurrentModificationException in Installer GUI 120

Error while unpacking the ear file 121

A Second Login Screen Appears After Single Sign-On Login 121

Error Connecting to Database URL 122

Installer Fails because of missing .jar in $ORACLE_HOME/utils/ccr/lib 122
Files not available to copy at the end of installation results in non working applications – WebLogic only 123
GUI screens fail to open when running Installer 123
Log in fails with invalid username/password or user unauthorized errors............ 123
SIM-WS URL fails with Error: SIMFaultApiMessage: An Error occurred accessing StoreServices in Clustered Environment 124
The “TEST page” link in SIM-WS URL fails with Error: 404 124
Installer fails with sun.security.validator.KeyStores exception 124

E Appendix: Setting up SIM Reports in BI Publisher 125
BI Publisher 11g – BI Server Component Installation Tasks 125
BI Publisher 11g – Installation Process Overview 126
BI Publisher 11g – Install Oracle BI EE 11g.. 126
BI Publisher 11g – Configuring the SIM JDBC connection 138
BI Publisher 11g – Configuring the SIM Application with BI Publisher:............ 140
Configuring SIM for CUPS printers using BI Publisher 11g 141

F Appendix: Oracle Single Sign-On for Oracle Application Server (OAS) 145
What Do I Need for Oracle Single Sign-On? 145
Can Oracle Single Sign-On Work with Other SSO Implementations? 145
Oracle Single Sign-on Terms and Definitions.. 146
What Single Sign-On is not 147
How Oracle Single Sign-On Works 147
Installation Overview 149
User Management... 150
Setting up SIM for Single Sign-on 150

G Appendix: Oracle Single Sign-On for WebLogic 153
What Do I Need for Oracle Single Sign-On? 153
Can Oracle Access Manager Work with Other SSO Implementations?..................... 153
Oracle Single Sign-on Terms and Definitions.. 154
What Single Sign-On is not 155
How Oracle Single Sign-On Works 156
Installation Overview 157
User Management... 158

H Appendix: Setting Up Password Stores with Oracle Wallet 161
About Password Stores and Oracle Wallet 161
Setting Up Password Stores for Database User Accounts 162
Setting Up Wallets for Database User Accounts 163
For RMS, RPM Plsql Batch, RETL DB, RWMS batch, and ARI 163
For Java Applications (SIM, ReIM, RPM, Alloc, RIB, RSL, AIP, RETL) 165
How Does the Wallet Relate to the Application? 168
How Does the Wallet Relate to Java Batch Program Use? 168
Setting up RETL Wallets 168

Quick Guide for Retail Wallets 171

I Appendix: Preinstallation for Secured Setup of SIM in Oracle Application Server (OAS) 177

J Appendix: Preinstallation for Secured Setup of SIM in WebLogic 181

Get an SSL Certificate and Set up a Keystore 181

Configure the Application Server for SSL 182

Verify SSL Connections 185

Securing Nodemanager with SSL Certificates 185

Using Secured LDAP 186

Batch Setup for SSL Communication 187

K Appendix: Certificate Import Topology 189

L Appendix: Oracle 11g Database Parameter File 191

M Appendix: Oracle Database 12cR1 Parameter File 193

N Appendix: Configuring Listener and Tnsnames 195

O Appendix: Installation Order 199

Enterprise Installation Order 199

Send Us Your Comments

Oracle Retail Store Inventory Management, Installation Guide, Release 13.2.9.

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

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

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

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

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

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

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

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

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

Preface

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

Audience

This Installation Guide is written for the following audiences:

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

Related Documents

For more information, see the following documents in the Oracle Retail Store Inventory Management Release 13.2.9 documentation set:

- *Oracle Retail Store Inventory Management Release Notes*
- *Oracle Retail Store Inventory Management Data Model*

Customer Support

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

https://support.oracle.com

When contacting Customer Support, please provide the following:

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

Review Patch Documentation

When you install the application for the first time, you install either a base release (for example, 13.2) or a later patch release (for example, 13.2.9). If you are installing the base release or additional patch releases, read the documentation for all releases that have occurred since the base release before you begin installation. Documentation for patch releases can contain critical information related to the base release, as well as information about code changes since the base release.

Improved Process for Oracle Retail Documentation Corrections

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

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

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

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

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

Oracle Retail Documentation on the Oracle Technology Network

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

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

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

Conventions

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

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

1 Preinstallation Tasks

This chapter discusses the tasks to complete before installation.

Implementation Capacity Planning

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

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

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

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

Upgrading SIM

SIM 13.2.9 is a patch installation. It is possible to upgrade a previous release (for example, from SIM 13.2.0.3) installation to version SIM 13.2.9. If you would like to perform an upgrade from SIM 13.2.0.x, refer to the My Oracle Support document, *Oracle Retail Upgrade Guide* (ID 1073414.1).

Requesting Infrastructure Software

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

Check Supported Database Server Requirements

General Requirements for a database server running SIM include:

Supported on:	Versions Supported:
Database Server OS	OS certified with Oracle Database 11gR2 (11gR2) and 12cR1 (12.1.0.2) Enterprise Edition. Options are: ▪ Oracle Enterprise Linux 5 update x for x86-64 (Actual hardware or Oracle virtual machine). ▪ Red Hat Enterprise Linux 5 update x for x86-64 (Actual hardware or Oracle virtual machine). ▪ Oracle Enterprise Linux 6 for x86-64 (Actual hardware or Oracle virtual machine). ▪ Red Hat Enterprise Linux 6 for x86-64 (Actual hardware or Oracle virtual machine). ▪ AIX 6.1 (Actual hardware or LPARs) ▪ AIX 7.1 (Actual hardware or LPARs) ▪ Solaris 10, 11 Sparc (Actual hardware or Oracle VM Server for SPARC). ▪ HP-UX 11.31 Integrity (Actual hardware or HPVM)
Database Server 11gR2	Oracle Database Enterprise Edition 11gR2 (11.2.0.4) with the following specifications: **Components:** ▪ Oracle Partitioning ▪ Examples CD (Formerly the companion CD) **Oneoff Patches:** ▪ 18465025: MERGE REQUEST ON TOP OF 11.2.0.4.0 FOR BUGS 18016963 18302329. **Other components:** ▪ Perl compiler 5.0 or later ▪ X-Windows interface

Supported on:	**Versions Supported:**
Database Server 12cR1	Oracle Database Enterprise Edition 12cR1 (12.1.0.2) with the following specifications: **Components:** ▪ Oracle Partitioning ▪ Examples CD **Oneoffs:** ▪ 19623450: MISSING JAVA CLASSES AFTER UPGRADE TO JDK 7 ▪ 20406840: PROC 12.1.0.2 THROWS ORA-600 [17998] WHEN PRECOMPILING BY 'OTHER' USER ▪ 20925154: ORA-39126: WORKER UNEXPECTED FATAL ERROR IN KUPW$WORKER GATHER_PARSE_ITEMS JAVA ▪ 18760297: DUMP IN QERTRCROWP WHEN TRACING WITH OPERAND LENGTH CHECK ▪ 21614112: ORA-01732 ON DML ON A PARTITIONED TABLE **RAC only:** ▪ 21260431: APPSST 12C : GETTING ORA-4031 AFTER 12C UPGRADE ▪ 21373473: INSTANCE TERMINATED AS LMD0 AND LMD2 HUNG FOR MORE THAN 70 SECS **Other components:** ▪ Perl interpreter 5.0 or later ▪ X-Windows interface ▪ ANSI compliant C-compiler (certified with OS and database version). ▪ JDK 1.7

Note: By default, JDK is at 1.6. After installing the rdbms binary, apply patch 19623450. Then follow the instructions on Oracle Database Java Developer’s Guide 12c Release 1 to change JDK to 1.7. The document is available at:

http://docs.oracle.com/database/121/JJDEV/chone.htm#JJDEV01000

Check Supported Application Server Requirements

The SIM application can be deployed on either Oracle WebLogic 10.3.6 or Oracle Application Server 10g 10.1.3.4.

> **Note:** If you are integrating with RMS 13.1.x products, then SIM 13.2.9 must be run on Oracle Application server (OAS).

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

> **Note:** Files required for OCM (Oracle Configuration Manager) are removed after OPatch is used to patch the WebLogic server. This will cause the product installers and OCM installation to fail. To work around this issue, back up the content of the $ORACLE_HOME/utils/ccr/lib directory prior to applying a patch using OPatch, and recopy the content back after you apply any patches. ORACLE_HOME is the location where WebLogic Server has been installed.
>
> **Note:** If using an OPatch on Linux 64-bit platforms, see Installer Fails because of missing .jar in $ORACLE_HOME/utils/ccr/lib in Appendix: Common Installation Errors.

> **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.

Supported On	Versions Supported
Application Server OS	OS certified with Oracle Application Server 10g 10.1.3.4. Options are: ▪ Oracle Enterprise Linux 5 update x for x86-64 (Actual hardware or Oracle virtual machine). ▪ Red Hat Enterprise Linux 5 update x for x86-64 (Actual hardware or Oracle virtual machine). ▪ Oracle Enterprise Linux 6 for x86-64 (Actual hardware or Oracle virtual machine). ▪ Red Hat Enterprise Linux 6 for x86-64 (Actual hardware or Oracle virtual machine). ▪ AIX 6.1 (Actual hardware or LPARs) ▪ AIX 7.1 (Actual hardware or LPARs) ▪ Solaris 10, 11 Sparc (Actual hardware or Oracle VM Server for SPARC). ▪ HP-UX 11.31 Integrity (Actual hardware or HPVM)

Supported On	Versions Supported
Application Server	Oracle Application Server 10g 10.1.3.4 with the following patches: ▪ 4601861 - NEED TO EXPOSE NZOS_SETIOSEMANTICS - Sun ▪ 5632264 - NEED UPDATED TIMEZONE FILES (VERSION 4) FOR MORE DST RULE CHANGES CORE - Generic Platform ▪ 5649850 - IF STRONG VERIFIER, GETCONNECTION FAIL AFTER INVOKE SETCONNECTIONCACHEPROPERTIES - Generic Platform (patch to help with uppercase passwords) Java: OC4J instance(s) running JDK 1.6.18

Note: This release of SIM is only supported in a managed OC4J instance as part of OracleAS 10g. It is not supported on OC4J standalone.

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

Supported on:	Versions Supported:
Application Server OS	OS certified with Oracle Fusion Middleware 11g Release. Options are: ▪ Oracle Linux 5.x for x86-64 (Actual hardware or Oracle virtual machine). ▪ Red Hat Enterprise Linux 5.x for x86-64 (Actual hardware or Oracle virtual machine). ▪ Oracle Linux 6 for x86-64 (Actual hardware or Oracle virtual machine). ▪ Red Hat Enterprise Linux 6 for x86-64 (Actual hardware or Oracle virtual machine). ▪ AIX 7.1 (Actual hardware or LPARs) ▪ Solaris 11 SPARC (Actual hardware or logical domains) ▪ HP-UX 11.31 Integrity (Actual hardware, HPVM, or vPars)

Supported on:	**Versions Supported:**
Application Server	Oracle Fusion Middleware 11g **Components:** ▪ Oracle WebLogic Server 11g version 10.3.6 ▪ Java: JDK 1.7+ 64 bit **IMPORTANT:** If there is an existing WebLogic installation on the server, you must upgrade it to WebLogic 10.3.6. Back up the weblogic.policy file ($WLS_HOME/wlserver_10.3/server/lib) before upgrading your WebLogic server, because this file could be overwritten. Copy over the weblogic.policy backup file after the WebLogic upgrade is finished and the post patching installation steps are completed. **Other components:** ▪ Oracle BI Publisher 11g (11.1.1.9) ▪ Oracle Internet Directory 10gR3 (10.1.4) or ▪ Oracle Identity Management 11gR1 (11.1.1.9) **Optional (SSO required)** ▪ Oracle WebTier 11g (11.1.1.9) **Supported SSO configurations:** ▪ Oracle Internet Directory 10gR3 (10.1.4) optionally with Oracle Single Sign-On 10gR3 (10.1.4) or ▪ Oracle Identity Management 11gR1 (11.1.1.9) optionally with Oracle Single Sign-On 10gR3 (10.1.4) or ▪ Oracle Identity Management 11gR1 (11.1.1.9) optionally with Oracle Access Manager 11gR2 (11.1.2.3) using OSSO agent. Must have separate WebLogic 10.3.6 for Oracle Access Manager 11gR2. or ▪ Oracle Identity Management 11gR1 (11.1.1.9) optionally with Oracle Access Manager 11gR2 (11.1.2.3) using webgate 11gR2 (11.1.2.3) agent. Must have separate WebLogic 10.3.6 for Oracle Access Manager 11gR2.

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 Internet Directory 10gR3 version 10.1.4 or Oracle Identity Management 11gR1 version 11.1.1.9 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 11gR2 as a partner application.

Check Directory Server Requirements

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

- Oracle Internet Directory 10gR3 version 10.1.4

or

- Oracle Identity Management 11gR1 version 11.1.1.9

Check Third-Party Software Dependencies

- Oracle Retail Wireless Foundation Server, provided by Wavelink 4.x.

Check Client PC and Web Browser Requirements

Requirement	Versions
Operating system	Windows 7
Display resolution	1024x768 or higher
Processor	1GHz or higher
Memory	512MBytes or higher
Oracle (Sun) Java Runtime Environment	Java 1.7.80+ or 1.8.65+ For SIM deployed on WLS Java 1.7.40 For SIM deployed on OAS
Browser	Microsoft Internet Explorer 9 or 11 Mozilla Firefox ESR 31+ 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) 13.2.9 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) 13.2.9 – Optional
- Oracle Retail Price Management 13.2.9 – Optional
- Oracle Retail POS Suite 13.3.6 or 13.4.8 – Optional

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

> **Note:** SIM 13.2.9 also support integration to RMS 13.1.x, RPM 13.1.x through RIB 13.1.x. The supported applications server for integrating with RIB13.1.x is OAS server.

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 or OAS) if it has not been installed
3. Set role-based access control. See Chapter 3 of the *Oracle Retail Store Inventory Management Implementation Guide, Volume 1* for instructions.
4. Install the SIM application.
5. Run data-seeding from RMS.

Customer Profiles

SIM 13.2.9 supports multiple installation scenarios. Find your scenario below and proceed with the instructions listed for your scenario.

- If you are doing a fresh install of SIM 13.2.9 and have Oracle Retail Merchandising 13.1 applications OR ORPOS 13.2 then proceed with installing Oracle Application server 10g and Database install. That is, all these products run on Oracle Application server 10g.
- If you are doing a fresh install of SIM 13.2.9 and have Oracle Retail Merchandising 13.2 applications OR ORPOS 13.4 then proceed with installing Oracle Web logic server 11g and Database install. That is, all these products run on Oracle Web logic server 11g.
- If you are upgrading from SIM 13.2.0.3 to SIM 13.2.9, please see the *Oracle Retail Upgrade Guide* for database upgrade. Your choice of application server will be determined by the release levels of other Oracle Retail software with which SIM integrates.

2

RAC and Clustering

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

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

The Oracle Retail products have been validated against an 11.2.0.4 and/or 12.1.0.2 RAC database. When using a RAC database, all JDBC connections should be configured to use OCI connections rather than THIN connections. It is suggested that when using OCI connections, the Oracle Retail products database be configured in the tnsnames.ora file used by the Oracle Application Server or Web Logic Server installations.

Clustering for Oracle Application Server 10.1.3 is managed as an Active-Active cluster accessed through a hardware Load Balancer. It is suggested that a VirtualHost be added to the OAS 10.1.3 reflecting the Virtual Server Name configured in the load balancer. It is also suggested that the OC4J select method be configured to prefer the use of local OC4J instances. The Oracle Retail products are currently not validated to be distributable at the application level in an OAS 10.1.3 cluster.

Clustering for Oracle Application Server 10.1.2 is managed as an Active-Active cluster accessed through a hardware Load Balancer. It is suggested that the Web Cache installation included with OAS 10.1.2 be configured to reflect all application server Mid-Tier installations. Validation has been completed utilizing a RAC 11.2.0.4 and/or 12.1.0.2 Oracle Internet Directory database with the OAS 10.1.2 cluster.

Clustering for Web Logic Server 10.3.6 is managed as an Active-Active cluster accessed through a Load Balancer. Validation has been completed utilizing a RAC 11.2.0.4 and/or 12.1.0.2 Oracle Internet Directory database with the Web Logic 10.3.6 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® Application Server High Availability Guide 10g Release 3 (10.1.3) Part Number B15977-02
- Oracle® Fusion Middleware High Availability Guide 11g Release 1 (11.1.1) Part Number E10106-09
- Oracle® Real Application Clusters Administration and Deployment Guide 11g Release 2 (11.2) Part Number E16795-11; and/or

  Oracle Real Application Clusters Administration and Deployment Guide 12*c* Release 1 (12.1) E48838-10

3 Database Patch Installation Tasks

This chapter describes the tasks required for database patch installation.

Upgrading to the Latest Version

These instructions assume that you are upgrading SIM from 13.2.7 to 13.2.9. If you are currently using a version of SIM prior to 13.2.7 that you want to upgrade to 13.2.9, you must first upgrade to 13.2.7. Refer to the *Oracle Retail Store Inventory Management Installation Guide* for 13.2.7 before proceeding.

Expand the SIM Database Patch

To expand the SIM database schema installation distribution, complete the following steps.

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 patch (sim-database-change.zip). There should be a minimum of 90 MB disk space available for the database patch files. This location is referred to as INSTALL_DIR for the remainder of this chapter.
3. Copy sim-database-change.zip to <INSTALL_DIR> and extract its contents.

Patching the Database

This step will upgrade your database from version 13.2.7 to version 13.2.9.

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

   Example: Export NLS_LANG=AMERICAN_AMERICA.UTF8

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

4

Application Installation

This chapter explains application installation.

Application Server Deployment Options

SIM 13.2.9 supports two different application servers for deployment:

- Oracle WebLogic Server 11g (10.3.6)
- Oracle Application Server 10g Enterprise Edition (10.1.3.4)

Your choice of application server is determined by the release levels of Oracle Retail software with which SIM integrates.

- You must use Oracle WebLogic Server 11g to integrate with
  - Oracle Retail Merchandising 13.2 applications using Oracle Retail Integration Bus (RIB) 13.2.9
  - Oracle Retail Point-of-Service 13.4
- You must use Oracle Application Server 10g to integrate with
  - Oracle Retail Merchandising 13.1 applications using Oracle Retail Integration Bus 13.1
  - Oracle Retail Point-of-Service 13.2

Your application installation steps will vary depending on which application server you are using. Perform your application installation using the appropriate procedure:

- See Chapter 5, Installing the SIM Application on Oracle Application Server (OAS).
- See Chapter 6, Installing the SIM Application on WebLogic.

5

Installing the SIM Application on Oracle Application Server (OAS)

Before proceeding you must install Oracle Application Server 10g 10.1.3.4 plus the patches listed in Chapter 1 of this document. The SIM application is deployed to an OC4J instance within the OracleAS 10g installation. It is assumed Oracle database has already been configured and loaded with the appropriate SIM schema for your installation.

Oracle Configuration Manager

The Oracle Retail OCM Installer packaged with this release installs the latest version of OCM and will be the first set of screens in both the OAS and WebLogic application installers.

See the My Oracle Support document, *Oracle Configuration Manager Installer Guide* (ID 1071030.1).

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

Access My Oracle Support at the following URL:

`https://support.oracle.com`

OCM Documentation Link

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

Note: OCM is not supported on AIX 7.1

Create a New OC4J Instance and Group for SIM

You can skip this section if you are redeploying to an existing OC4J group in Oracle Application Server 10.1.3.4.

The SIM application must be deployed to its own dedicated OC4J group that is running with Java 1.6. For instructions on how to create a new OC4J group and instance, see "Adding and Deleting OC4J Instances" in the "Reconfiguring Application Server Instances" chapter of the *Oracle Application Server Administrator's Guide*.

1. Log in to the server which is running your OracleAS 10g installation. Set your ORACLE_HOME environment variable to point to this installation.
2. Choose a name for the new OC4J instance and group.

   Example: sim-oc4j-instance

   Example: sim_group

   Create this OC4J instance and group as documented in the *Oracle Application Server Administrator's Guide*.

Example:
$ORACLE_HOME/bin/createinstance
–instanceName sim-oc4j-instance –groupName sim_group

When prompted for the oc4jadmin password, provide the same administrative password you gave for the Oracle Application Server installation. All OC4J instances running Oracle Retail applications must have the same oc4jadmin password.

3. (**Linux only**) Increase memory for the new OC4J instance by modifying $ORACLE_HOME/opmn/conf/opmn.xml. Locate the OC4J instance you just created, and add the -XX:PermSize=256m -XX:MaxPermSize=512m -Xms256m -Xmx256m options to the start-parameters section.

   Example:

   ```
   <process-type id=”orco-inst” module-id=”OC4J”
   status=”enabled”>
      <module-data>
         <category id=”start-parameters”>
            <data id=”java-options” value=”-server
   -XX:PermSize=256m -XX:MaxPermSize=512m -Xms256m -
   Xmx256m -
   Djava.security.policy=$ORACLE_HOME/j2ee/orco-
   inst/config/java2.policy –Djava.awt.headless=true
   –Dhttp.webdir.enabled=false”/>
         </category>
   ```

4. Force OPMN to reload the configuration file.

   Example: $ORACLE_HOME/opmn/bin/opmnctl reload

5. Start the OC4J group. You can do this through the Enterprise Manager Web interface, or on the command line using the opmnctl utility:

   Clustered Example: $ORACLE_HOME/opmn/bin/opmnctl @cluster startproc ias-component=sim_group

   Non-clustered Example:
   $ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=sim_group

6. Verify that the OC4J group was fully started. If you are using the Enterprise Manager Web interface, the instance should have a green arrow indicating that it is running. On the command line, verify that the instance has a status of Alive.

   Example: $ORACLE_HOME/opmn/bin/opmnctl status

   If you are unable to start the OC4J instance after several attempts, try increasing the startup timeouts in ORACLE_HOME/opmn/conf/opmn.xml. If that does not help, consult the Oracle Application Server documentation for further assistance.

Configure Apache for JNLP Files

If this is the first WebStart application that is being installed in the HTTP server, you need to configure the **mime.types** file with the jnlp file type. If you are using the Apache distribution that is included with OracleAS, this file can be found under ORACLE_HOME/Apache/Apache/conf. Add the following line to the file:

```
application/x-java-jnlp-file        jnlp
```

Restart the Apache server for this change to take effect. If you do not add this line then jnlp files are served as plain text and you cannot launch the application.

Example: $ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server

Set the LANG Environment Variable

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

Example:

LANG=en_US

export LANG

For instructions on how to restart the Application Server, see the *opmnctl Commands* chapter of the *Oracle® Process Manager and Notification Server Administrator's Guide*.

Example:

$ORACLE_HOME/opmn/bin/opmnctl stopall

$ORACLE_HOME/opmn/bin/opmnctl startall

Expand the SIM Application Distribution

To expand the SIM application distribution, complete the following steps.

1. Log into the UNIX server as the user who owns the OracleAS 10g installation. Create a new staging directory for the SIM application distribution (sim13application.zip). There should be a minimum of 250 MB disk space available for the application installation files.

   Example: /u00/webadmin/media/sim

2. Copy sim13application.zip to <INSTALL_DIR> and extract its contents.

   Example: unzip sim13application.zip

   Note: If you are using AIX 7.1, the **"retail-OCM-withAnt.zip"** file present in the INSTALL_DIR/sim must be renamed or removed **before** running the installer. See Appendix: Common Installation Errors for more information.

Run the SIM Application Installer

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

1. If you are installing to a clustered Application Server, perform the preinstallation tasks.
2. Set the ORACLE_HOME and JAVA_HOME environment variables. ORACLE_HOME should point to your OracleAS installation. JAVA_HOME should point to $ORACLE_HOME/jdk (if Java 6) or your Java 6 installation.
3. 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.
4. Verify that the OC4J instances that you install SIM to are currently running. See the section, "Create a New OC4J Instance and Group for SIM," for how to start the oc4j instances.
5. Run the install.sh script. This launches the installer.
6. After installation is completed, a detailed installation log file is created: <INSTALL_DIR>/sim/application/logs/sim-install-app.<timestamp>.log.

> **Note:** See Appendix: SIM Application Oracle Application Server (OAS) Installer Screens for details on every screen and field in the Oracle Application Server application installer.

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

Review and/or Configure Oracle Single Sign-On

Skip this section if you are not using Single Sign-On for user identification and authentication.

Single Sign-On is applicable only to the JnlpLaunch Servlet. The JnlpLaunch Servlet is a dynamically protected application. The JnlpLaunch Servlet causes the SIM client application to execute under the SSO user name with a temporary password.

> **Note:** The JnlpLaunch servlet may be configured for either an SSO or non-SSO environment.

HTTP Server configuration requirements: The HTTP Server must be registered with the Oracle Single Sign-On server and the mod_osso module enabled. The registration process typically involves running the ssoreg.sh script at the OSSO server installation and copying the output osso.conf file to the HTTP Server. This process is documented in the Oracle Single Sign-On administration documentation.

JnlpLaunch requirements: The JnlpLaunch Servlet uses the configuration file, JnlpLaunch.properties, to control its behavior. Due to security considerations, this file must not be published or readable to the general public.

JnlpLaunch.properties has the following configuration entries that apply to Single Sign-On:

- `secret.key – Used` to create the temporary password, this property should contain a random string. If JnlpLaunch is deployed in a different JVM than the SIM Server EJBs, this string must be an exact match between the JnlpLaunch Servlet and the one available to the SIM EJBs. For security purposes, each separate instance of the SIM application (for example, test versus development) should have a different secret key.
- `user.validation.timeout` – Number of seconds the SIM Server uses to determine if a temporary password is still valid.
- `osso.used` – Determines if the JnlpLaunch Servlet will throw a 499 error when an unathenticated user has been detected. This property must be set to true if Oracle Single Sign-On is used and false if not.

The JnlpLaunch.properties file is initialized by the SIM installer and should contain valid entries for SSO when the Enable Single Sign-On in SIM? prompt was answered with Y or Yes. However, an administrator may want to alter the user.validation.timeout or other property after the initial installation.

SIM Batch Scripts

The SIM application installer places the SIM batch programs with the rest of the SIM application files under $ORACLE_HOME/j2ee/<oc4j-instance-name>/<sim-client-deployment-name>/batch

The batch programs can be run from a different location if you cannot run them from under the application server ORACLE_HOME. To install the batch files in a different location just copy the entire $ORACLE_HOME/j2ee/<oc4j-instance-name>/<sim-client-deployment-name>/batch directory to the appropriate destination.

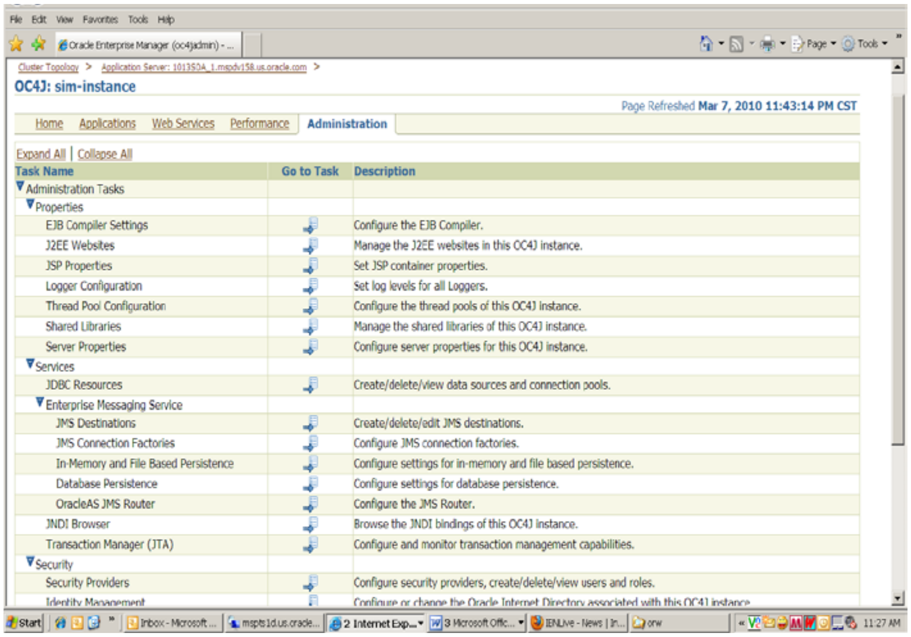
The batch location is assumed to be located on the same server as the application server. If you copy the batch to a location on a different server, then you need to configure the file path to the sim-batch.log file, which is defined in batch /resources/log4j.xml.

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

Adding Users to Application Server for Web Services

Once the application has been installed, you need to add users to the user role for web services.

1. Go to the Enterprise Manager console for the Application Server where you installed SIM.
2. Click the SIM instance where you installed the application.
3. Click the Administration link.
4. Click the **Security Provider** task icon in the Security category.



Cluster Topology > Application Server: 1013SOA_1.mspdv158.us.oracle.com >

OC4J: sim-instance

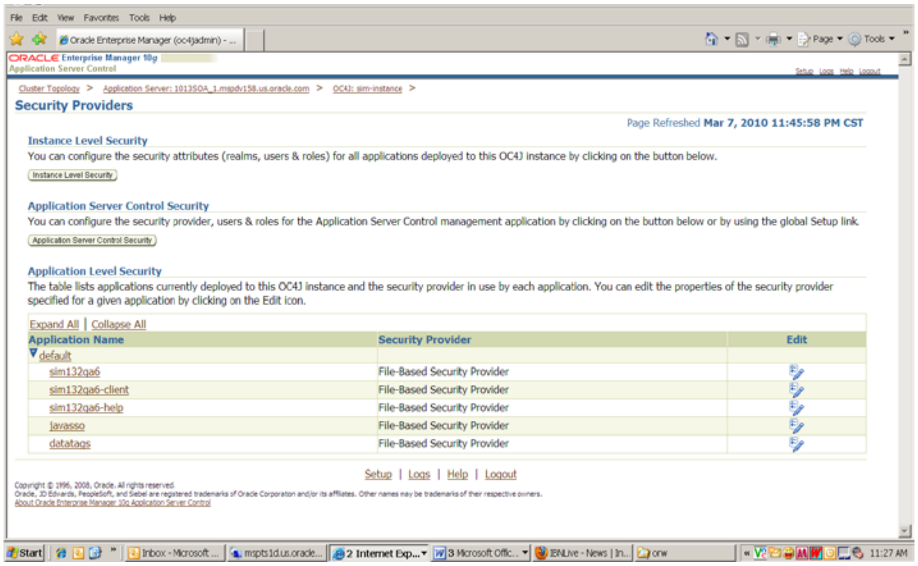
Page Refreshed **Mar 7, 2010 11:43:14 PM CST**

Home | Applications | Web Services | Performance | **Administration**

Expand All | Collapse All

Task Name	Go to Task	Description
▼Administration Tasks		
▼Properties		
EJB Compiler Settings		Configure the EJB Compiler.
J2EE Websites		Manage the J2EE websites in this OC4J instance.
JSP Properties		Set JSP container properties.
Logger Configuration		Set log levels for all Loggers.
Thread Pool Configuration		Configure the thread pools of this OC4J instance.
Shared Libraries		Manage the shared libraries of this OC4J instance.
Server Properties		Configure server properties for this OC4J instance.
▼Services		
JDBC Resources		Create/delete/view data sources and connection pools.
▼Enterprise Messaging Service		
JMS Destinations		Create/delete/edit JMS destinations.
JMS Connection Factories		Configure JMS connection factories.
In-Memory and File Based Persistence		Configure settings for in-memory and file based persistence.
Database Persistence		Configure settings for database persistence.
OracleAS JMS Router		Configure the JMS Router.
JNDI Browser		Browse the JNDI bindings of this OC4J instance.
Transaction Manager (JTA)		Configure and monitor transaction management capabilities.
▼Security		
Security Providers		Configure security providers, create/delete/view users and roles.
Identity Management		Configure or change the Oracle Internet Directory associated with this OC4J instance

5. Click **Instance Level Security**.



Cluster Topology > Application Server: 1013SOA_1.mspdv158.us.oracle.com > OC4J: sim-instance >

Security Providers

Page Refreshed **Mar 7, 2010 11:45:58 PM CST**

Instance Level Security

You can configure the security attributes (realms, users & roles) for all applications deployed to this OC4J instance by clicking on the button below.

Application Server Control Security

You can configure the security provider, users & roles for the Application Server Control management application by clicking on the button below or by using the global Setup link.

Application Level Security

The table lists applications currently deployed to this OC4J instance and the security provider in use by each application. You can edit the properties of the security provider specified for a given application by clicking on the Edit icon.

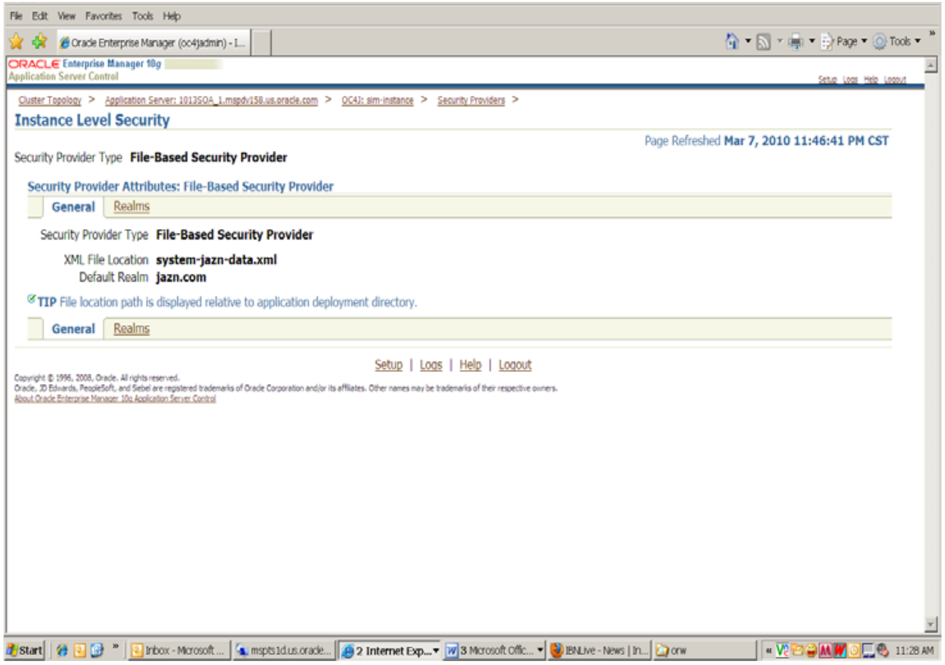
Expand All | Collapse All

Application Name	Security Provider	Edit
▼default		
sim132qa6	File-Based Security Provider	
sim132qa6-client	File-Based Security Provider	
sim132qa6-help	File-Based Security Provider	
javasso	File-Based Security Provider	
datatags	File-Based Security Provider	

Setup | Logs | Help | Logout

Copyright © 1996, 2008, Oracle. All rights reserved.
Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
About Oracle Enterprise Manager 10g Application Server Control

6. Click **Realms**.



Cluster Topology > Application Server: 1013SOA_1.mspdv158.us.oracle.com > OC4J: sim-instance > Security Providers >

Instance Level Security

Page Refreshed **Mar 7, 2010 11:46:41 PM CST**

Security Provider Type **File-Based Security Provider**

Security Provider Attributes: File-Based Security Provider

General | Realms

Security Provider Type **File-Based Security Provider**

XML File Location **system-jazn-data.xml**

Default Realm **jazn.com**

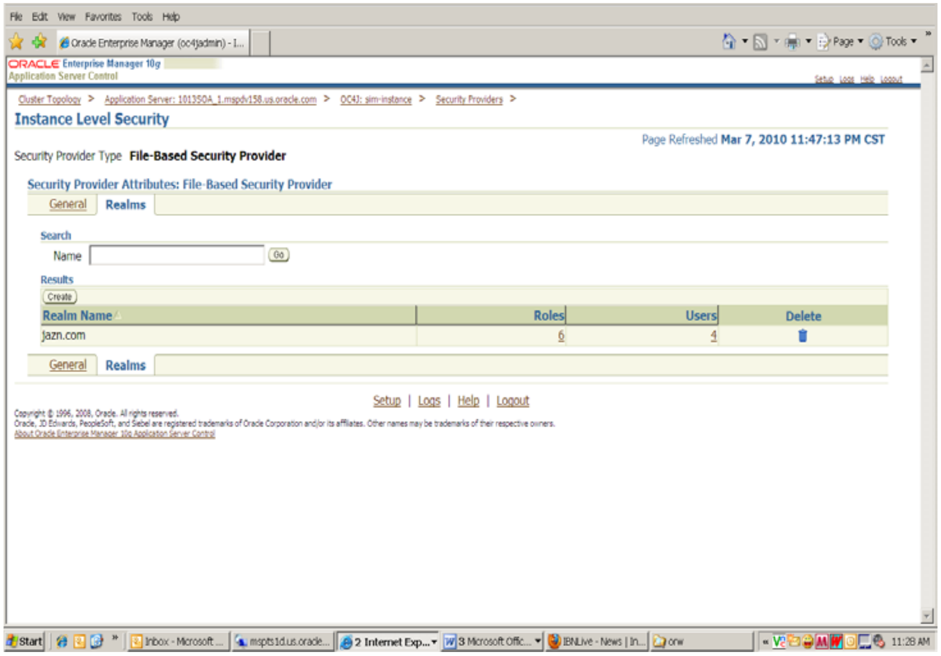
TIP File location path is displayed relative to application deployment directory.

General | Realms

Setup | Logs | Help | Logout

Copyright © 1996, 2008, Oracle. All rights reserved.
Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
About Oracle Enterprise Manager 10g Application Server Control

7. Click **Users** (click the number under the Users column).



Cluster Topology > Application Server: 1013SOA_1.mspdv158.us.oracle.com > OC4J: sim-instance > Security Providers >

Instance Level Security

Page Refreshed **Mar 7, 2010 11:47:13 PM CST**

Security Provider Type **File-Based Security Provider**

Security Provider Attributes: File-Based Security Provider

General | **Realms**

Search

Name

Results

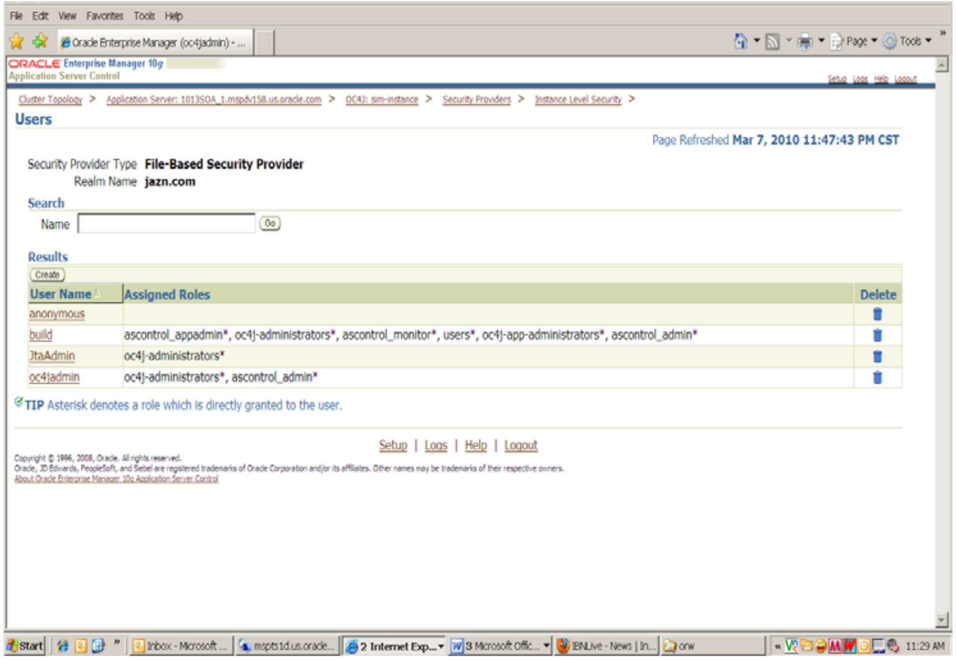
Realm Name	Roles	Users	Delete
jazn.com	6	4	🗑

General | **Realms**

Setup | Logs | Help | Logout

Copyright © 1996, 2008, Oracle. All rights reserved.
Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
About Oracle Enterprise Manager 10g Application Server Control

8. Create the user by clicking the **Create** button:


File Edit View Favorites Tools Help
Oracle Enterprise Manager (oc4jadmin) - ...
Page Tools
ORACLE Enterprise Manager 10g
Application Server Control
Setup Logs Help Logout

Cluster Topology > Application Server: 1013SOA_1.mspdv158.us.oracle.com > OC4J: sim-instance > Security Providers > Instance Level Security >

Users

Page Refreshed **Mar 7, 2010 11:47:43 PM CST**

Security Provider Type **File-Based Security Provider**
Realm Name **jazn.com**

Search

Name [ ] Go

Results

Create

User Name	Assigned Roles	Delete
anonymous		🗑
build	ascontrol_appadmin*, oc4j-administrators*, ascontrol_monitor*, users*, oc4j-app-administrators*, ascontrol_admin*	🗑
JtaAdmin	oc4j-administrators*	🗑
oc4jadmin	oc4j-administrators*, ascontrol_admin*	🗑

TIP Asterisk denotes a role which is directly granted to the user.

Setup | Logs | Help | Logout

Copyright © 1996, 2008, Oracle. All rights reserved.
Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
About Oracle Enterprise Manager 10g Application Server Control

9. Create the user by adding user name, password, choosing the user role. Click **OK**.

Resolving Errors Encountered During Application Installation

If the application installer encounters any errors, it halts execution immediately. You can run the installer in silent mode so that you do not have to retype the settings for your environment. See "Appendix: Installer Silent Mode" for information about 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 SIM

SIM can also be restarted by using the Enterprise Manager to restart the OC4J instance that contains SIM. However, if you use the Enterprise Manager to restart SIM, the Wavelink server needs to be restarted manually.

Starting and Stopping the Wavelink Server

To use handheld wireless devices with SIM, the Wavelink server must be running.

Note: If you use the Enterprise Manager to restart SIM you must restart the Wavelink server manually.

If you use the Enterprise Manager to restart SIM, the Wavelink server is not affected. So it must be restarted manually once SIM is running again.

The Wavelink server scripts can be found here:

ORACLE_HOME/ j2ee/<oc4j-instance-name>/<sim-deployment-name>/wireless/bin/wavelink-startup.sh

ORACLE_HOME/ j2ee/<oc4j-instance-name>/<sim-deployment-name>/wireless/bin/wavelink-shutdown.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.

Please 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.

Note: For additional information about LDAP configuration see the *Oracle Retail Store Inventory Management Implementation Guide*.

6

Installing the SIM Application on WebLogic

Before proceeding, you must install Oracle WebLogic Server 11g (10.3.6) and patches listed in the Chapter 1 of this document. The Oracle Retail Allocation 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 RMS and Oracle Retail Allocation schemas for your installation.

IMPORTANT: If there is an existing WebLogic installation on the server, you must upgrade it to WebLogic 10.3.6.

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

If Oracle Forms 11g has been installed in the same WebLogic that is being used for this application, a domain called “ClassicDomain” is installed. Installing a separate domain under the same WebLogic server is recommended. It can be called “APPDomain” (or something similar) and will be used to install the non-ORACLE Forms managed servers. Applications such as RPM, SIM, Allocation, ReIM, RIB, AIP, and RSL can be installed in the “APPDomain.”

Oracle Configuration Manager

The Oracle Retail OCM Installer packaged with this release installs the latest version of OCM and will be the first set of screens in both the OAS and WebLogic application installers.

The following document is available through My Oracle Support.

Access My Oracle Support at the following URL:

`https://metalink.oracle.com`

Oracle Configuration Manager Installer Guide (ID 1071030.1)

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

OCM Documentation Link

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

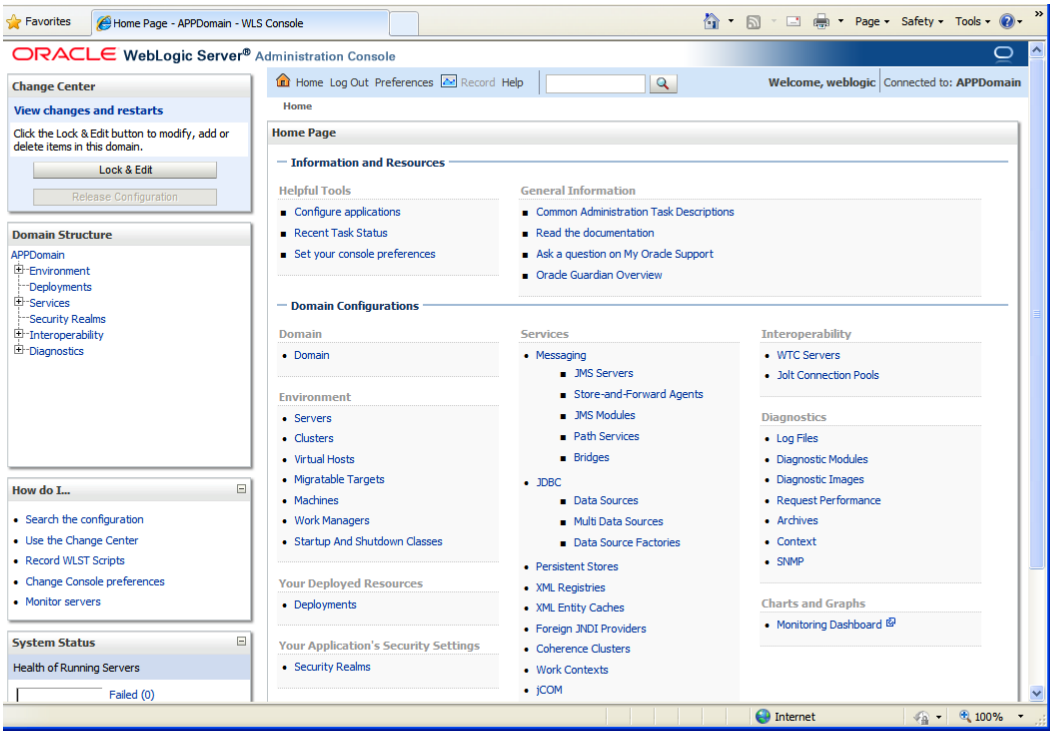
Note: OCM is not supported on AIX 7.1

Install Managed Server in WebLogic

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

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

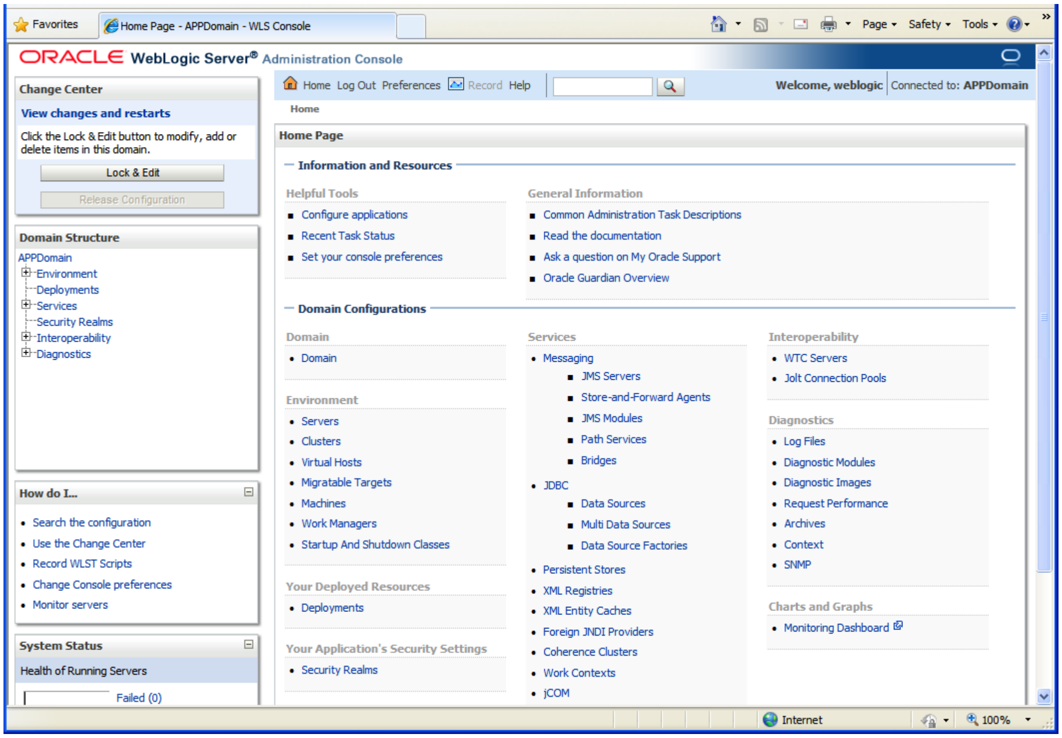
1. Log in to the admin console



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

2. Click **Lock & Edit**.

3. Navigate to Environment->Servers and select new tab of the servers on the right side.



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

4. Set the following variables:

   - **Server Name**: These should be some name specific to your application targeted

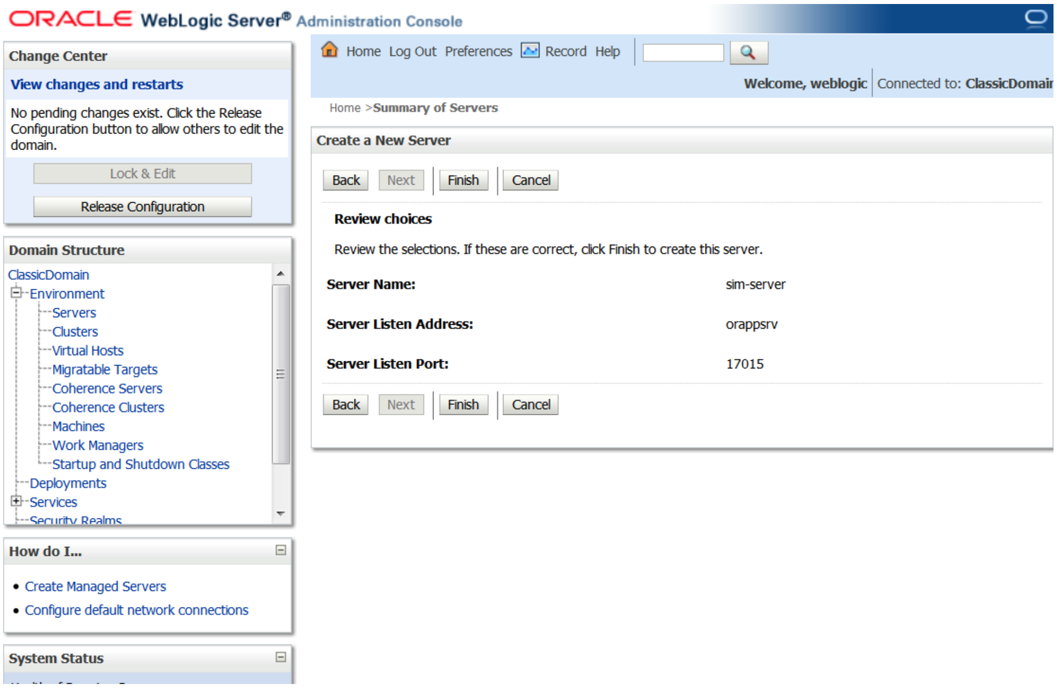
     Example: sim-server

   - **Server Listen Address**: <weblogic server> (for example, orappserv).

   - **Server Listen Port**: A free port; you should check for availability.

     A suggestion is to increment the AdminServer port by two and keep incrementing by two for each managed server (for example, 18003, 18005, 18007 and so on).

5. Click **Next**.



No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Create a New Server

Review choices

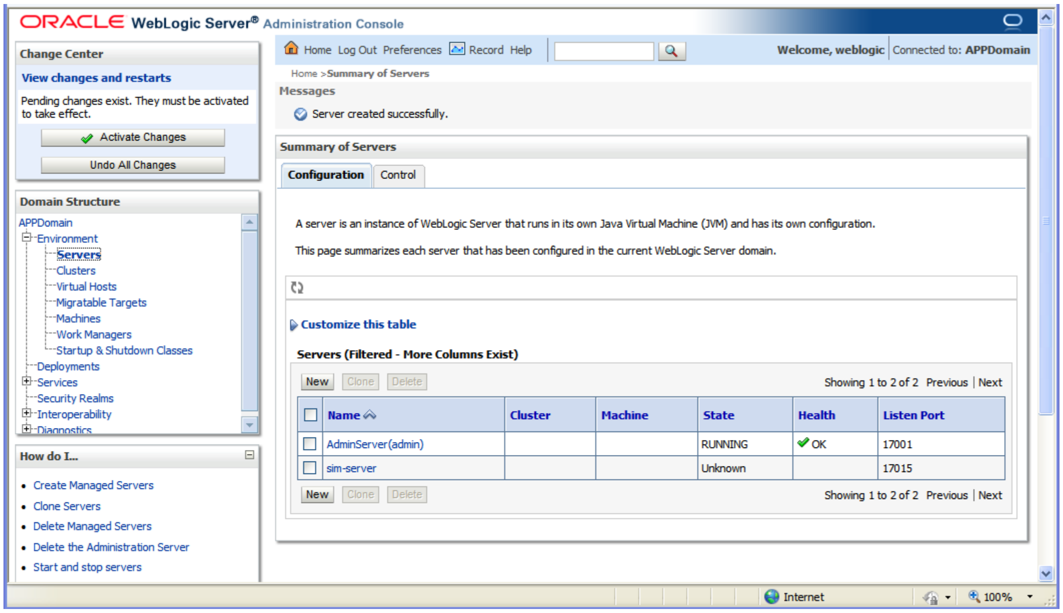
Review the selections. If these are correct, click Finish to create this server.

Server Name: sim-server

Server Listen Address: orappsrv

Server Listen Port: 17015

6. Click **Finish**.



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

Messages

Server created successfully.

Summary of Servers

A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration.

This page summarizes each server that has been configured in the current WebLogic Server domain.

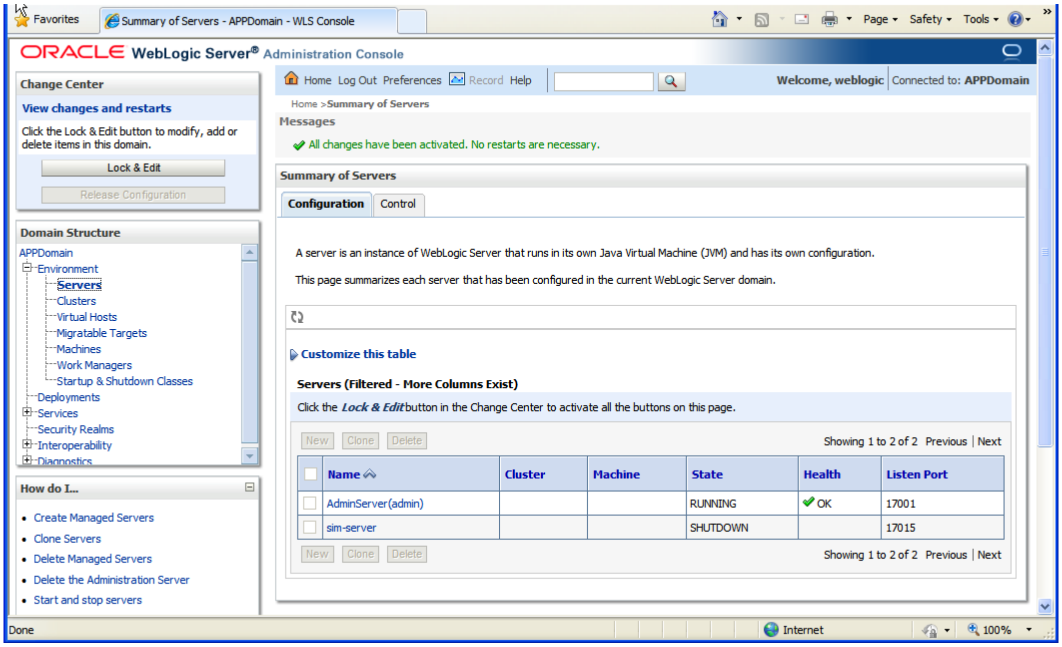
Servers (Filtered - More Columns Exist)

Showing 1 to 2 of 2 Previous | Next

□	Name	Cluster	Machine	State	Health	Listen Port
□	AdminServer(admin)			RUNNING	✓ OK	17001
□	sim-server			Unknown		17015

Showing 1 to 2 of 2 Previous | Next

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



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

✓ All changes have been activated. No restarts are necessary.

A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration.

This page summarizes each server that has been configured in the current WebLogic Server domain.

Servers (Filtered - More Columns Exist)

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

Showing 1 to 2 of 2 Previous | Next

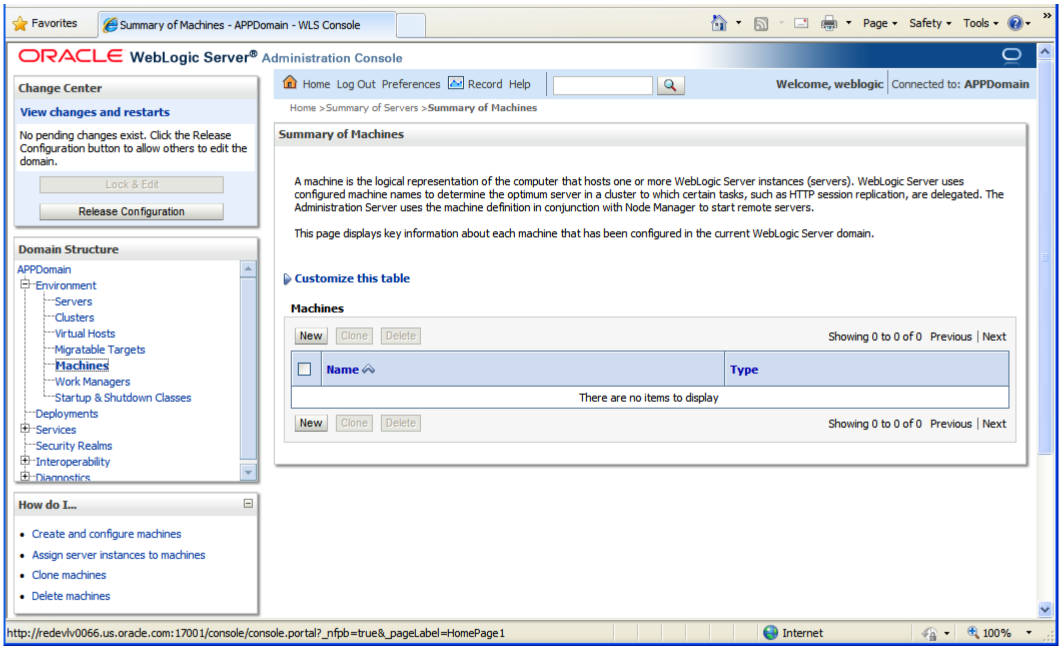
□	Name	Cluster	Machine	State	Health	Listen Port
□	AdminServer(admin)			RUNNING	✓ OK	17001
□	sim-server			SHUTDOWN		17015

Showing 1 to 2 of 2 Previous | Next

Install NodeManager

Install NodeManager if it was not created during domain install. NodeManager is required so that the managed servers can be started and stopped via the admin console. Only one NodeManager is needed per WebLogic install.

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



No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

A machine is the logical representation of the computer that hosts one or more WebLogic Server instances (servers). WebLogic Server uses configured machine names to determine the optimum server in a cluster to which certain tasks, such as HTTP session replication, are delegated. The Administration Server uses the machine definition in conjunction with Node Manager to start remote servers.

This page displays key information about each machine that has been configured in the current WebLogic Server domain.

Machines

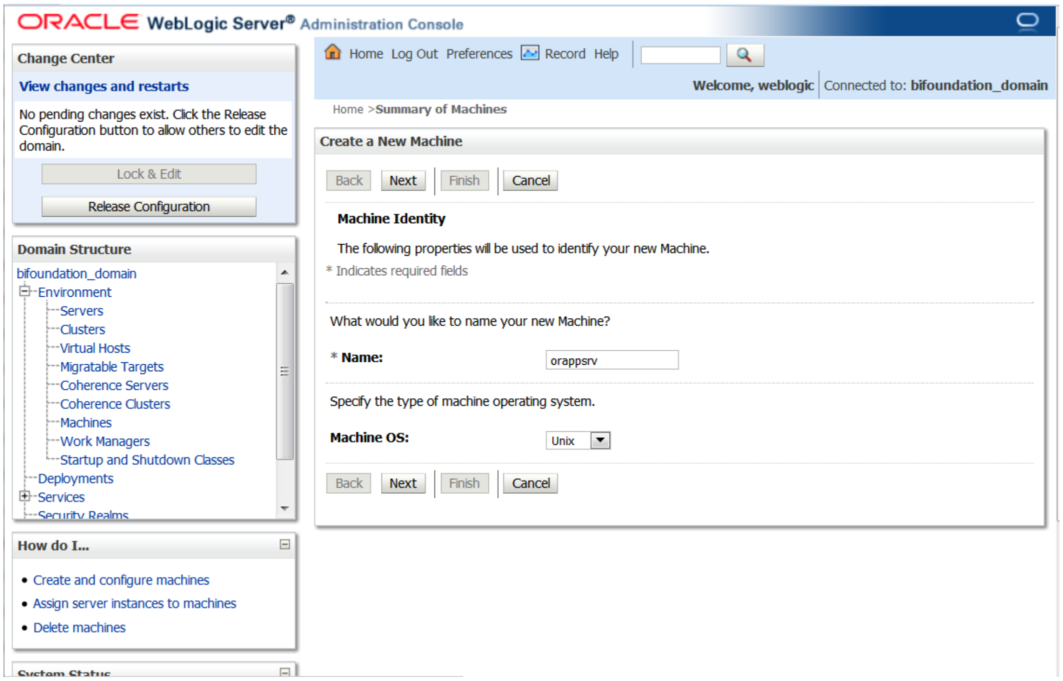
Showing 0 to 0 of 0 Previous | Next

□	Name	Type
There are no items to display		

Showing 0 to 0 of 0 Previous | Next

http://redevlv0066.us.oracle.com:17001/console/console.portal?_nfpb=true&_pageLabel=HomePage1

3. Click **New**.



No pending changes exist. Click the Release Configuration button to allow others to edit the domain.

Create a New Machine

Machine Identity

The following properties will be used to identify your new Machine.

* Indicates required fields

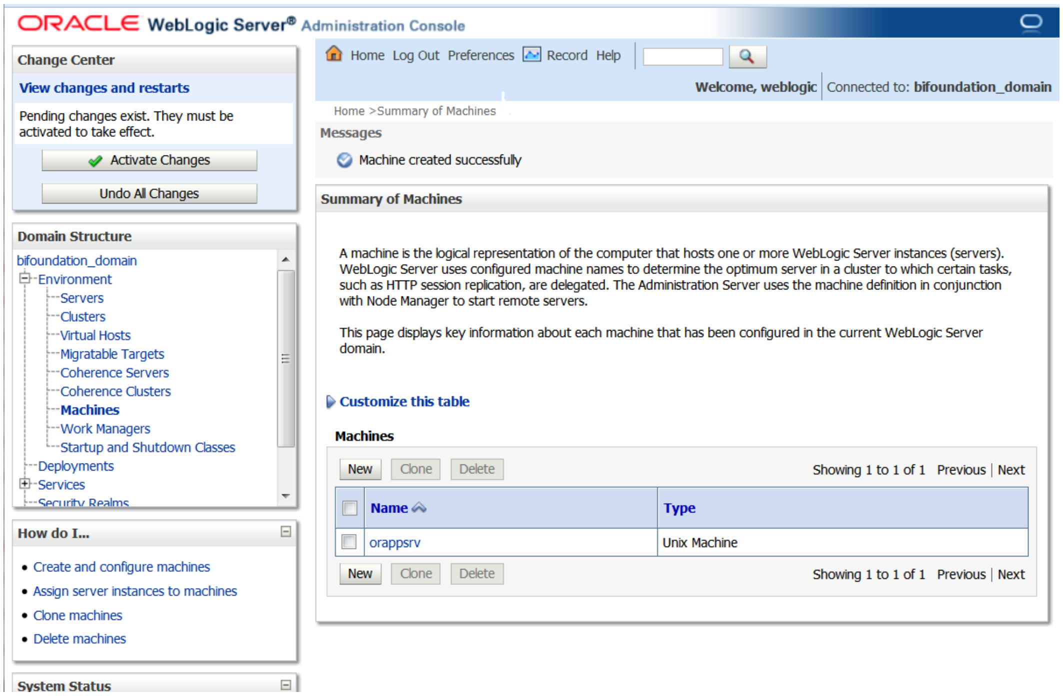
What would you like to name your new Machine?

* **Name:** orappsrv

Specify the type of machine operating system.

Machine OS: Unix

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



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

Messages

Machine created successfully

Summary of Machines

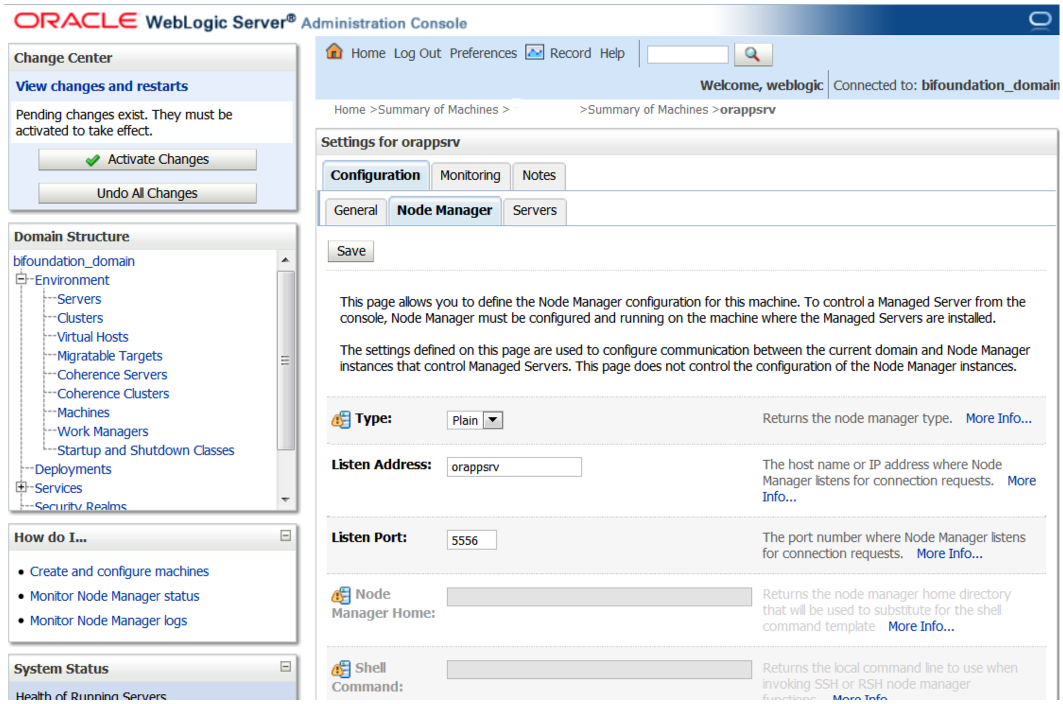
A machine is the logical representation of the computer that hosts one or more WebLogic Server instances (servers). WebLogic Server uses configured machine names to determine the optimum server in a cluster to which certain tasks, such as HTTP session replication, are delegated. The Administration Server uses the machine definition in conjunction with Node Manager to start remote servers.

This page displays key information about each machine that has been configured in the current WebLogic Server domain.

Machines

□	Name	Type
□	orappsrv	Unix Machine

7. Click on the NodeManager tab and update the details below.
   - **Type**: Plain
   - **Listen Address**: e.g.: orappsrv
   - **Listen Port**: NodeManager will be assigned a default port (for example, 5556)


ORACLE WebLogic Server® Administration Console
Change Center
View changes and restarts
Activate Changes
Undo All Changes
Domain Structure
bifoundation_domain
Environment
Servers
Clusters
Virtual Hosts
Migratable Targets
Coherence Servers
Coherence Clusters
Machines
Work Managers
Startup and Shutdown Classes
Deployments
Services
Security Realms
How do I...
Create and configure machines
Monitor Node Manager status
Monitor Node Manager logs
System Status
Health of Running Servers
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: bifoundation_domain
Home >Summary of Machines > >Summary of Machines >orappsrv
Settings for orappsrv
Configuration Monitoring Notes
General Node Manager Servers
Save

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

This page allows you to define the Node Manager configuration for this machine. To control a Managed Server from the console, Node Manager must be configured and running on the machine where the Managed Servers are installed.

The settings defined on this page are used to configure communication between the current domain and Node Manager instances that control Managed Servers. This page does not control the configuration of the Node Manager instances.

Type: Plain — Returns the node manager type. More Info...

Listen Address: orappsrv — The host name or IP address where Node Manager listens for connection requests. More Info...

Listen Port: 5556 — The port number where Node Manager listens for connection requests. More Info...

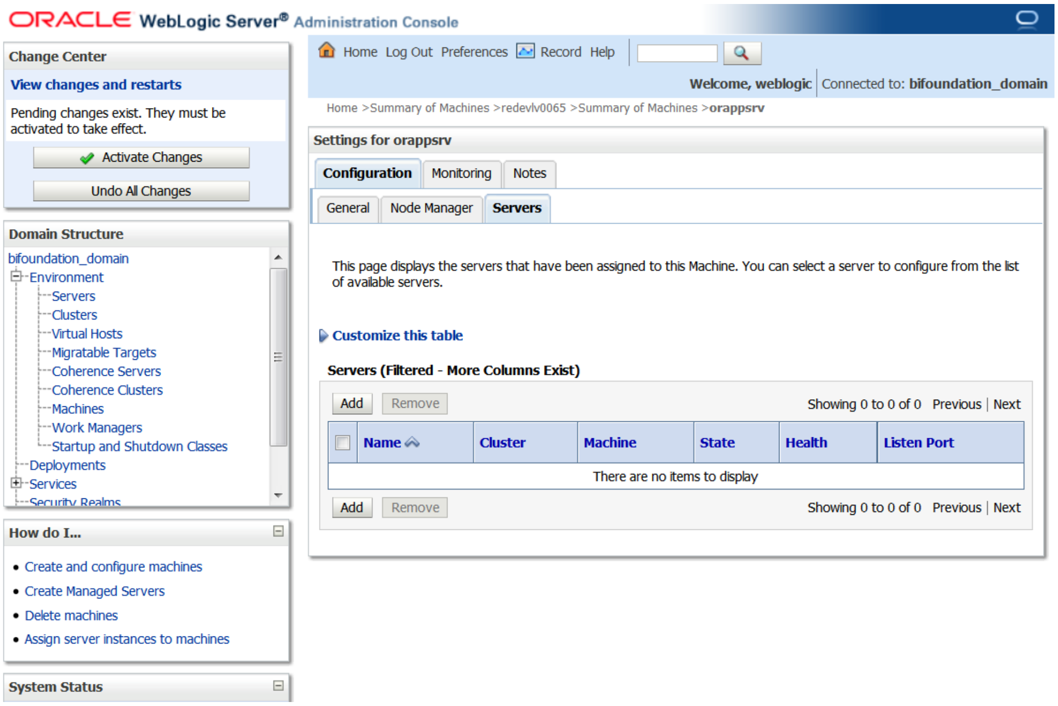
Node Manager Home: — Returns the node manager home directory that will be used to substitute for the shell command template More Info...

Shell Command: — Returns the local command line to use when invoking SSH or RSH node manager functions. More Info...

8. Click **Save**.
9. Click **Activate Changes**.

10. Click **Lock & Edit**.

11. Navigate to Environments > machines. Click on the machine name. Select the Servers tab.



Home >Summary of Machines >redevlv0065 >Summary of Machines >orappsrv

Settings for orappsrv

This page displays the servers that have been assigned to this Machine. You can select a server to configure from the list of available servers.

Servers (Filtered - More Columns Exist)

Showing 0 to 0 of 0 Previous | Next

□	Name	Cluster	Machine	State	Health	Listen Port
There are no items to display						

Showing 0 to 0 of 0 Previous | Next

Change Center

View changes and restarts

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

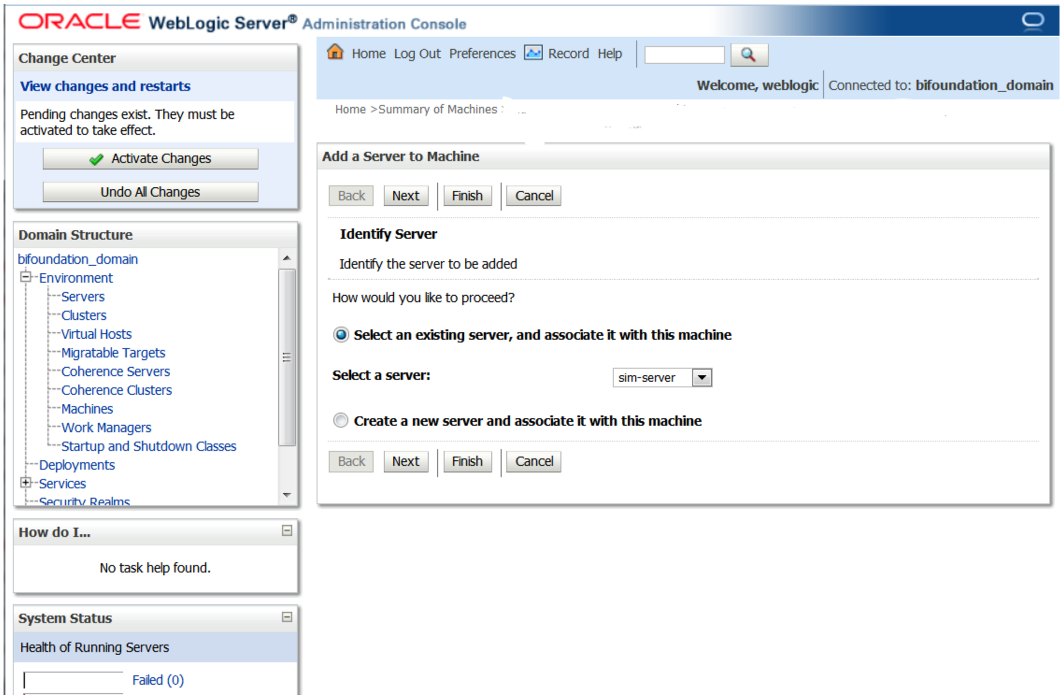
Domain Structure

bifoundation_domain
- Environment
  - Servers
  - Clusters
  - Virtual Hosts
  - Migratable Targets
  - Coherence Servers
  - Coherence Clusters
  - Machines
  - Work Managers
  - Startup and Shutdown Classes
- Deployments
- Services
- Security Realms

How do I...

- Create and configure machines
- Create Managed Servers
- Delete machines
- Assign server instances to machines

12. Click **Add**. Add the managed servers that need to be configured with NodeManager.



● Select an existing server, and associate it with this machine

Select a server: sim-server

○ Create a new server and associate it with this machine

13. Set the following variables:
    - Server: <sim-server>
14. Click **Next.** Click **Finish**.
15. Click **Activate Changes**.
16. Edit the nodemanager.properties file at the following location with the below values:

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

    - SecureListener=false
    - StartScriptEnabled=true
    - StartScriptName=startWebLogic.sh.
17. After making changes to the nodemanager.properties file, the NodeManager must be killed and restarted. You start the NodeManager using the startNodeManager.sh at $WLS_HOME/wlserver_10.3/server/bin.

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

Start the Managed Server

After NodeManager is started, the managed servers can be started via the admin console.

1. First, update <WLS_HOME>/wlserver_10.3/server/lib/weblogic.policy file with the information below.

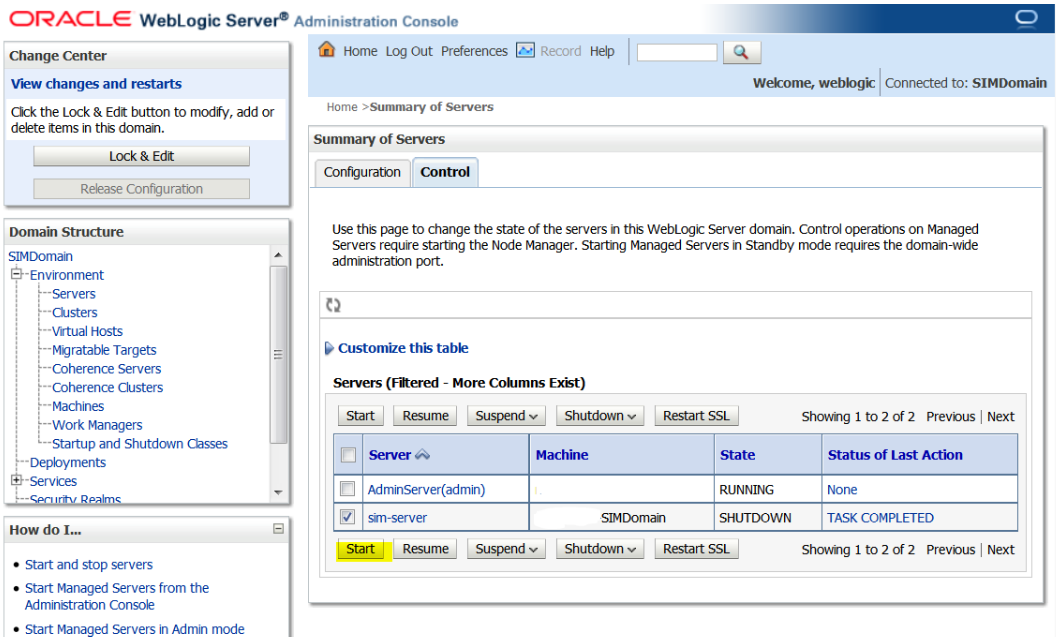
Note: If copying the following text from this guide to UNIX, ensure that it is properly formatted in UNIX. Each line entry beginning with "permission" must terminate on the same line with a semi colon. Also, **the AdminServer must be restarted for these changes to take effect**.

Note: <WEBLOGIC_DOMAIN_HOME> in the example below is the full path of the WebLogic domain; <managed_server> is the SIM managed server created. See the example. There should not be any space between file:<WEBLOGIC_DOMAIN_HOME.

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

An example of the full entry that might be entered is:
grant codeBase
"file:/u00/webadmin/product/10.3.x/WLS/user_projects/domains/APPDomai
n/servers/sim-server/tmp/_WL_user/-" {
permission java.security.AllPermission;
permission
oracle.security.jps.service.credstore.CredentialAccessPermission "
credstoressp.credstore", "read,write,update,delete";
permission
oracle.security.jps.service.credstore.CredentialAccessPermission "
credstoressp.credstore.*", "read,write,update,delete";
};
grant codeBase
"file:/u00/webadmin/product/10.3.x/WLS/user_projects/domains/APPDomai
n/servers/sim-server/cache/EJBCompilerCache/-" {
permission java.security.AllPermission;
permission
oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore", "read,write,update,delete";
permission
oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore.*", "read,write,update,delete";
};
```

2. Start the sim-server. Navigate to Environments > Servers > Control Tab. Select the sim-server and click **Start**.



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

- Start and stop servers
- Start Managed Servers from the Administration Console
- Start Managed Servers in Admin mode

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

Servers (Filtered - More Columns Exist)

☐	Server	Machine	State	Status of Last Action
☐	AdminServer(admin)		RUNNING	None
☑	sim-server	SIMDomain	SHUTDOWN	TASK COMPLETED

Set the LANG Environment Variable

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

Example:

```
LANG=en_US
export LANG
```

Expand the SIM Application Distribution

To expand the SIM application distribution, do the following.

1. Log in to the UNIX server as the user who owns the Web Logic installation. Create a new staging directory for the SIM application distribution (sim13application.zip).

   This location is referred to as INSTALL_DIR for the remainder of this chapter.
2. Copy sim13application.zip to <INSTALL_DIR> and unzip its contents.

SIM Custom Security Providers

There are two new authentication security providers for SIM 13.2.9. The SimWlsDbAuthenticator provider is used for SIM with the internal database security model, where users are authenticated through the sim datasource, and approves access to the sim_secure_users group. The sim_secure_users group is used to access SIM restricted resources. The SimWlsDbAuthenticator is not for providing access to the database, it is using the database for authentication/authorization information.

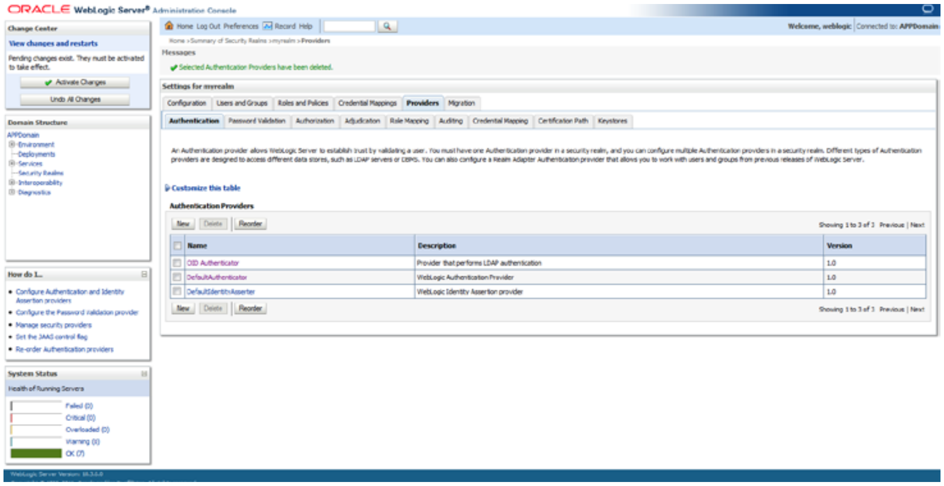
The SimWlsSsoAuthenticator provider is used for SIM in SSO environments, where the SSO token is authenticated and the provider approves access to the sim_secure_users group.

SIM continues to support a third provider through OID. This is able to be configured using the existing WLS OID security provider (where the SSO and database cases require SIM custom provider implementations).

Below are the illustrate steps to configure the security providers based on the selected security model to be used.

SIM Database Authentication Provider Set up

1. Shut down all the servers of the WebLogic domain created.
2. Once you copy the contents to <INSTALL_DIR> copy the sim-security.zip present in <INSTALL_DIR>/sim/application/sim13 to the WEBLOGIC_DOMAIN_HOME/lib and extract it contents in the folder.
3. Confirm these jar files under Domain_home/lib -> sim-security.jar , sim-security-mbean.jar and sim-security-resources.jar.
4. Start the domain admin server.
5. Log into the WebLogic console.
6. Under Security realms -> myrealm -> User and Groups, create a group called sim_secure_users.
7. Navigate to security realms -> myrealm (default realm) -> providers.



Home >Summary of Security Realms >myrealm >Providers

Messages

✓ Selected Authentication Providers have been deleted.

Settings for myrealm

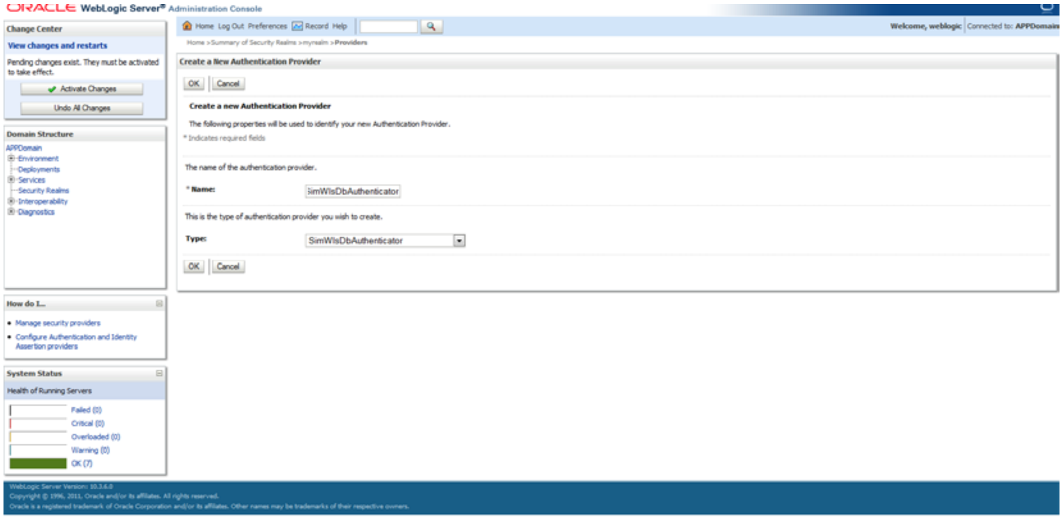
Pending changes exist. They must be activated to take effect.

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

Authentication Providers

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

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


ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: APPDomain
Change Center
View changes and restarts
Activate Changes
Undo All Changes
Domain Structure
APPDomain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Manage security providers
Configure Authentication and Identity Assertion providers
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (7)
OK
Cancel
WebLogic Server Version: 10.3.6.0
Copyright © 1996, 2011, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Home >Summary of Security Realms >myrealm >Providers

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

Create a New Authentication Provider

Create a new Authentication Provider

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

* Indicates required fields

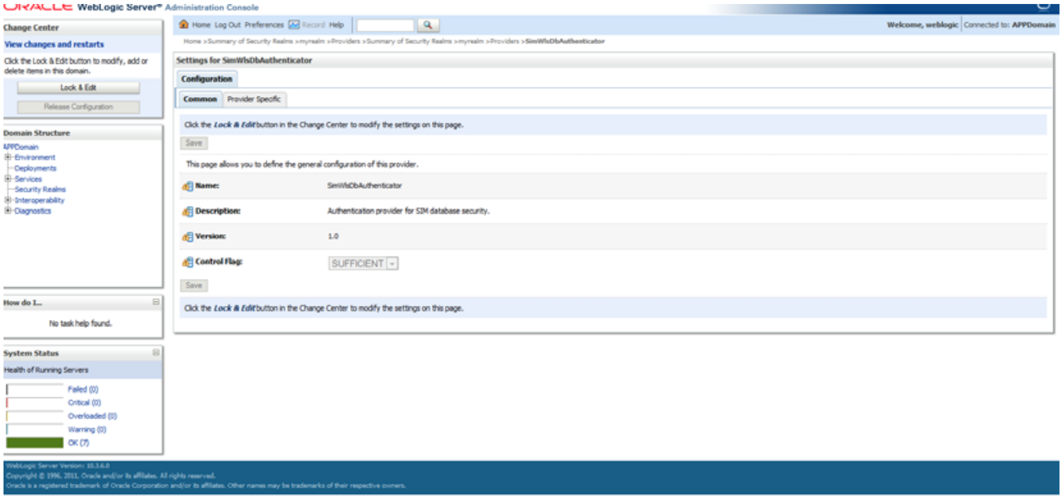
The name of the authentication provider.

* Name: SimWlsDbAuthenticator

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

Type: SimWlsDbAuthenticator

12. Click **OK**.
13. Open the new provider configuration.
14. Under Common, set the Control Flag to SUFFICIENT.



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

No task help found.

Home >Summary of Security Realms >myrealm >Providers >Summary of Security Realms >myrealm >Providers >SimWlsDbAuthenticator

Settings for SimWlsDbAuthenticator

Click the *Lock & Edit* button in the Change Center to modify the settings on this page.

This page allows you to define the general configuration of this provider.

Name: SimWlsDbAuthenticator

Description: Authentication provider for SIM database security.

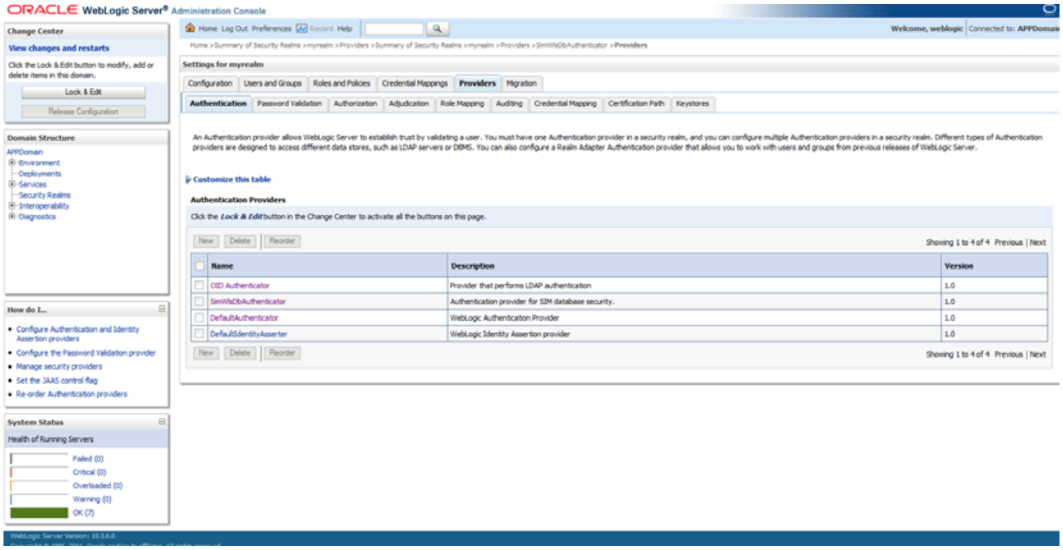
Version: 1.0

Control Flag: SUFFICIENT

Click the *Lock & Edit* button in the Change Center to modify the settings on this page.

WebLogic Server Version: 10.3.6.0
Copyright © 1996, 2011, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

15. Click **Save**.
16. On the provider list, click **Reorder**.



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

Home >Summary of Security Realms >myrealm >Providers >Summary of Security Realms >myrealm >Providers >SimWlsDbAuthenticator >Providers

Settings for myrealm

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

Authentication Providers

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

□	Name	Description	Version
□	OID Authenticator	Provider that performs LDAP authentication	1.0
□	SimWlsDbAuthenticator	Authentication provider for SIM database security.	1.0
□	DefaultAuthenticator	WebLogic Authentication Provider	1.0
□	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0

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

SIM SSO Authentication Provider set up (if SSO is configured)

1. Shut down all the servers of the WEBLOGIC_DOMAIN created.
2. After you extracted the SIM installation media, unzip the contents of <INSTALL_DIR>/sim/application/sim13/sim-security.zip to WEBLOGIC_DOMAIN/lib.
3. Start the WEBLOGIC_DOMAIN admin server.
4. Log into the Administrative console.
5. Navigate to: security realms -> myrealm (default realm) -> providers.
6. Acquire a Lock and Edit session.
7. Click "New" provider.
8. Select the provider type from the list: SimWlsSsoAuthenticator.
9. Set the provider name (i.e.: SimWlsSsoAuthenticator).
10. Click **OK**.
11. Click on the newly created SimWlsSsoAuthenticator provider to get to the configuration screen.
12. Under the "Common"tab, set the Control Flag to SUFFICIENT.
13. Click the "Provider Specific" tab.
14. Check that the Group Name is set to the name of the group used for SIM secure users (default is "sim_secure_users")   This group name must exist in LDAP and all SIM users must be a member.
15. Click **OK**.
16. Go back to the list of the providers by clicking the "Providers" tab in the security realm.
17. On the provider list, click **Reorder**.
18. Move the SimWlsSsoAuthenticator to the top of the list
19. Click **OK**.
20. Click **Activate Changes**.
21. Shutdown the WEBLOGIC_DOMAIN.
22. Start the admin and managed servers for the domain.
23. Each time SIM is deployed it generates a new SSO "Secret Key" which needs to be updated in the sim-security-resources.jar file we have previously extracted to the WEBLOGIC_DOMAIN/lib folder.

    This key is stored in the "JnlpLaunch.properties" file of the sim-client deployment in the WebLogic domain. For Example:

    ```
    > cd <WEBLOGIC_DOMAIN>/servers/sim-server/tmp/_WL_user/sim-client
    > grep secret.key= */conf/JnlpLaunch.properties
    secret.key=TS2Cp%zPpHHh9cbvV4g.8nnwE7V.mkNa$42kn%.8
    ```

    Now update the sim-security-resources.jar with this new key:

    ```
    > cd <WEBLOGIC_DOMAIN>/lib
    > jar xf sim-security-resources.jar conf/security.cfg
    > vi conf/security.cfg
        SSO_SECRET_KEY=TS2Cp%zPpHHh9cbvV4g.8nnwE7V.mkNa2kn%.8
    > jar uf sim-security-resources.jar conf/security.cfg
    ```

    You will need to stop/restart the WEBLOGIC_DOMAIN for the changes to take effect. Note that this will need to be updated if SIM is reinstalled as the key will change every time SIM is deployed.

If this is using a Webgate agent then 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 orappsrv.us.com:17015
 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 unprotect the rest:

Resource URL: /sim-client/launch

Protection Level: Protected

Authentication Policy: Protected Resource Policy

Authorization Policy: Protected Resource Policy

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

Protection Level: Unprotected

Authentication Policy: Public Resource Policy

Authorization Policy: Public Resource Policy

Run the SIM Application Installer

> **Note:** If you are using AIX 7.1, the **"retail-OCM-withAnt.zip"** file present in the INSTALL_DIR/sim must be renamed or removed **before** running the installer. See Appendix: Common Installation Errors for more information.

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

1. Set the ORACLE_HOME, JAVA_HOME, and WEBLOGIC_DOMAIN_HOME environment variables. ORACLE_HOME should point to your WebLogic installation. JAVA_HOME should point to a valid Java 1.7 installation that is being used by WebLogic Application server. WEBLOGIC_DOMAIN_HOME should point to the full path of the domain into which SIM will be installed.
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.
3. Verify that the managed servers to which SIM will be installed are currently running.
4. Run the install.sh script. This launches the installer. After installation is completed, a detailed installation log file is created: <INSTALL_DIR>/sim/application/logs/sim-install-app.<timestamp>.log.

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

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

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

Clustered Installations – Post-Installation Steps

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

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

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

Review and/or Configure Oracle Single Sign-On

Skip this section if you are not using Single Sign-On for user identification and authentication.

Single Sign-On is applicable only to the JnlpLaunch Servlet. The JnlpLaunch Servlet is a dynamically protected application. The JnlpLaunch Servlet causes the SIM client application to execute under the SSO user name with a temporary password.

Note: The JnlpLaunch servlet may be configured for either an SSO or non-SSO environment.

HTTP Server configuration requirements: If using OSSO the HTTP Server must be registered with the Oracle Single Sign-On server and the mod_osso module enabled. The registration process typically involves running the ssoreg.sh script at the OSSO server installation and copying the output osso.conf file to the HTTP Server. This process is documented in the Oracle Single Sign-On administration documentation.

JnlpLaunch requirements: The JnlpLaunch Servlet uses the configuration file, JnlpLaunch.properties, to control its behavior. Due to security considerations, this file must not be published or readable to the general public.

JnlpLaunch.properties has the following configuration entries that apply to Single Sign-On:

- `secret.key` – Used to create the temporary password, this property should contain a random string. If JnlpLaunch is deployed in a different JVM than the SIM Server EJBs, this string must be an exact match between the JnlpLaunch Servlet and the one available to the SIM EJBs. For security purposes, each separate instance of the SIM application (for example, test versus development) should have a different secret key.

- `user.validation.timeout` – Number of seconds the SIM Server uses to determine if a temporary password is still valid.
- `osso.used` – Determines if the JnlpLaunch Servlet will throw a 499 error when an unathenticated user has been detected. This property must be set to True if Oracle Single Sign-On is used and False if not.

The JnlpLaunch.properties file is initialized by the SIM installer and should contain valid entries for SSO when the Enable Single Sign-On in SIM? prompt was answered by a Y or Yes. However, an administrator may want to alter the user.validation.timeout or other property after the initial installation.

For instructions for setting up SSO for WebLogic, see Appendix: Oracle Single Sign-On for WebLogic.

SIM Batch Scripts

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

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

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

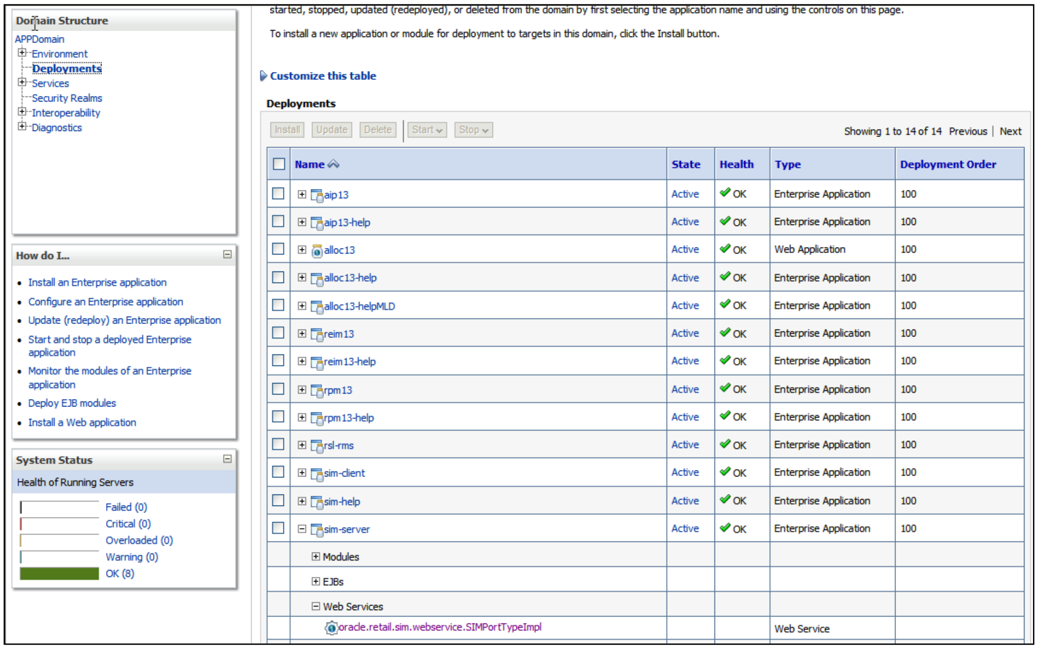
See the "Batch Detail" section of the *Oracle Retail Store Inventory Management Operations Guide* for information about how to run batches.

Configure Web Service Security in SIM

SIM web service is pre-configured with username-token-digest security policy.

User and role must be configured through WebLogic admin console as follows.

1. Create the user for the Web service. Click the **Security Realms** link in the **Domain Structure** window.
2. Default realm is displayed (for example, my realm). Click the link for the realm.
3. Click the **Users and Groups** tab.
4. Click **New**. Enter user name (for example, simwsuser) and password on the next screen. Leave the default value for Provider.
5. Click **OK** to save the changes. It will show the new user in the list of users
6. Navigate to the SIM web service deployment. Click on **Deployments** link in the **Domain Structure** window. Expand the **sim-server** deployment by clicking the plus sign next to it. There should be a SIM Webservice link at the bottom of the sim-client deployment list:


Domain Structure
APPDomain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Install an Enterprise application
Configure an Enterprise application
Update (redeploy) an Enterprise application
Start and stop a deployed Enterprise application
Monitor the modules of an Enterprise application
Deploy EJB modules
Install a Web application
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (8)
Customize this table
Install
Update
Delete
Start
Stop
Showing 1 to 14 of 14 Previous | Next

started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on this page.

To install a new application or module for deployment to targets in this domain, click the Install button.

Deployments

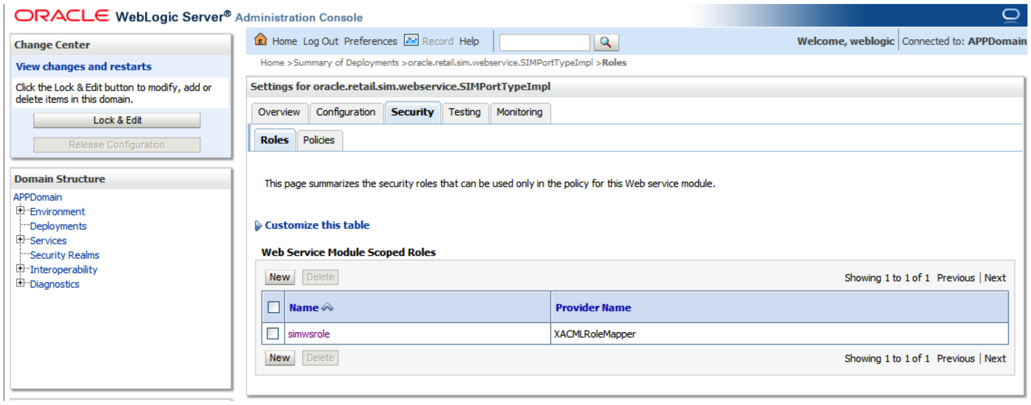
□	Name	State	Health	Type	Deployment Order
□	aip13	Active	✓ OK	Enterprise Application	100
□	aip13-help	Active	✓ OK	Enterprise Application	100
□	alloc13	Active	✓ OK	Web Application	100
□	alloc13-help	Active	✓ OK	Enterprise Application	100
□	alloc13-helpMLD	Active	✓ OK	Enterprise Application	100
□	reim13	Active	✓ OK	Enterprise Application	100
□	reim13-help	Active	✓ OK	Enterprise Application	100
□	rpm13	Active	✓ OK	Enterprise Application	100
□	rpm13-help	Active	✓ OK	Enterprise Application	100
□	rsl-rms	Active	✓ OK	Enterprise Application	100
□	sim-client	Active	✓ OK	Enterprise Application	100
□	sim-help	Active	✓ OK	Enterprise Application	100
□	sim-server	Active	✓ OK	Enterprise Application	100
	Modules				
	EJBs				
	Web Services				
	oracle.retail.sim.webservice.SIMPortTypeImpl			Web Service	

7. Click the Web Service link. Select Security tab. Select Roles tab.

8. In the Roles tab, click **New**.

9. Enter the role name in the **Name** field (for example, simwsrole). Leave the **Provider Name** as the default.

10. Click **OK**. The newly created role is now listed.


ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic | Connected to: APPDomain
Home >Summary of Deployments >oracle.retail.sim.webservice.SIMPortTypeImpl >Roles
Change Center
View changes and restarts
Lock & Edit
Release Configuration
Domain Structure
APPDomain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
Overview
Configuration
Security
Testing
Monitoring
Roles
Policies
Customize this table
New
Delete
Showing 1 to 1 of 1 Previous | Next

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

Settings for oracle.retail.sim.webservice.SIMPortTypeImpl

This page summarizes the security roles that can be used only in the policy for this Web service module.

Web Service Module Scoped Roles

□	Name	Provider Name
□	simwsrole	XACMLRoleMapper

11. Associate the user to the role. Click the newly created role.

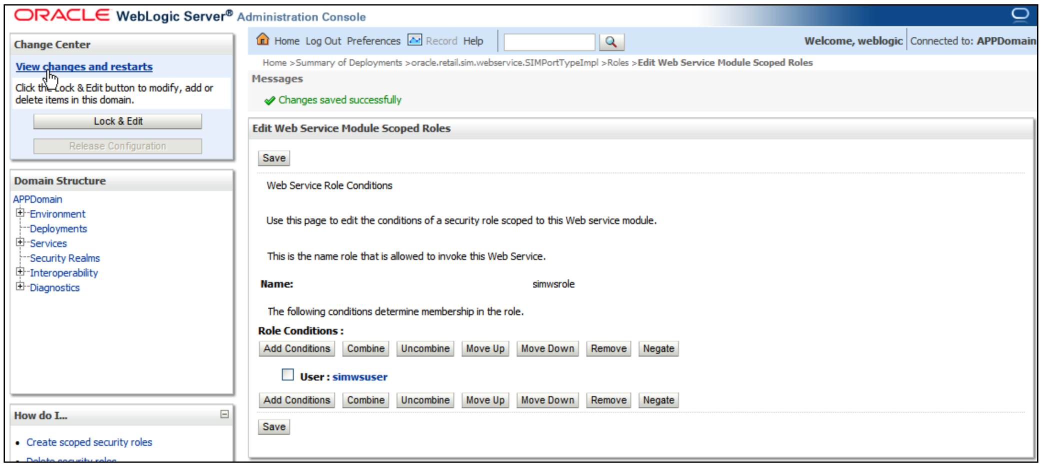
12. Click **Add Conditions**.

13. Select **User** in the **Predicate List** drop-down and click **Next**.

14. Enter the user name that was created in the security realm (for example, simwsuser) and click **Add**. It will get added to the list below the text box.

15. Click **Finish**.

16. Click **Save**. The SIM Web Service user is now associated to the SIM Web Service role:



Home >Summary of Deployments >oracle.retail.sim.webservice.SIMPortTypeImpl >Roles >Edit Web Service Module Scoped Roles

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

Messages

✓ Changes saved successfully

Edit Web Service Module Scoped Roles

Web Service Role Conditions

Use this page to edit the conditions of a security role scoped to this Web service module.

This is the name role that is allowed to invoke this Web Service.

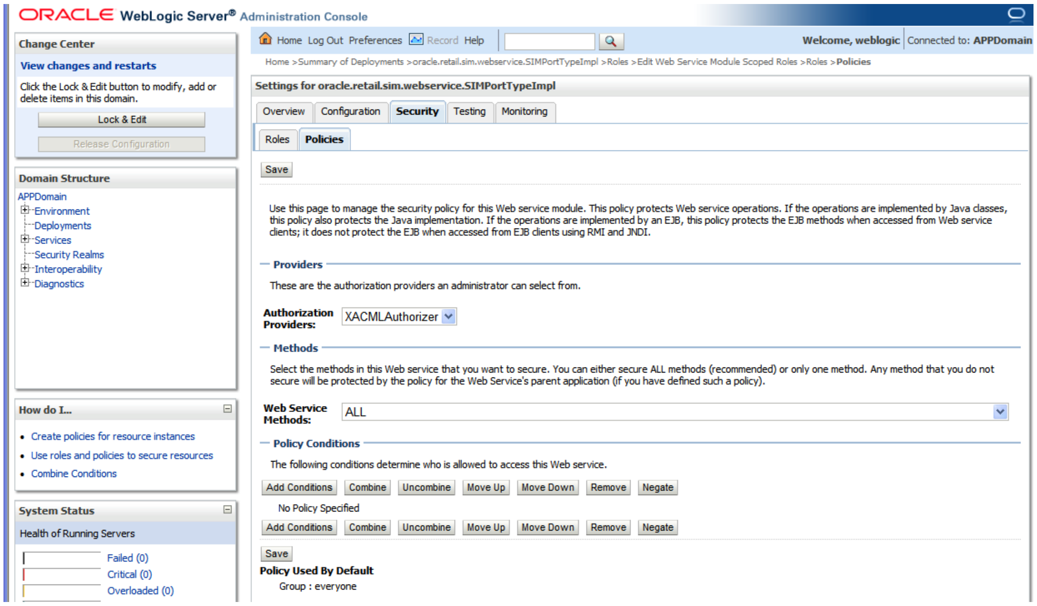
Name: simwsrole

The following conditions determine membership in the role.

Role Conditions :

□ **User : simwsuser**

17. Navigate back to the **Security > Policies** tab of the Web service.



Home >Summary of Deployments >oracle.retail.sim.webservice.SIMPortTypeImpl >Roles >Edit Web Service Module Scoped Roles >Roles >Policies

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

Settings for oracle.retail.sim.webservice.SIMPortTypeImpl

Use this page to manage the security policy for this Web service module. This policy protects Web service operations. If the operations are implemented by Java classes, this policy also protects the Java implementation. If the operations are implemented by an EJB, this policy protects the EJB methods when accessed from Web service clients; it does not protect the EJB when accessed from EJB clients using RMI and JNDI.

Providers

These are the authorization providers an administrator can select from.

Authorization Providers: XACMLAuthorizer

Methods

Select the methods in this Web service that you want to secure. You can either secure ALL methods (recommended) or only one method. Any method that you do not secure will be protected by the policy for the Web Service's parent application (if you have defined such a policy).

Web Service Methods: ALL

Policy Conditions

The following conditions determine who is allowed to access this Web service.

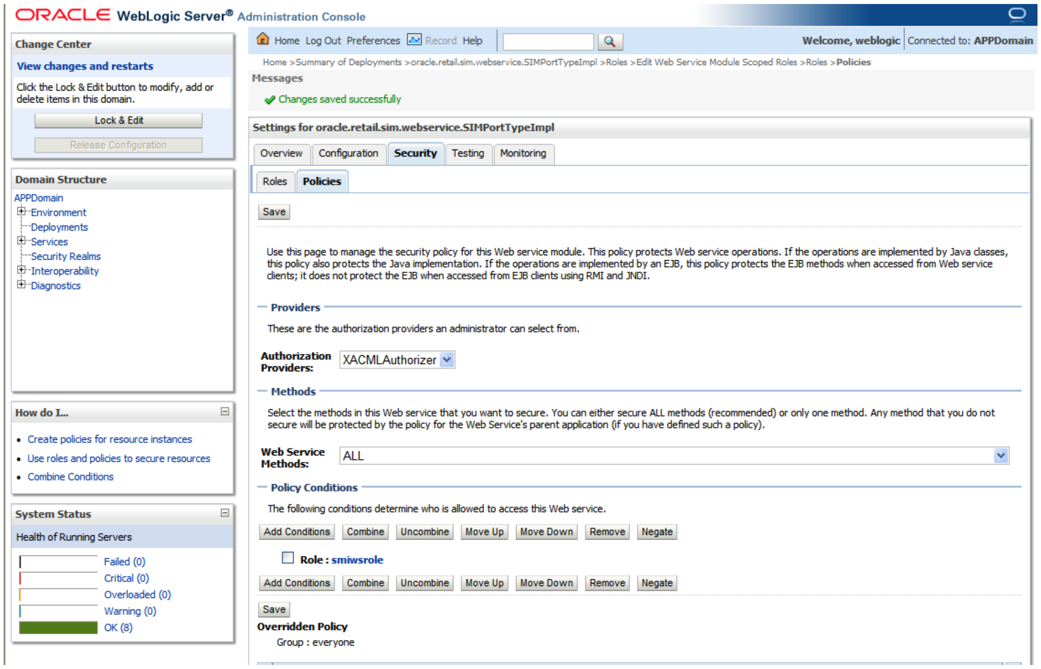
No Policy Specified

Policy Used By Default

Group : everyone

18. Click **Add Conditions**.

19. Select **Role** in the **Predicate List** drop down. Click **Next**.



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

Home >Summary of Deployments >oracle.retail.sim.webservice.SIMPortTypeImpl >Roles >Edit Web Service Module Scoped Roles >Roles >Policies

Messages

✓ Changes saved successfully

Settings for oracle.retail.sim.webservice.SIMPortTypeImpl

Use this page to manage the security policy for this Web service module. This policy protects Web service operations. If the operations are implemented by Java classes, this policy also protects the Java implementation. If the operations are implemented by an EJB, this policy protects the EJB methods when accessed from Web service clients; it does not protect the EJB when accessed from EJB clients using RMI and JNDI.

Providers

These are the authorization providers an administrator can select from.

Authorization Providers: XACMLAuthorizer

Methods

Select the methods in this Web service that you want to secure. You can either secure ALL methods (recommended) or only one method. Any method that you do not secure will be protected by the policy for the Web Service's parent application (if you have defined such a policy).

Web Service Methods: ALL

Policy Conditions

The following conditions determine who is allowed to access this Web service.

□ Role : smiwsrole

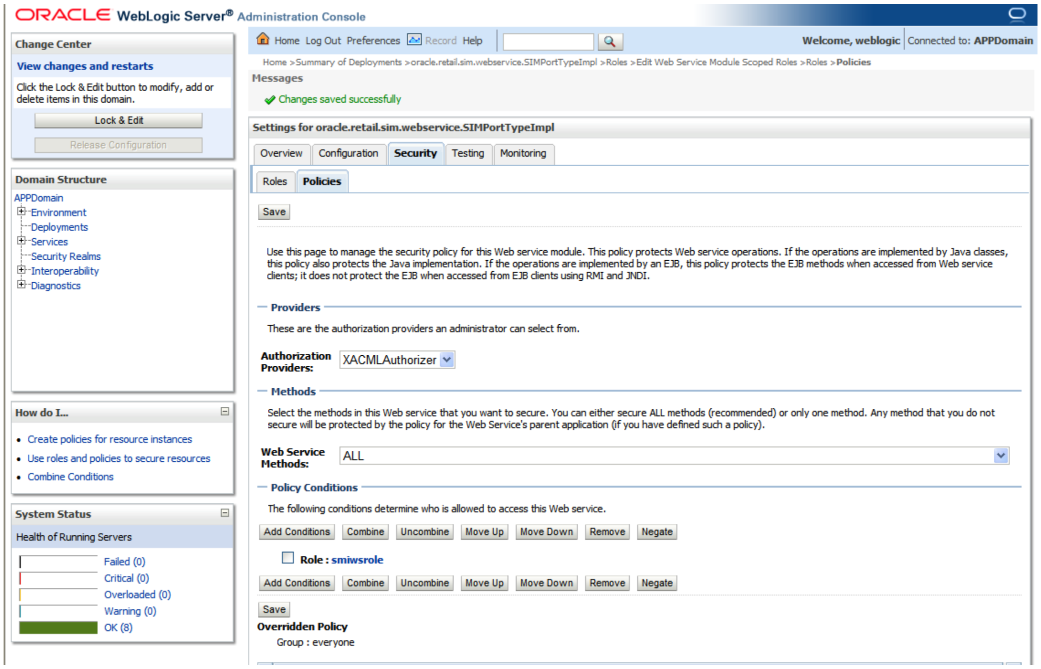
Overridden Policy

Group : everyone

20. Enter the role name that was created earlier (for example, simwsrole). Click **Add**. The role is added to the list below the text box.

21. Click **Finish**.

22. Click **Save**.



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

Home >Summary of Deployments >oracle.retail.sim.webservice.SIMPortTypeImpl >Roles >Edit Web Service Module Scoped Roles >Roles >Policies

Messages

✓ Changes saved successfully

Settings for oracle.retail.sim.webservice.SIMPortTypeImpl

Use this page to manage the security policy for this Web service module. This policy protects Web service operations. If the operations are implemented by Java classes, this policy also protects the Java implementation. If the operations are implemented by an EJB, this policy protects the EJB methods when accessed from Web service clients; it does not protect the EJB when accessed from EJB clients using RMI and JNDI.

Providers

These are the authorization providers an administrator can select from.

Authorization Providers: XACMLAuthorizer

Methods

Select the methods in this Web service that you want to secure. You can either secure ALL methods (recommended) or only one method. Any method that you do not secure will be protected by the policy for the Web Service's parent application (if you have defined such a policy).

Web Service Methods: ALL

Policy Conditions

The following conditions determine who is allowed to access this Web service.

□ Role : smiwsrole

Overridden Policy

Group : everyone

Resolving Errors Encountered During Application Installation

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

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

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

Web Help Files

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

Starting and Stopping the Wavelink Server

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

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

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

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

```
# cd /u00/webadmin/product/10.3.x/WLS/user_projects/domains/APPDomain/
/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.

Set the SSO_TIMEOUT Parameter

After installing, users are logged out if the SIM application is left idle for more than 60 seconds. This issue is caused by the SSO_TIMEOUT parameter being set to a default value of 60 seconds during SIM install.

> **Note:** This procedure only needs to be performed if you are using an SSO configuration.

Perform the following procedure after installation is complete and log in testing is successful:

1. Shut down SIM.
2. Under SIM_DOMAIN_HOME/lib, locate the sim-security-resources.jar file.
3. Extract this jar to get a file named "security.cfg" under the conf directory.
4. Update the SSO_TIMEOUT parameter to a higher value. (The default is 60 seconds. Increase the value to 20 minutes by specifying the value as 1200 seconds.)

   The SSO_TIMEOUT parameter must be set in order to prevent user log outs if the SIM application is left idle for more than a minute
5. Update the "sim-security-resources.jar" file with the updated security.cfg file and bounce the SIM domain.
6. Edit the jnlpLaunch.properties file found in sim-server and sim-client and set the value of the user.validation.timeout property to the same value specified in Step 4 above

   For example set the value of the parameter to 1200 seconds:

   ```
   # number of seconds a temporary password is valid user.validation.timeout=1200
   ```

7

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:

OAS: http://myhost:7778/sim-client/launch?template=sim_jnlp_template.vm

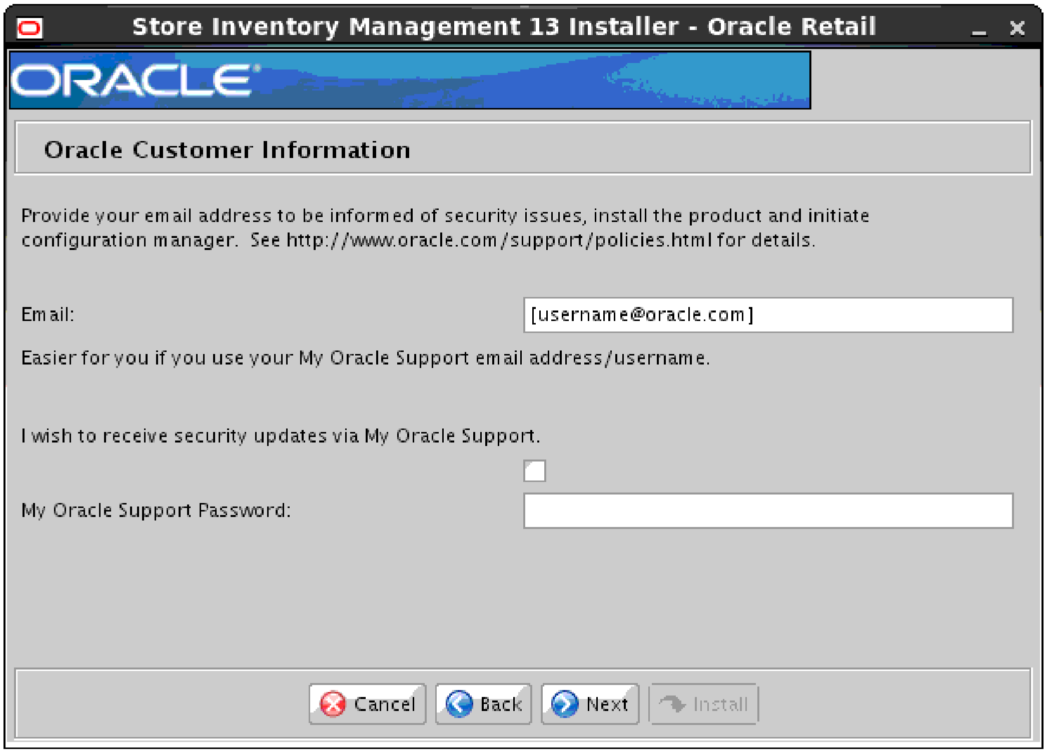
WLS: http://redevlv0066.us.oracle.com:17015/sim-client/launch?template=sim_jnlp_template.vm

A

Appendix: SIM Application Oracle Application Server (OAS) 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: Customer Information



Store Inventory Management 13 Installer - Oracle Retail

Oracle Customer Information

Provide your email address to be informed of security issues, install the product and initiate configuration manager. See http://www.oracle.com/support/policies.html for details.

Email: [username@oracle.com]

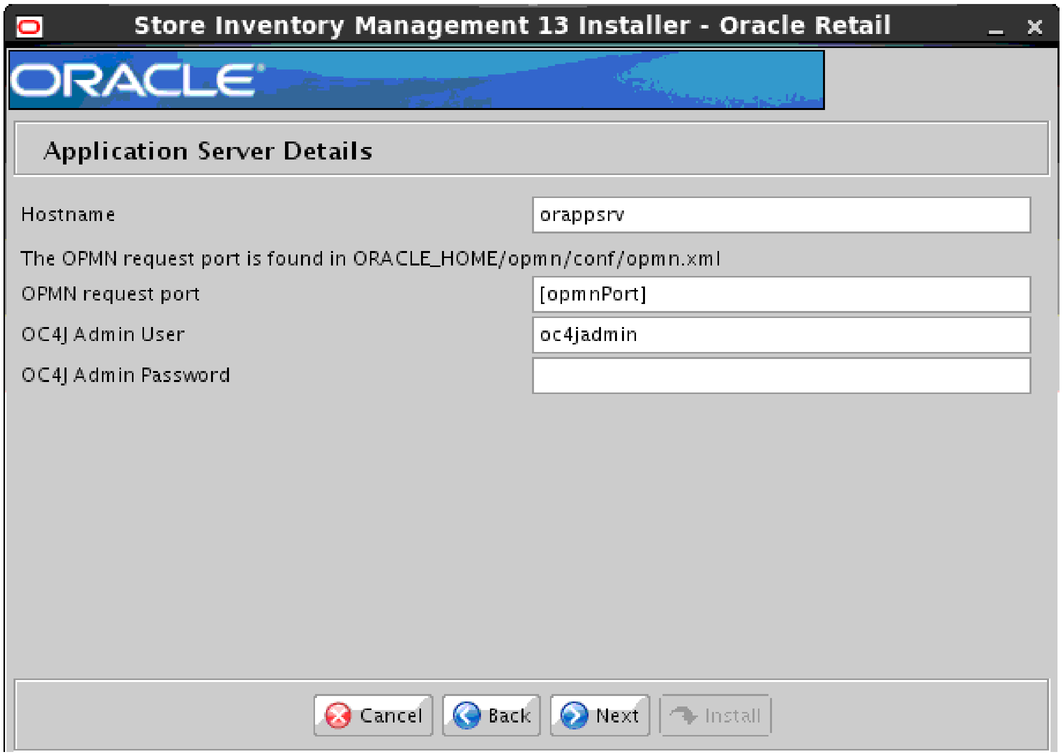
Easier for you if you use your My Oracle Support email address/username.

I wish to receive security updates via My Oracle Support. □

My Oracle Support Password:

Enter your customer information if you desire, or you can check the box to not receive updates automatically.

Screen: Application Server Details



Application Server Details

Hostname: orappsrv

The OPMN request port is found in ORACLE_HOME/opmn/conf/opmn.xml

OPMN request port: [opmnPort]

OC4J Admin User: oc4jadmin

OC4J Admin Password:

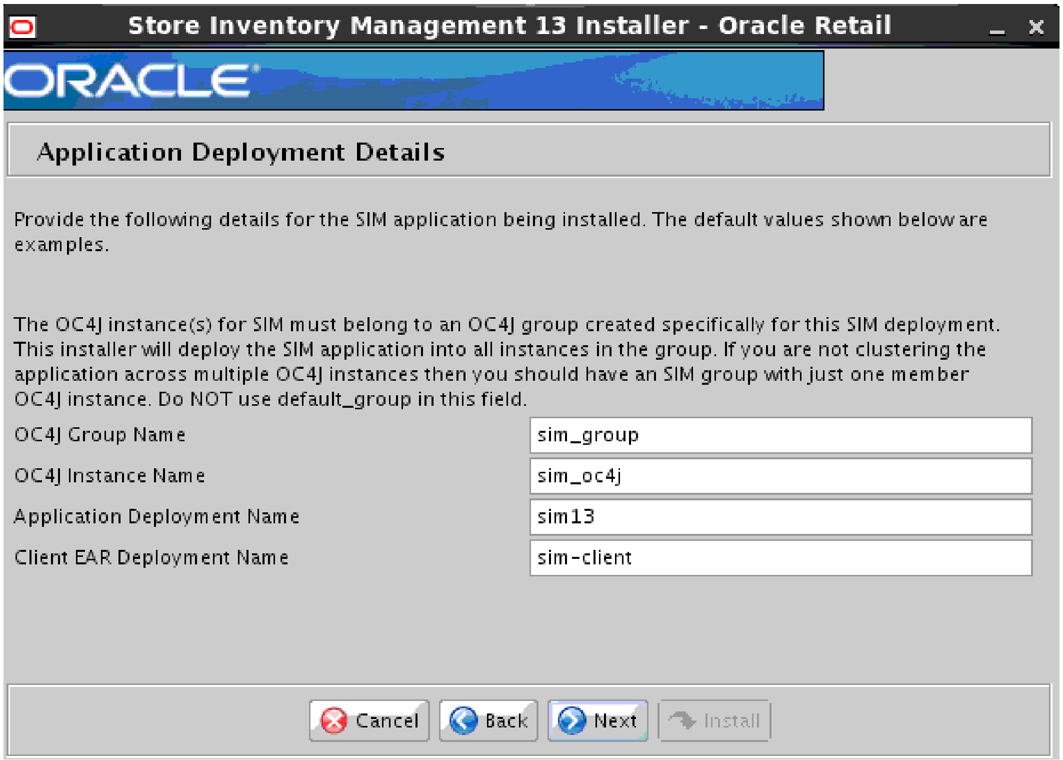
Field Title	Hostname
Field Description	The hostname of the server where the application server is installed
Destination	client.cfg, jndi.cfg,JnlpLaunch.properties
Example	orappsrv
Notes	Used by installer scripts to deploy EAR and WAR files and to create default inputs for client codebase and JNDI provider URL

Field Title	OPMN request port
Field Description	The OPMN request port found in $ORACLE_HOME/opmn/conf/opmn.xml <port local="6100" remote="6200" request="6003"/>
Example	6014
Notes	Used by installer scripts to deploy EAR and WAR files and to create default input for JNDI provider URL

Field Title	OC4J Admin User
Destination	jndi.cfg, JnlpLaunch.properties
Example	oc4jadmin
Notes	Used by installer scripts to deploy EAR and WAR files

Field Title	OC4J Admin Password
Field Description	The password of the OC4J Admin User
Destination	jndi.cfg, JnlpLaunch.properties
Notes	Used by installer scripts to deploy EAR and WAR files

Screen: Application Deployment Details



Application Deployment Details

Provide the following details for the SIM application being installed. The default values shown below are examples.

The OC4J instance(s) for SIM must belong to an OC4J group created specifically for this SIM deployment. This installer will deploy the SIM application into all instances in the group. If you are not clustering the application across multiple OC4J instances then you should have an SIM group with just one member OC4J instance. Do NOT use default_group in this field.

OC4J Group Name	sim_group
OC4J Instance Name	sim_oc4j
Application Deployment Name	sim13
Client EAR Deployment Name	sim-client

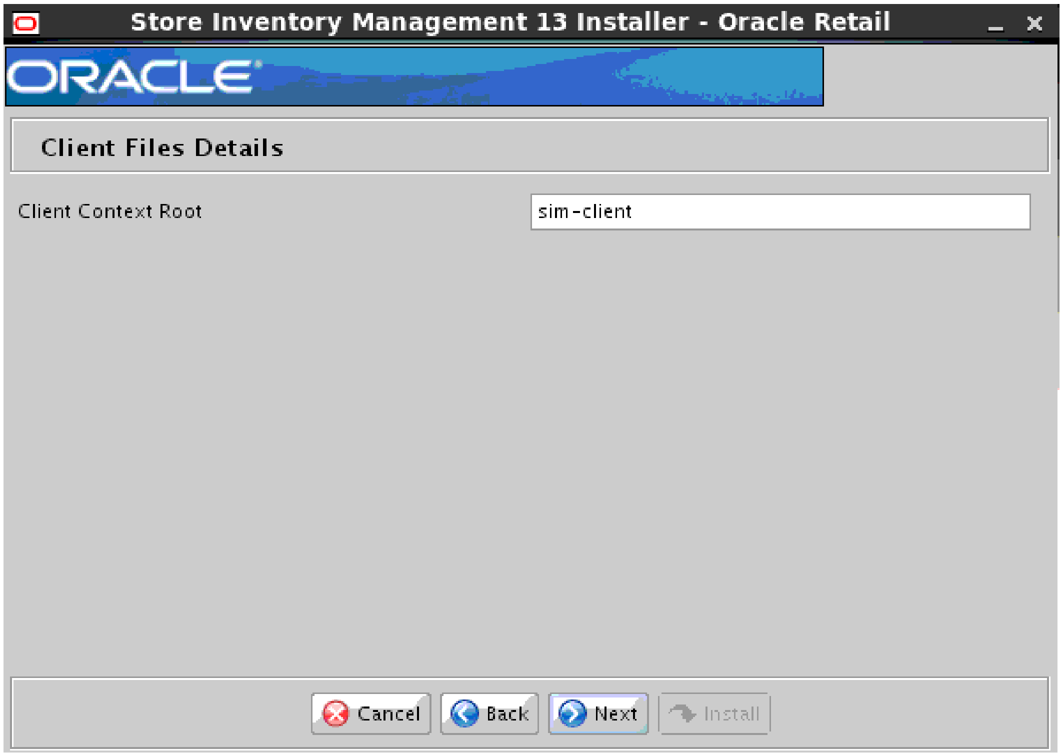
Field Title	OC4J Group Name
Field Description	Name of the OC4J group that was created for this SIM application. The OC4J instance given in the OC4J Instance Name field should be a member of this group. The installer deploys the SIM application to all OC4J instances which are members of this group. For this reason, you should not use default_group. A new group dedicated to SIM should be created instead.
Example	sim_group

Field Title	OC4J Instance Name
Field Description	The name of the OC4J instance that the SIM application will be deployed to
Destination	log4j.xml, MANIFEST.MF, startup.sh, shutdown.sh
Example	sim-instance

Field Title	Application Deployment Name
Field Description	The name that will be used by the application server to identify the SIM application
Example	sim13
Notes	Used by installer scripts to deploy the application and to create default values for JNDI provider URL

Field Title	Client EAR Deployment Name
Field Description	The name that will be used by the application server to deploy the sim-client.ear file.
Example	sim-client

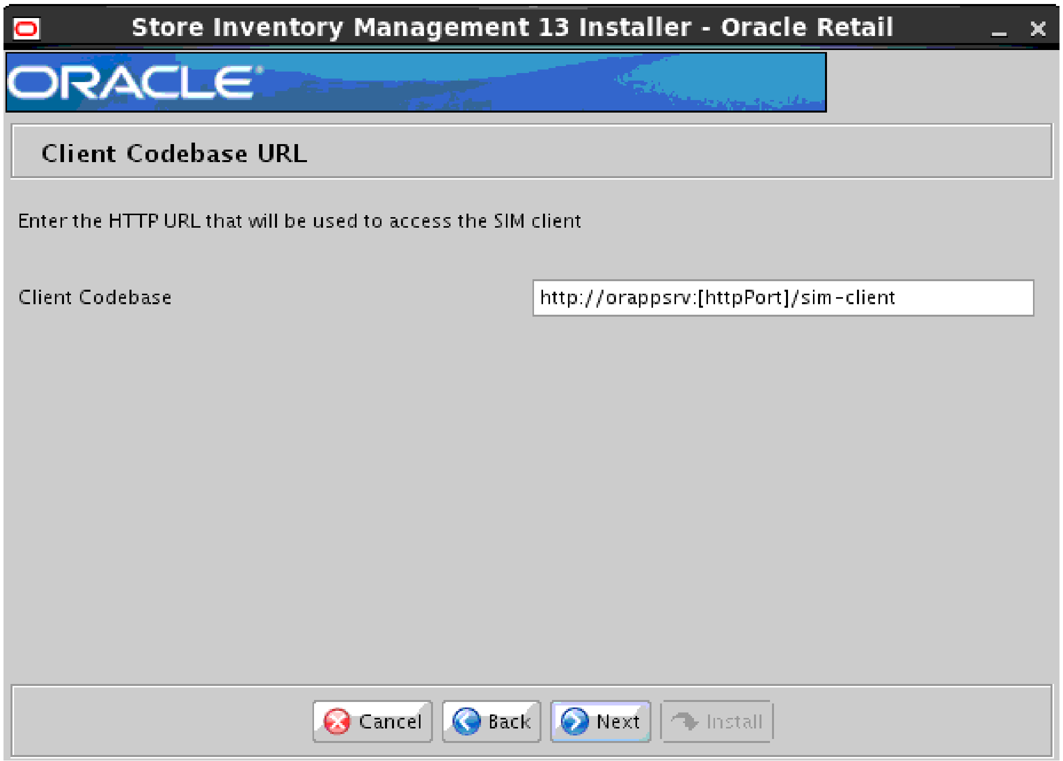
Screen: Client Files Details



Client Context Root: sim-client

Field Title	Client Context Root
Field Description	Context root for sim-client.war
Destination	JnlpLaunch.properties
Example	sim-client
Notes	Used by installer to create default value for Client Codebase URL

Screen: Client Codebase URL



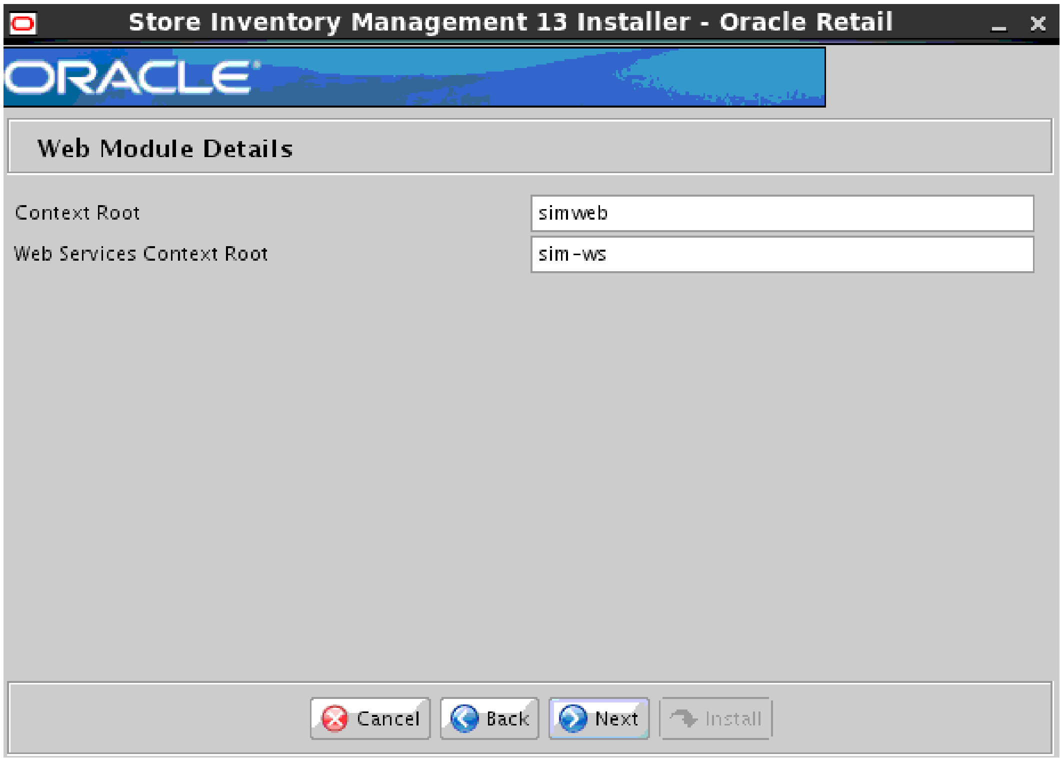
Client Codebase URL

Enter the HTTP URL that will be used to access the SIM client

Client Codebase: http://orappsrv:[httpPort]/sim-client

Field Title	Client Codebase
Field Description	The HTTP URL that points to the SIM client installation. The URL is made up of the Hostname, the HTTP port, and the Client Context Root.
Destination	JNLPLaunch.properties, sim_config.jnlp, client.cfg
Example	http://orapsrv.us.com:7778/sim-client
Notes	The Client Codebase URL must match the Client Context Root from the previous screen.

Screen: Web Module Details



Web Module Details

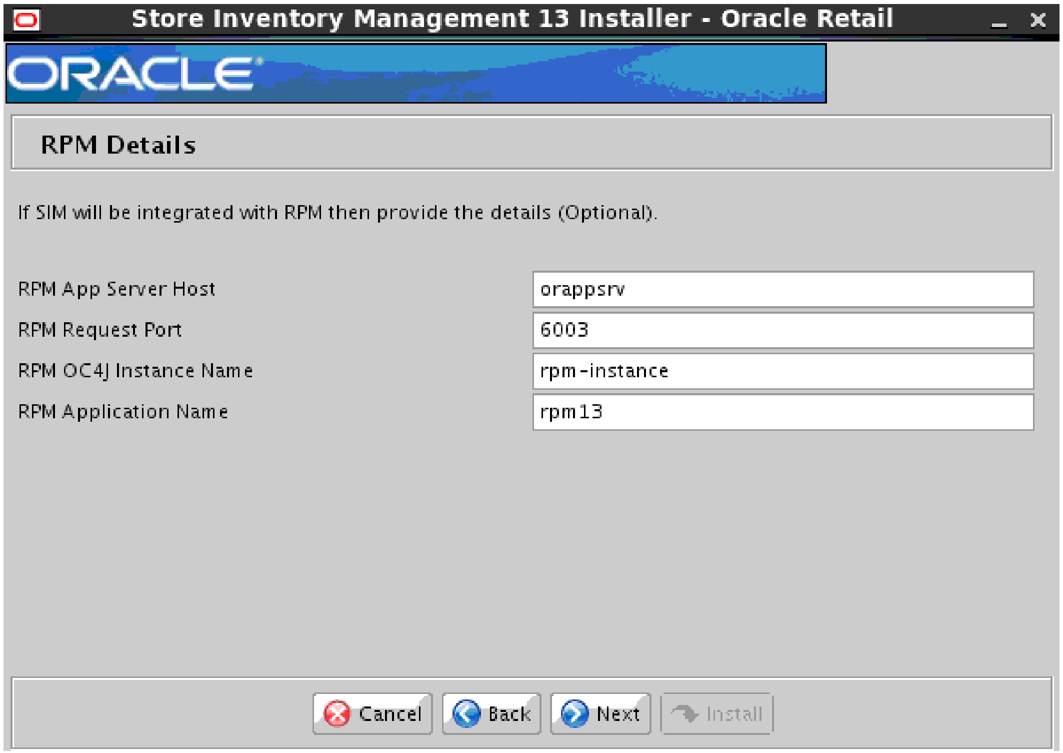
Context Root: simweb

Web Services Context Root: sim-ws

Field Title	Context Root
Field Description	The context root for sim.war
Destination	application.xml
Example	simweb

Field Title	Web Services Context Root
Field Description	The context root for sim-ws.war
Destination	application.xml
Example	sim-ws

Screen: RPM Details



RPM Details

If SIM will be integrated with RPM then provide the details (Optional).

RPM App Server Host	orappsrv
RPM Request Port	6003
RPM OC4J Instance Name	rpm-instance
RPM Application Name	rpm13

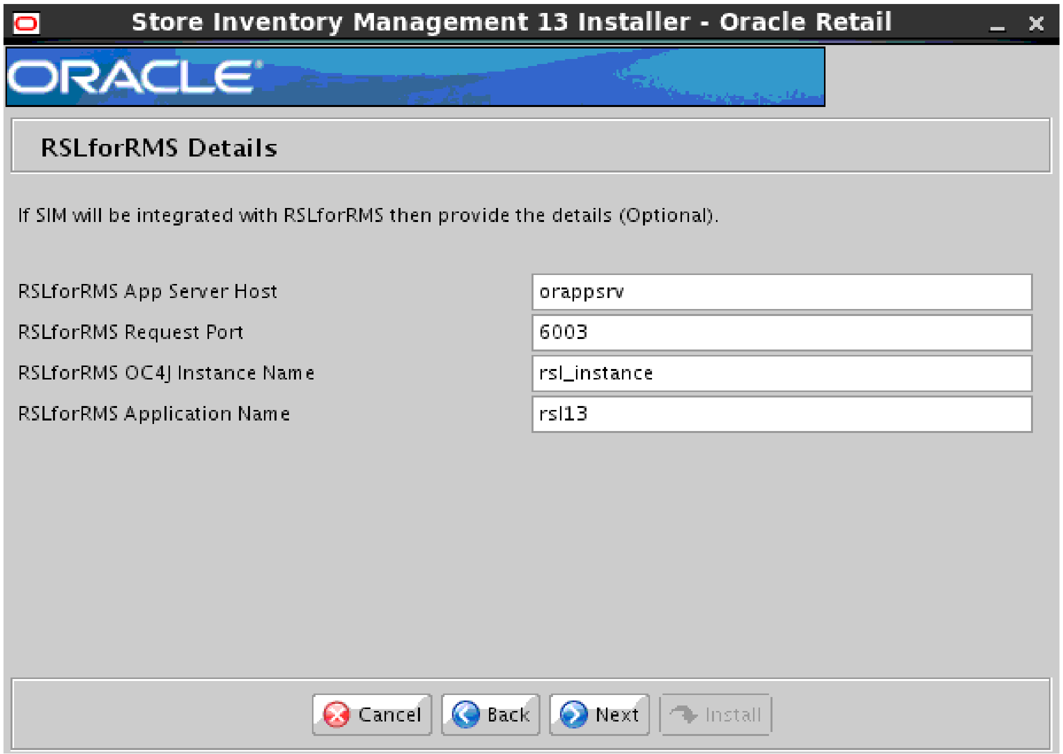
Field Title	RPM App Server Host
Field Description	The name of the application server host where the RPM application is installed
Destination	jndi_providers.xml
Example	orappsrv
Notes	Used only if integrating SIM with RPM

Field Title	RPM Request Port
Field Description	The OPMN request port for the application server where RPM is intalled. The OPMN request port is found in $ORACLE_HOME/opmn/conf/opmn.xml <port local="6100" remote="6200" request="6003"/>
Destination	jndi_providers.xml
Example	6003
Notes	Used only if integrating SIM with RPM

Field Title	RPM OC4J Instance Name
Field Description	The name of the OC4J instance where the RPM application is installed
Destination	jndi_providers.xml
Example	rpm_instance
Notes	Used only if integrating SIM with RPM

Field Title	RPM Application Name
Field Description	The name that will be used by the application server to identify the RPM application
Destination	jndi_providers.xml
Example	rpm13
Notes	Used only if integrating SIM with RPM

Screen: RSLforRMS Details



RSLforRMS Details

If SIM will be integrated with RSLforRMS then provide the details (Optional).

RSLforRMS App Server Host	orappsrv
RSLforRMS Request Port	6003
RSLforRMS OC4J Instance Name	rsl_instance
RSLforRMS Application Name	rsl13

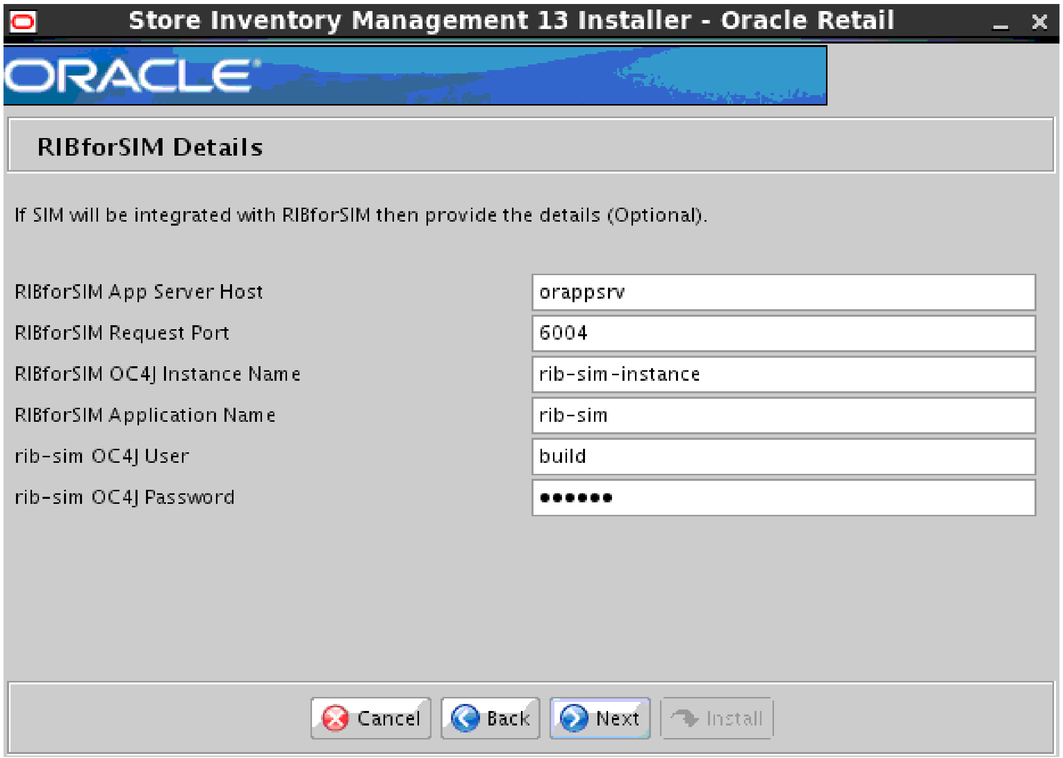
Field Title	RSLforRMS App Server Host
Field Description	The name of the application server host where the RSLforRMS application is installed
Destination	jndi_providers.xml
Example	orappsrv
Notes	Used only if integrating SIM with RSLforRMS

Field Title	RSLforRMS Request Port
Field Description	The OPMN request port for the application server where RSLforRMS is intalled. The OPMN request port is found in $ORACLE_HOME/opmn/conf/opmn.xml <port local="6100" remote="6200" request="6003"/>
Destination	jndi_providers.xml
Example	6003
Notes	Used only if integrating SIM with RSLforRMS

Field Title	RSLforRMS OC4J Instance Name
Field Description	The name of the OC4J instance where the RSLforRMS application is installed
Destination	jndi_providers.xml
Example	rsl_instance
Notes	Used only if integrating SIM with RSLforRMS

Field Title	RSLforRMS Application Name
Field Description	The name that will be used by the application server to identify the RSLforRMS application
Destination	jndi_providers.xml
Example	rsl13
Notes	Used only if integrating SIM with RSLforRMS

Screen: RIBforSIM Details



RIBforSIM Details

If SIM will be integrated with RIBforSIM then provide the details (Optional).

RIBforSIM App Server Host	orappsrv
RIBforSIM Request Port	6004
RIBforSIM OC4J Instance Name	rib-sim-instance
RIBforSIM Application Name	rib-sim
rib-sim OC4J User	build
rib-sim OC4J Password	••••••

Field Title	RIBforSIM App Server Host
Field Description	The name of the application server host where the RIBforSIM application is installed
Destination	jndi_providers_ribclient.xml
Example	orappsrv
Notes	Used only if integrating SIM with RIBforSIM

Field Title	RIBforSIM Request Port
Field Description	The OPMN request port for the application server where RIBforSIM is intalled. The OPMN request port is found in $ORACLE_HOME/opmn/conf/opmn.xml <port local="6100" remote="6200" request="6003"/>
Destination	jndi_providers_ribclient.xml
Example	6004
Notes	Used only if integrating SIM with RIBforSIM

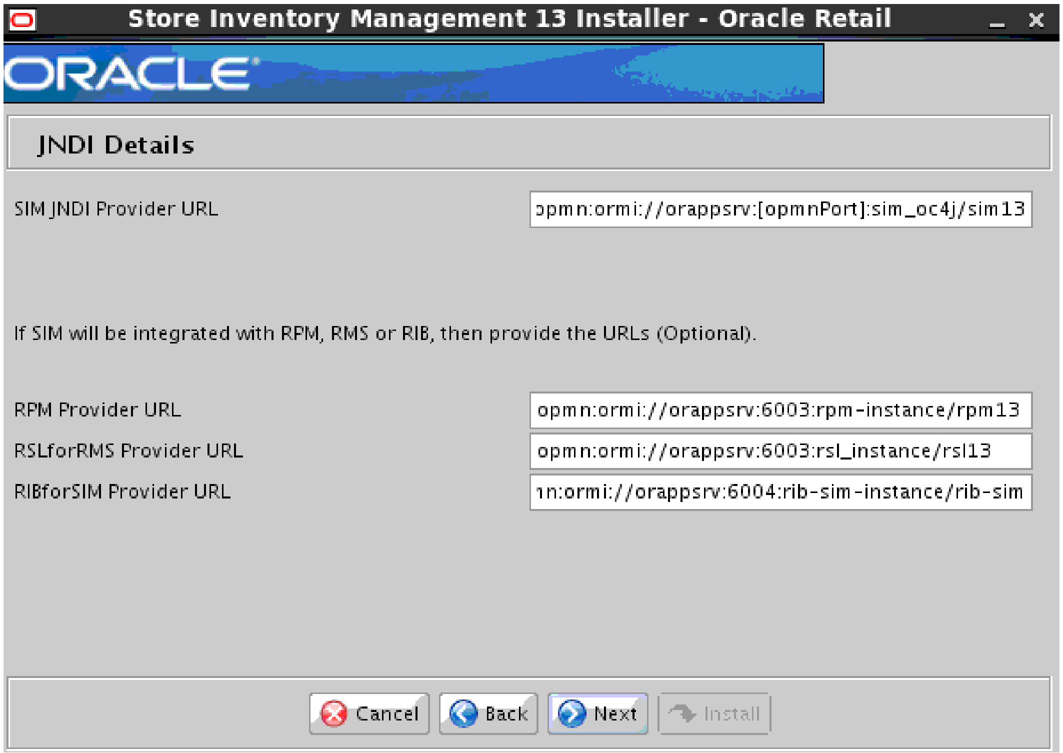
Field Title	RIBforSIM OC4J Instance Name
Field Description	The name of the OC4J instance where the RIBforSIM application is installed
Destination	jndi_providers_ribclient.xml
Example	rib-sim-instance
Notes	Used only if integrating SIM with RIBforSIM

Field Title	RIBforSIM Application Name
Field Description	The name that will be used by the application server to identify the RIBforSIM application
Destination	jndi_providers_ribclient.xml
Example	rib-sim
Notes	Used only if integrating SIM with RIBforSIM

Field Title	rib-sim OC4J User
Field Description	The OC4J Admin User for the OC4J instance where rib-sim is installed.
Destination	jndi_providers_ribclient.xml
Example	build
Notes	Used only if integrating SIM with RIBforSIM

Field Title	rib-sim OC4J Password
Field Description	The password of the OC4J Admin User for the OC4J instance where rib-sim is installed.
Destination	jndi_providers_ribclient.xml
Notes	Used only if integrating SIM with RIBforSIM

Screen: JNDI Details



JNDI Details

SIM JNDI Provider URL: ɔpmn:ormi://orappsrv:[opmnPort]:sim_oc4j/sim13

If SIM will be integrated with RPM, RMS or RIB, then provide the URLs (Optional).

RPM Provider URL: opmn:ormi://orappsrv:6003:rpm-instance/rpm13

RSLforRMS Provider URL: opmn:ormi://orappsrv:6003:rsl_instance/rsl13

RIBforSIM Provider URL: ın:ormi://orappsrv:6004:rib-sim-instance/rib-sim

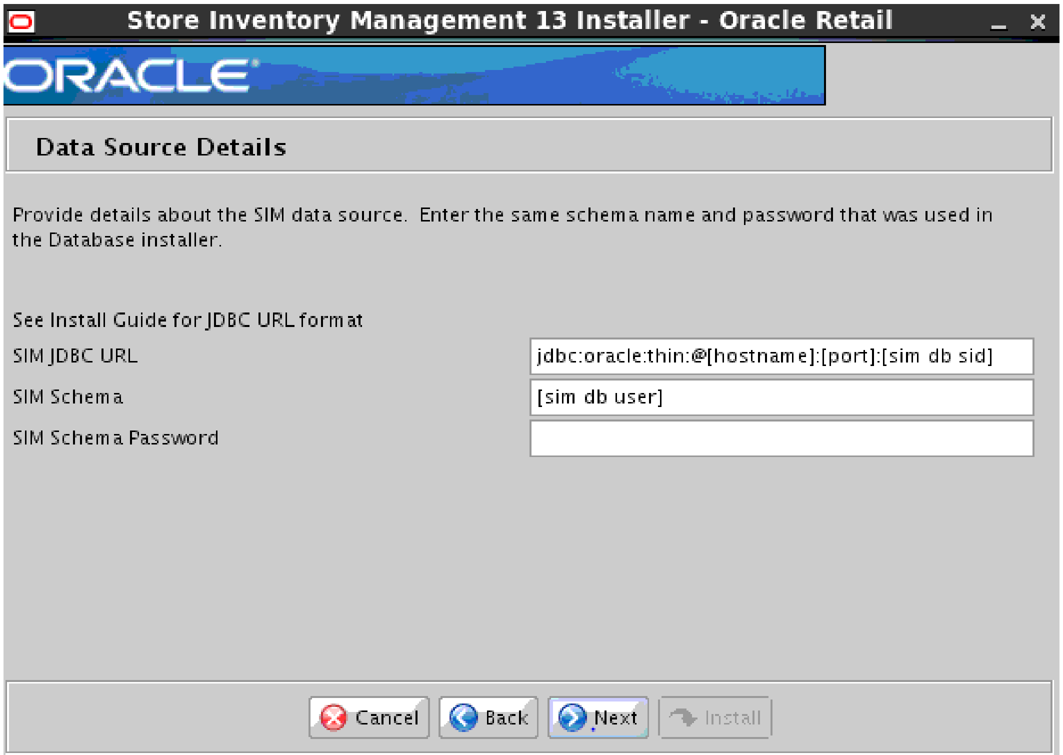
Field Title	SIM JNDI Provider URL
Field Description	JNDI provider URL for the SIM application
Destination	jndi.cfg, JnlpLaunch.properties
Example	opmn:ormi://orappsrv:6005:sim-instance/sim13
Notes	Confirm the JNDI provider URL, which is constructed based on previous inputs for Hostname, OPMN Request Port, OC4J Instance Name, and Application Deployment Name

Field Title	RPM Provider URL
Field Description	JNDI provider URL for the RPM application
Destination	jndi_providers.xml
Example	opmn:ormi://orappsrv:6005:rpm_instance/rpm13
Notes	Confirm the JNDI provider URL, which is constructed based on previous inputs for Hostname, OPMN Request Port, OC4J Instance Name, and Application Deployment Name

Field Title	RSLforRMS Provider URL
Field Description	JNDI provider URL for the RSLforRMS application
Destination	jndi_providers.xml
Example	opmn:ormi://orappsrv:6005:rsl_instance/rsl13
Notes	Confirm the JNDI provider URL, which is constructed based on previous inputs for Hostname, OPMN Request Port, OC4J Instance Name, and Application Deployment Name

Field Title	RIBforSIM Provider URL
Field Description	JNDI provider URL for the RIBforSIM application
Destination	jndi_providers.xml
Example	opmn:ormi://orappsrv:6003:rib-sim-instance/rib-sim
Notes	Confirm the JNDI provider URL, which is constructed based on previous inputs for Hostname, OPMN Request Port, OC4J Instance Name, and Application Deployment Name

Screen: Data Source Details



Data Source Details

Provide details about the SIM data source. Enter the same schema name and password that was used in the Database installer.

See Install Guide for JDBC URL format

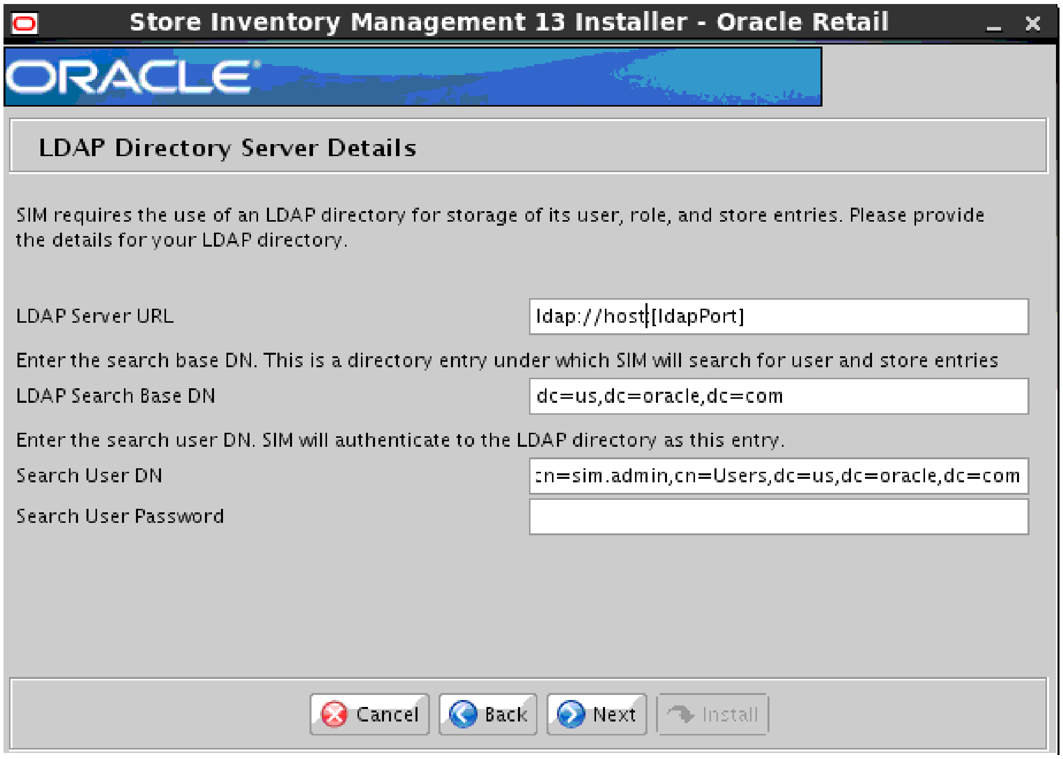
SIM JDBC URL	jdbc:oracle:thin:@[hostname]:[port]:[sim db sid]
SIM Schema	[sim db user]
SIM Schema Password	

Field Title	SIM JDBC URL
Field Description	URL used by the SIM application to access the SIM database schema.
Destination	data-sources.xml
Example	Standard Thin Connection: jdbc:oracle:thin:@ordbsrv:1521:pkols07 If it is an pluggable db then use the URL as shown below: jdbc:oracle:thin:@ordbsrv:1521/pkols07 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 = mydatabase)))

Field Title	SIM Schema
Field Description	The schema name
Destination	data-sources.xml
Example	sim132mockOAS
Notes	The schema name should match the name you provided when you ran the database schema installer.

Field Title	SIM Schema Password
Field Description	The password for the SIM Schema
Destination	data-sources.xml

Screen: LDAP Directory Server Details



LDAP Directory Server Details

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

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

Enter the search base DN. This is a directory entry under 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 LDAP directory as this entry.

Search User DN: :n=sim.admin,cn=Users,dc=us,dc=oracle,dc=com

Search User Password:

Field Title	LDAP Server URL
Field Description	URL for your LDAP directory server.
Destination	<INSTALL_DIR>/CDROM/WLS/sim/application/sim13/Sim-server.ear/lib/sim-server-resources.jar/conf/ldap.cfg
Example	ldap://orappsrv.us.oracle.com:389

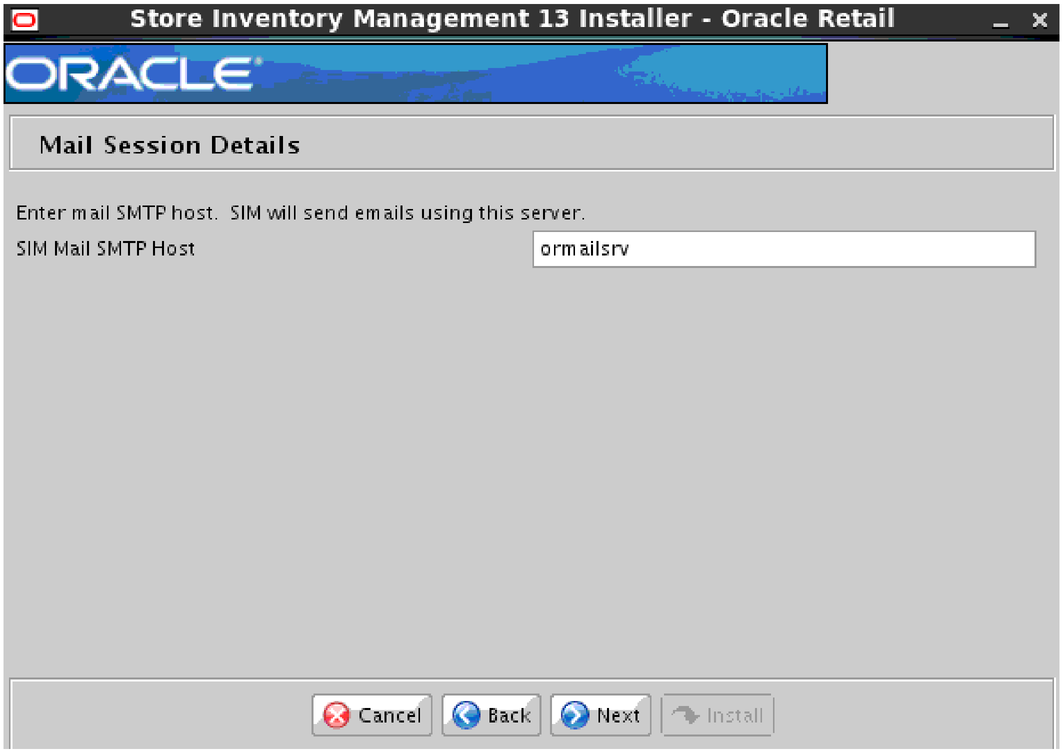
Field Title	LDAP Search Base DN
Field Description	Distinguished name of the LDAP directory entry under which SIM should search for users.
Destination	<INSTALL_DIR>/CDROM/WLS/sim/application/sim13/Sim-server.ear/lib/sim-server-resources.jar/conf/ldap.cfg
Example	dc=us,dc=oracle,dc=com

Field Title	Search User DN
Field Description	Distinguished name of the user that SIM will use to authenticate to the LDAP directory.
Destination	<INSTALL_DIR>/CDROM/WLS/sim/application/sim13/Sim-server.ear/lib/sim-server-resources.jar/conf/ldap.cfg
Example	cn=sim.admin,cn=Users,dc=us,dc=oracle,dc=com

Field Title	Search User Password
Field Description	Password for the search user DN.
Destination	<INSTALL_DIR>/CDROM/WLS/sim/application/sim13/Sim-server.ear/lib/sim-server-resources.jar/conf/ldap.cfg

Note: For additional information about LDAP configuration see the *Oracle Retail Store Inventory Management Implementation Guide*.

Screen: Mail Session Details

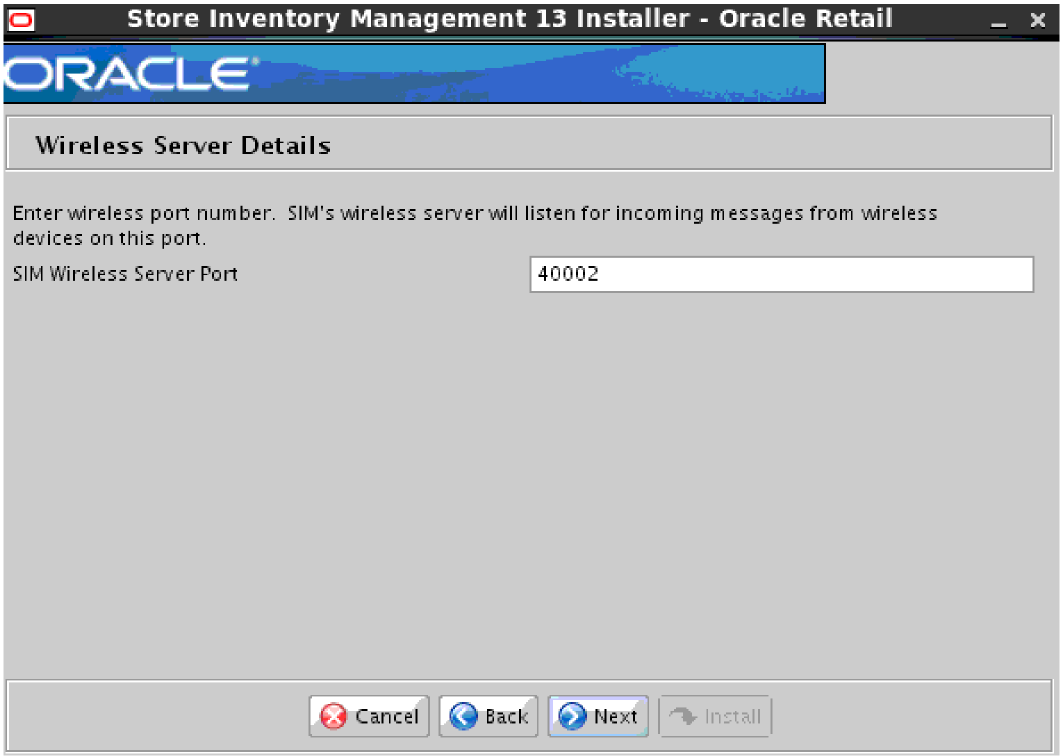


Enter mail SMTP host. SIM will send emails using this server.

SIM Mail SMTP Host: ormailsrv

Field Title	SIM Mail SMTP Host
Field Description	Enter mail SMTP host. SIM will send emails using this server.
Destination	mail.cfg
Example	ormailsrv

Screen: Wireless Server Details



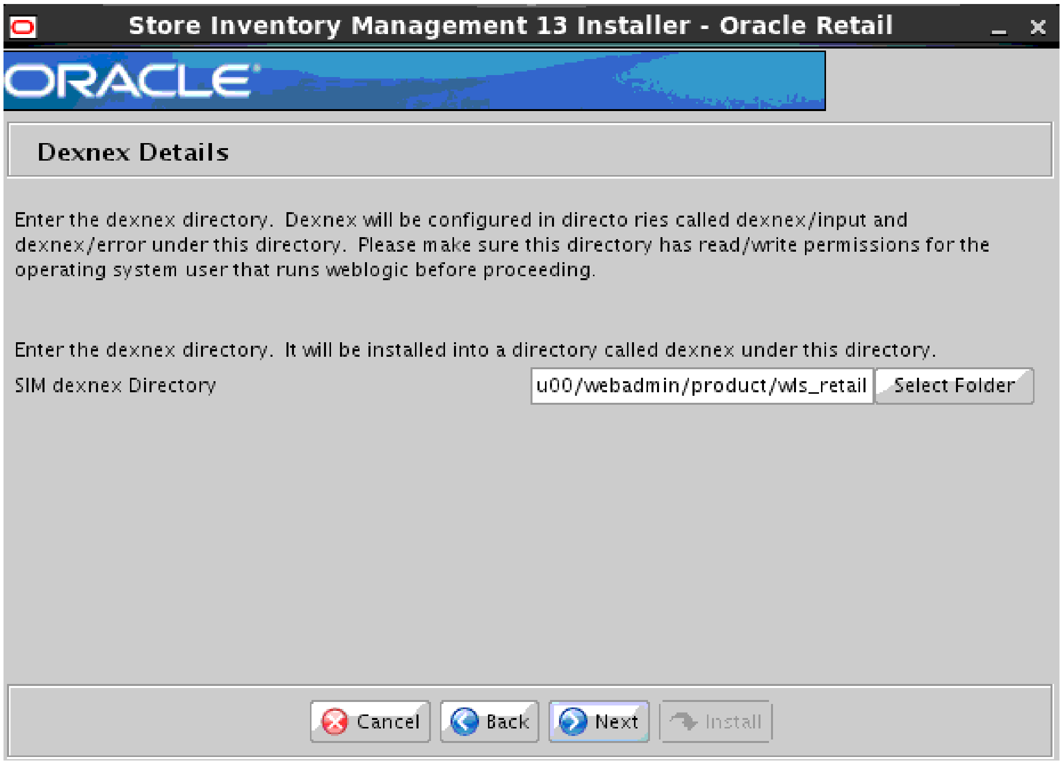
Wireless Server Details

Enter wireless port number. SIM's wireless server will listen for incoming messages from wireless devices on this port.

SIM Wireless Server Port: 40002

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_services.cfg, wavelink-startup.sh
Example	40002

Screen: Dexnex Details



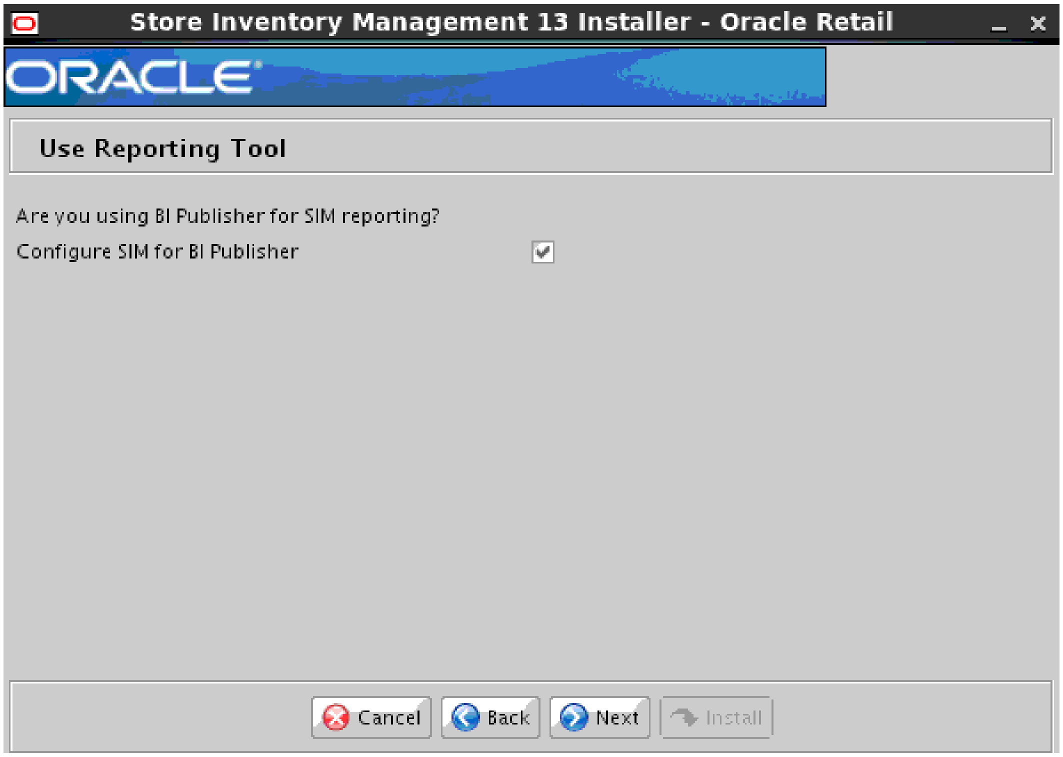
Enter the dexnex directory. Dexnex will be configured in directo ries called dexnex/input and dexnex/error under this directory. Please make sure this directory has read/write permissions for the operating system user that runs weblogic before proceeding.

Enter the dexnex directory. It will be installed into a directory called dexnex under this directory.

SIM dexnex Directory: u00/webadmin/product/wls_retail

Field Title	SIM dexnex Directory
Field Description	The dexnex directory
Example	/u00/webadmin/product/10.1.3_9/OAS/j2ee/sim-instance/dexnex

Screen: Use Reporting Tool



Use Reporting Tool

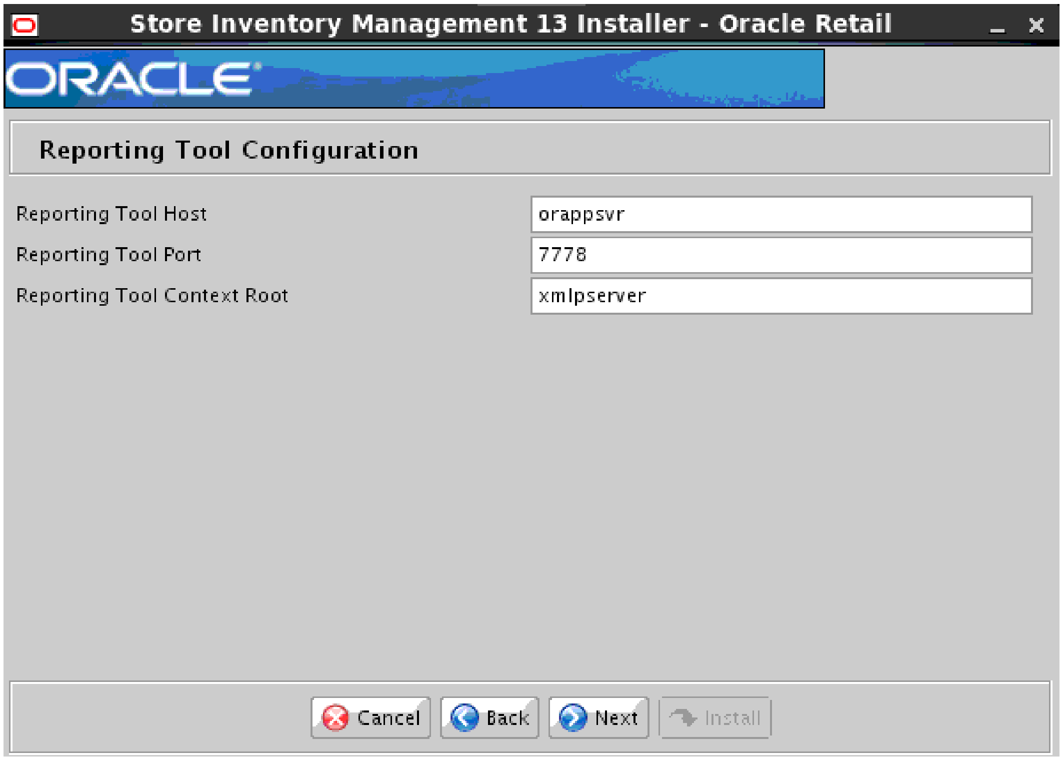
Are you using BI Publisher for SIM reporting?

Configure SIM for BI Publisher ☑

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

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

Screen: Reporting Tool Configuration



Reporting Tool Configuration

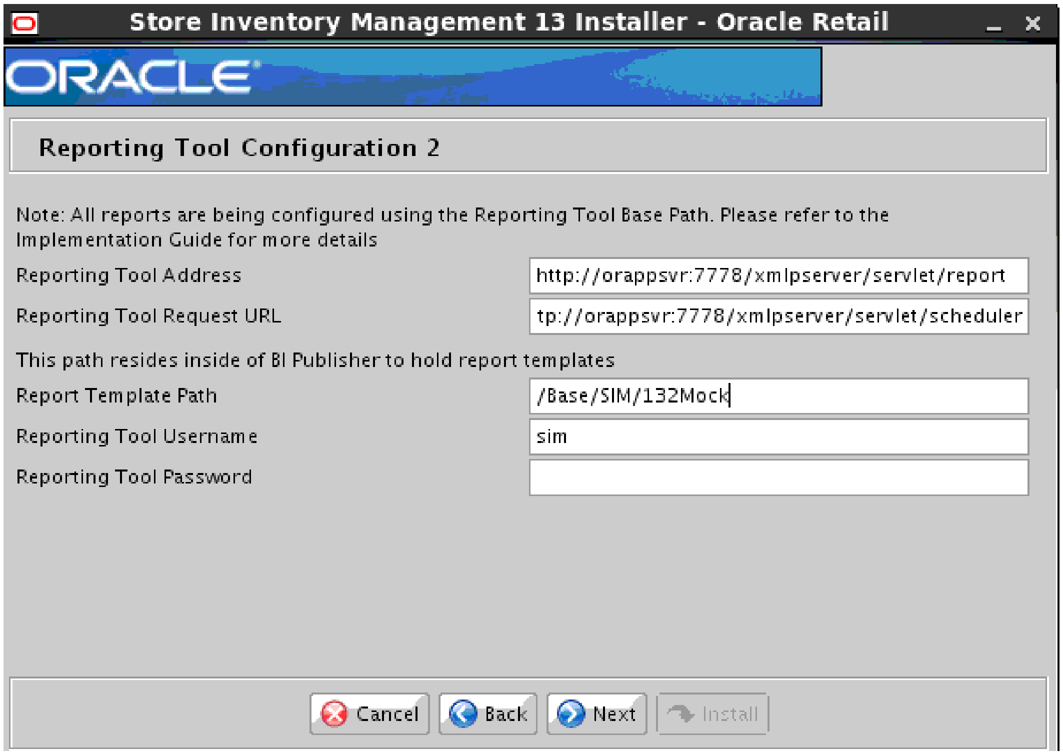
Reporting Tool Host	orappsvr
Reporting Tool Port	7778
Reporting Tool Context Root	xmlpserver

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

Field Title	Reporting Tool Port
Field Description	Port where Reporting Tool is configured.
Destination	Updates the reporting tool related default values in SIM database.
Example	7778

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

Screen: Reporting Tool Configuration 2


Store Inventory Management 13 Installer - Oracle Retail
ORACLE
Reporting Tool Configuration 2

Note: All reports are being configured using the Reporting Tool Base Path. Please refer to the Implementation Guide for more details

Reporting Tool Address: http://orappsvr:7778/xmlpserver/servlet/report

Reporting Tool Request URL: tp://orappsvr:7778/xmlpserver/servlet/scheduler

This path resides inside of BI Publisher to hold report templates

Report Template Path: /Base/SIM/132Mock

Reporting Tool Username: sim

Reporting Tool Password:

Field Title	Reporting Tool Address
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://orappsrv:7778/xmlpserver/servlet/report

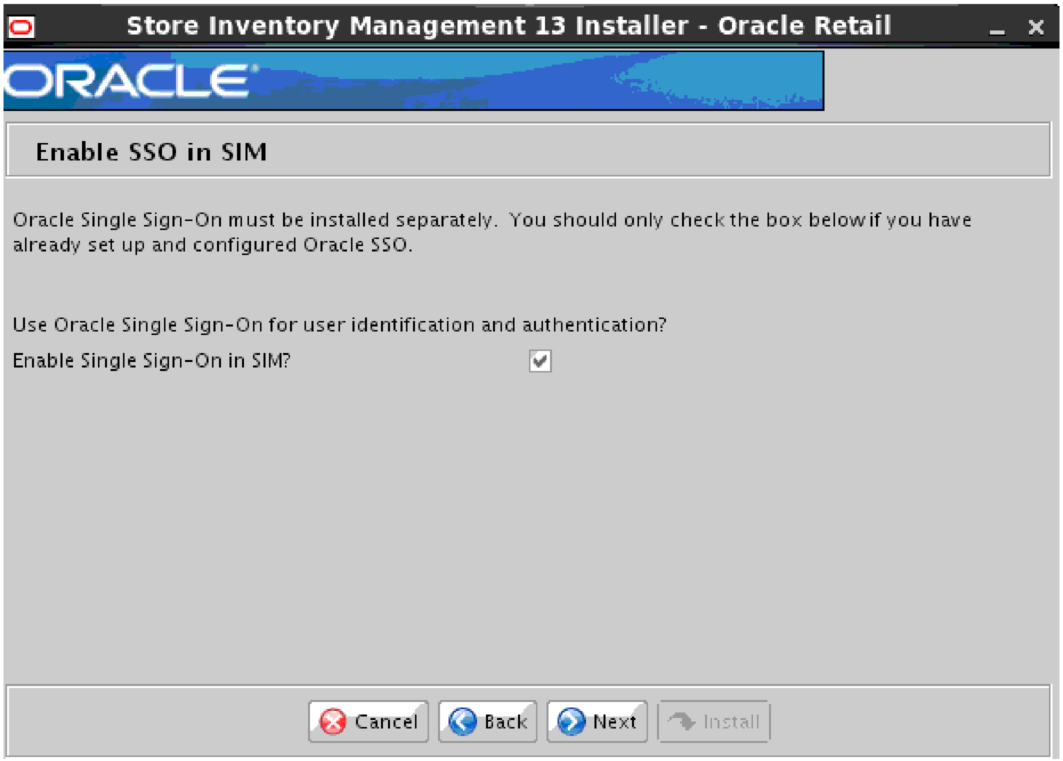
Field Title	Reporting Tool Request URL
Field Description	Confirmation field of address configured from values provided on previous screen
Destination	Updates the reporting tool related default values in SIM database.
Example	http://orappsrv:7778/xmlpserver/servlet/scheduler

Field Title	Reporting Template Path
Field Description	The folder where SIM report templates have been uploaded on the BI Publisher server. For example, if they have been uploaded in the Guest folder, it is /Guest.
Destination	Updates the reporting tool related default values in SIM database.
Example	/Guest/sim132Mock

Field Title	Reporting Tool Username
Field Description	<BIP_REPORTS_USER> or <OSSO_USER>
Destination	Updates the reporting tool related default values in SIM database.
Example	sim

Field Title	Reporting Tool Password
Field Description	<BIP_REPORTS_USER_PASSWORD> or <OSSO_PASSWORD>
Destination	Updates the reporting tool related default values in SIM database.

Screen: Enable SSO in SIM



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?

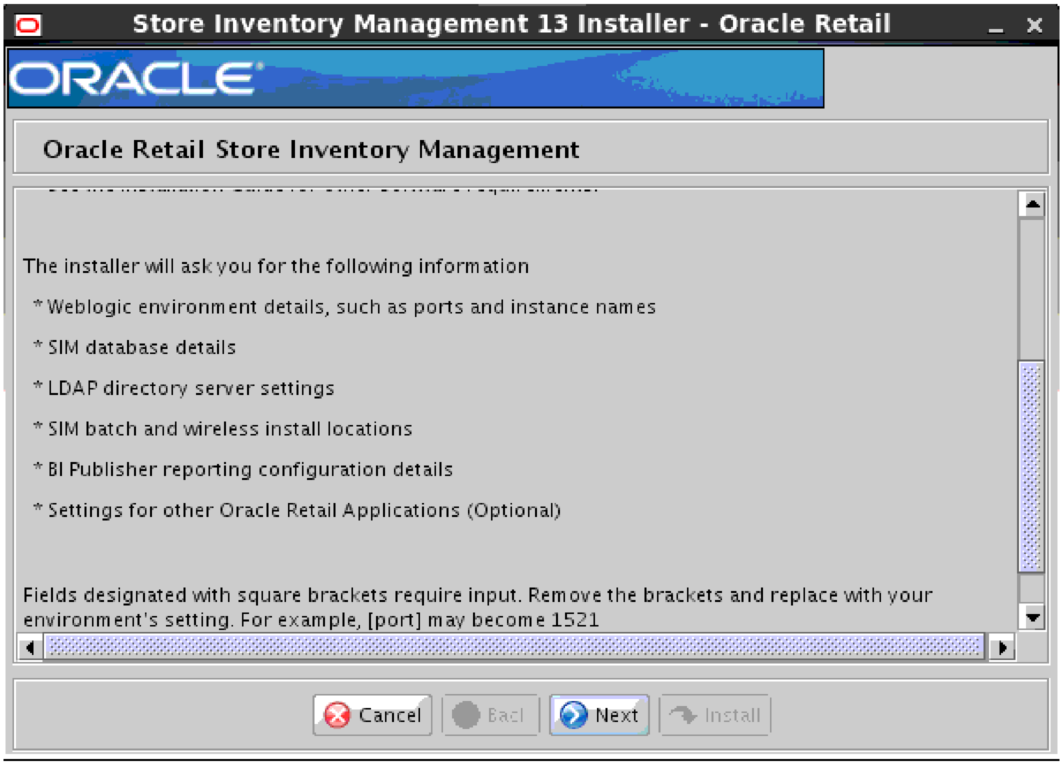
Enable Single Sign-On in SIM? ☑

Field Title	Enable Single Sign-On in SIM?
Field Description	Configures SIM to enable/disable SSO
Destination	JnlpLaunch.properties

B

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.



Store Inventory Management 13 Installer - Oracle Retail
ORACLE
Oracle Retail Store Inventory Management
Cancel
Back
Next
Install

The installer will ask you for the following information

* Weblogic environment details, such as ports and instance names

* SIM database details

* LDAP directory server settings

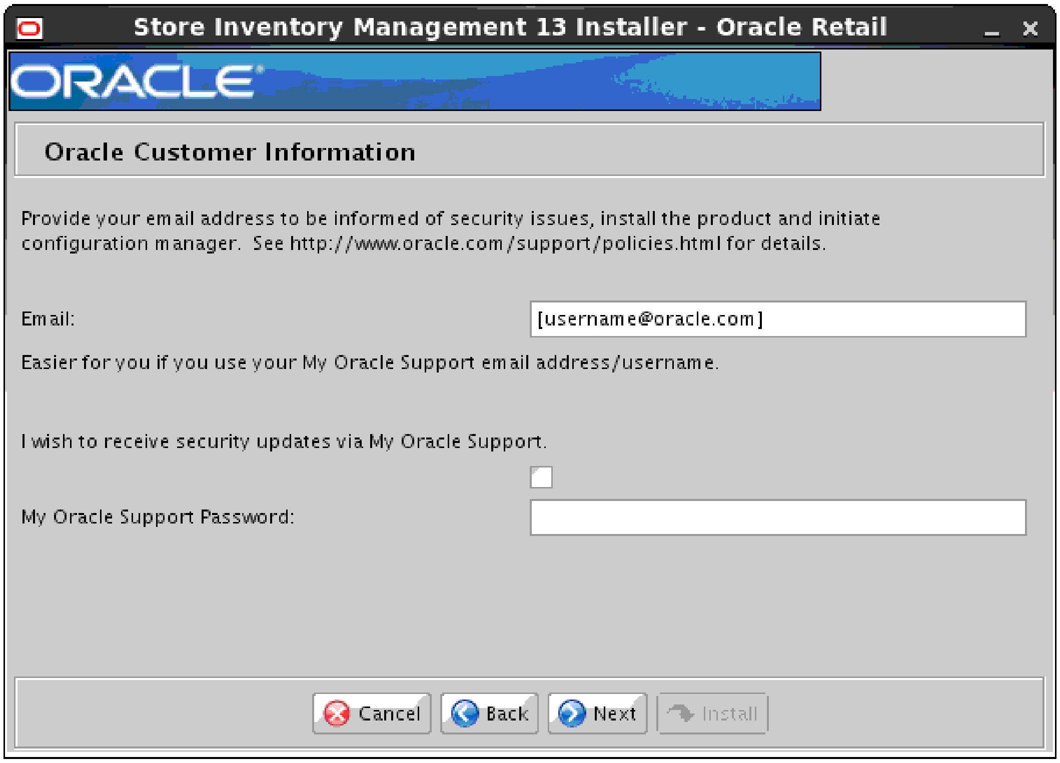
* SIM batch and wireless install locations

* BI Publisher reporting configuration details

* Settings for other Oracle Retail Applications (Optional)

Fields designated with square brackets require input. Remove the brackets and replace with your environment's setting. For example, [port] may become 1521

Screen: Customer Information



Oracle Customer Information

Provide your email address to be informed of security issues, install the product and initiate configuration manager. See http://www.oracle.com/support/policies.html for details.

Email: [username@oracle.com]

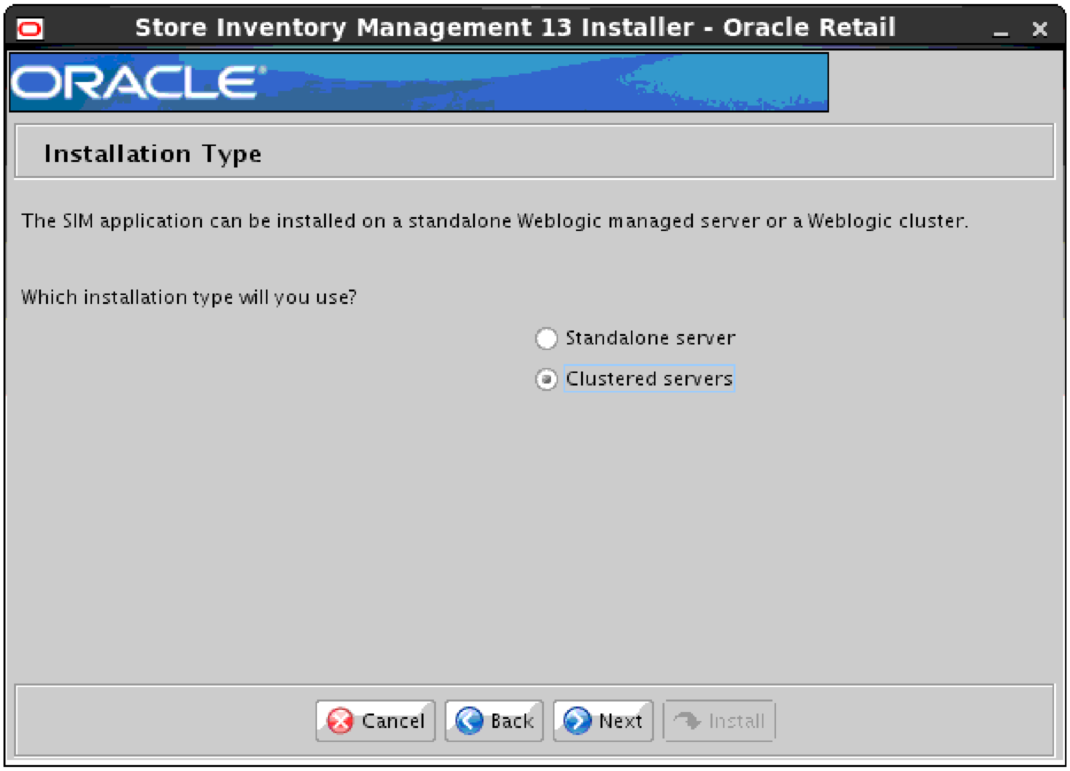
Easier for you if you use your My Oracle Support email address/username.

I wish to receive security updates via My Oracle Support. □

My Oracle Support Password:

Enter your customer information if you desire, or you can check the box to not receive updates automatically.

Screen: Installation Type



The SIM application can be installed on a standalone Weblogic managed server or a Weblogic cluster.

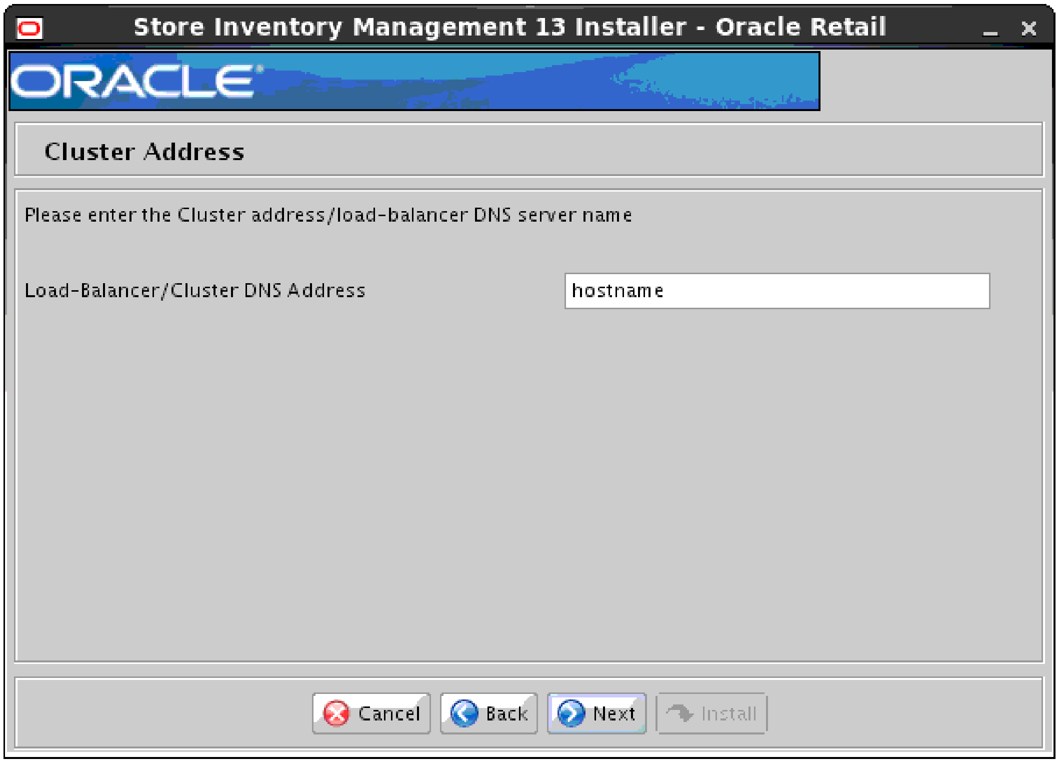
Which installation type will you use?

○ Standalone server

● Clustered servers

Field Title	Which installation type will you use?
Field Description	Select “Standalone server” to deploy SIM to a single, non-clustered WebLogic server. Select “Clustered servers” to deploy SIM to a clustered WebLogic environment

Screen: Cluster Address

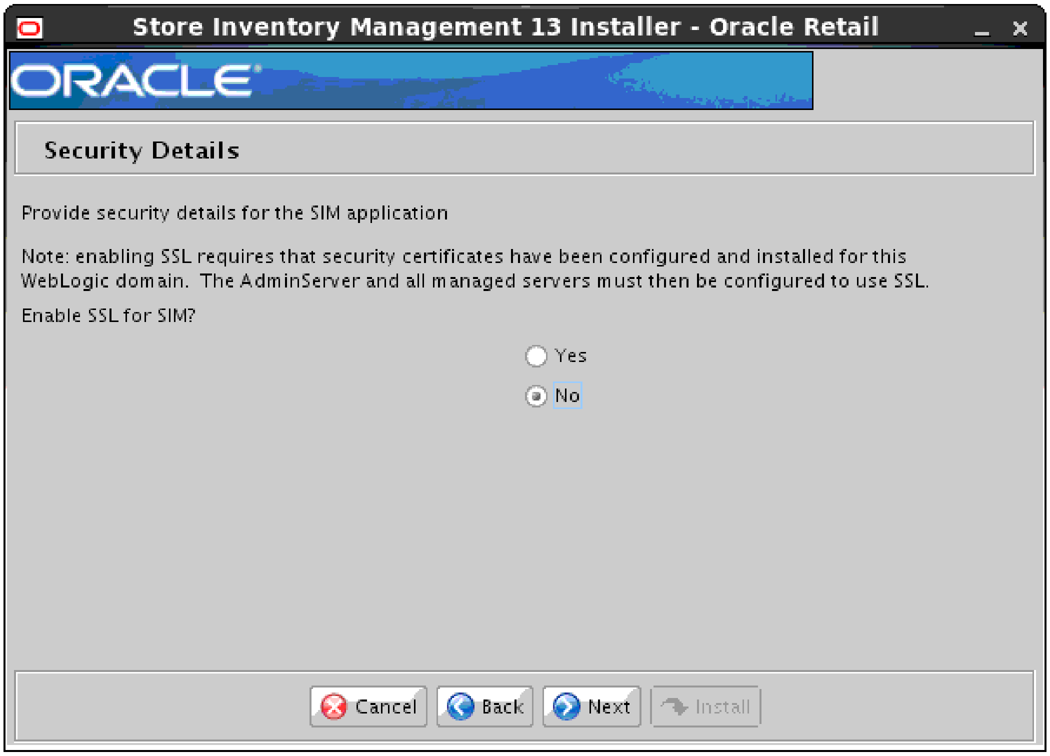


Please enter the Cluster address/load-balancer DNS server name

Load-Balancer/Cluster DNS Address: hostname

Field Title	Load Balancer/Cluster DNS Address
Field Description	The address for the load balancer that will be used to access SIM if it is deployed to a clustered environment.
Example	hostname
Note	This screen will only be displayed if “Clustered Servers” is selected on the previous screen “Installation Type”

Screen: 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.

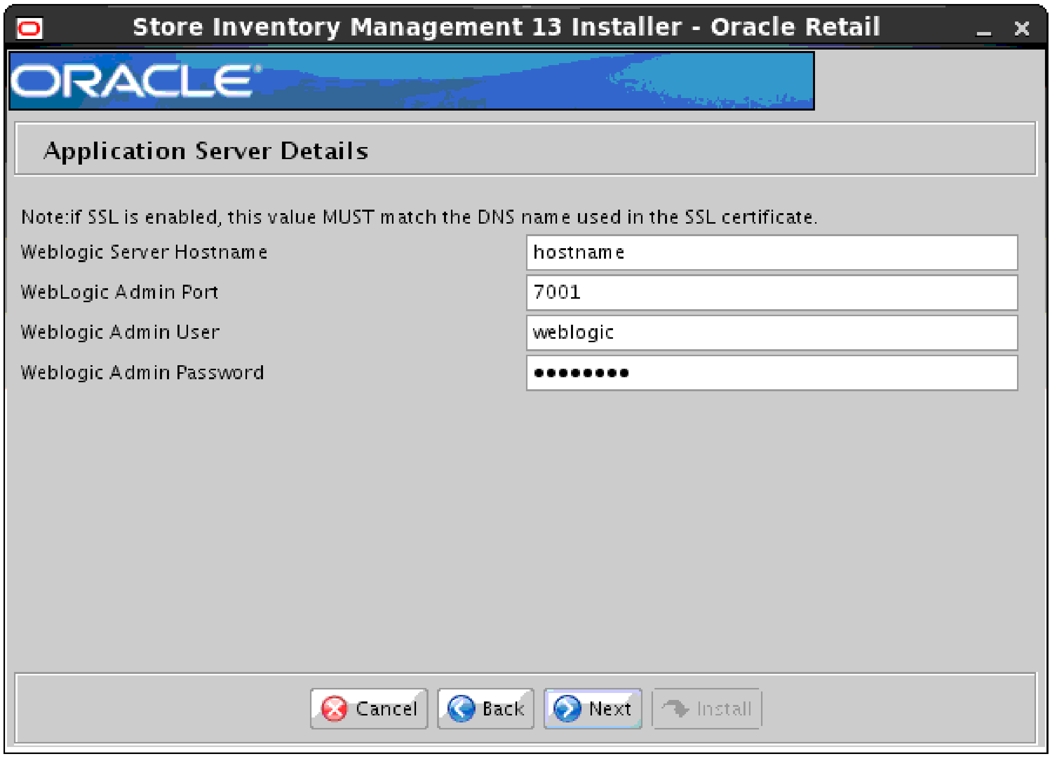
Enable SSL for SIM?

○ Yes

● No

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

Screen: Application Server Details


Store Inventory Management 13 Installer - Oracle Retail
ORACLE
Application Server Details
Cancel
Back
Next
Install

Note:if SSL is enabled, this value MUST match the DNS name used in the SSL certificate.

Weblogic Server Hostname	hostname
WebLogic Admin Port	7001
Weblogic Admin User	weblogic
Weblogic Admin Password	●●●●●●●●●

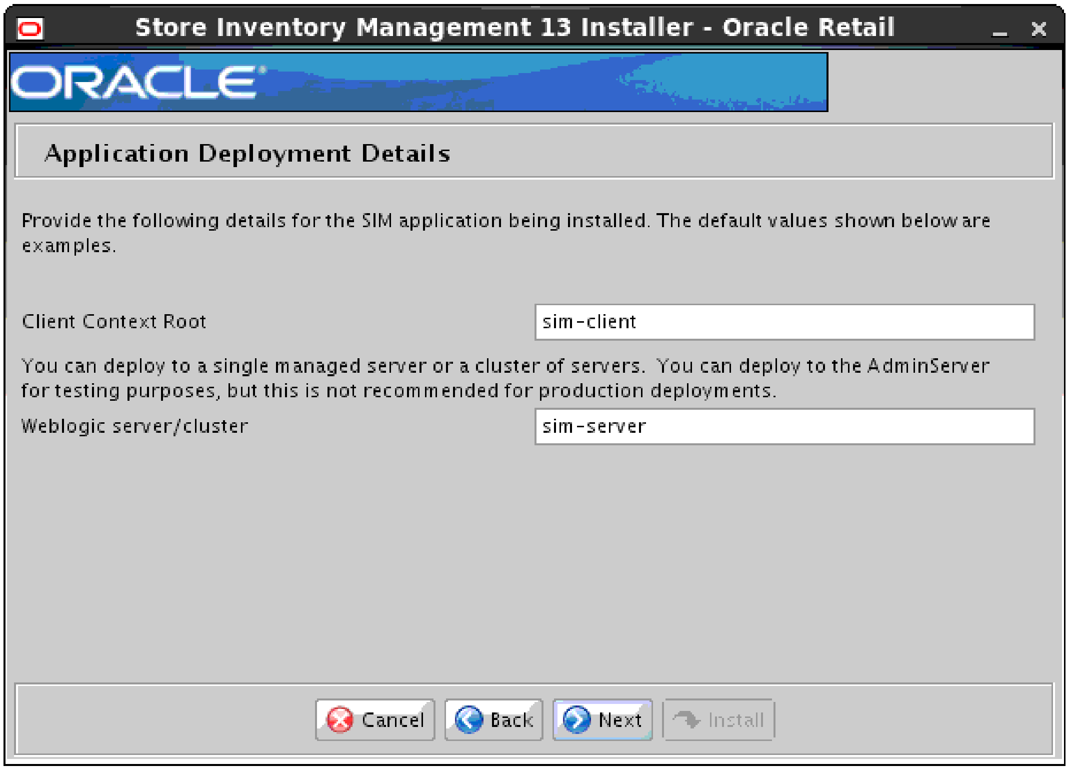
Field Title	WebLogic Server Hostname
Field Description	The hostname of the server where the WebLogic server is installed
Destination	client.cfg, jnlplaunch.properties
Example	hostname
Notes	Used by installer scripts to deploy EAR and WAR files and to create default inputs for client codebase and JNDI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

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

Field Title	WebLogic Admin User
Destination	jndi.cfg, jnlplaunch.properties
Example	weblogic
Notes	Used by installer scripts to deploy EAR and WAR files

Field Title	WebLogic Admin Password
Field Description	The password of the WebLogic Admin User
Destination	jndi.cfg, jnlplaunch.properties
Notes	Used by installer scripts to deploy EAR and WAR files

Screen: Application Deployment Details



Application Deployment Details

Provide the following details for the SIM application being installed. The default values shown below are examples.

Client Context Root: sim-client

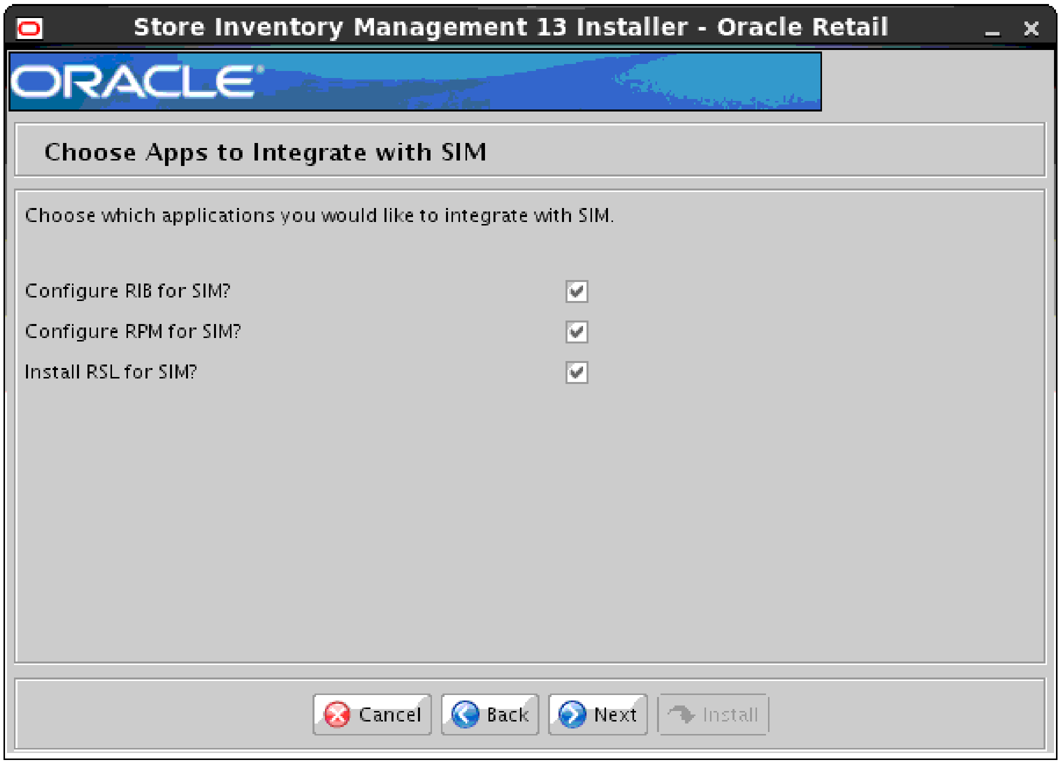
You can deploy to a single managed server or a cluster of servers. You can deploy to the AdminServer for testing purposes, but this is not recommended for production deployments.

Weblogic server/cluster: sim-server

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

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

Screen: Choose Apps to Integrate with SIM



Choose Apps to Integrate with SIM

Choose which applications you would like to integrate with SIM.

Configure RIB for SIM? ☑

Configure RPM for SIM? ☑

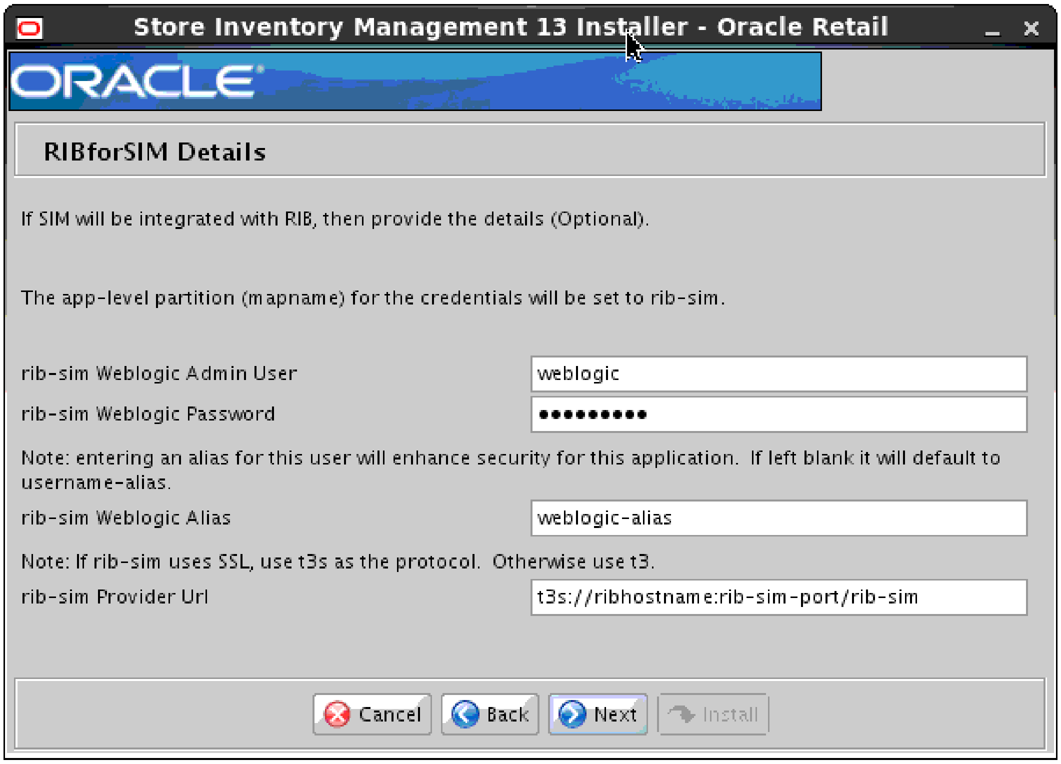
Install RSL for SIM? ☑

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

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

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

Screen: RIBforSIM Details



RIBforSIM Details

If SIM will be integrated with RIB, then provide the details (Optional).

The app-level partition (mapname) for the credentials will be set to rib-sim.

rib-sim Weblogic Admin User: weblogic

rib-sim Weblogic Password: ●●●●●●●●●●

Note: entering an alias for this user will enhance security for this application. If left blank it will default to username-alias.

rib-sim Weblogic Alias: weblogic-alias

Note: If rib-sim uses SSL, use t3s as the protocol. Otherwise use t3.

rib-sim Provider Url: t3s://ribhostname:rib-sim-port/rib-sim

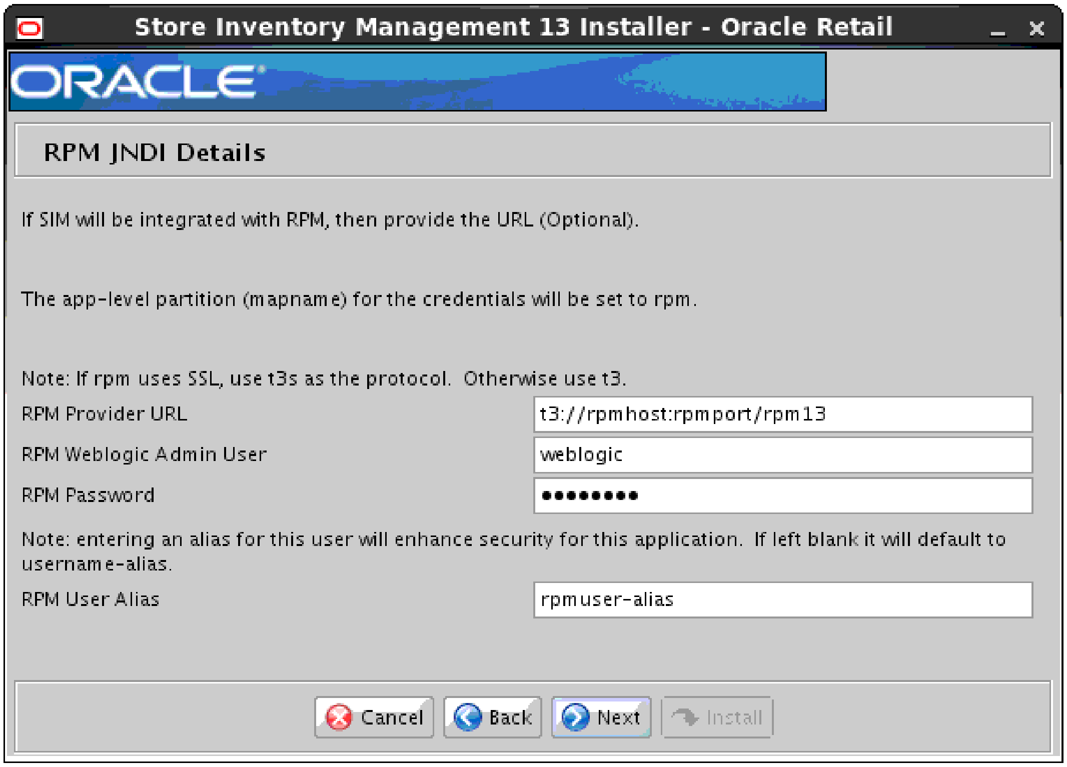
Field Title	rib-sim WebLogic User
Field Description	This is the user name with access to Admin console
Destination	remote_service_locator_info_ribclient.xml
Example	Weblogic

Field Title	rib-sim WebLogic Password
Field Description	Password for the RIBforRPM 13 user.

Field Title	rib-sim WebLogic Alias
Field Description	This is the alias for the user name.
Example	weblogic-alias
Note	This alias must be unique. Do not use the same value for any other alias fields in the installer. If the same alias is used, entries in the wallet can override each other and cause problems with the application.

Field Title	rib-sim Provider URL
Field Description	This the provider URL of the rib-<app>
Examples	t3://ribhostname:rib-sim-port/rib-sim

Screen: RPM JNDI Details



RPM JNDI Details

If SIM will be integrated with RPM, then provide the URL (Optional).

The app-level partition (mapname) for the credentials will be set to rpm.

Note: If rpm uses SSL, use t3s as the protocol. Otherwise use t3.

RPM Provider URL: t3://rpmhost:rpmport/rpm13

RPM Weblogic Admin User: weblogic

RPM Password: ●●●●●●●●●

Note: entering an alias for this user will enhance security for this application. If left blank it will default to username-alias.

RPM User Alias: rpmuser-alias

Field Title	RPM Provider URL
Field Description	This is the provider URl for <app>
Destination	jndi_providers.xml
Example	t3://rpmhost:rpmport/rpm13

Field Title	RPM Weblogic Admin User
Field Description	This is the user which has access to RPM WebLogic server.
Example	weblogic

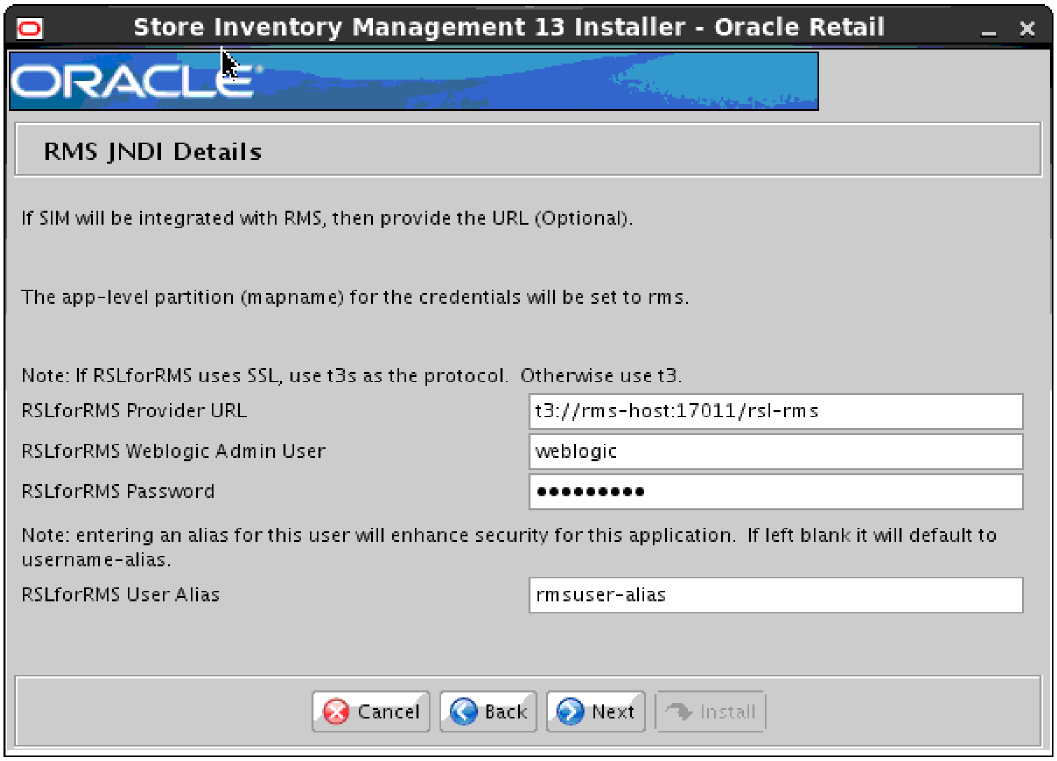
Field Title	RPM Password
Field Description	This is the password of the user provided for RPM WebLogic Admin user in the above.

Field Title	RPM User Alias
Field Description	This is the alias for <RPM WebLogic Admin User>
Examples	rpmuser-alias (Make sure to give the same name as provided for <RPM WebLogic Admin User>
Note	This alias must be unique. Do not use the same value for any other alias fields in the installer. If the same alias is used, entries in the wallet can override each other and cause problems with the application.

Note: In SIM Database, verify that rk_config table has a valid RPM application login user name for config_key=RPM_APP_USER_NAME, RPM_APP_USER_FIRST_NAME and RPM_APP_USER_LAST_NAME.
This is required for SIM-RPM integration to work properly.

For example, retail.user (validate this user by logging into the RPM application).

Screen: RMS JNDI Details



If SIM will be integrated with RMS, then provide the URL (Optional).

The app-level partition (mapname) for the credentials will be set to rms.

Note: If RSLforRMS uses SSL, use t3s as the protocol. Otherwise use t3.

RSLforRMS Provider URL: t3://rms-host:17011/rsl-rms

RSLforRMS Weblogic Admin User: weblogic

RSLforRMS Password: ●●●●●●●●●●

Note: entering an alias for this user will enhance security for this application. If left blank it will default to username-alias.

RSLforRMS User Alias: rmsuser-alias

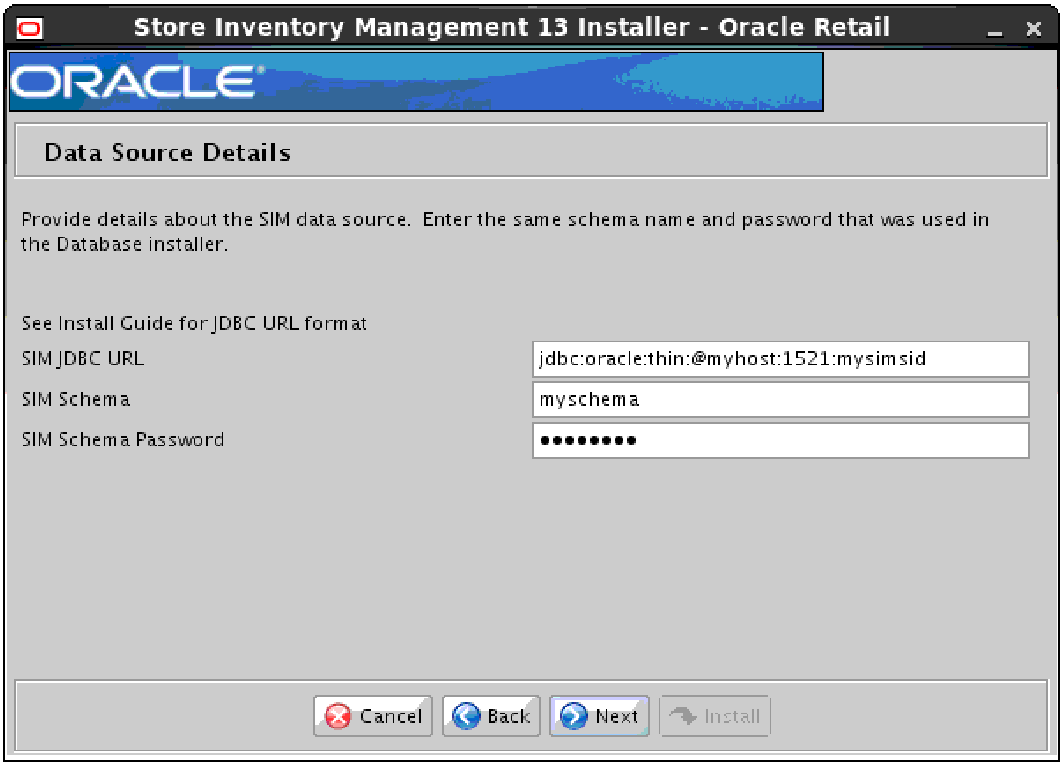
Field Title	RSLforRMS Provider URL
Field Description	This is the provider URL for the RSLforRMS
Destination	jndi_providers.xml
Example	t3://rms-host:17011/rsl-rms

Field Title	RSLforRMS Weblogic Admin User
Field Description	This is the user name for login to RSLforRSM WebLogic Server.
Example	weblogic

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

Field Title	RSLforRMS User Alias
Field Description	This is the alias for RSLforRMS WebLogic Admin User.
Examples	rmsuser-alias (Make sure to give the same name as provided for <RSLforRMS WebLogic Admin User>
Note	This alias must be unique. Do not use the same value for any other alias fields in the installer. If the same alias is used, entries in the wallet can override each other and cause problems with the application.

Screen: Data Source Details



Provide details about the SIM data source. Enter the same schema name and password that was used in the Database installer.

See Install Guide for JDBC URL format

SIM JDBC URL: jdbc:oracle:thin:@myhost:1521:mysimsid

SIM Schema: myschema

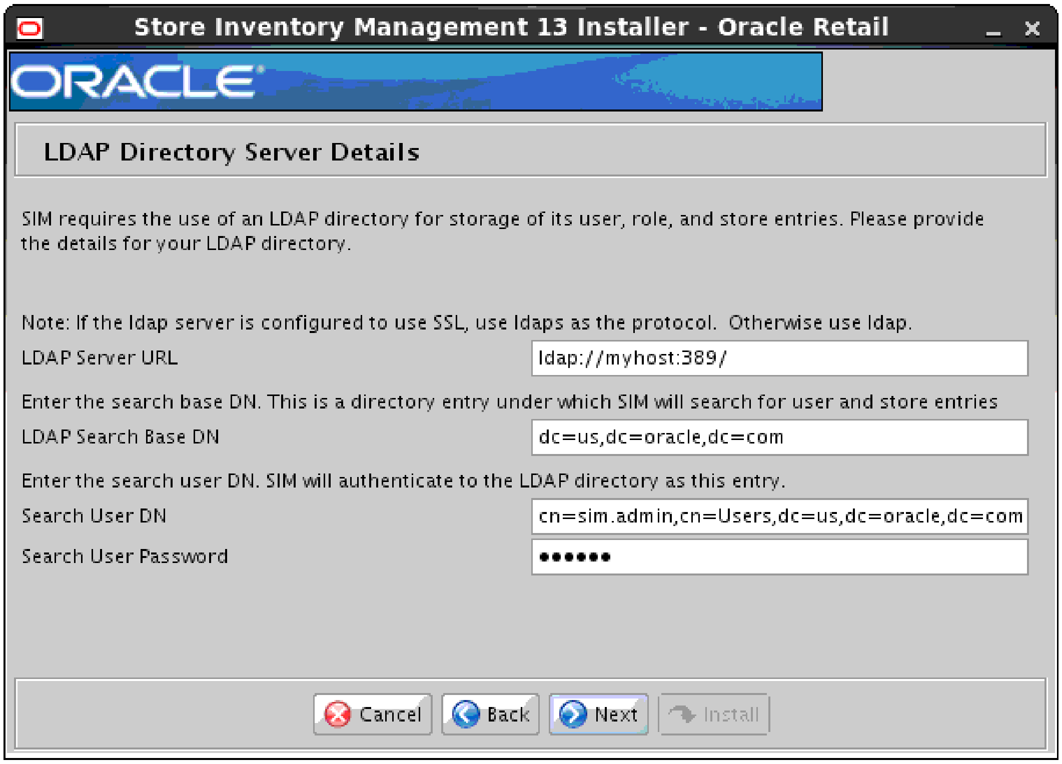
SIM Schema Password: ●●●●●●●●●

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 an pluggable db the n use the URL as shown below: jdbc:oracle:thin@myhost:1521/mysimsid 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)))

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

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

Screen: LDAP Directory Server Details



LDAP Directory Server Details

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

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

LDAP Server URL: ldap://myhost:389/

Enter the search base DN. This is a directory entry under 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 LDAP directory as this entry.

Search User DN: cn=sim.admin,cn=Users,dc=us,dc=oracle,dc=com

Search User Password: ●●●●●●

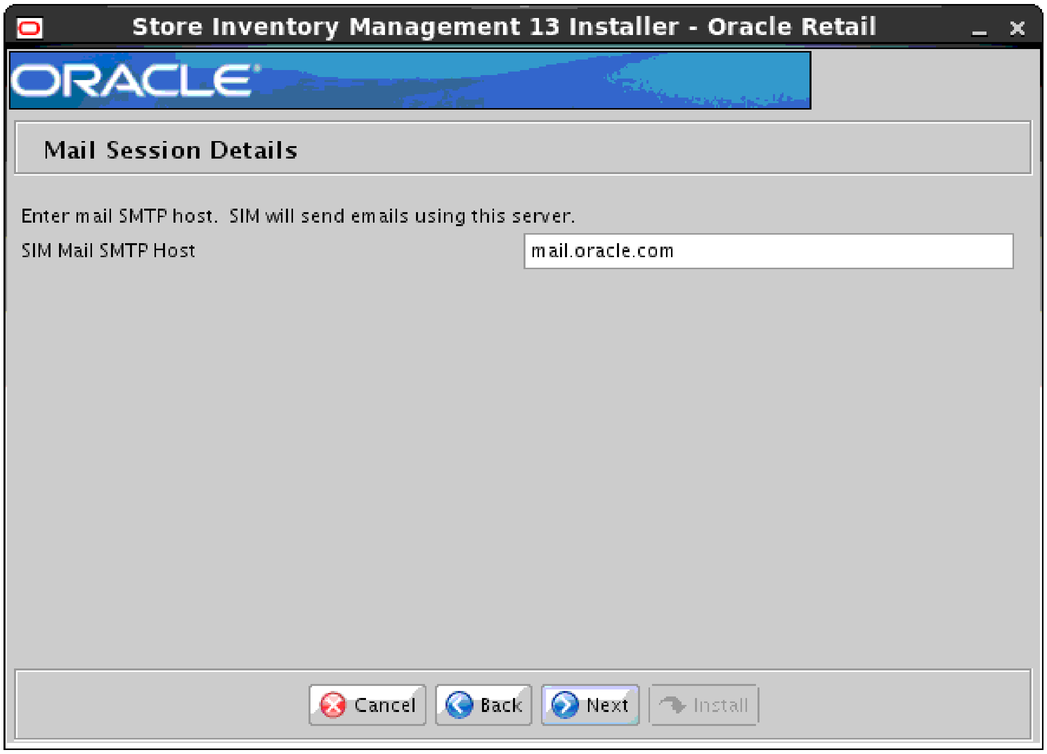
Field Title	LDAP server URL
Field Description	URL for your LDAP directory server.
Example	ldap://myhost:389/

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

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

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

Screen: Mail Session Details



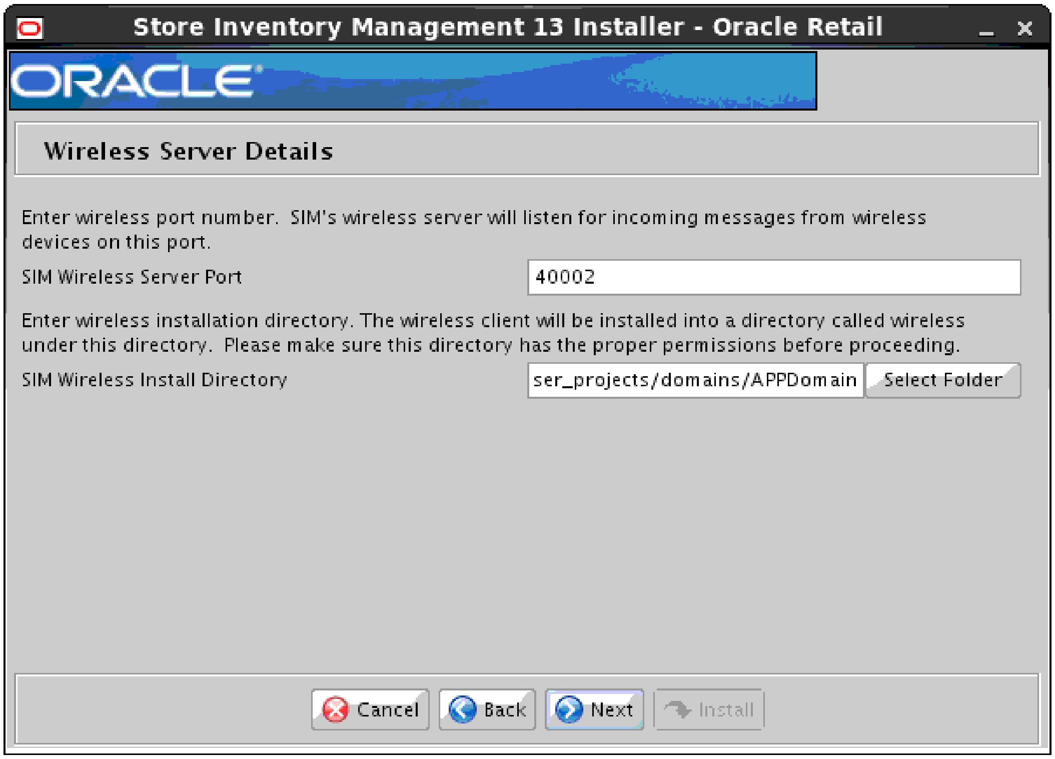
Mail Session Details

Enter mail SMTP host. SIM will send emails using this server.

SIM Mail SMTP Host: mail.oracle.com

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

Screen: Wireless Server Details



Enter wireless port number. SIM's wireless server will listen for incoming messages from wireless devices on this port.

SIM Wireless Server Port: 40002

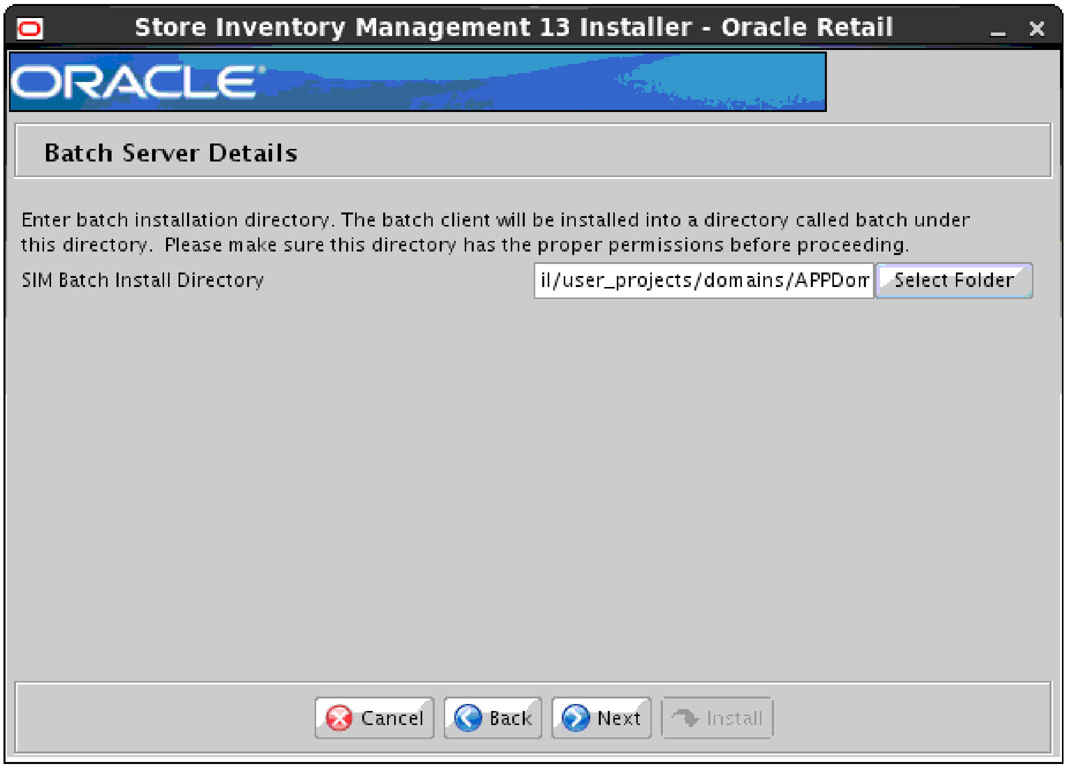
Enter wireless installation directory. The wireless client will be installed into a directory called wireless under this directory. Please make sure this directory has the proper permissions before proceeding.

SIM Wireless Install Directory: ser_projects/domains/APPDomain

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	SIM Wireless Install Directory
Field Description	The wireless installation directory.
Example	/u00/webadmin/product/10.3.X/WLS/user_projects/domains/APPDomain

Screen: Batch Server Details

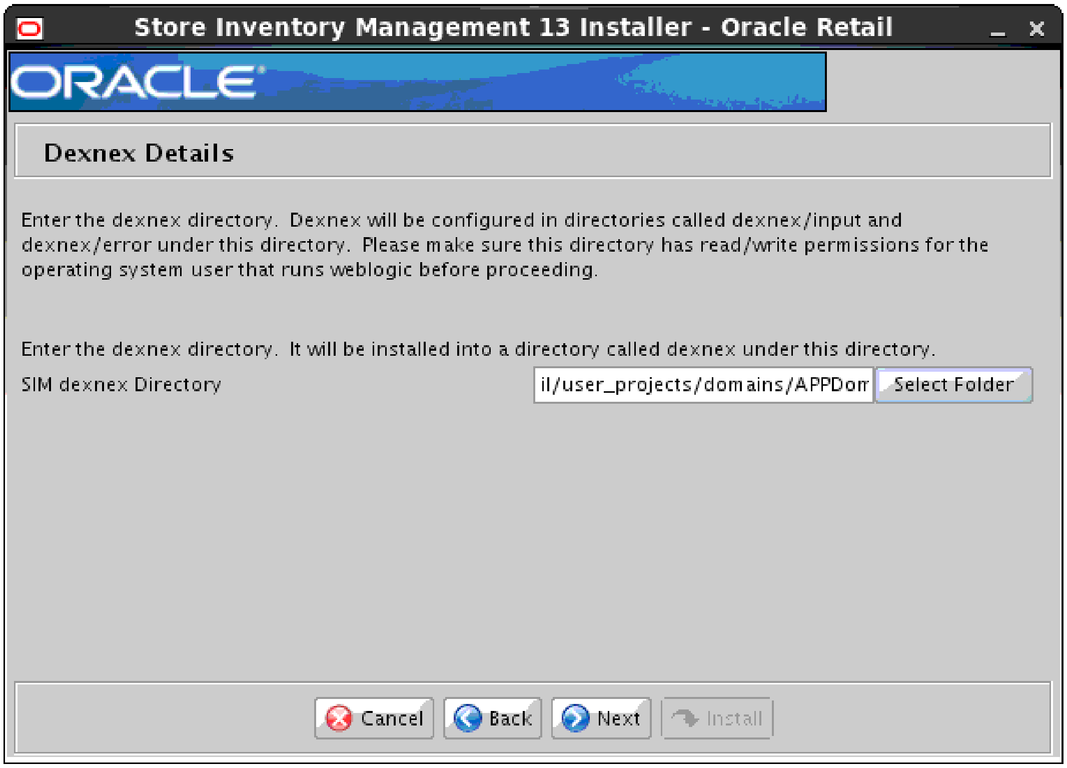


Enter batch installation directory. The batch client will be installed into a directory called batch under this directory. Please make sure this directory has the proper permissions before proceeding.

SIM Batch Install Directory il/user_projects/domains/APPDom

Field Title	SIM Batch Install Directory
Field Description	The batch installation directory.
Example	/u00/webadmin/product/10.3.x/WLS/user_projects/domains/APPDomain

Screen: Dexnex Details



Dexnex Details

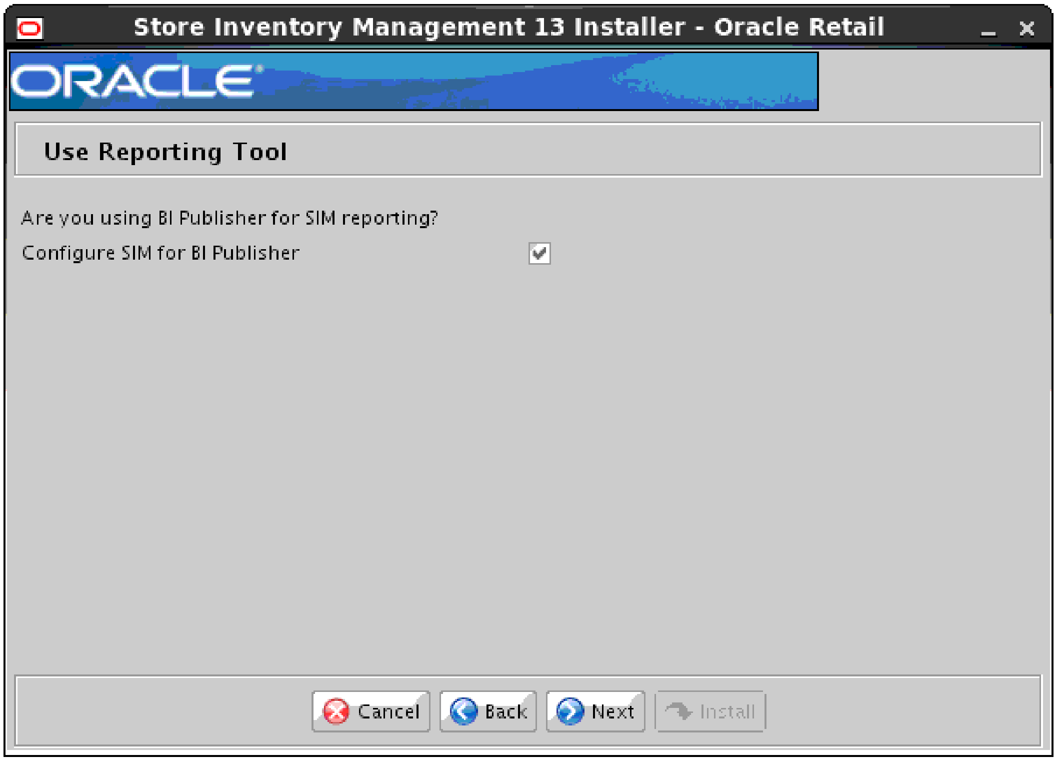
Enter the dexnex directory. Dexnex will be configured in directories called dexnex/input and dexnex/error under this directory. Please make sure this directory has read/write permissions for the operating system user that runs weblogic before proceeding.

Enter the dexnex directory. It will be installed into a directory called dexnex under this directory.

SIM dexnex Directory: il/user_projects/domains/APPDom

Field Title	SIM dexnex Directory
Field Description	The dexnex directory.
Example	/u00/webadmin/product/10.3.x/WLS/user_projects/domains/APPDomain

Screen: Use Reporting Tool



Store Inventory Management 13 Installer - Oracle Retail

Use Reporting Tool

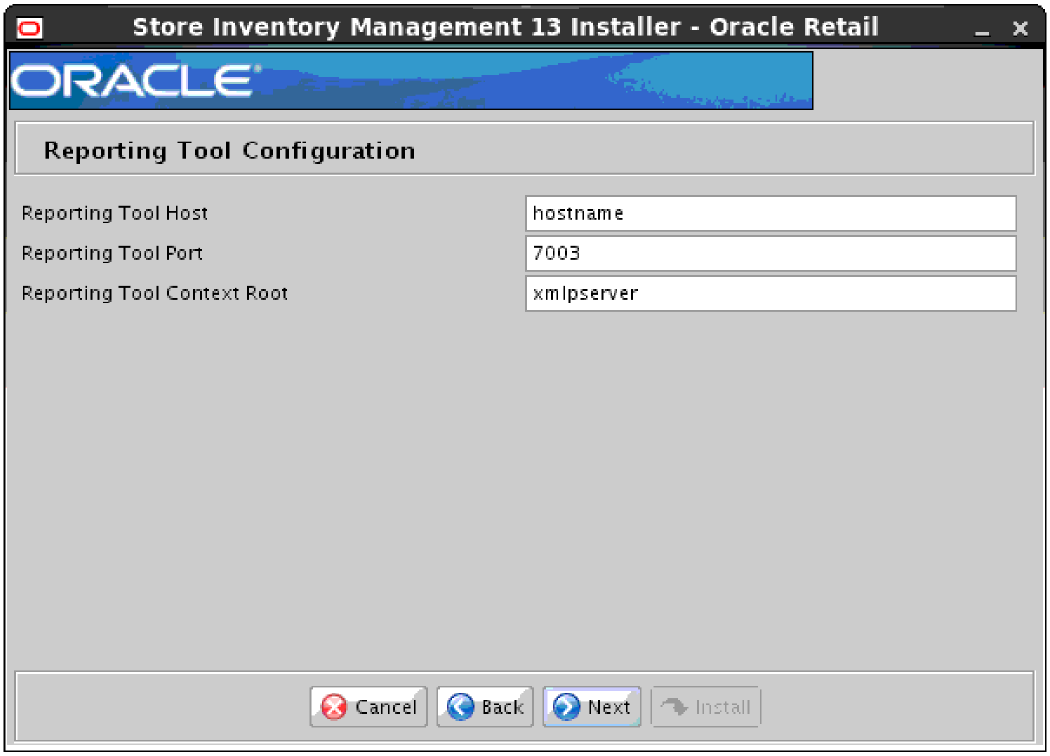
Are you using BI Publisher for SIM reporting?

Configure SIM for BI Publisher ☑

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

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

Screen: Reporting Tool Configuration


Store Inventory Management 13 Installer - Oracle Retail
ORACLE
Reporting Tool Configuration

Reporting Tool Host: hostname

Reporting Tool Port: 7003

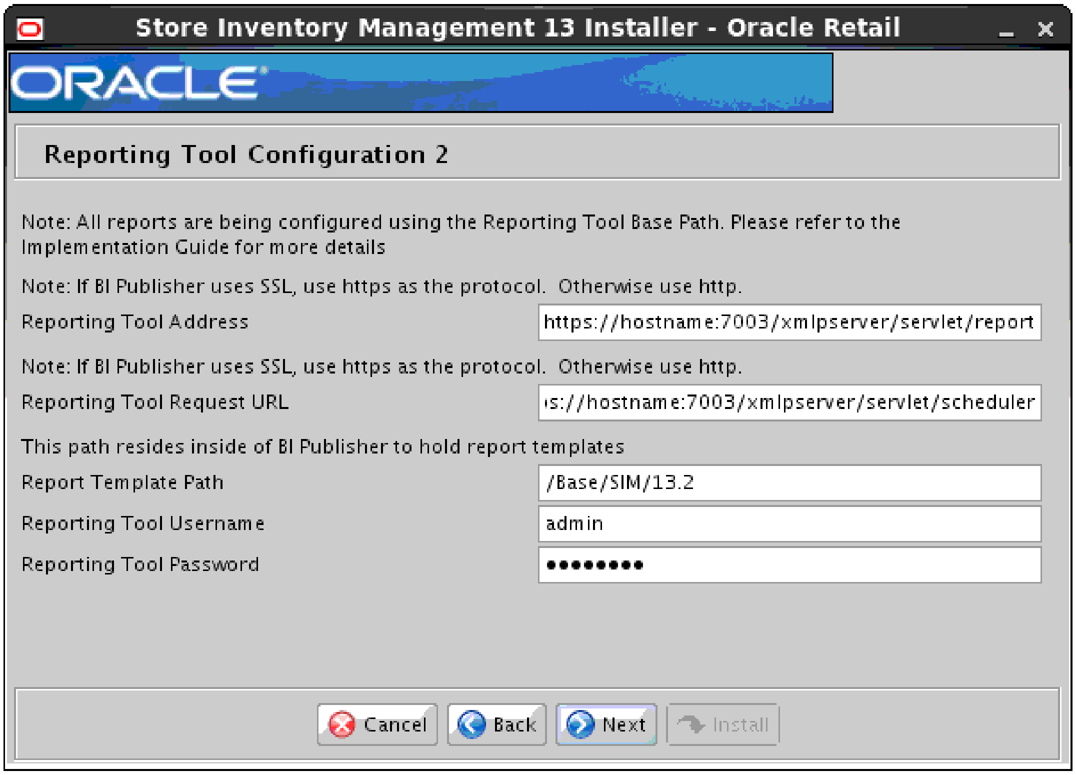
Reporting Tool Context Root: xmlpserver

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

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

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

Screen: Reporting Tool Configuration 2



Reporting Tool Configuration 2

Note: All reports are being configured using the Reporting Tool 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 Tool Address: https://hostname:7003/xmlpserver/servlet/report

Note: If BI Publisher uses SSL, use https as the protocol. Otherwise use http.

Reporting Tool Request URL: ıs://hostname:7003/xmlpserver/servlet/scheduler

This path resides inside of BI Publisher to hold report templates

Report Template Path: /Base/SIM/13.2

Reporting Tool Username: admin

Reporting Tool Password: ●●●●●●●●●

Field Title	Reporting Tool Address
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://hostname7003/xmlpserver/servlet/report

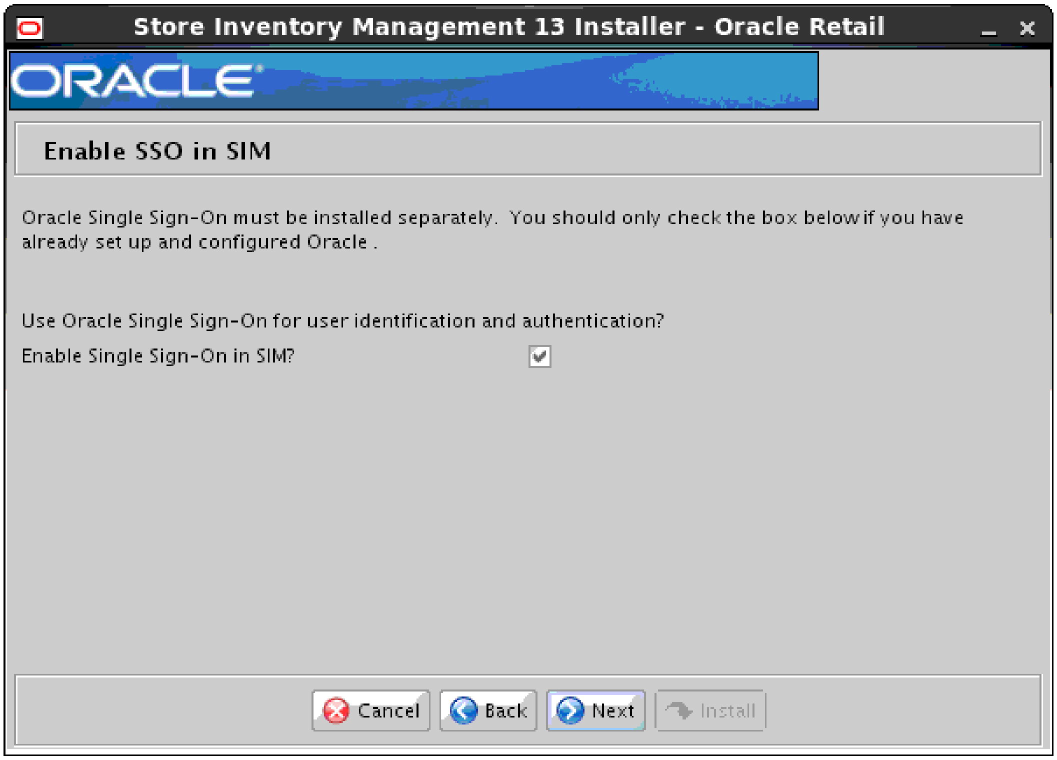
Field Title	Reporting Tool Address URL
Field Description	Confirmation field of address configured from values provided on previous screen
Destination	Updates the reporting tool related default values in SIM database.
Example	http://hostname:7003/xmlpserver/servlet/scheduler

Field Title	Report Template Path
Field Description	The root directory in which your SIM report templates are located.
Example	/Base/SIM/13.2

Field Title	Reporting Tool Username
Field Description	From the *Oracle Retail Store Inventory Management Implementation Guide:* <*BIP_REPORTS_USER*> or <*OSSO_USER*>
Destination	Updates the reporting tool related default values in SIM database.
Example	admin

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

Screen: Enable SSO in SIM



Enable SSO in SIM

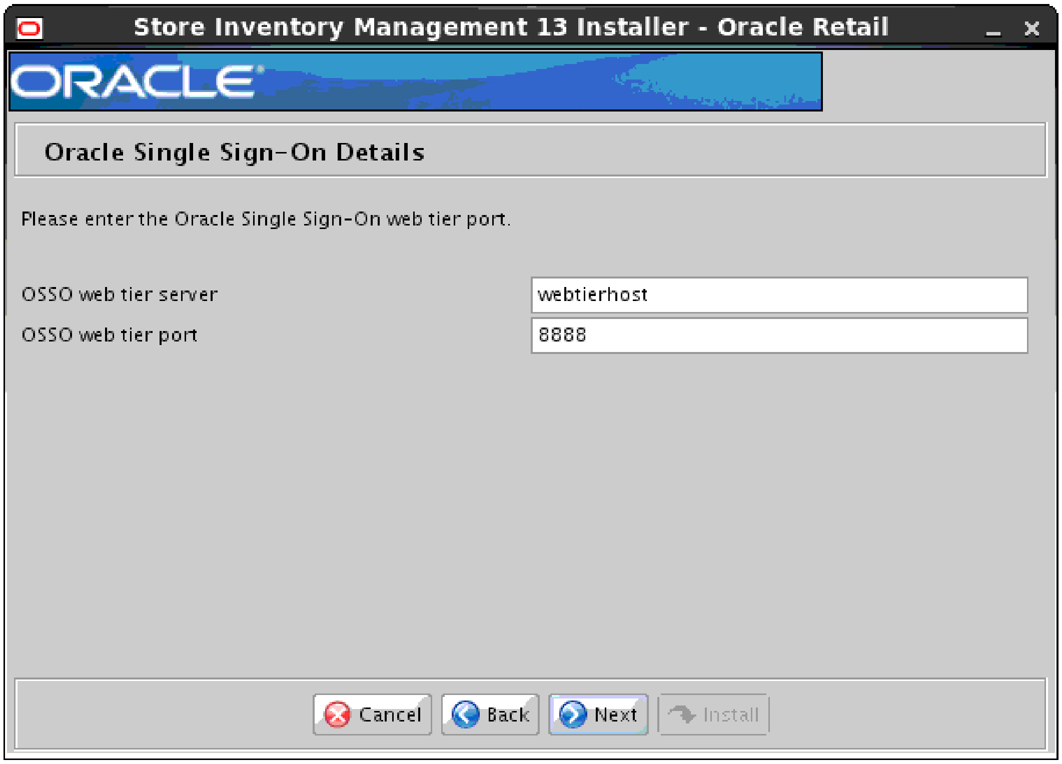
Oracle Single Sign-On must be installed separately. You should only check the box below if you have already set up and configured Oracle .

Use Oracle Single Sign-On for user identification and authentication?

Enable Single Sign-On in SIM? ☑

Field Title	Use Oracle Single Sign-On for user identification and authentication?
Field Description	This version of SIM has the option to use Oracle Single Sign-On (OSSO) technology to authenticate users. If OSSO is being used in your environment, choose Yes. A choice of No will configure SIM to use its own LDAP directory settings for authentication.
Destination	JnlpLaunch.properties

Screen: Oracle Single Sign-On Details



Store Inventory Management 13 Installer - Oracle Retail
ORACLE
Oracle Single Sign-On Details

Please enter the Oracle Single Sign-On web tier port.

OSSO web tier server: webtierhost

OSSO web tier port: 8888

Field Title	OSSO web tier server
Field Description	This is the Single Sign-On webtier server
Example	webtierhost

Field Title	OSSO web tier port
Field Description	This is the port used to access the Single Sign-On webtier
Example	8888

C

Appendix: Installer Silent Mode

In addition to the GUI and text interfaces of the installer, there is a silent mode that can be run. This mode is useful if you wish to run a repeat installation without retyping the settings you provided in the previous installation. It is also useful if you encounter errors in the middle of an installation and wish to continue.

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

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

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

Example: install.sh silent

D

Appendix: Common Installation Errors

This section provides some common errors encountered during installation.

EJB Deployment Errors during Installation to WebLogic

Symptom

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

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

Solution

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

XML Processing Errors while configuring sim-client.ear or sim-server.ear

Symptom

The installer fails while attempting to configure sim-client.ear or sim-server.ear. When updating META-INF/application.xml, the following error occurs:

```
   [mkdir] Created dir:
/work/sources/13.3/SIM_13.2.9/CDROM/WLS/sim/application/sim13/configured-
output/tmp/client/earcontents/afterconfig/META-INF
  [xmltask] It looks like you've got a network error. The probable cause
  [xmltask] is that you're trying to resolve a DTD on the internet although
  [xmltask] you don't know it! Check your XML for DTDs external to your network
  [xmltask] and read the Ant documentation for <xmlcatalog>. XMLTask will support
  [xmltask] usage of <xmlcatalog>. See the following:
  [xmltask] http://ant.apache.org/manual/CoreTypes/xmlcatalog.html
  [xmltask] http://www.oopsconsultancy.com/software/xmltask
  [xmltask] If this isn't the problem, then please report this error to the
support
  [xmltask] mailing list. Thanks!
```

Solution

This error occurs because the server on which SIM is being installed is not able to connect to the internet (for example, java.sun.com). Do either of the following.

- Establish a connection to the internet and re-run the installer, or:
- Perform the following configuration steps:

  i. cd sim/application/sim13/sim-client

  ii. jar xf sim-client.ear META-INF/application.xml

  iii. edit META-INF/application.xml, and remove the <DTD…> tag.

  iv. jar uf sim-client.ear META-INF/application.xml

  v. perform the same steps for sim/application/sim13/sim-server/sim-server.ear.

  vi. re-run the installer.

Output Freezes during Text Mode Installation to OAS and WebLogic

Symptom

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

Solution

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

Database Installer Hangs on Startup

Symptom

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

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

Solution

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

Unreadable Buttons in the Installer

If you are unable to read the text within the installer buttons, it probably means that your JAVA_HOME is pointed to a pre-1.4.2 JDK. Set JAVA_HOME to a Java development kit, the version of which is being used by the Application server, and run the installer again.

Message: Unable to get a deployment manager

Symptom

The application installer quits with the following error message:

```
[oracle:deploy] Unable to get a deployment manager.
[oracle:deploy]
[oracle:deploy] This is typically the result of an invalid deployer URI format
being supplied, the target server not being in a started state or incorrect
authentication details being supplied.
[oracle:deploy]
[oracle:deploy] More information is available by enabling logging -- please see
the Oracle Containers for J2EE Configuration and Administration Guide for details.
```

Solution

This error can be caused by any of the following conditions:

- OC4J instance provided is not running.
- Incorrect OC4J instance name provided
- Incorrect OC4J administrative username and/or password
- Incorrect OPMN request port provided.

Make sure that the OC4J instance is running, and then check the **ant.install.properties** file for entry mistakes. Pay close attention to the input.deployer.uri, input.oc4j.instance, input.admin.user, and input.admin.password properties. If you need to make a correction, you can run the installer again with this file as input by running silent mode (see “Appendix: Installer Silent Mode”).

Warning: Could not create system preferences directory

Symptom

The following text appears in the installer Errors tab:

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

Solution

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

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

Warning: Couldn't find X Input Context

Symptom

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

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

Solution

This message is harmless and can be ignored.

ConcurrentModificationException in Installer GUI

Symptom

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

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

Solution

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

Error while unpacking the ear file

Symptom

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

07/12/19 10:53:17 Notification ==>Error while unpacking sim13.ear
java.util.zip.ZipException: error in opening zip file
```

Solution

This is a known bug (BugID 6330834) related to Solaris and NFS in Oracle Application Server 10.1.3.4. Follow the workaround documented for this bug: in the opmn.xml file in $ORACLE_HOME/opmn/conf add the following parameter to the java-options for the instance you are installing.

-Doc4j.autoUnpackLockCount=-1

After making this change you should reload OPMN, restart the affected OC4J instance(s), and retry the retail application installation.

A Second Login Screen Appears After Single Sign-On Login

If you are using Oracle 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 wrong on the server.
- SSO timed out. (This can happen especially the first time you launch SIM. Try launching SIM again.)

Symptom

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

Solution

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

Error Connecting to Database URL

Symptom

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

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

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

Solution

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

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

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

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

Symptom

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

Solution

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

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

Symptom

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

Solution

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

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

GUI screens fail to open when running Installer

Symptom

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

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

Solution

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

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

Symptom

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

Solution

In SIM Database, in the RK_CONFIG 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.

SIM-WS URL fails with Error: SIMFaultApiMessage: An Error occurred accessing StoreServices in Clustered Environment

Symptom

SIM-WS URL fails with this error message “SIMFaultApiMessage: An Error occurred accessing StoreServices.” when Node1 is down and Node 2 is down. The SIM Client is not affected in this scenario.

Solution

Login to the Node 1 server and correct jndi.cfg with its own (Node1) hostname instead of Node 2 hostname. Jndi.cfg is available inside sim-server-resources.jar. in the following location on the server.

Location: <WLS_DOMAIN_HOME>/servers/<sim-server>/tmp/_WL_user/sim-server/<exsx6p>/lib>/sim-server-resources.jar

The hostname will appear in jndi.cfg in the value of NAMING_SERVER_URL as below.

# The URL for the naming server (Required)

NAMING_SERVER_URL=t3://<hostname>:<port>

> **IMPORTANT:** Take a back up of sim-server-resources.jar before any changes.

You will need to unjar the sim-server-resources.jar, update the jndi.cfg file with the correct Node 1 hostname and rejar sim-server-resources.jar.

After the update is done, restart the Node 1 server.

The “TEST page” link in SIM-WS URL fails with Error: 404

Symptom

The “TEST page” link shown in the SIM-WS URL (http://<simserver:port>/sim-ws/simWebService) fails with “Error: 404 Not Found” error.

Solution

This is a known issue. This does not indicate any SIM-WS failure.

Installer fails with sun.security.validator.KeyStores exception

Symptom

Installer first throws the error

```
Exception in thread "main" java.lang.NoClassDefFoundError:
sun.security.validator.KeyStores
```

And then on continuing aborts with the same error.

Solution

OCM does not work on AIX 7.1. The workaround after facing this exception, is to recreate the INSTALL_DIR and then delete the **"retail-OCM-withAnt.zip"** file present in INSTALL_DIR/sim directory **before** running the installer.

E

Appendix: Setting up SIM Reports in BI Publisher

SIM 13.2.9 reports now supports ONLY BI Publisher 11g.

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

Note: If BI Publisher application 11g is already deployed to a BI Publisher managed server in WebLogic, you can directly go to the "BI Publisher 11g – Configuring the SIM JDBC connection" section. If not, continue with the "BI Server Component Installation Tasks".

BI Publisher 11g – BI Server Component Installation Tasks

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

If you are installing BI Publisher as a part the Oracle BI EE suite (which you will if installing BI Publisher 11g), refer to the appropriate Fusion Middleware guides for the installation of the product in a WebLogic server environment. Otherwise, you must perform the steps described in the next section to deploy Oracle BI Publisher 10g as a standalone web application into a WebLogic server environment.

BI Publisher 11g – Installation Process Overview

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

1. Run RCU to create BI Publisher related database schemas and other db objects.
2. Install Oracle BI EE under an existing WebLogic Server (WLS) 10.3.6 and choose “software only install”.
3. Configure Oracle BI EE, create default bifoundation_domain and configure component “Business Intelligence Publisher” only.
4. Select the BIPlatform schema for update of the ORACLE 11.2.0.4 and/or 12.1.0.2 DB
5. Configure ports and document and test the URL’s that are created.

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

6. Configure the BI Publisher repository. Set security model, add users, assign roles, add reports, add printers, set repository path, set data source, etc.
7. Set up the SIM reports in BI Publisher report repository.
8. Set up for the SIM application specific configuration files to integrate BI Publisher.

BI Publisher 11g – Install Oracle BI EE 11g

1. Run the Repository Creation Utility to create the BI Publisher-related database schemas and other database objects. Create the BIPlatform schema into an existing ORACLE 11.2.0.4 and/or 12.1.0.2 DB

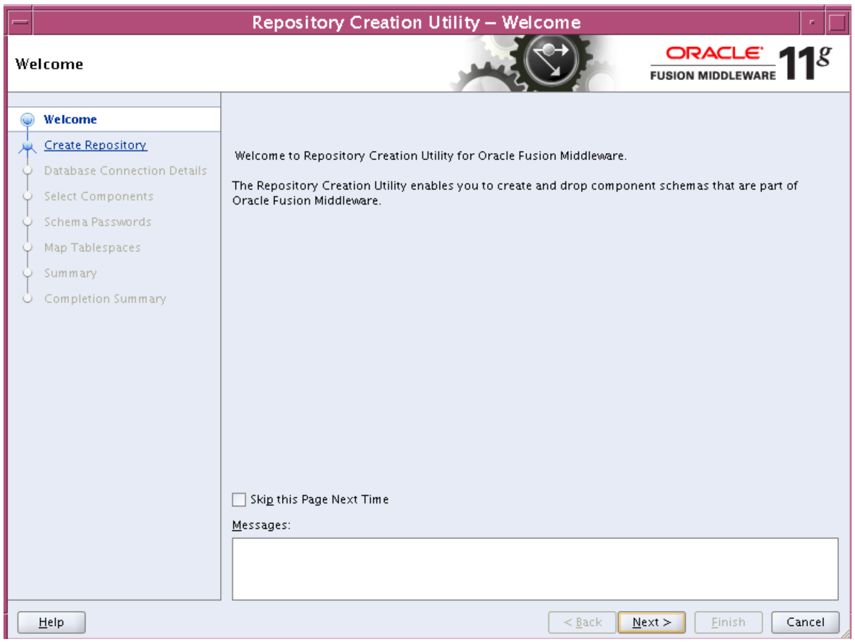
   Note: Download Repository Creation Utility software from http://www.oracle.com/technetwork/middleware/bi-enterprise-edition/downloads/bi-downloads-1525270.html. Install it on your desktop

2. Export your DISPLAY.

   Ex: Export DISPLAY=10.141.10.110:0.0
3. Go to $RCU_HOME/bin

   Ex: /linux/x86_64/ofm_11g/RCU_11.1.1.7/rcuHome/bin>

   ```
   Start RCU:  ./rcu
   ```



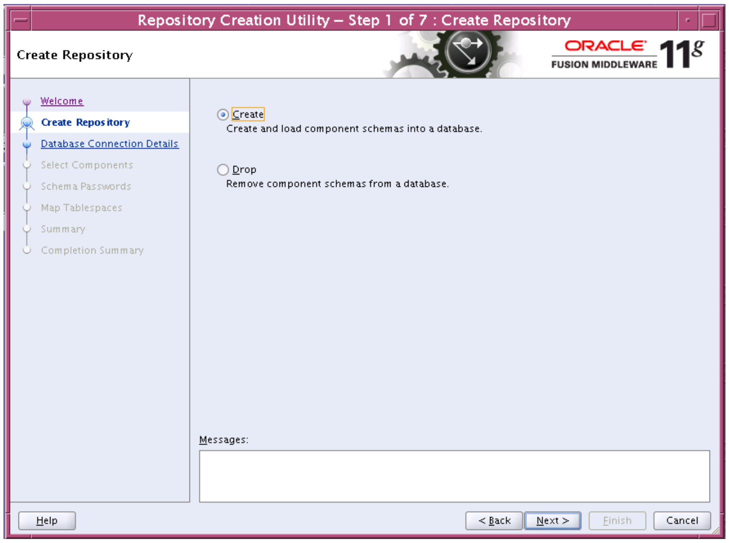
Welcome to Repository Creation Utility for Oracle Fusion Middleware.

The Repository Creation Utility enables you to create and drop component schemas that are part of Oracle Fusion Middleware.

□ Skip this Page Next Time

Messages:

4. Click Next.

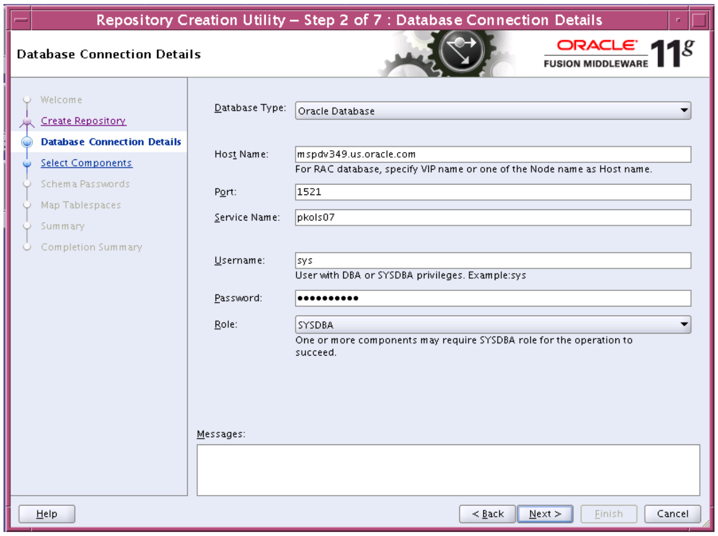


● Create
Create and load component schemas into a database.

○ Drop
Remove component schemas from a database.

Messages:

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


Repository Creation Utility – Step 2 of 7 : Database Connection Details
Database Connection Details
ORACLE FUSION MIDDLEWARE 11g
Welcome
Create Repository
Database Connection Details
Select Components
Schema Passwords
Map Tablespaces
Summary
Completion Summary
Help
< Back
Next >
Finish
Cancel

Database Type: Oracle Database

Host Name: mspdv349.us.oracle.com
For RAC database, specify VIP name or one of the Node name as Host name.

Port: 1521

Service Name: pkols07

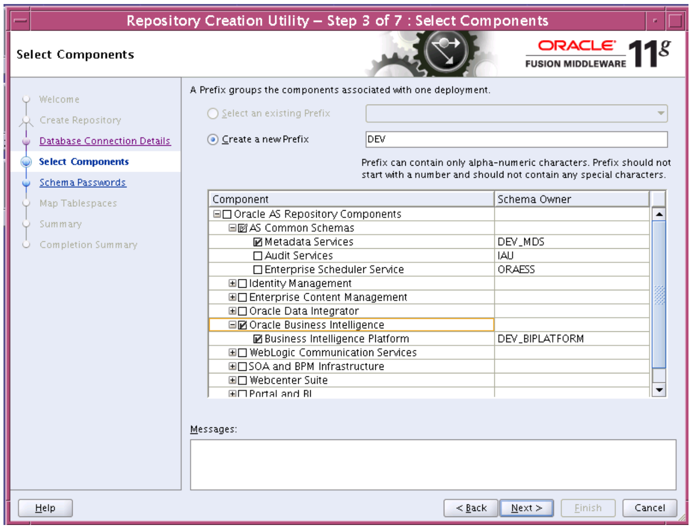
Username: sys
User with DBA or SYSDBA privileges. Example:sys

Password: ●●●●●●●●●●

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

Messages:

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



A Prefix groups the components associated with one deployment.

○ Select an existing Prefix

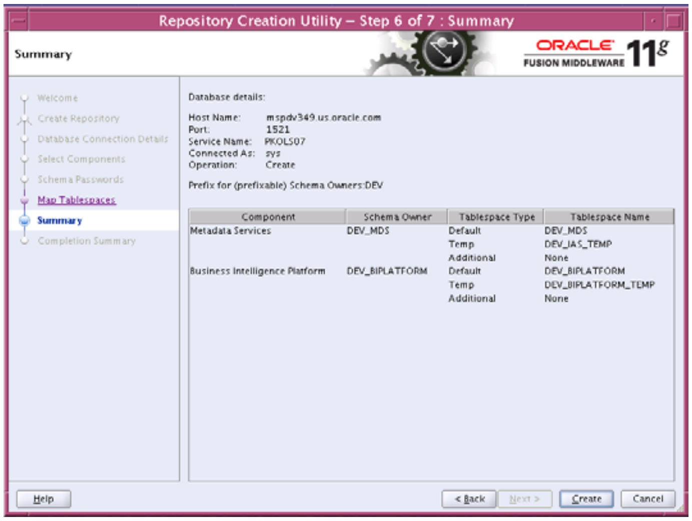
● Create a new Prefix DEV

Prefix can contain only alpha-numeric characters. Prefix should not start with a number and should not contain any special characters.

Component	Schema Owner
⊟☐ Oracle AS Repository Components	
⊟☑ AS Common Schemas	
☑ Metadata Services	DEV_MDS
☐ Audit Services	IAU
☐ Enterprise Scheduler Service	ORAESS
⊞☐ Identity Management	
⊞☐ Enterprise Content Management	
⊞☐ Oracle Data Integrator	
⊟☑ Oracle Business Intelligence	
☑ Business Intelligence Platform	DEV_BIPLATFORM
⊞☐ WebLogic Communication Services	
⊞☐ SOA and BPM Infrastructure	
⊞☐ Webcenter Suite	
⊞☐ Portal and BI	

Messages:

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



Database details:

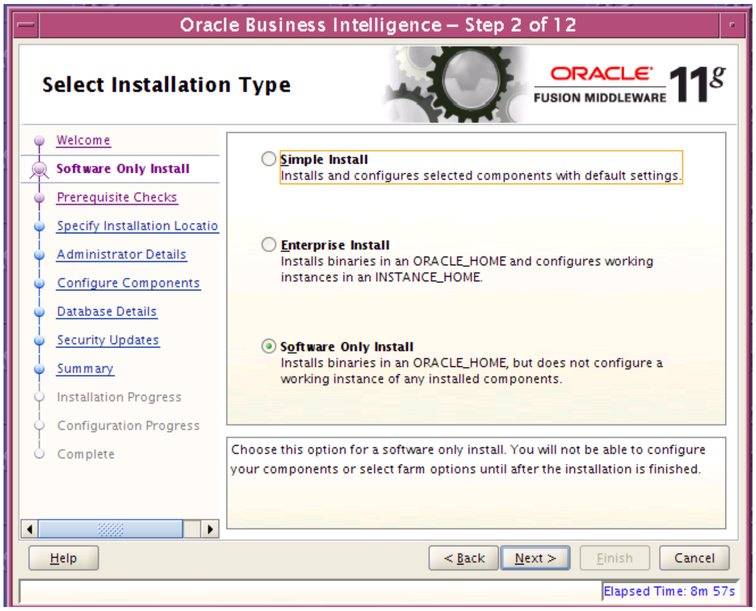
Host Name: mspdv349.us.oracle.com
Port: 1521
Service Name: PKOLS07
Connected As: sys
Operation: Create

Prefix for (prefixable) Schema Owners:DEV

Component	Schema Owner	Tablespace Type	Tablespace Name
Metadata Services	DEV_MDS	Default	DEV_MDS
		Temp	DEV_IAS_TEMP
		Additional	None
Business Intelligence Platform	DEV_BIPLATFORM	Default	DEV_BIPLATFORM
		Temp	DEV_BIPLATFORM_TEMP
		Additional	None

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

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



Oracle Business Intelligence – Step 2 of 12

Select Installation Type

○ Simple Install
Installs and configures selected components with default settings.

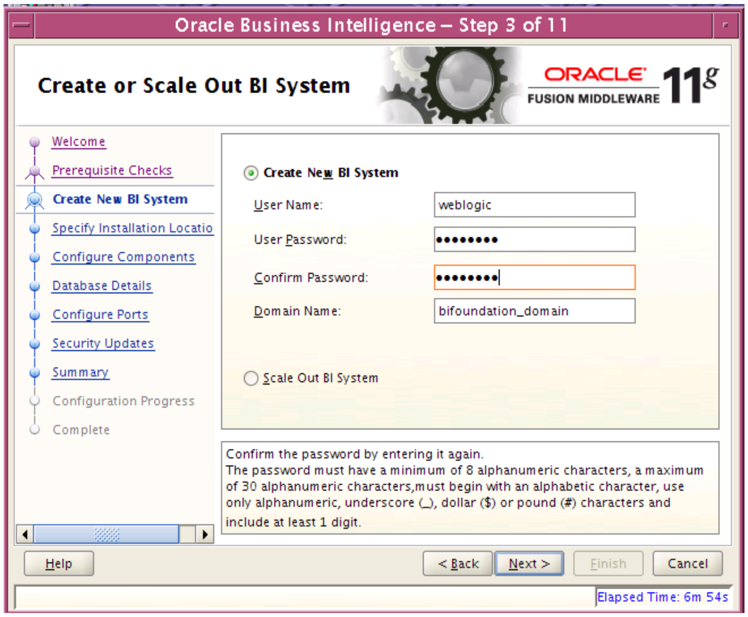
○ Enterprise Install
Installs binaries in an ORACLE_HOME and configures working instances in an INSTANCE_HOME.

● Software Only Install
Installs binaries in an ORACLE_HOME, but does not configure a working instance of any installed components.

Choose this option for a software only install. You will not be able to configure your components or select farm options until after the installation is finished.

Elapsed Time: 8m 57s

10. Configure Oracle BI EE, create default bifoundation_domain and configure component “Business Intelligence Publisher” only.



Oracle Business Intelligence – Step 3 of 11

Create or Scale Out BI System

● Create New BI System

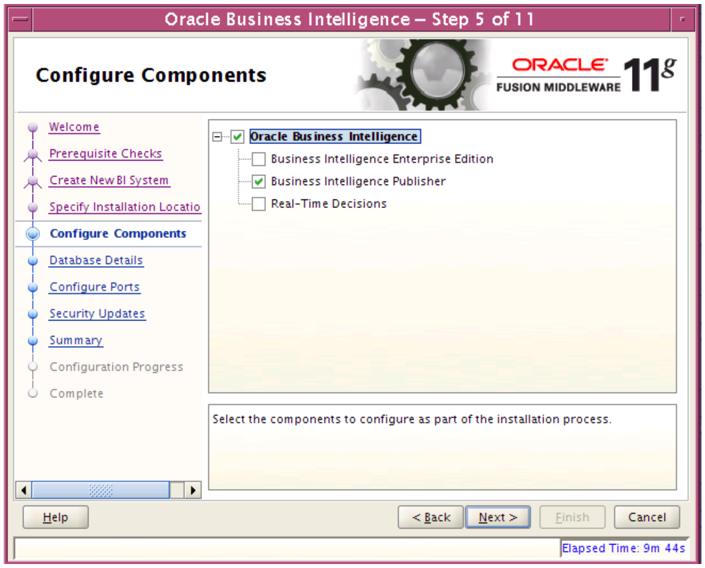
User Name: weblogic
User Password: ••••••••
Confirm Password: ••••••••
Domain Name: bifoundation_domain

○ Scale Out BI System

Confirm the password by entering it again.
The password must have a minimum of 8 alphanumeric characters, a maximum of 30 alphanumeric characters,must begin with an alphabetic character, use only alphanumeric, underscore (_), dollar ($) or pound (#) characters and include at least 1 digit.

Elapsed Time: 6m 54s

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



Oracle Business Intelligence – Step 5 of 11

Configure Components

☑ Oracle Business Intelligence
☐ Business Intelligence Enterprise Edition
☑ Business Intelligence Publisher
☐ Real-Time Decisions

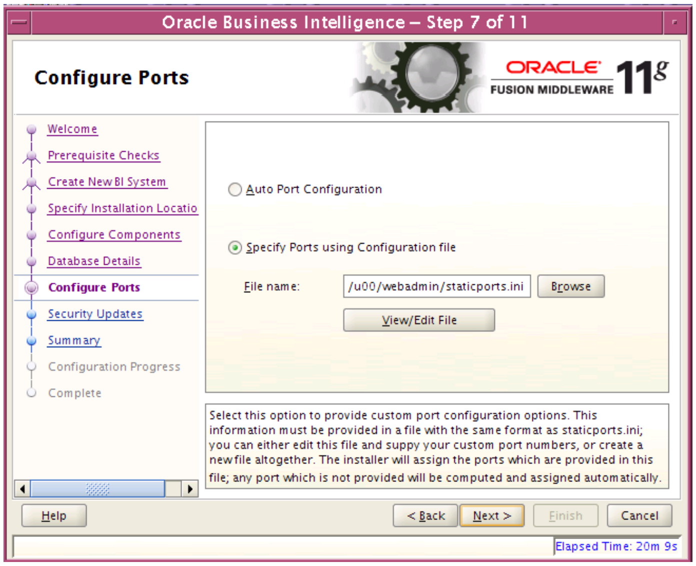
Select the components to configure as part of the installation process.

Elapsed Time: 9m 44s

12. On the Configure Components screen, select only “Business Intelligence Publisher”

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

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



Oracle Business Intelligence – Step 7 of 11

Configure Ports

○ Auto Port Configuration

● Specify Ports using Configuration file

File name: /u00/webadmin/staticports.ini

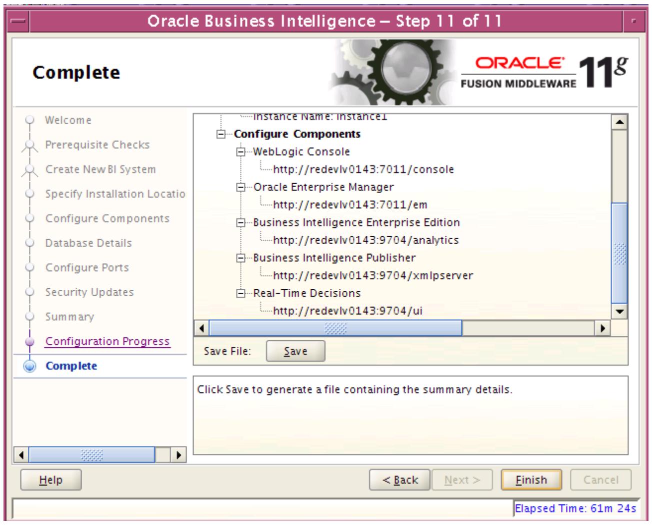
Select this option to provide custom port configuration options. This information must be provided in a file with the same format as staticports.ini; you can either edit this file and suppy your custom port numbers, or create a new file altogether. The installer will assign the ports which are provided in this file; any port which is not provided will be computed and assigned automatically.

Elapsed Time: 20m 9s

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

15. Document and test the URLs that are created.

This screen contains the URL’s for the components that got installed.

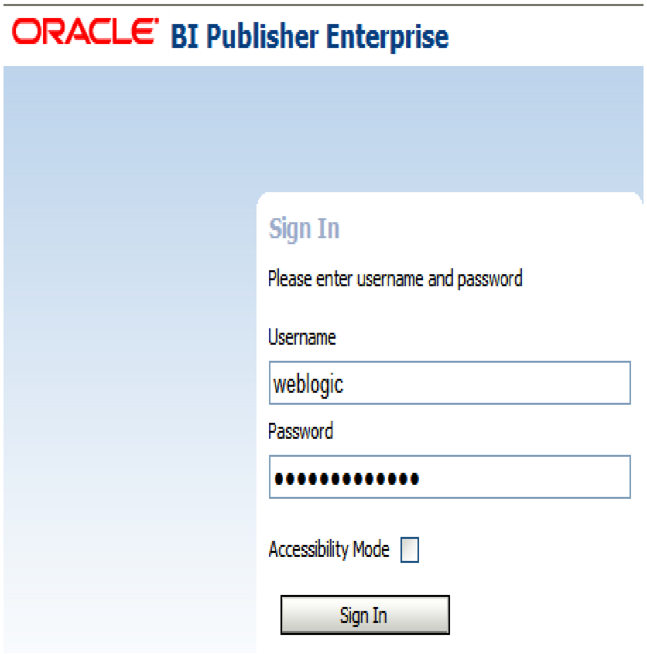


```
Instance Name: instance1
⊟ Configure Components
   ⊟ WebLogic Console
      http://redevlv0143:7011/console
   ⊟ Oracle Enterprise Manager
      http://redevlv0143:7011/em
   ⊟ Business Intelligence Enterprise Edition
      http://redevlv0143:9704/analytics
   ⊟ Business Intelligence Publisher
      http://redevlv0143:9704/xmlpserver
   ⊟ Real-Time Decisions
      http://redevlv0143:9704/ui
```

Click Save to generate a file containing the summary details.

Elapsed Time: 61m 24s

16. Save this screen, so that you know the right URL's for your installation.
17. To test your BI Publisher installation, launch xmlpserver. Login with the credentials you entered in your Oracle BI EE configuration (weblogic / password).

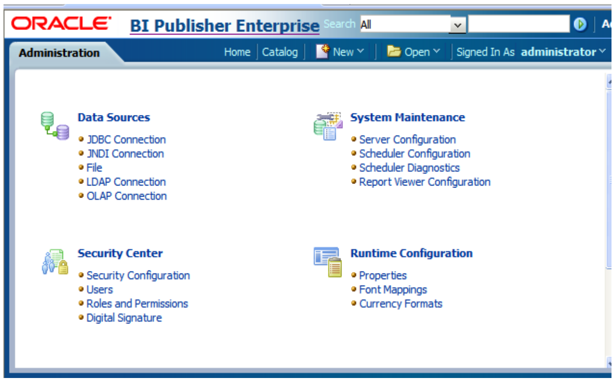


Please enter username and password

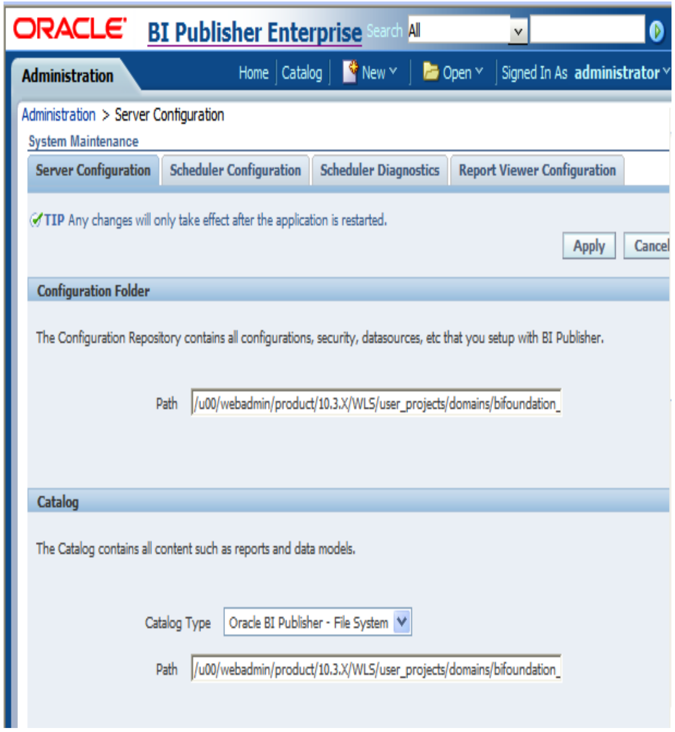
Username: weblogic

Password: •••••••••••••

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



19. On the System Maintenance Section, press Server Configuration
20. Navigate to the Configuration Screen.



TIP Any changes will only take effect after the application is restarted.

The Configuration Repository contains all configurations, security, datasources, etc that you setup with BI Publisher.

Path /u00/webadmin/product/10.3.X/WLS/user_projects/domains/bifoundation_

The Catalog contains all content such as reports and data models.

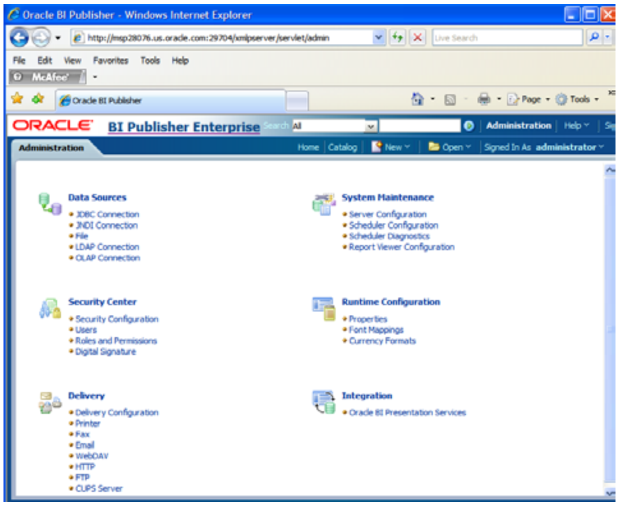
Catalog Type Oracle BI Publisher - File System

Path /u00/webadmin/product/10.3.X/WLS/user_projects/domains/bifoundation_

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

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

    ```
    $OBIEE_HOME/WLS/user_projects/domains/bifoundation_domain/config/bipublisher/r
    epository
    ```
22. Post install step: Set BI Publisher security model


Oracle BI Publisher - Windows Internet Explorer
http://msp28076.us.oracle.com:29704/xmlpserver/servlet/admin
Live Search
File Edit View Favorites Tools Help
McAfee
Oracle BI Publisher
Page Tools
ORACLE BI Publisher Enterprise Search All
Administration Help
Administration
Home Catalog New Open Signed In As administrator

Data Sources
- JDBC Connection
- JNDI Connection
- File
- LDAP Connection
- OLAP Connection

System Maintenance
- Server Configuration
- Scheduler Configuration
- Scheduler Diagnostics
- Report Viewer Configuration

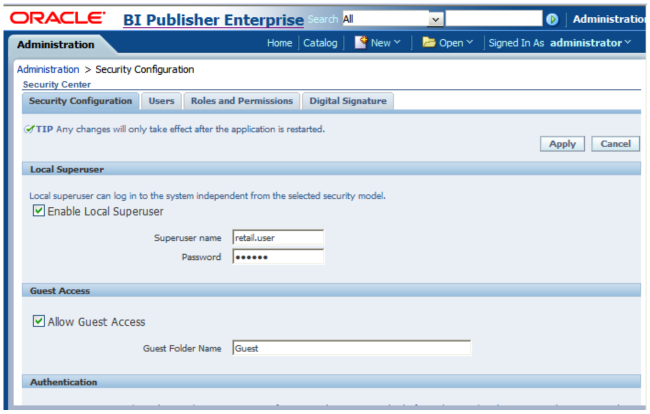
Security Center
- Security Configuration
- Users
- Roles and Permissions
- Digital Signature

Runtime Configuration
- Properties
- Font Mappings
- Currency Formats

Delivery
- Delivery Configuration
- Printer
- Fax
- Email
- WebDAV
- HTTP
- FTP
- CUPS Server

Integration
- Oracle BI Presentation Services

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



Administration > Security Configuration

Security Center

TIP Any changes will only take effect after the application is restarted.

Local Superuser

Local superuser can log in to the system independent from the selected security model.

☑ Enable Local Superuser

Superuser name: retail.user

Password: ••••••

Guest Access

☑ Allow Guest Access

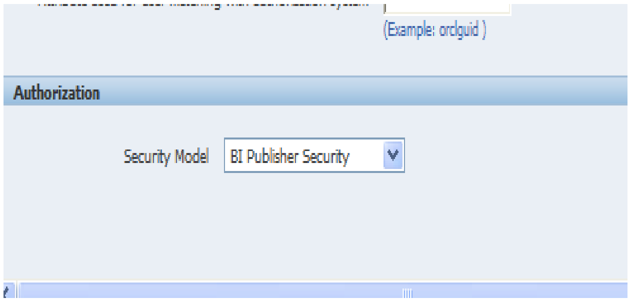
Guest Folder Name: Guest

Authentication

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

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

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



(Example: orclguid)

Authorization

Security Model: BI Publisher Security

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

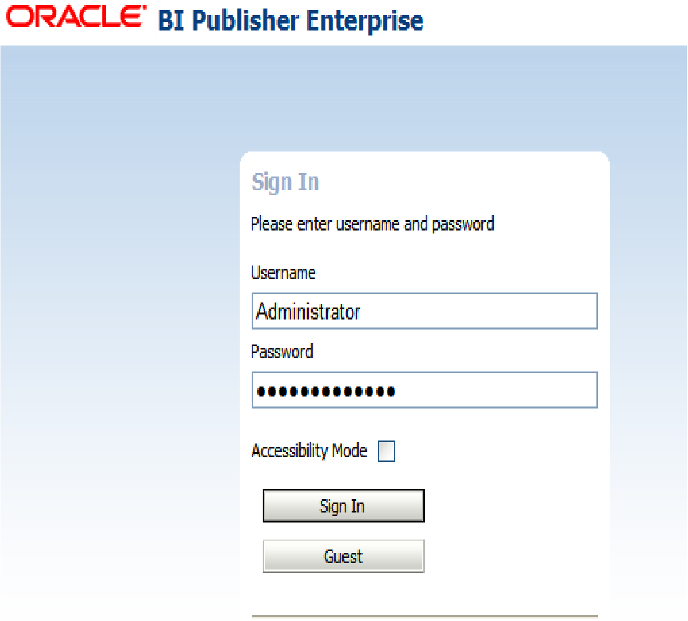
f. The default user name for the BI Publisher Security Model is Administrator

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

h. Save the changes and re-start the BI Publisher server.

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

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


ORACLE BI Publisher Enterprise
Sign In
Please enter username and password
Username
Password
Accessibility Mode □
Sign In
Guest

Username: Administrator

Password: ●●●●●●●●●●●●●

23. Post install step: Set the repository path.

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

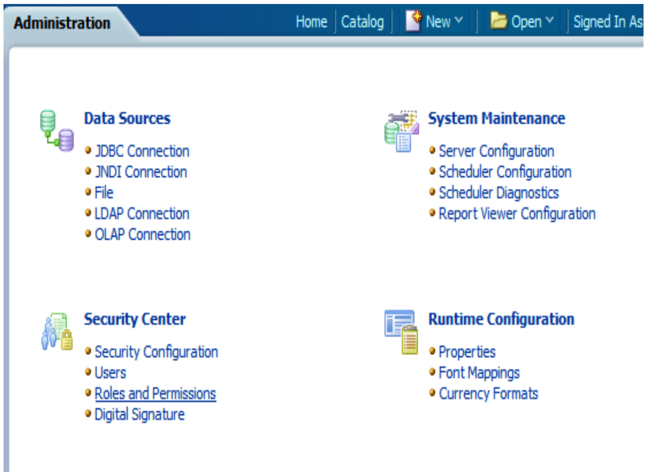
    ```
    $OBIEE/wls/user_projects/domains/bifoundation_domain/config/bipublisher/reposi
    tory
    ```

    In the repository you will see the following directories:

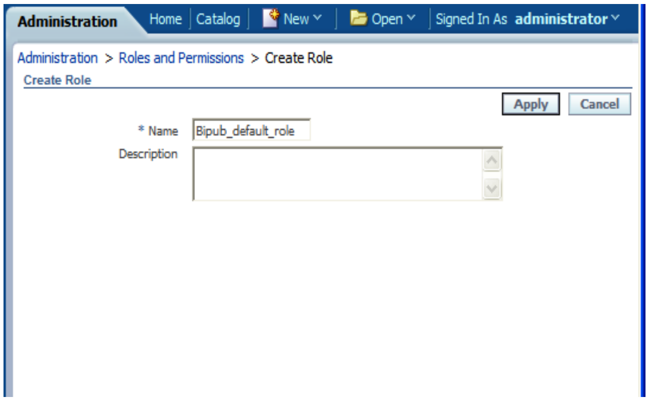
    - Admin
    - DemoFiles
    - Reports
    - Tools
    - Users

24. Post install step: Create role Bipub_default_role.

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



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


Administration
Home
Catalog
New
Open
Signed In As administrator
Administration > Roles and Permissions > Create Role
Create Role
Apply
Cancel

* Name: Bipub_default_role

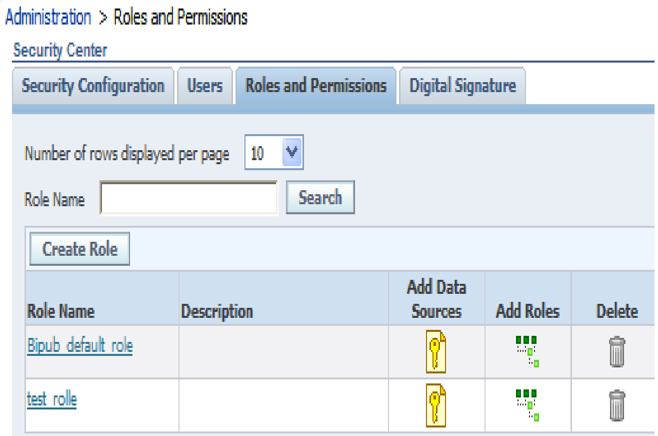
Description:

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.

25. 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:

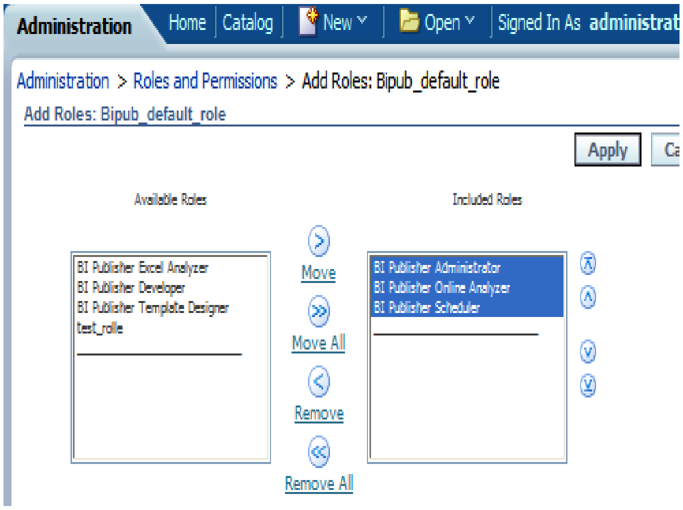


Number of rows displayed per page: 10

Role Name:

Role Name	Description	Add Data Sources	Add Roles	Delete
Bipub_default_role		🔑	▦	🗑
test_rolle		🔑	▦	🗑

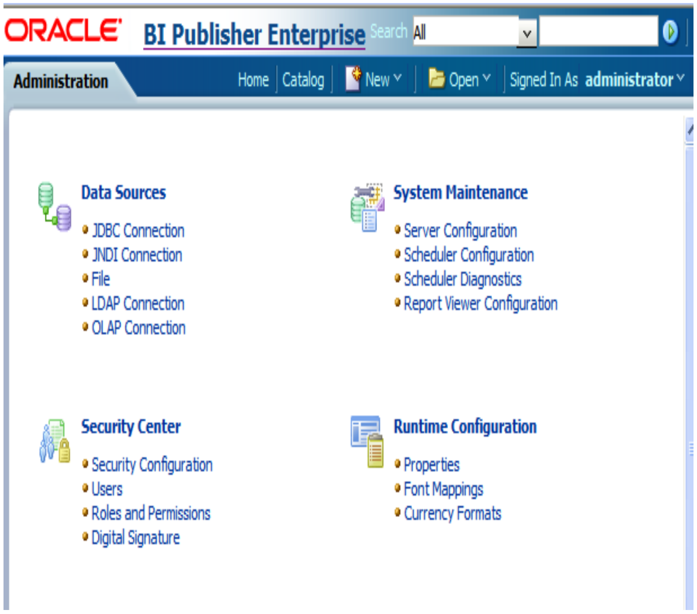
b. On the Roles and Permissions screen you should see the new role created: “Bipub_default_role”. Add multiple roles to the Bipub_Default_Role by pressing the corresponding green icon on the Add Roles column


Administration
Home
Catalog
New
Open
Signed In As administrat
Administration > Roles and Permissions > Add Roles: Bipub_default_role
Add Roles: Bipub_default_role
Apply
Ca
Available Roles
BI Publisher Excel Analyzer
BI Publisher Developer
BI Publisher Template Designer
test_role
Move
Move All
Remove
Remove All
Included Roles
BI Publisher Administrator
BI Publisher Online Analyzer
BI Publisher Scheduler

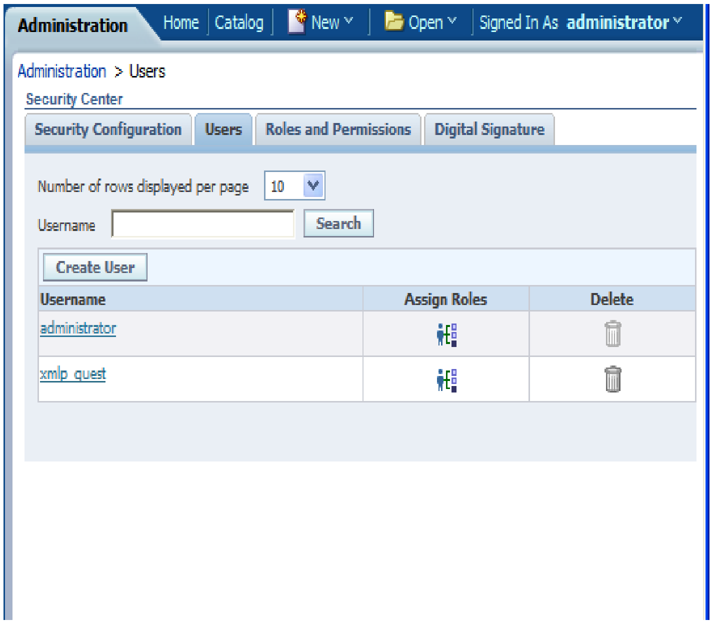
c. From the “Available Roles” panel, select the ones needed for your reports and move them to the “Included Roles” panel

d. Press the Apply button to save your changes.

26. 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



Number of rows displayed per page 10

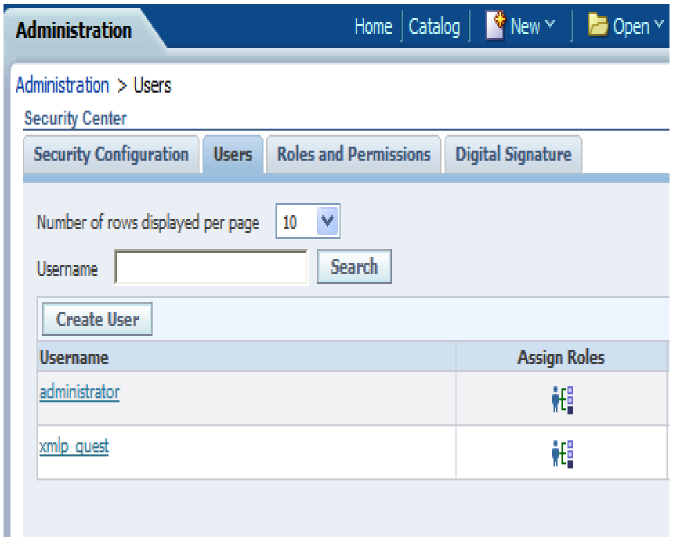
Username

Username	Assign Roles	Delete
administrator		
xmlp_guest		

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

27. Post install step: Adding the Bipub_default_role to XMLP_GUEST user.

a. Open the Users section:

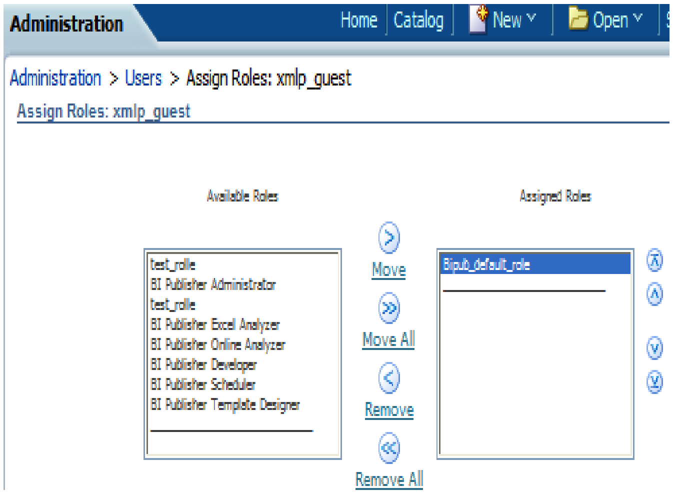


Number of rows displayed per page 10

Username

Username	Assign Roles
administrator	
xmlp_guest	

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



Administration > Users > Assign Roles: xmlp_guest

Assign Roles: xmlp_guest

Available Roles

- test_rolle
- BI Publisher Administrator
- test_rolle
- BI Publisher Excel Analyzer
- BI Publisher Online Analyzer
- BI Publisher Developer
- BI Publisher Scheduler
- BI Publisher Template Designer

Assigned Roles

- Bipub_default_role

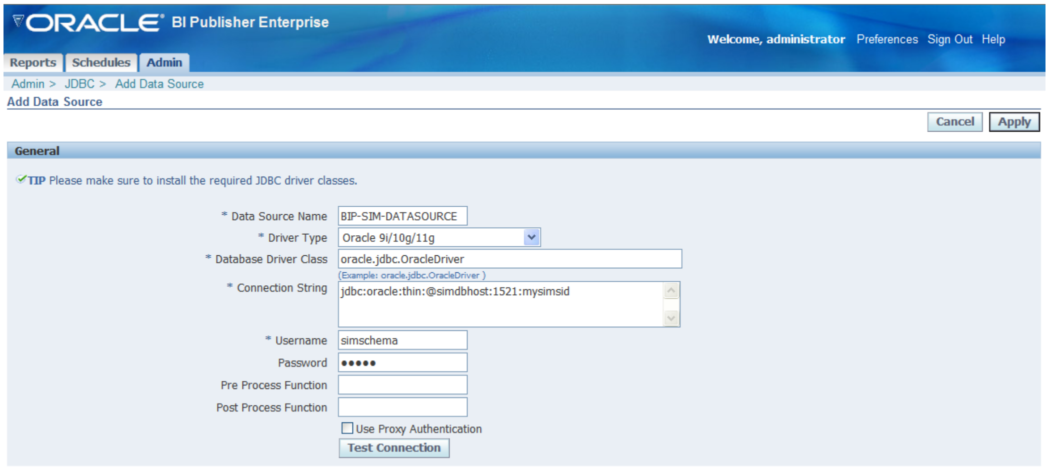
c. On the Assign Roles screen, select the BiPub_default_role from the Available Roles panel to the "Assigned Roles" panel and press the Apply button to save your changes.

BI Publisher 11g – Configuring the SIM JDBC connection

Log in to BI Publisher as the Administrator user. The instructions below are valid for BI Publisher 11g.

Create the data source for BI Publisher to connect to the SIM schema.

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



Admin > JDBC > Add Data Source

Add Data Source

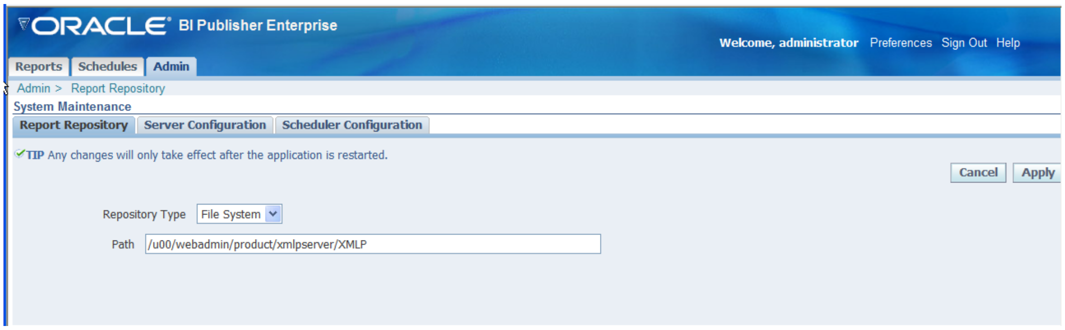
General

TIP Please make sure to install the required JDBC driver classes.

* Data Source Name	BIP-SIM-DATASOURCE
* Driver Type	Oracle 9i/10g/11g
* Database Driver Class	oracle.jdbc.OracleDriver (Example: oracle.jdbc.OracleDriver)
* Connection String	jdbc:oracle:thin:@simdbhost:1521:mysimsid
* Username	simschema
Password	•••••
Pre Process Function	
Post Process Function	
	□ Use Proxy Authentication

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

2. Click the Admin tab. Under System Maintenance, click the Report Repository link. This will show where the reports are located on the server running BI Publisher:



TIP Any changes will only take effect after the application is restarted.

Repository Type: File System

Path: /u00/webadmin/product/xmlpserver/XMLP

Note: If using BI Publisher 11g, the Report Repository is available at Administration->System Maintenance->Server Configuration.

The Path given is in the base directory for all the BIP reports.

11g example: /u00/webadmin/product/10.3.X/WLS/user_projects/domains/bifoundation_domain/config/bipublisher/repository/

3. Manually copy SIM Reports to Reports repository

The SIM reports will be copied to the 'Guest' location. Create a directory named 'SIM13' under 'Guest' and copy the reports into 'SIM13' directory:

```
BIPublisher 11g example,
/u00/webadmin/product/10.3.X/WLS/user_projects/domains/bifoundation_domain/con
fig/bipublisher/repository/Reports/Guest/SIM13
```

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

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

```
cp <SIM13.2.9_MEDIA>/sim/application/sim13/reports/sim-reports.zip <TEMP_DIR>
Where <TEMP_DIR> is a temporary directory where extract sim-reports.zip is
extracted.
 cd <TEMP_DIR>
unzip sim-reports.zip
cd <TEMP_DIR>/bip11g
cp *
/u00/webadmin/product/10.3.X/WLS/user_projects/domains/bifoundation_domain/config/
bipublisher/repository/Reports/Guest/SIM13
```

All the individual reports are available in their own zip files when the sim-reports.zip file is extracted:

```
AGSNDefaultReport.zip                    ItemTicketQRCodeReport.zip      sim-
reports.zip
BolReturnReport.zip                      ItemTicketReport1.zip
StockCountAllLocReport.zip
BolTransferReport.zip                    ItemTicketReport2.zip
StockCountExportReport.zip
DirectDeliveryDiscrepantItemsReport.zip  ItemUDATicketDefaultReport.zip
StockCountRejectedItemReport.zip
DirectDeliveryReport.zip                 PickListReport.zip
StockCountReport.zip
InventoryAdjustmentReport.zip            ReturnReport.zip
StoreOrderReport.zip
```

```
ItemBasketDefaultReport.zip              ShelfLabelDefaultReport.zip
TransferReport.zip
ItemDetailReport.zip                     ShelfLabelQRCodeReport.zip
WarehouseDeliveryReport.zip
ItemRequestReport.zip                    ShelfLabelReport1.zip
ItemTicketDefaultReport.zip              ShelfLabelReport2.zip
```

Each file needs to be unzipped in its own directory of the same name as the report. For example, to get the AGSNDefaultReport into place:

```
# mkdir AGSNDefaultReport
# mv AGSNDefaultReport.zip AGSNDefaultReport
# cd AGSNDefaultReport
# unzip AGSNDefaultReport.zip
Archive:  AGSNDefaultReport.zip
  inflating: AGSNDefaultReport.xdo
  inflating: AGSNBatchDefaultTemplate.rtf
# ls
AGSNBatchDefaultTemplate.rtf  AGSNDefaultReport.xdo  AGSNDefaultReport.zip
```

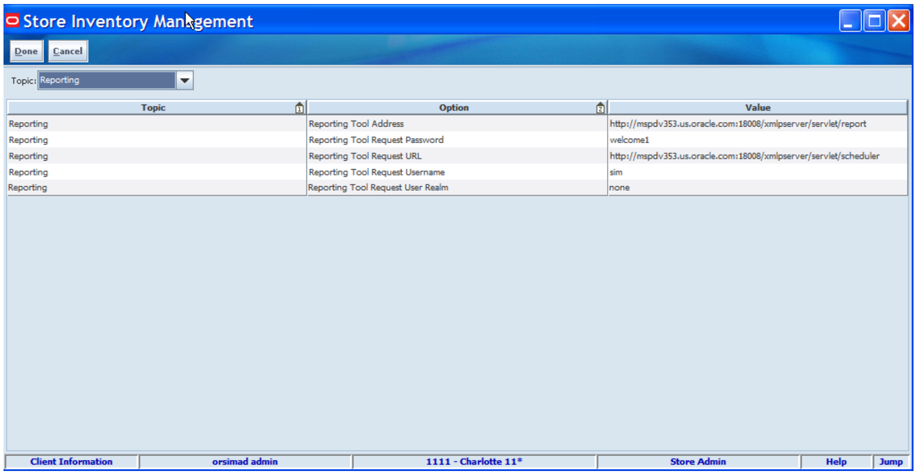
This needs to be done for all the reports. Once this is done all the zip files can be removed, they are not used.

Bounce the Bipub 11g application. The new SIM reports should be available in the “Shared Folders > Guest > SIM13” location of BI Publisher.

BI Publisher 11g – Configuring the SIM Application with BI Publisher:

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

From Admin, go to setup -> store admin. Select the reporting topic:



Topic: Reporting

Topic	Option	Value
Reporting	Reporting Tool Address	http://mspdv353.us.oracle.com:18008/xmlpserver/servlet/report
Reporting	Reporting Tool Request Password	welcome1
Reporting	Reporting Tool Request URL	http://mspdv353.us.oracle.com:18008/xmlpserver/servlet/scheduler
Reporting	Reporting Tool Request Username	sim
Reporting	Reporting Tool Request User Realm	none

Change the above URLs to match the host and port of where BI Publisher is running, along with the username/password it needs to log into the BI Publisher app.

> **Note:** This is not a global setting and will need to be done for each store.

The above info is put into these fields of the RK_STORE_CONFIG table of the SIM schema for each store in the database:

REPORTING_TOOL_ADDRESS

REPORTING_TOOL_REQUEST_PASSWORD

REPORTING_TOOL_REQUEST_URL

REPORTING_TOOL_REQUEST_USERNAME

REPORTING_TOOL_REQUEST_USERREALM

Validating Reports

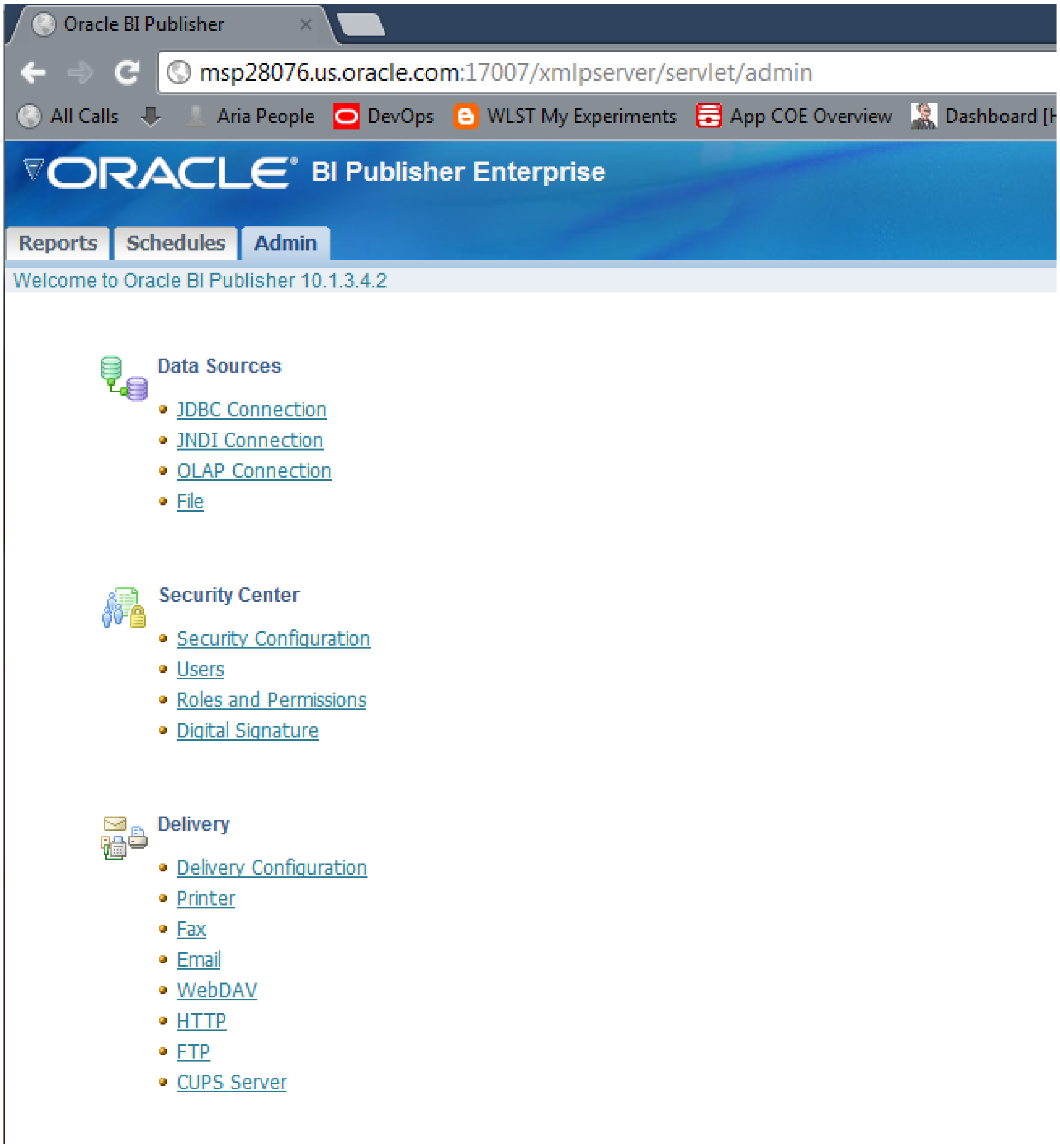
To test the reports, log into SIM application and click Reports. It should launch BI Publisher in a browser window. You can navigate to the SIM13 reports in BI Publisher window.

Configuring SIM for CUPS printers using BI Publisher 11g

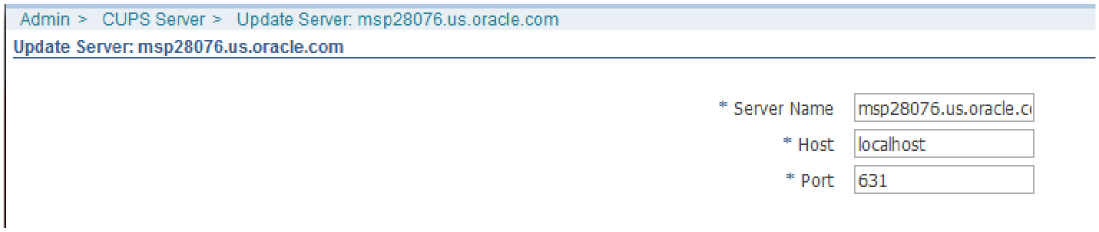
Prerequisite: CUPS printer has to be set up on the BI Publisher server.

1. Login to BI Publisher using Administrator user and navigate to Administrator user.

   Example: http://orappsrv.us.oracle.com:17007/xmlpserver
2. Click on the CUPS servers.



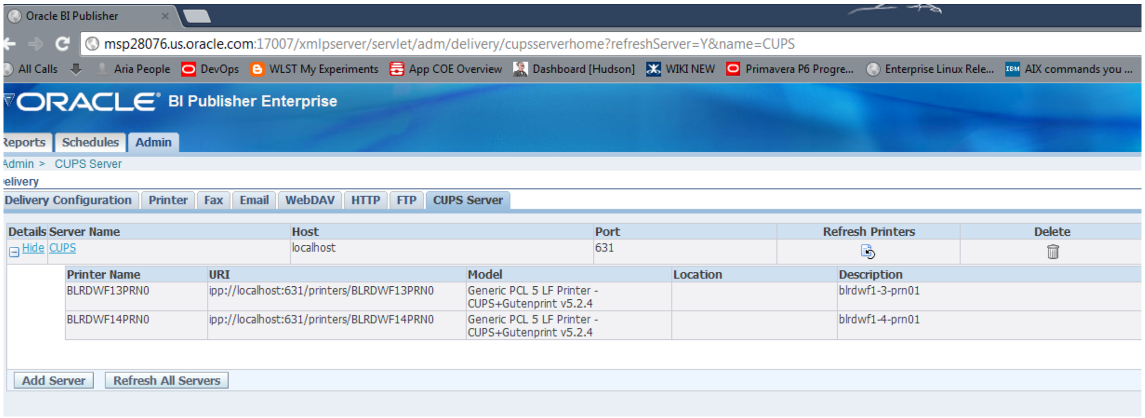
3. Click Add Servers.



Update Server: msp28076.us.oracle.com

* Server Name	msp28076.us.oracle.c
* Host	localhost
* Port	631

4. After adding, refresh the servers and printers.



msp28076.us.oracle.com:17007/xmlpserver/servlet/adm/delivery/cupsserverhome?refreshServer=Y&name=CUPS

Details	Server Name	Host	Port	Refresh Printers	Delete
⊟ Hide	CUPS	localhost	631		

Printer Name	URI	Model	Location	Description
BLRDWF13PRN0	ipp://localhost:631/printers/BLRDWF13PRN0	Generic PCL 5 LF Printer - CUPS+Gutenprint v5.2.4		blrdwf1-3-prn01
BLRDWF14PRN0	ipp://localhost:631/printers/BLRDWF14PRN0	Generic PCL 5 LF Printer - CUPS+Gutenprint v5.2.4		blrdwf1-4-prn01

F

Appendix: Oracle Single Sign-On for Oracle Application Server (OAS)

Single Sign-On (SSO) is a term for the ability to sign onto multiple web applications via a single user ID/Password. There are many implementations of SSO – Oracle currently provides three different implementations: Oracle Single Sign-On (SSO), Java SSO (with the 10.1.3.1 release of OC4J) and Oracle Access Manager (provides more comprehensive user access capabilities).

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

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

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

What Do I Need for Oracle Single Sign-On?

The nexus of an Oracle Single Sign-On system is the Oracle Identity Management Infrastructure installation. This consists of the following components:

- An Oracle Internet Directory (OID) LDAP server, used to store user, role, security, and other information. OID uses an Oracle database as the back-end storage of this information.
- An Oracle Single Sign-On servlet, used to authenticate the user and create the SSO session cookie. This servlet is deployed within the infrastructure Oracle Application Server (OAS)
- The Delegated Administration Services (DAS) application, used to administer users and group information. This information may also be loaded or modified via standard LDAP Data Interchange Format (LDIF) scripts.
- Additional administrative scripts for configuring the OSSO system and registering HTTP servers.

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

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

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

Oracle Single Sign-on Terms and Definitions

This section provides definitions for terms pertaining to Oracle Single Sign-on.

Authentication

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

Dynamically Protected URLs

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

Identity Management Infrastructure

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

MOD_OSSO

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

Oracle Internet Directory

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

Partner Application

A partner application is an application that delegates authentication to the Oracle Identity Management Infrastructure. One such partner application is the Oracle HTTP Server (OHS) supplied with the Oracle Application Server. OHS uses the MOD_OSSO module to configure this functionality.

All partner applications must be registered with the Oracle Single Sign-On server. An output product of this registration is a configuration file the partner application uses to verify a user has been previously authenticated.

Realm

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

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

Statically Protected URLs

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

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

What Single Sign-On is not

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

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

How Oracle Single Sign-On Works

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

- The Oracle Single Sign-On (OSSO) servlet, which is responsible for the back-end authentication of the user.
- The Oracle Internet Directory LDAP server, which stores user IDs, passwords, and group (role) membership.
- The Oracle HTTP Server associated with the web application, which verifies and controls browser redirection to the OSSO servlet.
- If the web application implements dynamic protection, then the web application itself is involved with the OSSO system.

Statically Protected URLs

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

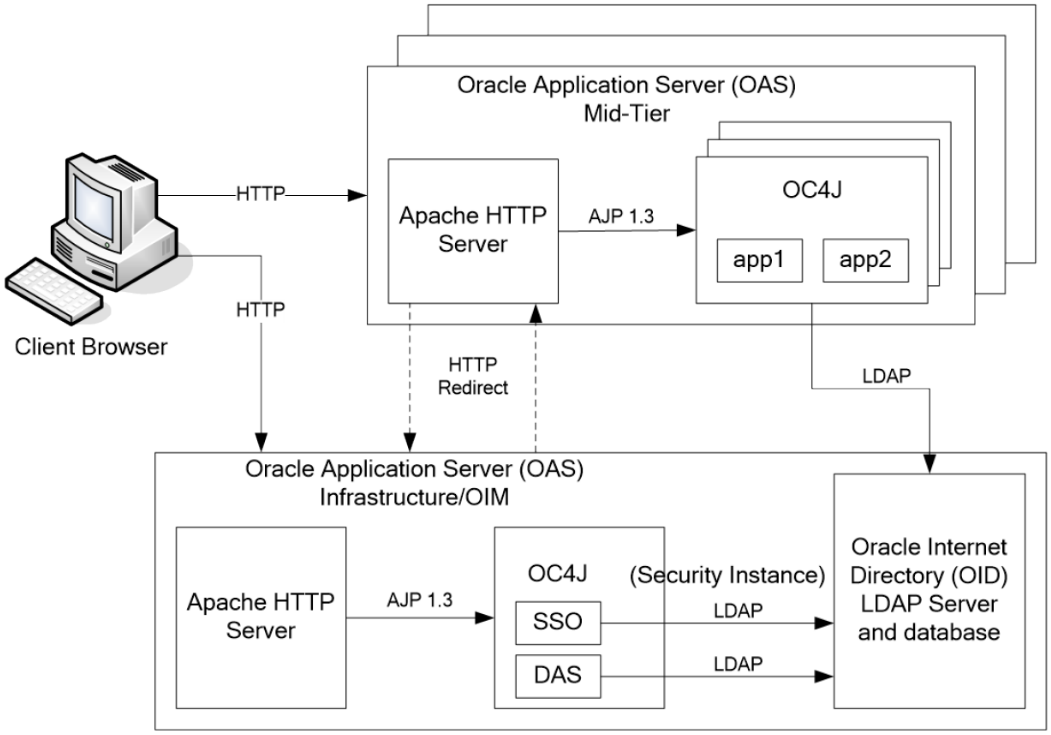
1. The Oracle HTTP server recognizes the user has not been authenticated and redirects the browser to the Oracle Single Sign-On servlet.
2. The OSSO servlet determines the user must authenticate, and displays the OSSO login page.
3. The user must sign in via a valid user ID and password. If the OSSO servlet has been configured to support multiple Realms, a valid realm must also be entered. The user ID, password, and realm information is validated against the Oracle Internet Directory LDAP server.
4. The OSSO servlet creates and sends the user’s browser an OSSO session cookie. This cookie is never persisted to disk and is specific only to the current browser session. This cookie contains the user’s authenticated identity. It does NOT contain the user’s password.
5. The OSSO servlet redirects the user back to the Oracle HTTP Server, along with OSSO specific information.
6. The Oracle HTTP Server decodes the OSSO information, stores it with the user’s session, and allows the user access to the original URL.

Dynamically Protected URLs

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

1. The Oracle HTTP server recognizes the user has not been authenticated, but allows the user to access the URL.
2. The application determines the user must be authenticated and sends the Oracle HTTP server a specific status to begin the authentication process.
3. The Oracle HTTP Server redirects the user's browser session to the OSSO Servlet.
4. The OSSO servlet determines the user must authenticate, and displays the OSSO login page.
5. The user must sign in via a valid user ID and password. If the OSSO servlet has been configured to support multiple Realms, a valid realm must also be entered. The user ID, password, and realm information is validated against the Oracle Internet Directory LDAP server.
6. The OSSO servlet creates and sends the user's browser an OSSO session cookie. This cookie is never persisted to disk and is specific only to the current browser session. This cookie contains the user's authenticated identity. It does NOT contain the user's password.
7. The OSSO servlet redirects the user back to the Oracle HTTP Server, along with OSSO specific information.
8. The Oracle HTTP Server decodes the OSSO information, stores it with the user's session, and allows the user access to the original URL.

Single Sign-on Topology



Installation Overview

Installing Oracle Single Sign-On consists of installing the following components:

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

   The Infrastructure OAS includes the Delegated Administration Services (DAS) application as well as the OSSO servlet. The DAS application can be used for user and realm management within OID.
2. Installing additional OAS 10.1.2 midtier instances for the Oracle Retail applications, such as RMS, that are based on Oracle Forms technologies. These instances must be registered with the Infrastructure OAS installed in step 1).
3. Installing additional application servers to deploy other Oracle Retail applications and performing application specific initialization and deployment activities.

Infrastructure Installation and Configuration

The Infrastructure installation for OSSO is dependent on the environment and requirements for its use. Deploying an Infrastructure OAS to be used in a test environment does not have the same availability requirements as for a production environment. Similarly, the Oracle Internet Directory (OID) LDAP server can be deployed in a variety of different configurations. See the *Oracle Application Server Installation Guide and the Oracle Internet Directory Installation Guide for more details.*

OID User Data

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

The current version of Oracle Single Sign-On only supports OID as its user storage facility. Customers with existing corporate LDAP implementations may need to synchronize user information between their existing LDAP directory servers and OID. OID supports standard LDIF file formats and provides a JNDI compliant set of Java classes as well. Moreover, OID provides additional synchronization and replication facilities to integrate with other corporate LDAP implementations.

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

OID with Multiple Realms

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

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

User Management

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

OID DAS

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

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

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

LDIF Scripts

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

User Data Synchronization

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

Setting up SIM for Single Sign-on

To set up Forms for Single Sign-on, the Forms framework must know and/or be configured to use SSO. To do this, the Forms framework configuration file formsweb.cfg must be configured to enable SSO and the mid-tier HTTP Server must be registered with the Oracle Single Sign-On server. In addition, the Forms framework uses Resource Access Descriptor (RAD), to map OSSO user IDs to Database connect strings.

Configuring formsweb.cfg

For each Forms application instance there are two attributes in the Forms framework configuration file `formsweb.cfg` that control SSO behavior:

Name	Value	Description
ssoMode	true/false	Enables/disables SSO
ssoDynamicResourceCreate	true/false	Enables/disables the dynamic RAD entry creation

Creating a RAD Entry

There are three ways by which a RAD entry (mapping an OSSO user ID to a Database connect string) may be created:

- Administrator Created

  An administrator uses the Delegated Administration Services (DAS) web application that comes with the infrastructure server and that can be launched using the URL http://*<host>:port/oiddas*.

- User Created

  The user can dynamically create a RAD entry when the Forms framework prompts the user for information. This however requires that the ssoDynamicResourceCreate attribute be set to true. If a RAD already exists, the user may also create additional RADs via the DAS application.

- LDIF Script

  More information about how to use an LDIF script to create a RAD entry may be found by accessing My Oracle Support document 244526.1.

G

Appendix: Oracle Single Sign-On for WebLogic

Single Sign-On (SSO) is a term for the ability to sign onto multiple Web applications via a single user ID/Password. There are many implementations of SSO. Oracle currently provides two different implementations: Oracle Single Sign-On (OSSO), and Oracle Access Manager (provides more comprehensive user access capabilities).

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

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

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

What Do I Need for Oracle Single Sign-On?

The nexus of an Oracle Single Sign-On system is the Oracle Identity and Access Management installation. This consists of the following components:

- An Oracle Internet Directory (OID) LDAP server, used to store user, role, security, and other information. OID uses an Oracle database as the back-end storage of this information.
- An Oracle Access Manager (OAM) 11g Release 1 server and administrative console for implementing and configuring policies for single sign-on.
- A Policy Enforcement Agent such as Oracle Access Manager 11g Agent (WebGate) or Oracle Single Sign-On Plug-in, used to authenticate the user and create the Single Sign-On cookies. Some Retail products require a WebGate agent and others require an OSSO plug-in. Both can interoperate in a single OAM environment.
- The Delegated Administration Services (DAS) application in Oracle Forms Services 11g Release 2 and Oracle Directory Services Manager (ODSM) application in OIM11g, used to administer users and group information. This information may also be loaded or modified via standard LDAP Data Interchange Format (LDIF) scripts.
- Additional administrative scripts for configuring the OAM system and registering HTTP servers.

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

Can Oracle Access Manager Work with Other SSO Implementations?

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

Oracle Single Sign-on Terms and Definitions

The following terms apply to single sign-on.

Authentication

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

Dynamically Protected URLs

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

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

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

MOD_OSSO

mod_osso is an Apache Web Server module an Oracle HTTP Server uses to function as a partner application within an Oracle Access Manager environment. The Oracle HTTP Server is based on the Apache HTTP Server.

MOD_WEBLOGIC

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

Oracle Access Manager 11g Agent (WebGate)

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

Oracle Internet Directory

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

Partner Application

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

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

Realm

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

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

Statically Protected URLs

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

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

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

What Single Sign-On is not

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

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

How Oracle Single Sign-On Works

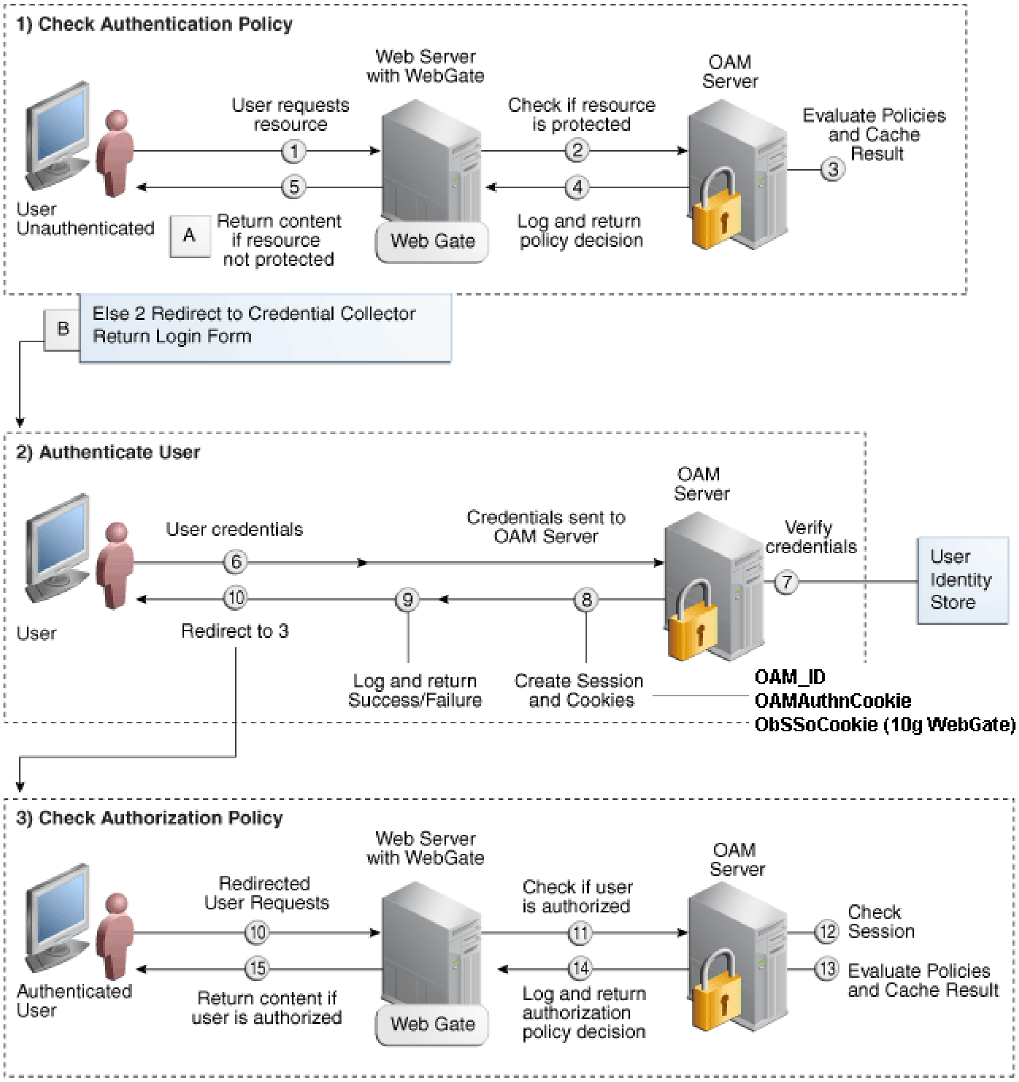
Oracle Access Manager involves several different components. These are:

- 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 Log In Processing with OAM Agents

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

SSO Login Processing with OAM Agents


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

Installation Overview

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

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

installation, see the Oracle Access Manager and Single Sign-On Whitepaper (My Oracle Support Doc ID 1492047.1).

Infrastructure Installation and Configuration

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

OID User Data

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

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

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

OID with Multiple Realms

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

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

User Management

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

ODSM

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

LDIF Scripts

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

User Data Synchronization

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

H

Appendix: Setting Up Password Stores with Oracle Wallet

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

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

About Password Stores and Oracle Wallet

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

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

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

```
sqlplus /@db_username
```

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

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

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

There are two different types of password stores or wallets. One type is for database connect strings used in program arguments (such as `sqlplus /@db_username`). The other type is for Java application installation and application use.

Setting Up Password Stores for Database User Accounts

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

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

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

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

1. Create a wallet using the following command:

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

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

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

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

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

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

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

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

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

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

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

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

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

Setting Up Wallets for Database User Accounts

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

- For RMS, RWMS, RPM Batch, RETL, RMS, RWMS, and ARI
- For Java Applications (SIM, ReIM, RPM, Alloc, RIB, RSL, AIP, RETL)

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

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

```
cd /projects/rms13.2/dev/
mkdir .wallet
```

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

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

```
WALLET_LOCATION =   (SOURCE =     (METHOD = FILE)     (METHOD_DATA =
(DIRECTORY =  /projects/rms13.2/dev/.wallet)) )
SQLNET.WALLET_OVERRIDE=TRUE
SSL_CLIENT_AUTHENTICATION=FALSE
```

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

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

```
ifile = /u00/oracle/product/11.2.0.4/network/admin/tnsnames.ora

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

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

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

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

   a. Ensure you are in the intended location.

```
$ pwd
/projects/rms13.2/dev/.wallet
```

b. Create the wallet files.

```
$ mkstore -wrl . –create
```

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

d. Enter the password again.

Two wallet files are created from the above command:

– ewallet.p12

– cwallet.sso

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

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

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

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

```
$ export TNS_ADMIN=/projects/rms13.2/dev/.wallet /* This is very import to use
wallet to point at the alternate tnsnames.ora created in this example */

$ sqlplus /@dvols29_rms01user

SQL*Plus: Release 11

Connected to:
Oracle Database 11g

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

Running batch programs or shell scripts would be similar:

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

Set the UP unix variable to help with some compiles :

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

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

Additional Database Wallet Commands

The following is a list of additional database wallet commands.

- Delete a credential on wallet

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

- Change the password for a credential on wallet

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

- List the wallet credential entries

  ```
  mkstore –wrl . –list
  ```

  This command returns values such as the following.

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

- View the details of a wallet entry

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

  Returns the value of the entry:

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

  Returns value of the entry:

  ```
  rms01user
  ```

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

  Returns value of the entry:

  ```
  passwd
  ```

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

For Java application, 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: orappsrv:[103x_WLS] /u00/webadmin/product/10.3.x/WLS/user_projects/domains/132_mck_soa_domain/retail/reim13/config
- Application installers should create the Java wallets for you, but it is good to know how this works for future use and understanding.
- Scripts are located in <WEBLOGIC_DOMAIN_HOME>/retail/<appname>/retail-public-security-api/bin for administering wallet entries.

  Example:

  orappsrv:[103x_WLS] /u00/webadmin/product/10.3.x/WLS/user_projects/domains/132_mck_soa_domain/retail/reim13/retail-public-security-api/bin
- In this directory is a script to help you update each alias entry without having to remember the wallet details. For example, if you set the RPM database alias to rms01user, you will find a script called update-RMS01USER.sh.

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

- Two main scripts are related to this script in the folder for more generic wallet operations: dump_credentials.sh and save_credential.sh.

- If you have not installed the application yet, you can unzip the application zip file and view these scripts in <app>/application/retail-public-security-api/bin.

  Example:

  orappsrv:[103x_WLS] /u00/webadmin/reim/application/retail-public-security-api/bin

update-<ALIAS>.sh

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

Usage:

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

Example:

```
orappsrv:[103xWLS]
/u00/webadmin/product/10.3.x/WLS/user_projects/domains/java_domain/retail/rpm1
32test/retail-public-security-api/bin> ./update-RMS01USER.sh
usage: update-RMS01USER.sh <username>
<username>: the username to update into this alias.
Example: update-RMS01USER.sh myuser
Note: this script will ask you for the password for the username that you pass
in.
orappsrv:[103xWLS]
/u00/webadmin/product/10.3.x/WLS/user_projects/domains/java_domain/retail/rpm1
32test/retail-public-security-api/bin>
```

dump_credentials.sh

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

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

Example:

dump_credentials.sh /u00/webadmin/product/10.3.x/WLS/user_projects/domains/132_mck_soa_domain/retail/reim13/config

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

Below are the credentials found in the wallet at the location:/u00/webadmin/product/10.3.x/WLS/user_projects/domains/132_mck_soa_domain/retail/reim13/config

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

Application level key partition name:reim13
User Name Alias:WLS-ALIAS User Name:weblogic
User Name Alias:RETAIL-ALIAS User Name:retail.user
User Name Alias:LDAP-ALIAS User Name:RETAIL.USER
User Name Alias:RMS-ALIAS User Name:rms132mock
User Name Alias:REIMBAT-ALIAS User Name:reimbat
```

save_credential.sh

save_credential.sh is used to update the information in wallet. If you are unsure about the information that is currently in the wallet, use dump_credentials.sh as indicated above. You can add new or update using save_credential.sh as shown below:

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

Example:

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

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

Enter password:
Verify password:
```

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

Usage

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

How Does the Wallet Relate to the Application?

The ORACLE Retail Java applications have the wallet alias information you create in an <app-name>.properties file. Below is the reim.properties file. Note the database information and the user are presented as well. The property called datasource.credential.alias=RMS-ALIAS uses the ORACLE wallet with the argument of RMS-ALIAS at the csm.wallet.path and csm.wallet.partition.name = reim13 to retrieve the password for application use.

Reim.properties code sample:

```
datasource.url=jdbc:oracle:thin:@ordbsrv.us.oracle.com:1521:pkols07
datasource.schema.owner=rms132mock
datasource.credential.alias=RMS-ALIAS
# =================================================================
# ossa related Configuration
#
# These settings are for ossa configuration to store credentials.
# =================================================================

csm.wallet.path=/u00/webadmin/product/10.3.x/WLS/user_projects/domains/132_mck_soa
_domain/retail/reim13/config
csm.wallet.partition.name=reim13
```

How Does the Wallet Relate to Java Batch Program Use?

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

Setting up RETL Wallets

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

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

To set up RETL wallets, perform the following steps:

1. Set the following environment variables:
   - `ORACLE_SID=<retaildb>`
   - `RFX_HOME=/u00/rfx/rfx-13.2.0`
   - `RFX_TMP=/u00/rfx/rfx-13.2.0/tmp`
   - `JAVA_HOME=/usr/jdk1.7.64bit`
   - `LD_LIBRARY_PATH=$ORACLE_HOME`
   - `PATH=$RFX_HOME/bin:$JAVA_HOME/bin:$PATH`
2. Change directory to `$RFX_HOME/bin`.
3. Run `setup-security-credential.sh`.
   - Enter 1 to add a new database credential.
   - Enter the dbuseralias. For example, `retl_java_rms01user`.
   - Enter the database user name. For example, `rms01user.`
   - Enter the database password.

- Re-enter the database password.
- Enter D to exit the setup script.

4. Update your RETL environment variable script to reflect the names of both the Oracle Networking wallet and the Java wallet.

   For example, to configure RETLforRPAS, modify the following entries in `$MMHOME/RETLforRPAS/rfx/etc/rmse_rpas_config.env.`

   - The RETL_WALLET_ALIAS should point to the Java wallet entry:

     ```
     export RETL_WALLET_ALIAS="retl_java_rms01user"
     ```

   - The ORACLE_WALLET_ALIAS should point to the Oracle network wallet entry:

     ```
     export ORACLE_WALLET_ALIAS="dvols29_rms01user"
     ```

   - The SQLPLUS_LOGON should use the ORACLE_WALLET_ALIAS:

     ```
     export SQLPLUS_LOGON="/@${ORACLE_WALLET_ALIAS}"
     ```

5. To change a password later, run `setup-security-credential.sh`.

   - Enter 2 to update a database credential.
   - Select the credential to update.
   - Enter the database user to update or change.
   - Enter the password of the database user.
   - Re-enter the password.

Quick Guide for Retail Wallets

Retail App	Wallet Type	Wallet Location	Wallet Partition	Alias Name	User Name	Use	Create By	Alias Example	Notes
RMS batch	DB	<RMS batch install dir (MMHOME)>/.wallet	n/a	<Database SID>_<Database schema owner>	<rms schema owner>	Compile, execution	Installer	n/a	Alias hard-coded by installer
RMS forms	DB	<forms install dir>/base/.wallet	n/a	<Database SID>_<Database schema owner>	<rms schema owner>	Compile	Installer	n/a	Alias hard-coded by installer
ARI forms	DB	<forms install dir>/base/.wallet	n/a	<Db_Ari01 >	<ari schema owner>	Compile	Manual	ari-alias	
RMWS forms	DB	<forms install dir>/base/.wallet	n/a	<Database SID>_<Database schema owner>	<rwms schema owner>	Compile forms, execute batch	Installer	n/a	Alias hard-coded by installer
RPM app	DB	<RPM batch install dir>/.wallet	n/a	<rms schema owner alias>	<rms schema owner>	Execute batch	Manual	rms-alias	
RWMS auto-login	JAVA	<forms install dir>/base/.javawallet							
			<RWMS Installation name>	<RWMS database user alias>	<RWMS schema owner>	RWMS forms app to avoid dblogin screen	Installer	rwms13inst	

Retail App	Wallet Type	Wallet Location	Wallet Partition	Alias Name	User Name	Use	Create By	Alias Example	Notes
			<RWMS Installation name>	BI_ALIAS	<BI Publisher administrative user>	RWMS forms app to connect to BI Publisher	Installer	n/a	Alias hard-coded by installer
AIP app	JAVA	<weblogic domain home>/retail/<deployed aip app name>/config							Each alias must be unique
			aip13	<AIP weblogic user alias>	<AIP weblogic user name>	App use	Installer	aip-weblogic-alias	
			aip13	<AIP database schema user alias>	<AIP database schema user name>	App use	Installer	aip01user-alias	
			aip13	<rib-aip weblogic user alias>	<rib-aip weblogic user name>	App use	Installer	rib-aip-weblogic-alias	
RPM app	JAVA	<weblogic domain home>/retail/<deployed rpm app name>/config							Each alias must be unique
			rpm13	<rpm weblogic user alias>	<rpm weblogic user name>	App use	Installer	rpm-weblogic-alias	
			rpm13	<rms shema user alias>	<rms shema user name>	App, batch use	Installer	rms01user-alias	

Retail App	Wallet Type	Wallet Location	Wallet Partition	Alias Name	User Name	Use	Create By	Alias Example	Notes
			rpm13	<rpm application user one alias>	<rpm application user one name>	App use	Installer	user1-alias	
			rpm13	<rpm application user two alias>	<rpm application user two name>	App use	Installer	user2-alias	
			rpm13	<rpm batch user alias>	<rpm batch user name>	App, batch use	Installer	rpmbatch-alias	
			rpm13	<rib-rpm weblogic user alias>	<rib-rpm weblogic user name>	App use	Installer	rib-rpm-weblogic-alias	
ReIM app	JAVA	<weblogic domain home>/retail/<deployed reim app name>/config							Each alias must be unique
			<installed app name>	<reim weblogic user alias>	<reim weblogic user name>	App use	Installer	weblogic-alias	
			<installed app name>	<rms shema user alias>	<rms shema user name>	App, batch use	Installer	rms01user-alias	
			<installed app name>	<reim webservice validation user alias>	<reim webservice validation user name>	App use	Installer	reimwebservice-alias	
			<installed app name>	<reim batch user alias>	<reim batch user name>	App, batch use	Installer	reimbatch-alias	

Retail App	Wallet Type	Wallet Location	Wallet Partition	Alias Name	User Name	Use	Create By	Alias Example	Notes
Alloc app	JAVA	<weblogic domain home>/retail/<deployed alloc app name>/config							Each alias must be unique
			<installed app name>	<alloc weblogic user alias>	<alloc weblogic user name>	App use	Installer	weblogic-alias	
			<installed app name>	<rms shema user alias>	<rms shema user name>	App use	Installer	rms01user-alias	
			<installed app name>	<rsl for rms weblogic user alias>	<rsl for rms weblogic user name>	App use	Installer	rsl-rms-weblogic-alias	
RSL app	JAVA	<RSL INSTALL DIR>/rsl-rms/security/config							Each alias must be unique
			rsl-rsm	<rsl weblogic user alias>	<rsl weblogic user name>	App use	Installer	weblogic-alias	
			rsl-rsm	<rms shema user alias>	<rms shema user name>	App use	Installer	rms01user-alias	
SIM app	JAVA	<weblogic domain home>/retail/<deployed sim app name>/config							
			rpm	<rpm weblogic user alias>	<rpm weblogic user name>	App use	Installer	rpm-weblogic-alias	

Retail App	Wallet Type	Wallet Location	Wallet Partition	Alias Name	User Name	Use	Create By	Alias Example	Notes
			rms	<rsl for rms weblogic user alias>	<rsl for rms weblogic user name>	App use	Installer	rsl-rms-weblogic-alias	
			rib-sim	<rib-sim weblogic user alias>	<rib-sim weblogic user name>	App use	Installer	rib-sim-weblogic-alias	
RETL	JAVA	<RETL home>/etc/security	n/a	<target application user alias>	<target application db userid>	App use	Manual	retl_java_rms01user	User may vary depending on RETL flow's target application
RETL	DB	<RETL home>/.wallet	n/a	<target application user alias>	<target application db userid>	App use	Manual	<db>_<user>	User may vary depending on RETL flow's target application
RIB	JAVA	<RIBHOME DIR>/deployment-home/conf/security							<app> is one of aip, rfm, rms, rpm, sim, rwms, tafr
JMS			jms<1-5>	<jms user alias> for jms<1-5>	<jms user name> for jms<1-5>	Integration use	Installer	jms-alias	
WebLogic			rib-<app>-app-server-instance	<rib-app weblogic user alias>	<rib-app weblogic user name>	Integration use	Installer	weblogic-alias	
Admin GUI			rib-<app>#web-app-user-alias	<rib-app admin gui user alias>	<rib-app admin gui user name>	Integration use	Installer	admin-gui-alias	

Retail App	Wallet Type	Wallet Location	Wallet Partition	Alias Name	User Name	Use	Create By	Alias Example	Notes
Application			rib-<app>#user-alias	<app weblogic user alias>	<app weblogic user name>	Integration use	Installer	app-user-alias	Valid only for aip, rpm, sim
DB			rib-<app>#app-db-user-alias	<rib-app database schema user alias>	<rib-app database schema user name>	Integration use	Installer	db-user-alias	Valid only for rfm, rms, rwms, tafr
Error Hospital			rib-<app>#hosp-user-alias	<rib-app error hospital database schema user alias>	<rib-app error hospital database schema user name>	Integration use	Installer	hosp-user-alias	

I

Appendix: Preinstallation for Secured Setup of SIM in Oracle Application Server (OAS)

The goal of the following steps is to set up secure communication between the MOD_OC4J and the OC4J instance via the AJPS protocol.

> **Note:** The following changes will make the Oracle Application Server work only with SSL, because in the current release, it is not possible for MOD_OC4J to selectively access some OC4J instances using AJP and others using AJPS. Once the Oc4jEnableSSL-on directive has been set in MOD_OC4J.CONF, AJPS will be used for all future communication to any OC4J instances.
>
> Therefore, any applications which do not support SSL and are deployed in the same OAS will not work. It is recommended that you use a separate OAS installation for SSL configured applications.

The information presented below is intended as a supplement to the following product documentation:

Oracle Containers for J2EE Security Guide 10g (10.1.3.1.0)

B28957-01

http://docs.oracle.com/cd/B31017_01/web.1013/b28957.pdf

Chapter 15: SSL Communication with OC4J pages 15-1 through 15-24

> **Note:** Securing your OC4J instance will result with DMS no longer working as DMS does NOT support the AJPS and HTTPS protocol.

Since DMS always makes requests to localhost, one workaround is to configure OC4Js to bind to only a local host for AJP and HTTP requests when SSL is enabled.

If you are using ajps for secure communication between the Oracle HTTP server and the Oracle Container 4 Java, the website name must be default-web-site.

1. For the application’s OC4J instance, back up the server.xml and default-web-site.xml files.

   ```
   %  cd  $ORACLE_HOME/j2ee/<instance-name>
   %  cp –r config config.orig
   %  cd config
   %  cp server.xml server.xml.orig
   %  cp default-web-site.xml default-web-site.xml.orig
   ```

2. This step is optional configuration change to MOD_OC4J, which will allow you to display to a browser the OC4J routing information that MOD_OC4J has dynamically discovered about the running OC4J instances, the ports those instance are using and the applications that those instances hold.

   a. Backup the existing “mod_oc4j.conf” file:

      ```
      % cd  $ORACLE_HOME/Apache/Apache/conf
      % cp mod_oc4j.conf mod_oc4j.conf.orig
      ```

   b. Edit the “mod_oc4j.conf” , and within this file, between the "<IfModule mod_oc4j.c>" and "</IfModule>" tags, add the following:

      ```
      oc4jSet StatusUri /oc4j-status
      ```

      This will allow you to invoke the following URL:

      http://<your_host>:<your_port>/oc4j-status

      This URL will display the dynamic routing information about all the apps that MOD_OC4J has discovered.

3. Next use keytool to create a keystore with certificate based on the fully qualified name of the machine.

   It is required to use the keytool utility to export a certificate from the keystore using following command:

   ```
   %  keytool –export –file cert_file_name –keystore keystore_file_name –
   storepass <password> -alias <keystore_alias>
   ```

   Reference:

   http://docs.oracle.com/cd/B31017_01/web.1013/b28957/configssl.htm#CIHEBDBH

   Oracle Containers for J2EE Security Guide 10g (10.1.3.1.0)
   15 SSL Communication with OC4J
   Configure AJPS between OC4J and Oracle HTTP Server

   See the steps describing the use of "keytool" contained within following note:
   Note 152363.1 - How to Enable SSL in OC4J Standalone

4. Now make the OC4J instance use AJPS instead of AJP. First,modify default-web-site.xml and within <web-site> tag at the top of the file, locate the attribute definition: protocol=”ajp13”. To the left of this insert: secure=”true” as shown below:

   ```
   <web-site
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:noNamespaceSchemaLocation="http://xmlns.oracle.com/oracleas/schema/web-
   site-10_0.xsd"
      port="12501" secure="true" protocol="ajp13" display-name="OC4J 10g (10.1.3)
   Default Web Site"
      schema-major-version="10" schema-minor-version="0"
   >
   ```

   At the bottom of the same file add the following <ssl-config> tag, just above the </web-site> tag:

   ```
   <ssl-config
      keystore="/path/to/your/java.keystore"
      keystore-password="keyStorePasswd"
   />
   ```

5. Ensure OPMN assigns an “ajps” port value to out app <instance-name>.

   Within “opmn.xml”, modify the “default-web-site” entry within the app <instance-name> xml entries and change the “ajp” to “ajps” as shown:

   <port id="default-web-site" range="12501-12600" protocol="ajps"/>

   After finishing above steps stop and start opmn and after starting the opmn instance, invoke “opmnctl status –l” and in the port section you should have “ajps” (rather than “ajp”) and the expected port value.

   At this point, the /oc4j-status (created above) should show all the targets.

   > **Note:** You will get an internal error attempting to access any page, because at this point we have made OC4J use SSL but have not configured MOD_OC4J to use SSL to talk to it, so the two cannot communicate.
   >
   > You will also notice if you look in $ORACLE_HOME/opmn/logs/opmn.log that there are "Ping Failures" and OC4J_AJPS is being killed and restarted once nearly every minute. This can be verified using "opmnctl status -l" which contains a column giving the "up time" for the container. Given that the OC4J_AJPS container is currently being identified as unresponsive and it will be restarted after three successive "ping" failures (20 seconds from each other), we will correct these two problems in the steps below.

6. First, configure OPMN with an SSL configuration that allows it to send AJPS requests to OC4J.

   a. Use the Oracle Wallet Manager tool to import the generated certificate (cert_file_name) from Step 3, into the wallet as a Trusted Certificate.

      The following technical document provides a thorough overview of how to achieve this:
      Note 341904.1 – Configuring HTTP Server to use SSL in Oracle Application Server 10g (10.1.2.XX)

   b. Add the same CA trusted root to the wallet.

      > **Note:** When creating the wallet, ensure that the wallet is enabled for the "auto-login" feature.

   Add an SSL configuration to OPMN, so OPMN can use SSL to invoke "pings" to the OC4J instance’s AJPS port.

   Edit the opmn.xml file and locate the "stop-parameters" section for the OC4J instance of interest:

```
 <category id="stop-parameters">
 <data id="java-options"
    value="-
Djava.security.policy=$ORACLE_HOME/j2ee/AJPS/config/java2.policy
    -Djava.awt.headless=true -Dhttp.webdir.enable=false"/>
 </category>
```

Immediately below the "stop-parameter" section, add the following new "security-parameters" section:

```
<category id="security-parameters">
   <data id="wallet-file" value="file:/path/to/wallet_dir"/>
   <data id="wallet-password" value="wallet_passwd"/>
</category>
```

> **Note:** The wallet-file is a path to a directory containing a file named "ewallet.p12" and does NOT include the "ewallet.p12" file name itself

7. After completing the above steps, stop and start the opmn instance.
   - a. Check the /oc4j-status page to verify that your applications have been discovered.
   - b. Check the opmn.log and verify that there are no “Ping Failures”.

While accessing the application you will still see “HTTP-500 Internal Server Error”. Use the following steps to fix this error.

8. Enable MOD_OC4J to send requests to OC4J via AJPS.
9. Backup the mod_oc4j.conf file at ($ORACLE_HOME/Apache/Apache/conf/mod_oc4j.conf)

```
% cd $ORACLE_HOME/Apache/Apache/conf
% cp mod_oc4j.conf mod_oc4j.conf.orig
```

10. Within MOD_OC4J.CONF, between the "<IfModule mod_oc4j.c>" and "</IfModule>" add:

```
Oc4jEnableSSL on
Oc4jSSLWalletFile /path/to/wallet_dir
```

11. Restart all opmn process and invoke “opmnctl status –l”, and in the port section of the result you will have “ajps” rather than “ajp” and expected port values and after 5mins if you repeat “opmnctl status –l” the uptime of application will not reset and will grow to five minutes and beyond.

    In addition, /oc4j-status page should have discovered all your applications and opmn.log should not have any “Ping Failures” and you should be able to access all your application pages from a browser.

After completing the above steps use the “https” protocol and https port of HTTPServer in your browser to access the application.

J

Appendix: Preinstallation for Secured Setup of SIM in WebLogic

WebLogic Server supports SSL on a dedicated listen port. The managed server can be configured to use SSL as well. To establish an SSL connection, a Web browser connects to WebLogic Server by supplying the SSL listen port and the HTTPs protocol in the connection URL, for example, https://myserver:7002.

SIM deployment is supported in WebLogic in secured mode. For enterprise deployment, it is recommended to use SSL certificates signed by certificate authorities.

> **Note:** Separate signed SSL certificates needs to be obtained for each host where application is being deployed.

Get an SSL Certificate and Set up a Keystore

1. Obtain an identity (private key and digital certificates) and trust (certificates of trusted certificate authorities) for WebLogic Server. Use the digital certificates, private keys, and trusted CA certificates provided by the WebLogic Server kit, the CertGen utility, Sun Microsystem's keytool utility, or a reputable vendor such as Entrust or Verisign to perform this step.

   a. Set appropriate JAVA_HOME and PATH to java.

      Example:

      ```
      export JAVA_HOME=/u00/webadmin/product/jdk
      export PATH=$JAVA_HOME/bin:$PATH
      ```

   b. Create a new keystore.

      ```
      keytool -genkey -keyalg RSA -keysize 2048 -keystore <keystore> -alias
      <alias>
      ```

      Example:

      ```
      keytool -genkey -keyalg RSA -keysize 2048 -keystore redevlv0126.keystore -
      alias redevlv0126
      ```

   c. Generate the signing request.

      ```
      keytool -certreq -keyalg RSA -file <certificate request file> -keystore
      <keystore> -alias <alias>
      ```

      Example:

      ```
      keytool -certreq -keyalg RSA -file redevlv0126.csr -keystore
      redevlv0126.keystore -alias redevlv0126
      ```

   d. Submit the certificate request to Certificate authority

2. Store the identity and trust. Private keys and trusted CA certificates which specify identity and trust are stored in a keystore.

   In following examples, we are using same keystore to store all certificates.

   a. Import the root certificate into the keystore.

      Example:

      ```
      keytool -import -trustcacerts -alias  verisignclass3g3ca -file Primary.pem
      -keystore  redevlv0126.keystore
      ```

b. Import the intermediary certificate (if required) into the keystore.

   Example:

```
keytool -import -trustcacerts -alias oracleclass3g3ca -file Secondary.pem
-keystore  redevlv0126.keystore
```

c. Import the received signed certificate for this request into the keystore.

   Example:

```
keytool -import -trustcacerts -alias redevlv0126 -file cert.cer -keystore
redevlv0126.keystore
```

Configure the Application Server for SSL

1. Configure the identity and trust keystores for WebLogic Server in the WebLogic Server Administration Console.

   a. In the Change Center of the Administration Console, click Lock & Edit.

   b. In the left pane of the Console, expand Environment and select Servers.

   c. Click the name of the server for which you want to configure the identity and trust keystores.

   d. Select Configuration > Keystores.

   e. In the Keystores field, select the method for storing and managing private keys/digital certificate pairs and trusted CA certificates. These options are available:

      – **Demo Identity and Demo Trust**: The demonstration identity and trust keystores, located in the BEA_HOME\server\lib directory and the JDK cacerts keystore, are configured by default. Use for development only.

      – **Custom Identity and Java Standard Trust**: A keystore you create and the trusted CAs defined in the cacerts file in the JAVA_HOME\jre\lib\security directory.

      – **Custom Identity and Custom Trust [Recommended]**: Identity and trust keystores you create.

      – **Custom Identity and Command Line Trust**: An identity keystore you create and command-line arguments that specify the location of the trust keystore.

      Select **Custom Identity and Custom Trust**.

   f. In the Identity section, define attributes for the identity keystore.

      – **Custom Identity Keystore**: The fully qualified path to the identity keystore.

      – **Custom Identity Keystore Type**: The type of the keystore. Generally, this attribute is Java KeyStore (JKS); if left blank, it defaults to JKS.

      – **Custom Identity Keystore Passphrase**: The password you will enter when reading or writing to the keystore. This attribute is optional or required depending on the type of keystore. All keystores require the passphrase in order to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore so whether or not you define this property depends on the requirements of the keystore.

   g. In the **Trust** section, define properties for the trust keystore.

      If you chose **Java Standard Trust** as your keystore, specify the password defined when creating the keystore. Confirm the password.

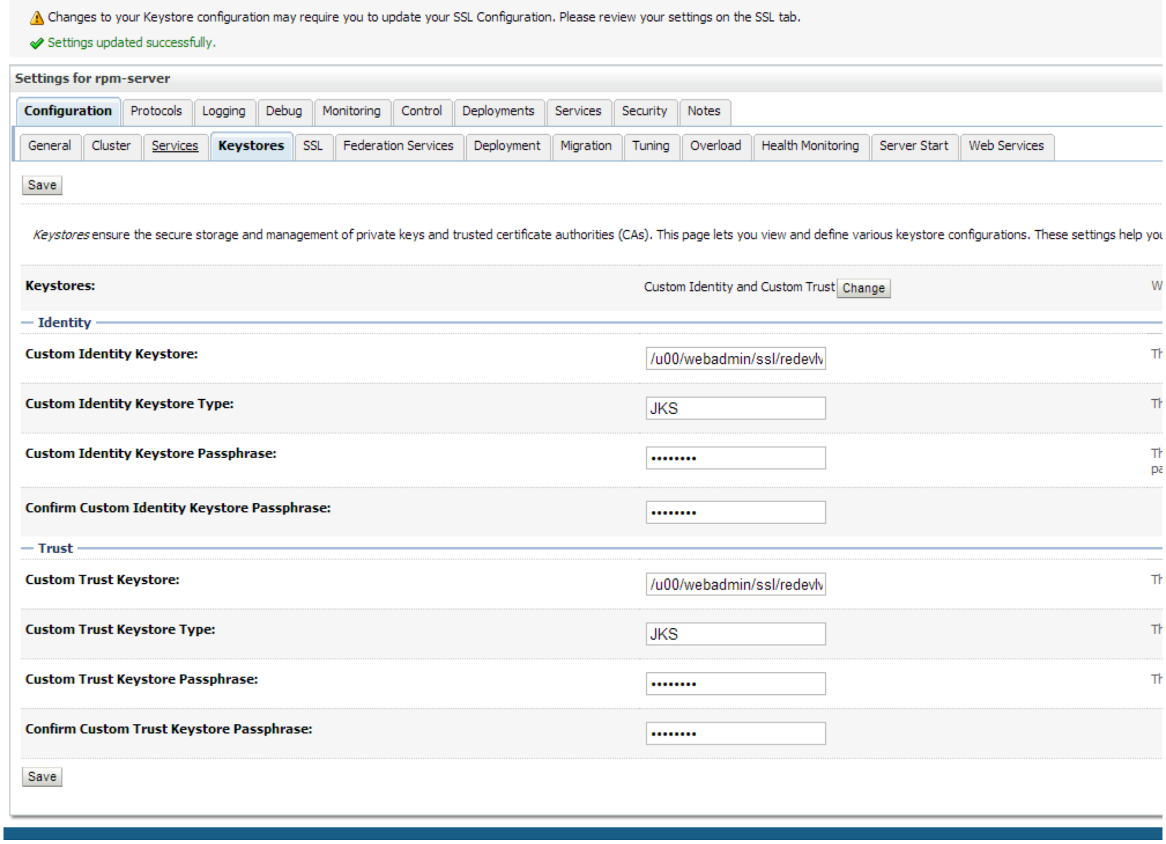
      If you chose **Custom Trust [Recommended]**, define the following attributes:

      – **Custom Trust Keystore**: The fully qualified path to the trust keystore.

- **Custom Trust Keystore Type**: The type of the keystore. Generally, this attribute is JKS; if left blank, it defaults to JKS.
- **Custom Trust Keystore Passphrase**: The password you will enter when reading or writing to the keystore. This attribute is optional or required depending on the type of keystore. All keystores require the passphrase in order to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore so whether or not you define this property depends on the requirements of the keystore.

h. Click Save.

i. To activate these changes, in the Change Center of the Administration Console, click Activate Changes.
Not all changes take effect immediately—some require a restart.



⚠ Changes to your Keystore configuration may require you to update your SSL Configuration. Please review your settings on the SSL tab.

✓ Settings updated successfully.

Settings for rpm-server

Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and define various keystore configurations. These settings help you

Keystores: Custom Identity and Custom Trust

— Identity

Custom Identity Keystore: /u00/webadmin/ssl/redevlv

Custom Identity Keystore Type: JKS

Custom Identity Keystore Passphrase: ••••••••

Confirm Custom Identity Keystore Passphrase: ••••••••

— Trust

Custom Trust Keystore: /u00/webadmin/ssl/redevlv

Custom Trust Keystore Type: JKS

Custom Trust Keystore Passphrase: ••••••••

Confirm Custom Trust Keystore Passphrase: ••••••••

For more details see "Configure Keystores" in the *Administration Console Online Help*.

2. Set SSL configuration options for the private key alias and password in the WebLogic Server Administration Console.

a. In the Change Center of the Administration Console, click Lock & Edit.

b. In the left pane of the Console, expand Environment and select Servers.

c. Click the name of the server for which you want to configure the identity and trust keystores.

d. Select Configuration > SSL.

e. In the Identity and Trust Locations, defaults to Keystores.

f. In the Private Key Alias, type the string alias used to store and retrieve the server's private key.

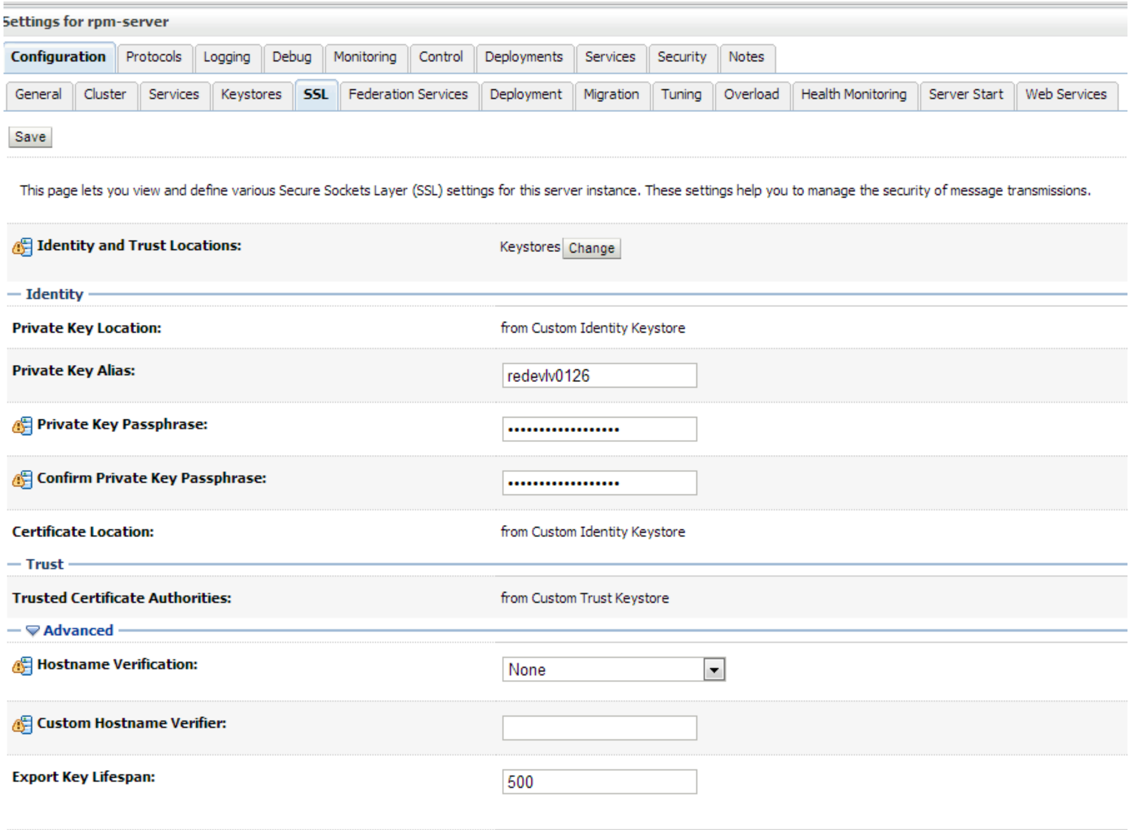
g. In the Private Key Passphrase, provide the keystore attribute that defines the passphrase used to retrieve the server's private key.

h. Save the changes.

i. Click on Advanced Section of SSL tab.

j. In the Hostname Verification, select as None. This specifies to ignore the installed implementation of the weblogic.security.SSL.HostnameVerifier interface (this interface is generally used when this server is acting as a client to another application server).

k. Save the changes



This page lets you view and define various Secure Sockets Layer (SSL) settings for this server instance. These settings help you to manage the security of message transmissions.

Identity and Trust Locations: Keystores Change

Identity

Private Key Location: from Custom Identity Keystore

Private Key Alias: redevlv0126

Private Key Passphrase: ••••••••••••••••••

Confirm Private Key Passphrase: ••••••••••••••••••

Certificate Location: from Custom Identity Keystore

Trust

Trusted Certificate Authorities: from Custom Trust Keystore

Advanced

Hostname Verification: None

Custom Hostname Verifier:

Export Key Lifespan: 500

For more details see "Configure SSL" in the *Administration Console Online Help*.

Verify SSL Connections

All the server SSL attributes are dynamic; when modified via the Console, they cause the corresponding SSL server or channel SSL server to restart and use the new settings for new connections. Old connections will continue to run with the old configuration. To ensure that all the SSL connections exist according to the specified configuration, you must reboot WebLogic Server.

Use the **Restart SSL** button on the Control: Start/Stop page to restart the SSL server when changes are made to the keystore files and need to be applied for subsequent connections without rebooting WebLogic Server.

Upon restart you can see similar entries in the log.

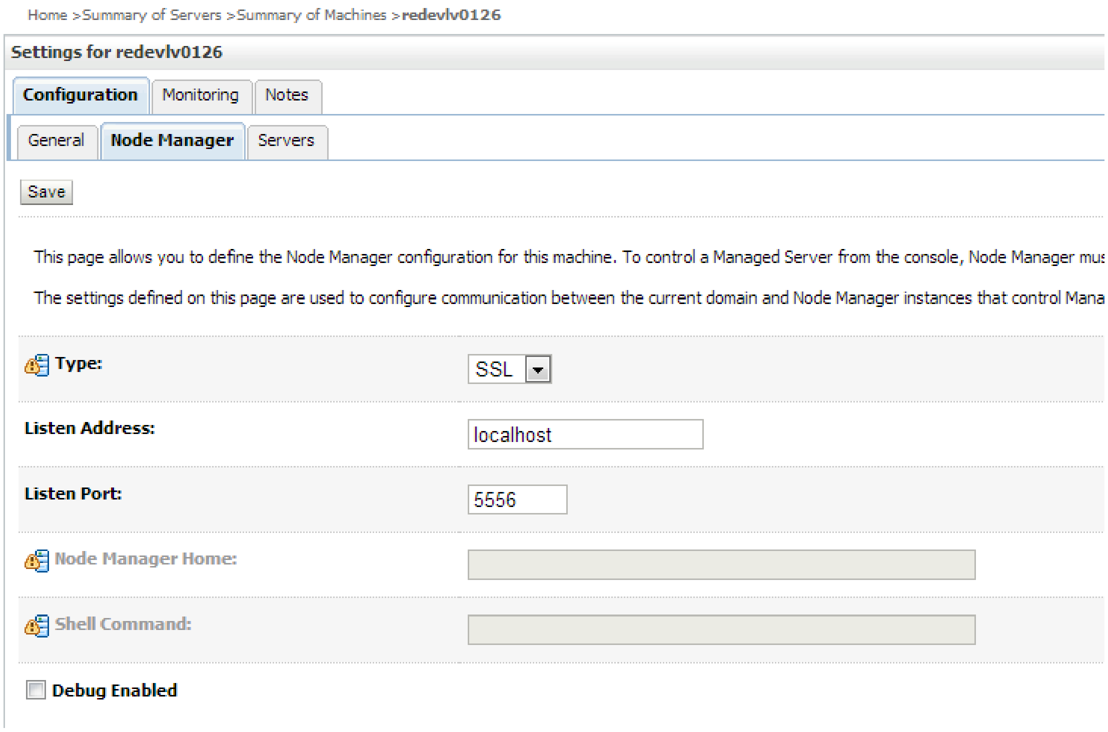
```
<Mar 11, 2013 5:18:27 AM CDT> <Notice> <WebLogicServer> <BEA-000365> <Server state
changed to RESUMING>
<Mar 11, 2013 5:18:27 AM CDT> <Notice> <Server> <BEA-002613> <Channel
"DefaultSecure" is now listening on 10.141.15.214:57002 for protocols iiops, t3s,
ldaps, https.>
<Mar 11, 2013 5:18:27 AM CDT> <Notice> <Server> <BEA-002613> <Channel
"DefaultSecure[1]" is now listening on 127.0.0.1:57002 for protocols iiops, t3s,
ldaps, https.>
<Mar 11, 2013 5:18:27 AM CDT> <Notice> <WebLogicServer> <BEA-000329> <Started
WebLogic Admin Server "AdminServer" for domain "APPDomain" running in Production
Mode>
<Mar 11, 2013 5:18:27 AM CDT> <Notice> <WebLogicServer> <BEA-000365> <Server state
changed to RUNNING>
<Mar 11, 2013 5:18:27 AM CDT> <Notice> <WebLogicServer> <BEA-000360> <Server
started in RUNNING mode>
```

Note: For complete security of the WebLogic Server, it is recommended to secure both **Administration** as well the **Managed server** where application is being deployed. You can choose to disable the non-SSL ports (HTTP). It is highly recommended to secure the Node Manager. The steps to secure Node Manager as provided in the following section.

Securing Nodemanager with SSL Certificates

1. Navigate to **<BEA_HOME>/wlserver_10.3/common/nodemanager** and take a backup of nodemanager.properties
2. Add similar entry to **nodemanager.properties**.
   - **KeyStores**=CustomIdentityAndCustomTrust
   - **CustomIdentityKeyStoreFileName**=/u00/webadmin/ssl/redevlv0126.keystore
   - **CustomIdentityKeyStorePassPhrase**=[password to keystore, this will get encrypted]
   - **CustomIdentityAlias**=redevlv0126
   - **CustomIdentityPrivateKeyPassPhrase**=[password to keystore, this will get encrypted]
   - **CustomTrustKeyStoreFileName**=/u00/webadmin/ssl/redevlv0126.keystore
   - **SecureListener**=true
3. Login to WebLogic console, navigate to **Environment** > **Machines**. Select the nodemanager created already and navigate to **Node Manager** tab. In the Change Center, click **Lock and Edit**.

For **Type**, select SSL and save and activate.



This page allows you to define the Node Manager configuration for this machine. To control a Managed Server from the console, Node Manager mus

The settings defined on this page are used to configure communication between the current domain and Node Manager instances that control Mana

Type: SSL

Listen Address: localhost

Listen Port: 5556

Node Manager Home:

Shell Command:

□ Debug Enabled

4. After activating the changes, bounce the entire WebLogic Domain for changes to take effect. Verify that the nodemanager is reachable in the **Monitoring** tab after the restart.

Using Secured LDAP

The application can communicate with the LDAP server on a secured port. It is recommended that you use secured an LDAP server for security.

Refer to Configuring Secure Sockets Layer (SSL) in the *Oracle Fusion Middleware Administration Guide* for more details.

In case secure LDAP is used for authentication, it is important to import the certificates used in LDAP server into the JRE of the WebLogic server for SSL handshake.

Example:

```
Set JAVA_HOME and PATH to the JDK being used by WebLogic Domain.
Backup the JAVA_HOME/jre/lib/security/cacerts

/u00/webadmin/product/jdk/jre/lib/security> cp -rp cacerts cacerts_ORIG
```

Import the Root and Intermediary (if required) certificates into the java keystore.

```
/u00/webadmin/product/jdk/jre/lib/security> keytool -import -trustcacerts -alias
verisignclass3g3ca -file ~/ssl/Primary.pem -keystore cacerts

/u00/webadmin/product/jdk/jre/lib/security> keytool -import -trustcacerts -alias
oracleclass3g3ca -file ~/ssl/Secondary.pem -keystore cacerts
```

Import the User certificate from LDAP server into the java keystore.

```
/u00/webadmin/product/jdk/jre/lib/security> keytool -import -trustcacerts -alias
redevlv0126 -file ~/ssl/cert.cer -keystore cacerts
```

The deployed application should be able to communicate with LDAP on the SSL port after a successful SSL handshake.

Batch Setup for SSL Communication

Batch programs communicate with Java applications deployed in WebLogic. The communication needs to have an SSL handshake with the deployed application.

K

Appendix: Certificate Import Topology

Implementation of SSL into the Retail deployment is driven by mapping the SSL certificates and wallets to various participating components in the topology. The table below describes the trust stores to be updated while confirming the certificates imported into middleware and repository of Retail applications. Please ensure you have updated the given trust stores with the signed (either self signed or issued by certifying authority) certificates.

	Java app-host		**Forms app-host**		**RIB app-host**		**BI Publisher-host**		**OID-host**	**Client-host**	
Certificates	**Java app - Managed server**	**Java app-JAVA cacerts**	**Forms app - Managed server**	**Forms app-JAVA cacerts**	**RIB app-Managed server**	**RIB app-JAVA cacerts**	**BI Publisher-Managed server**	**BI Publisher-JAVA cacerts**	**Wallet**	**Browser**	**Client-JAVA cacerts**
appserver.cer	Yes	No	No	No	No	No	No	No	No	No	No
approot.cer	Yes	Yes	No	No	No	Yes	No	Yes	Yes	Yes	Yes
frmserver.cer	No	No	Yes	No	No	No	No	No	No	No	No
frmroot.cer	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes
ribserver.cer	No	No	No	No	Yes	No	No	No	No	No	No
ribroot.cer	No	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes
biserver.cer	No	No	No	No	No	No	Yes	No	No	No	No
biroot.cer	No	Yes	No	Yes	No	No	Yes	Yes	No	Yes	Yes
oidcer.cer	No	No	No	No	No	No	No	No	Yes	No	No
oidroot.cer	No	Yes	No	Yes	No	No	No	Yes	Yes	Yes	Yes

L

Appendix: Oracle 11g Database Parameter File

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

```
processes             = 2000       # Max number of OS  processes that can connect
to the db
query_rewrite_enabled         = TRUE      # Oracle Retail required for function-
based indexes
session_cached_cursors                  = 900       # Oracle Retail required;
undo_management           = AUTO
undo_retention            = 1800      # Currently set for 30 minutes; set to avg
length of transactions in sec
undo_tablespace           = undo_ts
user_dump_dest            = <admin_path>/udump
utl_file_dir                            = <utl_file_path>
workarea_size_policy                    = auto           # Should be set to auto
when pga_aggregate_target is set
#
# ***  Set these parameters for Oracle Retail Data Warehouse (RDW) database ***
#nls_date_format              = DD-MON-RRRR  # Required by MicroStrategy
#query_rewrite_integrity                = TRUSTED
#star_transformation_enabled            = TRUE
#utl_file_dir                           = <Windows_utl_file_path>,
<UNIX_util_file_path>
#
# ***  Archive Logging, set if needed  ***
#log_archive_dest_1                     = 'location=<admin_path>/arch/'
#log_archive_format               = SIDarch_%r_%s_%t.log
#log_buffer           = 10485760    # Set to (512K or 128K)*CPUs
#log_checkpoint_interval                = 51200     # Default:0 - unlimited
#log_checkpoint_timeout                 = 7200      # Default:1800 seconds
```

M

Appendix: Oracle Database 12cR1 Parameter File

```
##############################################################################
# Copyright (c) 2015 by Oracle Corporation
# Oracle 12.1.0.x Parameter file
# NOTES: Before using this script:
#       1.  Change <datafile_path>, <admin_path>, <utl_file_path>, <diag_path>
and <hostname>
#           values as appropriate.
#       2.  Replace the word SID with the database name.
#       3.  Size parameters as necessary for development, test, and production
environments.
# ------------------------------------------------------------------------
*.audit_file_dest=full_path_of_audit_dir
*.audit_trail='db'
*.compatible='12.1.0.2'
*.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'
```

N

Appendix: Configuring Listener and Tnsnames

Note: This example illustrates the listener configuration for External procedures, container and non-container databases. It does not include environment specific settings that may be needed. Consult Oracle Net Services guides for additional information

```
#################################################################
#  File:  listener.ora
#  Desc:  Oracle Net8 listener file.
#  Notes: Modify <hostname>
#################################################################

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (PROTOCOL_STACK =
        (PRESENTATION = TTC)
        (SESSION = NS))
      (ADDRESS =
        (PROTOCOL = tcp)
        (HOST = <hostname>)
        (PORT = 1521))
      (ADDRESS =
        (PROTOCOL = IPC)
        (KEY = extproc_key))
    )
  )

SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (PROGRAM = extproc)
      (SID_NAME = extproc_agent_1521)
      (ORACLE_HOME = /u00/oracle/product/12.1.0.2)
      (ENVS='EXTPROC_DLLS=ANY')
    )
    (SID_DESC =
      (SID_NAME = prod_db1)
      (ORACLE_HOME = /u00/oracle/product/12.1.0.2)
      (ENVS='TNS_ADMIN=/dba/network/extproc_1521')
    )
    (SID_DESC =
      (SID_NAME = pdb1)
      (ORACLE_HOME = /u00/oracle/product/12.1.0.2)
      (ENVS='TNS_ADMIN=/dba/network/extproc_1521')
    )
  )
```

> **Note:** This example illustrates the configuration of net services for External procedures, container and non-container databases. It does not include environment specific settings that may be needed. Consult Oracle Net Services guides for additional information

```
##################################################################
# File: tnsnames.ora
# Desc: Net Services configuration file.
# Note: Change these values: <service_name>, <oracle_sid>, <hostname>,
#       <global_name>
##################################################################

EXTPROC_CONNECTION_DATA =
  (DESCRIPTION =
    (ADDRESS_LIST = (ADDRESS = (PROTOCOL = IPC)(Key = extproc_key)))
    (CONNECT_DATA = (SID = extproc_agent)))

EXTPROC_CONNECTION_DATA.world =
  (DESCRIPTION =
    (ADDRESS_LIST = (ADDRESS = (PROTOCOL = IPC)(Key = extproc_key)))
    (CONNECT_DATA = (SID = extproc_agent)))

< Connect_string> =
  (DESCRIPTION =
    (ADDRESS_LIST = (ADDRESS = (PROTOCOL = tcp)(host = <hostname>)(Port = 1521)))
    (CONNECT_DATA = (Service_Name = <Service_Name>) (GLOBAL_NAME =
<global_name>)))

<Connect_String>.world =
  (DESCRIPTION =
    (ADDRESS_LIST = (ADDRESS = (PROTOCOL = tcp)(host = <hostname>)(Port = 1521)))
    (CONNECT_DATA = (Service_Name = <Service_Name> >) (GLOBAL_NAME =
<global_name>)))

Example:
EXTPROC_CONNECTION_DATA =
  (DESCRIPTION =
    (ADDRESS_LIST = (ADDRESS = (PROTOCOL = IPC)(Key = extproc_key)))
    (CONNECT_DATA = (SID = extproc_agent)))

EXTPROC_CONNECTION_DATA.world =
  (DESCRIPTION =
    (ADDRESS_LIST = (ADDRESS = (PROTOCOL = IPC)(Key = extproc_key)))
    (CONNECT_DATA = (SID = extproc_agent)))
```

Non-Container database configuration for tnsnames entries:

```
prod_sid1 =
  (DESCRIPTION =
    (ADDRESS_LIST = (ADDRESS = (PROTOCOL = tcp)(host = server_01)(Port = 1521)))
    (CONNECT_DATA = (Service_Name = sid1) (GLOBAL_NAME = sid1.world)))

sid1.world =
  (DESCRIPTION =
    (ADDRESS_LIST = (ADDRESS = (PROTOCOL = tcp)(host = server_01)(Port = 1521)))
    (CONNECT_DATA = (Service_Name = sid1) (GLOBAL_NAME = sid1.world)))
```

Container database configuration for tnsnames entries:

```
pdb1 = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = tcp)(host =
server_01)(Port =  1521))) (CONNECT_DATA =  (SERVICE_NAME = pdb1)))
```

```
pdb1.world = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = tcp)(host =
server_01)(Port = 1521))) (CONNECT_DATA =  (SERVICE_NAME = pdb1)))
```

Appendix: Installation Order

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

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

Enterprise Installation Order

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

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

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

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

8. Oracle Retail Allocation
9. Oracle Retail Central Office (ORCO)
10. Oracle Retail Returns Management (ORRM)
11. Oracle Retail Back Office (ORBO) or Back Office with Labels and Tags (ORLAT)
12. Oracle Retail Store Inventory Management (SIM)

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

13. Oracle Retail Predictive Application Server (RPAS)
14. Oracle Retail Demand Forecasting (RDF)
15. Oracle Retail Category Management (CM)

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