Oracle® Retail Point-of-Service

Installation Guide, Volume 1 - Oracle Stack

Release 13.3.3

E37278-02

September 2012

ORACLE®

Oracle Retail Point-of-Service Installation Guide, Volume 1 - Oracle Stack, Release 13.3.3

E37278-02

Copyright © 2012, Oracle and/or its affiliates. All rights reserved.

Primary Author: Bernadette Goodman

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

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

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

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

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

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

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 xiii

Preface xv

Audience xv
Documentation Accessibility xv
Related Documents xvi
Customer Support xvi
Review Patch Documentation xvi
Oracle Retail Documentation on the Oracle Technology Network xvi
Conventions xvii

1 Preinstallation Tasks

Patch Contents 1-1
Check for the Current Version of the Installation Guide 1-1
Check Supported Store Server Software Requirements 1-2
ISD Software Version for Tender Authorization 1-2
Check Supported Client Hardware and Software Requirements 1-2
Install Optional Components for Microsoft POSReady2009 1-3
Check Oracle Retail Software Dependencies 1-3
Check Third-Party Software Dependencies 1-3
Check Additional Oracle Technologies 1-3
Integration with Other Applications 1-4
Oracle Retail Central Office and Back Office 1-4
Oracle Retail Store Inventory Management 1-4
Siebel 1-5
Oracle Retail Returns Management 1-5
Bill Payment 1-5
ISD 1-5
Hardware Requirements 1-5
Store Server 1-5
Client 1-7
Peripheral Devices for Clients 1-7
Check Supported Java Key Manager Requirement 1-7
Check Secure JDBC and Secure RMI 1-7

ISD Authorization Transaction Testing 1-8
Implementation Guidelines for Security 1-9

2 Installation on the Oracle Stack using Windows

Create the Database Schema Owner and Data Source Users 2-1
Installing Point-of-Service 2-2
Determining Tier Type 2-3
Installing the Database 2-3
Required Settings for the Database 2-4
Installing Point-of-Service on Machines 2-4
Updating Device Configuration 2-5
Expand the Point-of-Service Distribution 2-5
Obtaining Third-Party Library Files Required by Point-of-Service 2-6
Obtaining the JRE Required for Client Install 2-6
Obtaining the JRE Required for Client Install on HP Registers 2-6
Increase the Heap Size on the Client 2-6
Securing Communication 2-6
Database Install Options 2-7
Creating the Database Schema with Oracle Retail Back Office 2-7
Running the Point-of-Service Application Installer 2-7
Resolving Errors Encountered During Application Installation 2-8
Update JMS Configuration for Integration with Returns Management 2-8
Creating the Database Schema 2-9
Creating without Oracle Retail Back Office 2-9
Enabling Access for the Data Source User 2-9
Installing Multibyte Fonts for eReceipt in the Client Installation 2-10
Enabling the Printing of Receipts in Chinese on a Network Printer 2-11
Enabling Browser Functionality in the Client Installation 2-12
Accessing Web Sites Through a Secure HTTP Connection 2-12
Configuring for Offline Data Updates 2-12
Setting up the Server to use ISD for Tender Authorization 2-13
BIN Validation 2-13
Install the Java Cryptography Extension (JCE) 2-13
Results of a Point-of-Service Installation 2-14
Running Point-of-Service 2-15
Creating a Custom Installation 2-15

A Appendix: Installer Screens for Server Installation on Windows

B Appendix: Installer Screens for Client Installation on the Oracle Stack

C Appendix: Installer Silent Mode

D Appendix: URL Reference

JDBC URL for an Oracle 11g Database D-1
URL for the Siebel Web Service D-1

E Appendix: Common Installation Errors

"Pos installer finished with errors" E-1
"Dispatcher.main, Exception: java.security.AccessControlException: access denied (java.util.PropertyPermission * read,write)" E-1
"java.lang.NullPointerException" E-2

F Appendix: Troubleshooting Problems on the Oracle Stack

jndi.properties File Name F-1
Secure RMI and Secure JDBC F-1

G Appendix: Best Practices for Passwords

Password Guidelines G-1
Special Security Options for Oracle Databases G-2
Enforcing Password Policies Using Database Profiles G-2
Enforcing Password Policies Using a Verification Script G-2

H Appendix: Keytool Utility

Creating a Self-Signed Certificate H-1
Creating a Certificate Signing Request H-2
Exporting and Importing Certificates H-2

I Appendix: Secure JDBC with Oracle 11g Database

Creating the Oracle Wallet and Certificate for the Database Server I-1
Securing the Listener on the Server I-2
Examples of Network Configuration Files I-2
listener.ora I-3
sqlnet.ora I-3
tnsnames.ora I-3
Securing Client Access I-4
Specific Instructions for Point-of-Service I-4

J Appendix: Secure RMI

K Appendix: Device Configuration

Configuring Devices for an HP Register K-1
Configuring a Verifone Customer Interaction Device K-4

L Appendix: Installation Order

Enterprise Installation Order L-1

List of Figures

A–1 Introduction A-1
A–2 Previous POS Install A-2
A–3 License Agreement A-2
A–4 Supported Languages A-3
A–5 Enter Default Locale A-4
A–6 Tier Type A-5
A–7 Installation Location A-6
A–8 JRE Location A-7
A–9 JRE Vendor A-8
A–10 Derby Jars A-9
A–11 Store Server Details A-10
A–12 Store ID A-11
A–13 Integrate Applications A-12
A–14 Oracle Returns Management Messaging A-13
A–15 Application Server Type A-14
A–16 Database Type A-15
A–17 Database Owner A-16
A–18 Database Source User A-17
A–19 Install Database Option A-18
A–20 Enable Secure JDBC A-19
A–21 Data Source SSL Configuration A-20
A–22 Transaction Retrieval Location A-21
A–23 Scratchpad Database Information A-22
A–24 Scratchpad Database Install Options A-23
A–25 Enable Server Secure RMI A-24
A–26 POS Administrator User A-25
A–27 Server Journal Configuration A-26
A–28 Enter ORSIM Webservice URL A-27
A–29 ORSIM Integration Properties A-28
A–30 ORSIM Integration A-29
A–31 Enable POS-Siebel Webservice Access Over SSL A-30
A–32 POS-Siebel Webservice Authentication Type A-31
A–33 POS-Siebel Configuration A-32
A–34 Oracle Returns Management JMS Configuration A-33
A–35 POS - Returns Management Configuration A-34
A–36 Enable RMPOS Webservice access over SSL A-35
A–37 Enable Value-Added Tax (VAT) A-36
A–38 Enable RTLog Export A-37
A–39 Security Setup: Key Store Settings A-38
A–40 RSA Key Manager Requirements A-39
A–41 Key Store Details for RSA Key Manager 2.7.1 ..... A-40
A–42 Security Setup: Key Store JAR Files for RSA Key Manager 2.7.1 ..... A-41
A–43 RSA Key Store Configuration A-42
A–44 Key Store Pass Phrase for Simulator Key Manager A-43
A–45 Key Store Details for Other Key Manager A-44
A–46 Security Setup: Key Store JAR Files for Other Key Manager A-45
A–47 Logging Detail Options A-46
A–48 Logging Export Options A-47
A–49 Back Office Security A-48
A–50 Central Office Security Information A-49
A–51 Central Office Server Information A-50
A–52 Enable Transaction and Customer Retrieval Web Services A-51
A–53 Enable POS-CO Web Service Access Over SSL A-52
A–54 Back Office Server Information A-53

A–55 Tender Authorization ... A-54
A–56 Tender Authorization Parameters ... A-55
A–57 SSL Key Store Details ... A-56
A–58 SSL Trust Store Details ... A-57
A–59 Installation Progress ... A-58
A–60 Install Complete ... A-58
B–1 Introduction ... B-2
B–2 Previous POS Install ... B-2
B–3 License Agreement ... B-3
B–4 Supported Languages ... B-4
B–5 Enter Default Locale ... B-5
B–6 Tier Type ... B-6
B–7 Installation Location ... B-7
B–8 JRE Location ... B-8
B–9 JRE Vendor ... B-9
B–10 Derby Jars ... B-10
B–11 Store Server Details ... B-11
B–12 Store ID ... B-12
B–13 Register Number ... B-13
B–14 Integrate Applications ... B-14
B–15 Application Server Type ... B-15
B–16 Transaction Retrieval Location ... B-16
B–17 Enable Client Secure RMI ... B-17
B–18 ORSIM Integration ... B-18
B–19 Enable eReceipt ... B-19
B–20 eReceipt Properties ... B-20
B–21 Value-Added Tax (VAT) ... B-21
B–22 Security Setup: Key Store Settings ... B-22
B–23 RSA Key Manager Requirements ... B-23
B–24 Key Store Details for RSA Key Manager 2.7.1 ... B-24
B–25 Security Setup: Key Store JAR Files for RSA Key Manager 2.7.1 ... B-25
B–26 RSA Key Store Configuration ... B-26
B–27 Key Store Pass Phrase for Simulator Key Manager ... B-27
B–28 Key Store Details for Other Key Manager ... B-28
B–29 Security Setup: Key Store JAR Files for Other Key Manager ... B-29
B–30 Logging Detail Options ... B-30
B–31 POS Platform Components ... B-31
B–32 JPOS Device Setup: Library Files ... B-32
B–33 POS Devices ... B-33
B–34 CPOI Device Selection ... B-34
B–35 HP Environment Libraries ... B-35
B–36 JPOS Device Setup: jpos.xml directory ... B-36
B–37 CPOI Device Setup: Library files ... B-37
B–38 POS Printer Support ... B-38
B–39 Network Printer Support ... B-39
B–40 Network Printer Support Configuration ... B-40
B–41 EJournal Options ... B-41
B–42 JMS Queue Journal Support ... B-42
B–43 Back Office Security ... B-43
B–44 Parameter Distribution Information ... B-44
B–45 Back Office Server Information ... B-45
B–46 SSL Key Store Details ... B-46
B–47 SSL Trust Store Details ... B-47
B–48 User Interface Type ... B-48
B–49 Installation Progress ... B-49

B–50 Install Complete B-49

List of Tables

1–1 Store Server Requirements 1-2
1–2 Client Requirements 1-2
1–3 Supported Oracle Retail Products 1-3
1–4 Additional Oracle Technologies 1-3
1–5 ISD Authorization Transaction Set Tested 1-8
2–1 Server Tier Logical Components 2-3
2–2 Database Configuration Settings 2-4
2–3 <POS_install_directory> Subdirectories 2-14
2–4 <POS_install_directory>\pos Subdirectories 2-14

Send Us Your Comments

Oracle Retail Point-of-Service Installation Guide, Volume 1 - Oracle Stack, Release 13.3.3

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

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

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

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

> **Note:** Before sending us your comments, you might like to check that you have the latest version of the document and if any concerns are already addressed. To do this, access the Online Documentation available on the Oracle 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 http://www.oracle.com.

Preface

This Installation Guide describes the requirements and procedures to install this Oracle Retail Point-of-Service release.

Audience

This Installation Guide is written for the following audiences:

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

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/support/contact.html or visit http://www.oracle.com/accessibility/support.html if you are hearing impaired.

Related Documents

For more information, see the following document in the Oracle Retail Point-of-Service Release 13.3.3 documentation set:

- *Oracle Retail Point-of-Service Release Notes*
- *Oracle Retail POS Suite 13.3.3/Merchandising Operations Management 13.2.3 Implementation Guide*

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, 13.3) or a later patch release (for example, 13.3.3). If you are installing the base release, additional patch, and bundled hot fix releases, read the documentation for all releases that have occurred since the base release before you begin installation. Documentation for patch and bundled hot fix releases can contain critical information related to the base release, as well as information about code changes since the base release.

Oracle Retail Documentation on the Oracle Technology Network

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

http://www.oracle.com/technology/documentation/oracle_retail.html

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

Documentation should be available on this Web site within a month after a product release.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Preinstallation Tasks

This chapter describes the requirements for the Oracle stack that must be met before Oracle Retail Point-of-Service can be installed.

> **Note:** This is the Oracle stack configuration that was tested for this release. While Point-of-Service may work in other configurations, this configuration was tested.

If you will be installing multiple Oracle Retail applications, see Appendix L for a guideline for the order in which the applications should be installed.

Patch Contents

Patch releases include all defect fixes that have been released through bundled hot fix releases since the last patch release. Patch releases may also include new defect fixes and enhancements that have not previously been included in any bundled hot fix release. This patch release contains all fixes from the following bundled hot fix release:

- Oracle Retail Point-of-Service 13.3.0.1

Check for the Current Version of the Installation Guide

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

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

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

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

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

Check Supported Store Server Software Requirements

Table 1–1 lists the general requirements for a store server capable of running Point-of-Service and the versions supported for this release.

Table 1–1 Store Server Requirements

Supported on	Versions Supported
Operating System	Microsoft Windows 2008 Server R2 Standard Edition
Database	Oracle Database 11gR2 Enterprise Edition 11.2.0.1 (64-bit) **Note:** Oracle Retail Point-of-Service is not certified with Real Application Clusters (RAC).
JDK/JRE	Oracle JDK 5 Update 22

ISD Software Version for Tender Authorization

ISD Key Management messaging is used for encrypting all sensitive data in the request messages to the ISD host switch. If ISD is used for tender authorization, ensure you have one of the following versions, or newer, of the ISD software:

- ISD Payment Switch Authorization and Settlement Suite for Unix V5.3
- ISD Payment Switch Authorization and Settlement Suite for iSeries V5.3
- ISD Payment Switch Authorization and Settlement Suite for Java V6.4

Check Supported Client Hardware and Software Requirements

Table 1–2 lists the general requirements for a client capable of running Point-of-Service and the versions supported for this release. Mice are not supported for Point-of-Service. A touch screen may be used, but a keyboard is required for some functions. The configuration tested for this release included touch screens.

Note: It is the responsibility of the retailer to select peripheral devices that support the languages the retailer is using.

Table 1–2 Client Requirements

Supported on	Register Versions Supported
Register	HP POS RP5700, RP3000
Operating System	▪ Microsoft Windows Embedded POSReady 2009 **Note:** POSReady2009 must be installed with command-line utilities. See "Install Optional Components for Microsoft POSReady2009". ▪ Microsoft Windows 7 Pro FP-1 (32-bit)
JVM	Oracle JRE 5 Update 22
Cash drawer	HP Cash Drawer #EY024AA
Pole Display	VFD LD220
Keyboard	HP USB POS Keyboard Model SPOS
Scanner	HP USB Barcode Scanner LS2208
PIN Pad	Verifone MX860

Table 1–2 (Cont.) Client Requirements

Supported on	Register Versions Supported
Credit Card Reader	HP USB MSR Model IDRA-334133-HP
Receipt Printer	HP USB Hybrid Receipt Printer with MICR Model A776

Install Optional Components for Microsoft POSReady2009

To successfully use the install scripts, `findstr` must be available in Microsoft POSReady 2009. It is not available in a minimum installation of Microsoft POSReady, but is available in the Command-Line Utilities optional component. By default, the Command-Line Utilities optional component is included in the Accessories and Utilities optional component. For more information, see the following Web site:

`http://msdn.microsoft.com/en-us/library/dd458846(v=winembedded.20).aspx`

Check Oracle Retail Software Dependencies

Table 1–3 lists the Oracle Retail products that Oracle Retail Point-of-Service is integrated with and the required versions.

Table 1–3 Supported Oracle Retail Products

Integrates with	Version
Oracle Retail Back Office	13.3.3
Oracle Retail Central Office	13.3.3
Oracle Retail Merchandising System	13.2.3
Oracle Retail Price Management	13.2.3
Oracle Retail Returns Management	2.3.3
Oracle Retail Sales Audit	13.2.3
Oracle Retail Store Inventory Management	13.2.3 (on Oracle WebLogic)

Check Third-Party Software Dependencies

The Derby database files must be downloaded and the `derby.jar` and `derbytools.jar` files must be extracted. For more information on obtaining the software, see "Obtaining Third-Party Library Files Required by Point-of-Service" in Chapter 2.

Check Additional Oracle Technologies

Table 1–4 lists the Oracle technologies used by Oracle Retail Point-of-Service and the required versions.

Table 1–4 Additional Oracle Technologies

Integrates with	Version
Siebel	8.1.1.3

Integration with Other Applications

> **Note:** For the supported versions for integration with Oracle Retail Merchandising Operations Management products, see Table 1–3. For information on that integration, see the *Oracle Retail POS Suite/Merchandising Operations Management Implementation Guide*.

On the Integrate Applications screen, you select the applications that Oracle Retail Point-of-Service is integrated with.

- When installing the server, select all the applications that Point-of-Service is integrated with. See Figure A–13. You are prompted for any details needed for each selected application. For the server installer screens, see Appendix A.
- When installing a client, select the applications that the register is integrated with. See Figure B–14.

On the Tender Authorization screen, you select whether Oracle Retail Point-of-Service is integrated with ISD for tender authorization. See Figure A–55.

See the following sections for more information.

- "Oracle Retail Central Office and Back Office"
- "Oracle Retail Store Inventory Management"
- "Siebel"
- "Oracle Retail Returns Management"
- "Bill Payment"
- "ISD"

Oracle Retail Central Office and Back Office

Integration with Oracle Retail Central Office enables Centralized Transaction Retrieval and sending journal entries to the corporate office. The following details are required:

- Whether secure communication over HTTPS is used
- Details needed to access the Central Office server: host name, port number, User ID, and password

For integration with Oracle Retail Back Office, the following details are required:

- Whether secure communication over HTTPS is used
- Details needed to access the Back Office server: server name and port number

Oracle Retail Store Inventory Management

Integration with Oracle Retail Store Inventory Management is required to use the available features of Store Inventory Management. The following details are required:

- URL to access the Web service
- User ID and password to access the Web service if password-enabled access is selected
- Store Inventory Managment features to be integrated

Siebel

Siebel can be used for order management. The following details are required:

- Whether secure communication over HTTPS is used
- Type of Web service authentication
- URL to access the Web service
- User ID and password to access this store and all stores

Oracle Retail Returns Management

Oracle Retail Returns Management can be used to authorize returns. The following details are required:

- If JMS is the method used for sending return result messages, the port number is needed
- The following is needed for accessing the Returns Management Web service:
  - User ID and password
  - Whether secure communication over HTTPS is used
  - Port number

Bill Payment

The bill payment feature enables the retailer to to capture bill payments made by their subscribers or customers at a Point-of-Service register. The retailer is responsible for setting up and maintaining the integration with the bill payment application. For information on the parameters available for bill payment, see the *Oracle Retail POS Suite Configuration Guide*.

ISD

If Oracle Retail Point-of-Service is integrated with ISD for tender authorization, you provide the host name and port number of the tender authorizer.

- For the steps performed after the server installation, see "Setting up the Server to use ISD for Tender Authorization" in Chapter 2.
- For the list of transactions tested for this release, see "ISD Authorization Transaction Testing" in this chapter.

Hardware Requirements

The hardware requirements for the store server and client depend on different variables.

You need to determine your hardware requirements, based on the variables mentioned here, as well as any additional variables specific to your environment. For more information, contact Customer Support.

Store Server

Specific hardware requirements for the machines running the Oracle Retail Point-of-Service store server depend on variables including the number of users and other applications running on the same machine.

Please note the following about the hardware requirements:

- The CPU requirement depends on variables including the number of Point-of-Service clients and the operating system and middleware selected.
- Memory requirements and performance depend on variables including the number of active promotions and best deal calculations.

- Disk size can vary based on the operating system and middleware requirements as well as the amount of data storage needed. Data storage depends on variables including the number of items and promotions defined, data retention period, and so on.

Client

Specific hardware requirements for the machines running the Oracle Retail Point-of-Service client depend upon the point-of-sale system/register manufacturer and other applications and utilities running on the client.

Peripheral Devices for Clients

JavaPOS is the industry standard for Java compatibility for retail-oriented devices. A committee of prominent retail vendors and end users maintains the standard. Some of the more common devices used with point-of-sale applications include bar code scanners, cash drawers, printers, keyboards, magnetic stripe readers (MSR), wedge keyboards, hard totals, and magnetic ink check readers (MICR). Any JavaPOS-compliant peripheral devices should work with Oracle Retail Point-of-Service, however, some may require software modifications to work properly.

Check Supported Java Key Manager Requirement

Oracle Retail Point-of-Service requires that a Java Key Store is created prior to installation. Up to five jar files can be provided by the retailer to enable the connection between Oracle Retail Point-of-Service and the Key Manager. Specific information for configuring the Key Manager is entered on the Security Setup: Key Store installer screens.

If you are using the RSA Key Manager, you must use version 2.7.1 and install the Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files 5.0. See "Install the Java Cryptography Extension (JCE)" in Chapter 2.

Note: If you are using the simulator key manager, a pass phrase is used to access the Key Manager simulator. The pass phrase is entered on the Key Store Pass Phrase installer screen.

Use the same pass phrase for all Oracle Retail POS Suite applications in your configuration.

Caution: A simulated key management package is bundled with Oracle Retail Point-of-Service. It is not compliant with either the Payment Application Data Security Standard (PA-DSS) or Payment Card Industry Data Security Standard (PCI-DSS). It is made available as a convenience for retailers and integrators. If you use the simulated key manager, you will not be PCI-DSS compliant. Therefore, the simulated key manager should be replaced with a compliant key manager.

Check Secure JDBC and Secure RMI

For information on enabling secure JDBC and RMI, see "Securing Communication" in Chapter 2.

ISD Authorization Transaction Testing

ISD authorization transaction testing was done with ISD Standard Interface version 266. The capture method used was terminal capture. The following applications were tested:

- ISD Host Switch version 6.5.0.003

Note: Host capture is not supported.

Table 1–5 shows the transaction types and messages that were tested.

Table 1–5 ISD Authorization Transaction Set Tested

Transaction Type	Transaction Type Message Sent from ISD to Point-of-Service
Check Tender	■ Check Sale Approval ■ Check Sale Authorization Offline ■ Check Sale Decline ■ Check Sale Referral
Credit Card Tender	■ Credit Card Sale Approval ■ Credit Card Sale Authorization Offline ■ Credit Card Sale Decline ■ Credit Card Sale Referral
Debit Card Tender	■ Debit Sale Approval ■ Debit Sale Authorization Offline ■ Debit Sale Decline
Gift Card Issue	■ Gift Card Issue Approval ■ Gift Card Issue Authorization Offline ■ Gift Card Issue Decline ■ Gift Card Issue Referral
Gift Card Redeem	■ Gift Card Redeem Approval ■ Gift Card Redeem Authorization Offline
Gift Card Refund	■ Gift Card Issue Approval ■ Gift Card Issue Authorization Offline ■ Gift Card Issue Decline ■ Gift Card Issue Referral
Gift Card Reload	■ Gift Card Reload Approval ■ Gift Card Reload Authorization Offline ■ Gift Card Reload Decline
Gift Card Tender	■ Gift Card Sale Approval ■ Gift Card Sale Authorization Offline ■ Gift Card Sale Decline ■ Gift Card Sale Referral

Implementation Guidelines for Security

Note: A demonstration trust store is bundled with Oracle Retail Point-of-Service. It is recommended that the demonstration trust store is replaced with a secure trust store.

It is also recommended that the passwords for key stores and trust stores are changed from the values set by default.

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

https://support.oracle.com

Oracle Retail POS Suite Implementation Guide, Volume 2 - Security **(Doc ID: 1277445.1)**

This implementation guide volume describes specific security features and implementation guidelines for the POS Suite products.

2

Installation on the Oracle Stack using Windows

This chapter provides information about the installation procedures for Oracle Retail Point-of-Service on the Oracle Stack using Windows. For a list of tested components and supported versions for the Oracle stack, see Chapter 1.

Oracle Retail provides an installer for Point-of-Service, but customer installations typically develop custom procedures. Note that the installer is not appropriate for all installations. Oracle Retail expects implementation teams to develop custom procedures for actual register installations, which may or may not be based on the installer described here. For guidelines, see "Creating a Custom Installation".

Create the Database Schema Owner and Data Source Users

The following recommendations should be considered for schema owners:

- Database administrators should create an individual schema owner for each application, unless the applications share the same data. In the case of Oracle Retail Back Office and Point-of-Service, the database schema owner are the same because these applications share a database.
- The schema owners should only have enough privileges to install the database.

For information on the best practices for passwords, see Appendix G.

Whether the database schema owner user and the data source user need to be created is dependent on whether Point-of-Service shares the database with Back Office:

- If Point-of-Service is sharing the database with Back Office, the same database schema owner is used for both products. Point-of-Service and Back Office can use the same data source user or a separate data source user can be created for each product.
- If Point-of-Service is not sharing the database with Back Office, both the database schema owner and data source user need to be created.

To create the database schema owner:

1. Log in using the database administrator user ID.
2. Create a role in the database to be used for the schema owner.

   ```
   CREATE ROLE <schema_owner_role>;
   ```

3. Grant the privileges, shown in the following example, to the role.

   ```
   GRANT CREATE TABLE, CREATE VIEW, CREATE SEQUENCE, CREATE PROCEDURE, ALTER
   SESSION, CONNECT, SELECT_CATALOG_ROLE TO <schema_owner_role>;
   ```

4. Create the schema owner user in the database.

```
CREATE USER <schema_username>
IDENTIFIED BY <schema_password>
DEFAULT TABLESPACE users
TEMPORARY TABLESPACE TEMP
QUOTA UNLIMITED ON users;
```

5. Grant the schema owner role to the user.

```
GRANT <schema_owner_role> TO <schema_username>;
```

To create the data source user:

1. If not already logged in, log in using the database administrator user ID.
2. Create a role in the database to be used for the data source user.

```
CREATE ROLE <data_source_role>;
```

3. Grant the privileges, shown in the following example, to the role.

```
GRANT CONNECT, CREATE SYNONYM, SELECT_CATALOG_ROLE TO
<data_source_role>;
```

4. Create the data source user.

```
CREATE USER <data_source_username>
IDENTIFIED BY <data_source_password>
DEFAULT TABLESPACE users
TEMPORARY TABLESPACE TEMP
QUOTA UNLIMITED ON users;
```

5. Grant the data source role to the user.

```
GRANT <data_source_role> TO <data_source_username>;
```

The installer grants the data source user access to the application database objects.

Note: If the data source user, *<data_source_user>*, created for Point-of-Service is not the same user ID created for the Back Office data source user, the Point-of-Service user must be granted access to the database schema after the Point-of-Service server is installed. After running the installer, see "Enabling Access for the Data Source User".

Installing Point-of-Service

To establish an initial Oracle Retail Point-of-Service installation or to create a demonstration system, use the Point-of-Service installer as described in this section.

Determining Tier Type

Machines and logical components of the Oracle Retail Point-of-Service application are defined in Table 2–1:

Table 2–1 Server Tier Logical Components

Machine	Description
Store Server	The machine that runs the server component of Oracle Retail Point-of-Service. There is at least one store server for each store. This component runs as a service. This machine may also house the Back Office Server and other Oracle Retail POS Suite components such as the OracleRetailStore database.
Point-of-Service Clients	The machines that execute the Point-of-Service transactions; they are typically cash registers.
Database Server	The machine that houses the OracleRetailStore databases. This machine may or may not be the same as the store server.
JMS Server	The machine that houses the JMS server software.

When you run the installer, it asks you to specify a Tier Type. The following types are available:

- N-Tier Client—Choose this when installing the client component.
- N-Tier Store Server—Choose this when installing the store server component.

Installing the Database

Oracle Retail products such as Point-of-Service and Back Office use the OracleRetailStore database. One OracleRetailStore database is typically installed in each store. Data stored in the OracleRetailStore database includes employee names, logon information, and transaction data. The database can be located on the store server or on a separate machine acting as the database server. The database must be installed before Point-of-Service can be installed.

If you are using Centralized Transaction Retrieval, an additional database called the Scratchpad database is used. This database holds retrieved transactions. For more information on Centralized Transaction Retrieval, see the *Oracle Retail Point-of-Service Operations Guide*.

Separate Databases Used for the Store and Scratchpad Databases

If you are using two different databases for the store and scratchpad databases, you need to update the database URL for the scratchpad database after installation is complete.

Update the `<POS_install_directory>\Server\pos\config\technician\EnterpriseDataTechnician.xml` file. The `<POOL>` entry for the scratchpad database is the first pool entry in the file. It has the name `jdbcpool`. Update the URL in the following property:

```
<CONNECTIONPROPERTY propname="databaseUrl" propvalue="" />
```

Table 2–2 shows the database configuration information that is needed during installation.

Table 2–2 Database Configuration Settings

Installer Screen	Required Data
Transaction Retrieval Location	Choose the location for retrieving transactions. When using Centralized Transaction Retrieval, choose either the **Central** or **Central, Local Failover** option. **Note:** You must choose the same location for both the store server and client installations.
Database Configuration	Enter the following information for the database: ■ JDBC driver path ■ Driver class name ■ Database URL ■ Jar name ■ Database schema owner user ID and password ■ Data source user ID and password
Scratchpad Database Configuration	Enter the following information for the Scratchpad database: ■ JDBC driver path ■ Driver class name ■ Database URL ■ Jar name ■ Scratchpad database owner user ID and password
Logging Options	Choose how the log is exported. When using Centralized Transaction Retrieval, choose the **Data Replication Export** option.
Central Office/Back Office Server Information	Enter the host names and port numbers of the machines where the Central Office instance and the Back Office instance for this store server are located.

Required Settings for the Database

The following settings must be made during database creation:

- The database must be set to UTF8.
- When using the Oracle 11g database server, make the following changes to the system settings:

```
ALTER SYSTEM SET NLS_NUMERIC_CHARACTERS = '.,-' SCOPE=SPFILE;
ALTER SYSTEM SET NLS_DATE_FORMAT ='YYYY-MM-DD' SCOPE=SPFILE;
ALTER SYSTEM SET NLS_TIMESTAMP_FORMAT = 'YYYY-MM-DD HH24:MI:SS.FF'
SCOPE=SPFILE;
```

Installing Point-of-Service on Machines

If a previous version of Point-of-Service is installed on a machine, uninstall it by deleting the installation directory (the default directory is `c:\OracleRetailStore`) or choose a different installation directory from the default.

Run the installer one time for each machine in the Server Tier and once for each register.

The installer performs the following steps. Not all steps apply to client and server installations.

- Installs Foundation, Retail Domain, and Oracle Retail Point-of-Service jar files.
- Installs database build scripts and start-up files.
- Defines Server Tier in the conduit script that starts Point-of-Service for the given machine.
- Defines hostnames or IP addresses and port numbers for the Store Server and database server.
- Defines device availability.
- Defines application properties for Store ID and Register Number.

Updating Device Configuration

Instructions for configuring peripheral devices are in Appendix K. For more information, see the applicable section in the appendix:

- "Configuring Devices for an HP Register"
- "Configuring a Verifone Customer Interaction Device"

Expand the Point-of-Service Distribution

To extract the Point-of-Service files:

1. Extract the `ORPOS-13.3.3.zip` file from the Point-of-Service 13.3.3 distribution.
2. Create a new staging directory for the Point-of-Service application distribution `ORPOS-13.3.3.zip` file, for example, `c:\tmp\orpos\orpos-staging`.

   Note: The staging area (*<staging_directory>*) can exist anywhere on the system. It does not need to be under `ORACLE_HOME`.

3. Copy or upload `ORPOS-13.3.3.zip` to *<staging_directory>* and extract its contents. The following files and directories should be created under *<staging_directory>*`\ORPOS-13.3.3`:

```
ant\
ant-ext\
antinstall\
installer-resources\
installer-templates\
product\
antinstall-config.xml
build.xml
build-antinstall.xml
build-common.xml
build-common-oas.xml
build-common-retailinv.xml
build-common-was.xml
build-common-wl.xml
build-conditions.xml
build-filesets.xml
build-filters.xml
build-properties.xml
checkdeps.cmd
```

```
checkdeps.sh
install.cmd
install.sh
prepare.xml
wallet.xml
```

For the remainder of this chapter, *<staging_directory>*\ORPOS-13.3.3 is referred to as *<INSTALL_DIR>*.

Obtaining Third-Party Library Files Required by Point-of-Service

The Point-of-Service application uses specific files from Apache. Get the required files for the Derby database. You can get the download at the Web site:

http://db.apache.org/derby/releases/release-10.5.3.0.html

Extract the following files:

- derby.jar
- derbytools.jar

Obtaining the JRE Required for Client Install

Obtain the required JRE for the client install.

Obtaining the JRE Required for Client Install on HP Registers

This release requires Oracle's JRE 1.5 update 22 for client installs on HP registers. The download is available at the following Web site:

https://cds.sun.com/is-bin/INTERSHOP.enfinity/WFS/CDS-CDS_Developer-Site/en_US/-/USD/ViewProductDetail-Start?ProductRef=jre-1.5.0_22-oth-JPR@CDS-CDS_Developer

Increase the Heap Size on the Client

If Microsoft Windows 7 Pro FP-1 is being used for the client operating system, set the heap size in the *<INSTALL_DIR>*/product/client/bin/ClientConduit.bat file to the following:

```
set JAVA_MEM_OPTIONS=-Xms84m -Xmx256m
```

Securing Communication

Communication with the database and communication between the store server and registers can be secured.

- On the Enable Secure JDBC screen, you select whether secure JDBC will be used for communication with the database. See Figure A–20.
  - If **Yes** is selected, the installer sets up the secure JDBC.
  - If **No** is selected and you want to manually set up the secure JDBC after the installer completes, see Appendix I.

- On the Enable Secure RMI screen, you select whether secure RMI will be used for communication between the store server and registers. See Figure A–25 and Figure B–17.
  - If **Yes** is selected, the installer sets up the secure RMI.
  - If **No** is selected and you want to manually set up the secure RMI after the installer completes, see Appendix J.

Database Install Options

On the Install Database Option screen, you select whether the installer creates and populates the database schema or if you want to do this manually.

> **Caution:** If the database schema is already created and populated, select **Skip schema creation and data loading**. Selecting one of the other options will result in the loss of the data already in the database. If the database schema was created and populated using Back Office, Labels and Tags data, reports data, and Back Office parameters will be lost.

- If you choose **Create schema with sample dataset**, the installer creates and populates the database with sample data, such as item data. The sample dataset includes the minimum dataset. If you want data available to use for demonstrating Point-of-Service functionality after installation, you can select this option.
- If you choose **Create schema with minimum dataset**, the installer creates and populates the database with the minimum amount of data needed to launch and run Point-of-Service. If you want to load your own data after installation, you can select this option.
- If you choose **Skip schema creation and data loading**, the installer does not create and populate the database schema. This is the default selection on the screen. You choose this option if you want to create and populate the database schema manually or the database schema was created using Back Office.

  For information on manually creating and populating the database schema, see "Creating the Database Schema".

Creating the Database Schema with Oracle Retail Back Office

When Point-of-Service will be used with Back Office, create the database schema during the Back Office installation. See the *Oracle Retail Back Office Installation Guide* for information.

Running the Point-of-Service Application Installer

This installer will configure and deploy the Point-of-Service application.

> **Note:** To see details on every screen and field for a server installation, see Appendix A. To see details for a client installation, see Appendix B.

1. Change to the *<INSTALL_DIR>* directory.

2. Set the `JAVA_HOME` environment variable to the location of a version 1.5 JDK. The variable must be set to the location of the JDK and not the JRE.

   Note: The installer is not compatible with versions of Java earlier than 5 Update 22.

3. When installing the store server, set the account of the user running the installer to run as an administrator. Set the account using Microsoft Windows 2008 Server.
4. Run the `install.cmd` script. This will launch the installer. After installation is complete, a detailed installation log file is created at `<POS_install_directory>\pos-install-yyyyMMddHHmm.log`

   In the log file name, `yyyyMMddHHmm` is the timestamp of the install.

   Note: The typical usage for GUI mode does not use arguments.

   ```
   install.cmd
   ```

Resolving Errors Encountered During Application Installation

If the application installer encounters any errors, you can read them in the above mentioned log file.

For a list of common installation errors, see Appendix E.

Update JMS Configuration for Integration with Returns Management

If Point-of-Service will be integrated with Returns Management and a JMS queue is the method that will be used for sending return result messages to Returns Management, you can create a remote queue for the store server for processing the final result messages. Use of the remote queue is an optional alternative to the default released configuration.

Note: To use the remote queue, updates are also needed to the JMS configuration for Back Office. For more information, see the following guide:

- *Oracle Retail Back Office Installation Guide, Volume 1 -Oracle Stack*

In the `<POS_install_directory>\<server>\pos\config\conduit\StoreServerConduit.xml` file, update the following properties in `ReturnsTechnician` to correspond to the Back Office host and port:

```
<PROPERTY propname="returnsManagerServerName" propvalue="$RM_SERVER_HOSTNAME$"/>
<PROPERTY propname="returnsManagerServerPort" propvalue="$RM_SERVER_PORT$"/>
```

Creating the Database Schema

The scripts that create the database schema can be run from the installed `pos\bin` directory. The database server can be on the same system as the application server or on a different system.

Creating without Oracle Retail Back Office

> **Note:** Sample data can be used to evaluate the application and demonstrate core functions of the software. There are references in the sample data to store ID 01291. During installation, if 01291 is selected for the store ID, SQL errors occur during the loading of the database. The SQL errors are caused by those references.

When the database schema is not created with Back Office, perform the following steps to create the database schema:

1. Change to the *<POS_install_directory>*`\pos\bin` directory.
2. Set the `JAVA_HOME` and `ANT_HOME` environment variables.
3. Add `%JAVA_HOME%\bin` and `%ANT_HOME%\bin` to the front of the PATH environment variable.

   ```
   set PATH=%JAVA_HOME%\bin;%ANT_HOME%\bin;%PATH%;
   ```

4. Run one of the available `dbbuild.bat` targets to create the database schema, load data, and load the procedures for purging aged data in the database. For information on the purge procedures, see the *Oracle Retail Point-of-Service Operations Guide*.
   - sample: creates the database schema containing the sample dataset. The sample dataset includes the minimum dataset.
   - minimum: creates the database schema containing the minimum dataset.
   - load_purge_procedures: loads the database purge procedures.

   For example, `dbbuild.bat sample`
5. If you are using Centralized Transaction Retrieval, create the Scratchpad database if it is not already created. If **Central** or **Central, Local Failover** is selected for the Transaction Retrieval Location and **No** is selected for the Scratchpad Database Install Options, the installer assumes the Scratchpad database already exists and does not create it.

   To create the Scratchpad database, run `scratchpad.bat`.

Enabling Access for the Data Source User

If Back Office will be used and the data source user, *<data_source_username>*, created for Point-of-Service is not the same user ID created for the Back Office data source user, the Point-of-Service user must be granted access to the database schema after the Point-of-Service server is installed.

To grant access to the database:

1. Change to the *<POS_install_directory>*`\`*<server>*`\pos\bin` directory.
2. Set the `JAVA_HOME` and `ANT_HOME` environment variables.

3. Add %JAVA_HOME%\bin and %ANT_HOME%\bin to the front of the PATH environment variable.

```
set PATH=%JAVA_HOME%\bin;%ANT_HOME%\bin;%PATH%;
```

4. Run the following ant target.

```
ant -f db.xml -Dschema.user=<data_source_username> -Dschema.password=<data_
source_password> grant_schema
```

Installing Multibyte Fonts for eReceipt in the Client Installation

When an eReceipt is sent to a customer by e-mail, a pdf file that contains the eReceipt is attached to the e-mail. In order for this pdf file to print correctly with multibyte characters, the multibyte fonts must be defined in the client installation.

Point-of-Service uses Apache Formatting Objects Processor (FOP) to create eReceipts that are compatible with Adobe Acrobat. FOP and Adobe Acrobat require information about the fonts to use in the eReceipt. You must install and configure any mutlibyte fonts needed for eReceipts.

Note: Point-of-Service assumes that fonts are fixed-width for the formatting of receipts. If variable-width fonts are used, the fields on an eReceipt will not align properly.

To update the fonts in the client installation:

1. Install the required fonts to the Windows operating system of each client.
2. Generate a font metrics file.

   The fop.jar file provides a TTFReader program to generate this file. The fop.jar file is available in the *<POS_install_directory>**<client>*\common\lib\ext directory. The following are examples of the commands to use:

   - To specify a collection of fonts (TTC font):

     ```
     java -classpath <POS_install_directory>\<client>\common\lib\ext\fop.jar
     org.apache.fop.fonts.apps.TTFReader -ttcname "Gulim"
     c:\windows\fonts\gulim.ttc gulim.xml
     ```

   - To specify a specific font (TTF font):

     ```
     java -classpath <POS_install_directory>\<client>\common\lib\ext\fop.jar
     org.apache.fop.fonts.apps.TTFReader c:\windows\fonts\SIMSUN.TTF SIMSUN.xml
     ```

3. Update the configuration file at *<POS_install_directory>**<client>*\pos\receipts\printing\ereceipt\eReceiptFontConfig.xml. Point-of-Service updates the FOP configuration to use the new fonts in addition to the standard fonts available. The following is an example of the structure of the configuration file based on the commands in the previous step.

```
<configuration>
.................
<fonts>
.................
.................
  <font metrics-file="c:\windows\config\gulim.xml"
 embed-file="c:\windows\fonts\gulim.ttc" kerning="yes">
     <font-triplet name="Gulim" style="normal" weight="normal"/>
```

```
    <font-triplet name="Gulim" style="normal" weight="bold"/>
    <font-triplet name="Gulim" style="italic" weight="normal"/>
    <font-triplet name="Gulim" style="italic" weight="bold"/>
 </font>
.................
.................
</fonts>
.................
</configuration>
```

4. To use the new fonts, set the value for the `ereceipt.font.family` key in the *<POS_install_directory>*`\`*<client>*`\pos\config\application.properties` file. The following is an example of the setting:

```
ereceipt.font.family=Gulim, SimSun, MingLiU, Gothic, Courier
```

Note: eReceipt uses the Auto font selection strategy, which is the default font selection strategy. This strategy selects the first font from the list that is able to display the most characters in a word that contains characters that need different fonts.

Enabling the Printing of Receipts in Chinese on a Network Printer

To print receipts in Chinese on a network printer:

1. Make sure East Asian fonts are installed on Windows.
2. Install the client with Chinese language selected as a supported language and network printing enabled.
3. Change the font from Courier to MS Gothic in `OracleRetailStore\Client\pos\receipts\printing\templates\xsl\ipp_default.xsl`:

   ```
   <xsl:template match="text">
   ```

   ```
   <fo:block text-align="left" font-family="MS Gothic"
   ```

4. Set alwaysPrintLineFeeds to true in PrinterActionGroup in `OracleRetailStore\Client\pos\config\device\posdevices.xml`:

   ```
   <PROPERTY propname="alwaysPrintLineFeeds" propvalue="true"
   proptype="BOOLEAN" />
   ```

5. Start the client. Print a receipt in Chinese to the network printer. Verify that it aligned properly.

Enabling Browser Functionality in the Client Installation

Point-of-Service provides the capability to access a Web site from a register using the **Browser** button on the Main Options screen. JDIC is required for this functionality.

To enable browser functionality:

1. Install JDIC on the client:

   JDIC version 0.9.5 is available at the following Web site:

   http://java.net/projects/jdic/sources/svn/show/tags/RELEASE_JDIC_0_9_5/src/jdic/ndist?rev=1736

   a. Download the `jdic.jar` file.

   b. Download the `windows` folder and its contents into a local `windows` folder keeping the same directories and files that you see on the Web site:

   ```
   windows\
     x86\
       IeEmbed.exe
       jdic.dll
       jdic_native.jar
       MozEmbed.exe
       tray.dll
   ```

   c. Copy the `jdic.jar` file and `windows` directory to the *<POS_install_directory>*`\`*<client>*`\common\lib\ext` directory.

2. Set up the Browser URL parameter. For information on this parameter, see the *Oracle Retail POS Suite Configuration Guide*.

3. Verify that the desired browser is the system default.

Accessing Web Sites Through a Secure HTTP Connection

If a Web site is accessed through a secure HTTP connection, an SSL certificate is required. A non-trusted SSL certificate can be installed, but the JDIC does not handle certificate errors that occur for secured Web sites. To avoid the certificate errors on Microsoft Internet Explorer, the Internet options security settings for Trusted sites need to be set as follows:

1. Add the server or IP address, on which the secured application is deployed, to the list of Trusted sites.

2. Uncheck the option to require server verification (https:) for all sites in the zone.

Configuring for Offline Data Updates

Point-of-Service provides the capability to automatically update offline data to clients. The scheduling of the updates can be configured. This configuration involves updating parameters and the `ServiceContext.xml` file. For more information on offline data updates and how to configure the updates, see the *Oracle Retail Point-of-Service Operations Guide*.

Setting up the Server to use ISD for Tender Authorization

Note: ISD Key Management messaging is used for encrypting all sensitive data in the request messages to the ISD host switch. Ensure you have one of the following versions, or newer, of the ISD software:

- ISD Payment Switch Authorization and Settlement Suite for Unix V5.3
- ISD Payment Switch Authorization and Settlement Suite for iSeries V5.3
- ISD Payment Switch Authorization and Settlement Suite for Java V6.4

If **ISD** was selected on the Tender Authorization screen, you must update the security for your store server JRE. See "Install the Java Cryptography Extension (JCE)".

Note: This update is only needed on the store server.

BIN Validation

The Bin File Lookup parameter, in the Tender parameter group, determines if BIN validation on credit cards is performed using a BIN file provided by the retailer. While results will vary by retailer, this parameter enables the retailer to reduce their interchange fees, that is, the amount a retailer is charged for authorization of credit cards.

To use the BIN file provided by the retailer, set the Bin File Lookup parameter to Yes. The default for this parameter is Yes.

Install the Java Cryptography Extension (JCE)

If **ISD** was selected on the Tender Authorization screen or **RSA Key Manager v2.7.1** was selected on the Security Setup: Key Store Settings screen, you must update the security for your JRE. You need to obtain version 5.0 of the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.

1. Make a backup copy of `local_policy.jar` and `US_export_policy.jar`.
   - On the server:

     ```
     cd %JRE_HOME%\lib\security
     copy local_policy.jar local_policy.jar.bak
     copy US_export_policy.jar US_export_policy.jar.bak
     ```

   - On the client:

     ```
     cd %JRE_HOME%\lib\security
     copy local_policy.jar local_policy.jar.bak
     copy US_export_policy.jar US_export_policy.jar.bak
     ```

2. Download version 5.0 of the JCE.
   a. Go to the following Web site:

      http://www.oracle.com/technetwork/java/javase/downloads/index-jdk5-jsp-142662.html

b. Under Other Downloads, find **Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 5.0**.

c. Click **Download**.

d. Follow the instructions to download the JCE.

3. Copy the jar files into the JRE security directory. The files are bundled as `jce_policy-1_5_0.zip`.

Results of a Point-of-Service Installation

The default root directory for OracleRetailStore applications on Windows for the store server is `c:\OracleRetailStore\Server`. For the client, the default directory is `C:\OracleRetailStore\Client`. In this guide, these directories are referred to as *<POS_install_directory>*. The subdirectories listed in Table 2–3 are created:

Table 2–3 <POS_install_directory> Subdirectories

Name	Contents
common	Files shared by multiple Oracle Retail POS Suite applications including Foundation or 360Platform, Domain, and third-party jar files
pos	Point-of-Service files

Important subdirectories of the `\pos` directory are shown in Table 2–4:

Table 2–4 <POS_install_directory>\pos Subdirectories

Name	Contents
bin	Startup batch files and shell scripts
config	XML configuration files, `.properties` files, and `.dat` files
lib	Point-of-Service application and resource jar files
lib/locales	Text bundles for localization
logs	Log files (additional log files are in the `bin` directory)
receipts	Files for printing of receipts and blueprint jar file

Running Point-of-Service

You run the Oracle Retail Point-of-Service system by executing batch files or shell scripts, found in your installation's `bin` directory, to launch various components.

> **Note:** For each command, a Windows batch file (such as `dbstart.bat`) exists.

To run Point-of-Service:

1. Start the store server:

   `StoreServerConduit.bat`

   When the message TierManager Started appears, the server has started. The server component does not have a user interface.

2. Start the registers.

   For each of the Point-of-Service registers, execute the conduit script that starts the Point-of-Service client component. Use the following command:

   `ClientConduit.bat`

3. Verify the installation on each register by logging in to Point-of-Service.

   If the login is successful and the status bar indicates the database is online, the installation is complete.

Creating a Custom Installation

A custom installation of Point-of-Service can use one of several approaches:

- Install Point-of-Service using the installer on a reference machine, and copy the resulting installation to other machines.
  - With this method, you can change the configuration settings of the installation as described in the *Oracle Retail Point-of-Service Operations Guide* until the installation works as desired, then propagate those configurations to other machines.
  - You can copy just the installation directory to a new machine, or if the hardware is sufficiently similar, you can copy the entire hard drive image to the machine. Copying the entire hard drive retains the JavaPOS installation as well as any other customizations.
  - You must change the WorkstationID value for the target machines to a unique number. This value can be found in *<POS_install_directory>*`\pos\config\application.properties`.
- Create a custom installer which allows for various hardware options but specifies the software choices your company has chosen.

> **Note:** By default, installation of a register requires certain IBM Install Set parameters to have specific values:
>
> - Hard Total must be Off.

A

Appendix: Installer Screens for Server Installation on Windows

You need specific details about your environment for the installer to successfully install the Point-of-Service application on the Oracle Stack on Windows. This appendix shows the screens that are displayed during the installation of the Point-of-Service server. Depending on the options you select, you may not see some screens or fields.

For each field on a screen, a table is included in this appendix that describes the field.

For the installer screens for a client installation, see Appendix B.

Figure A–1 Introduction

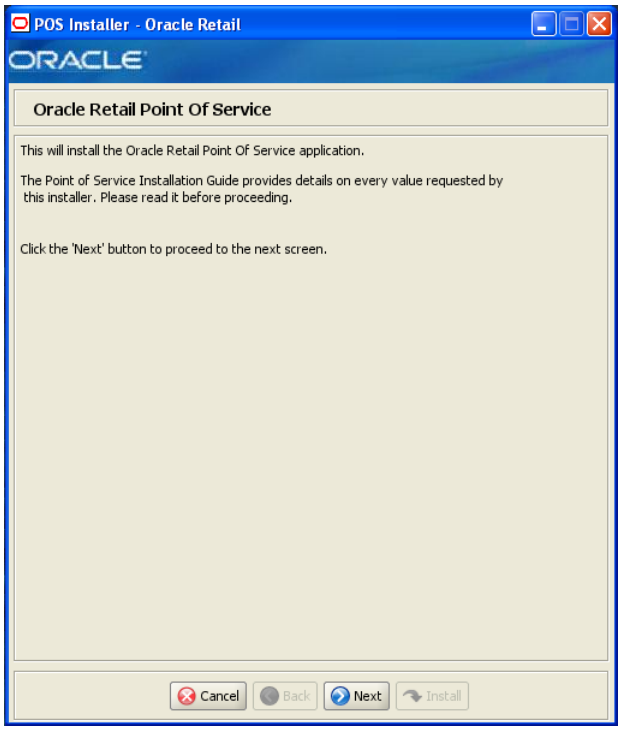


Figure A–2 Previous POS Install

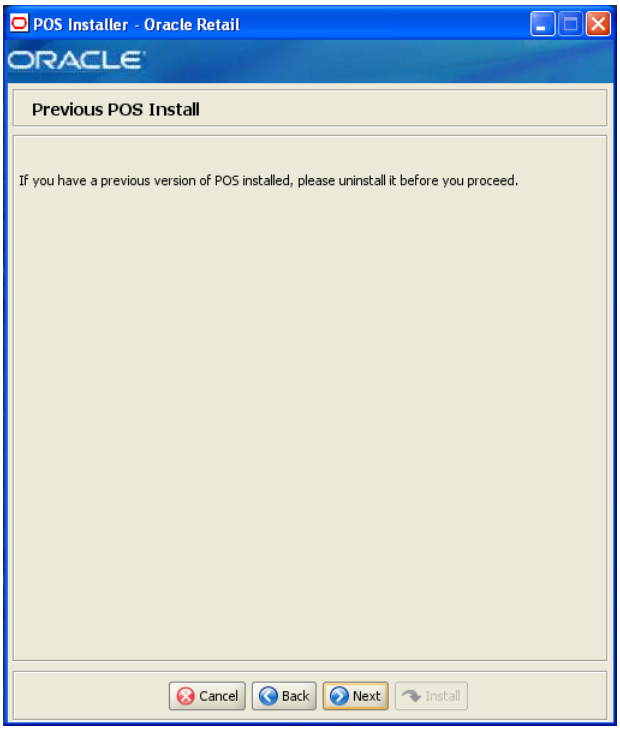
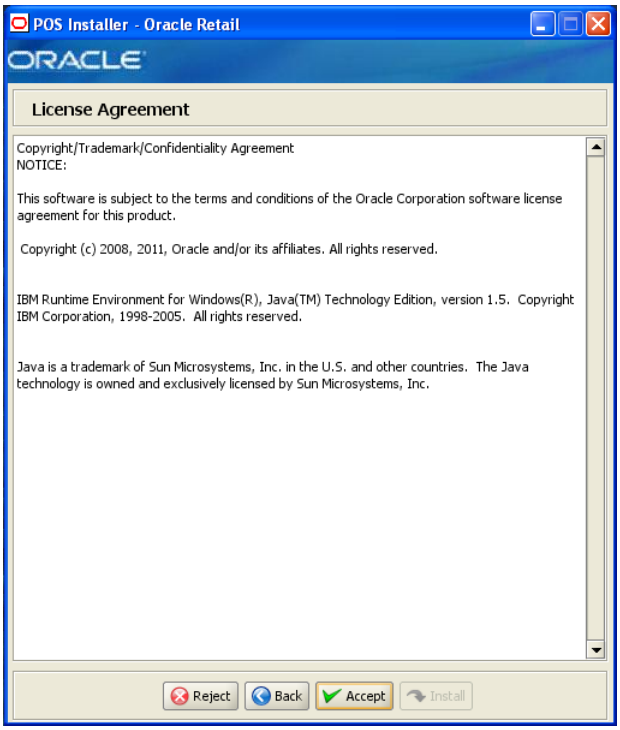
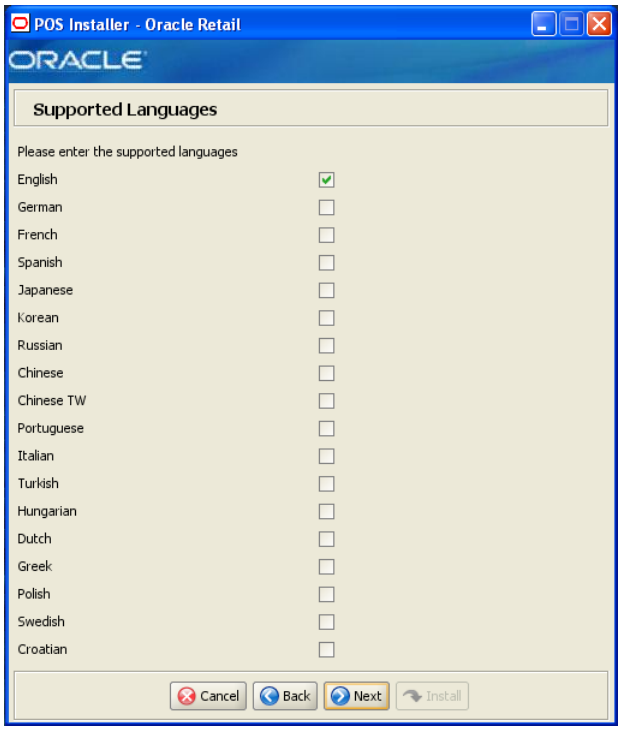


Figure A–3 License Agreement



Note: You must choose to accept the terms of the license agreement in order for the installation to continue.

Figure A–4 Supported Languages



The field on this screen is described in the following table.

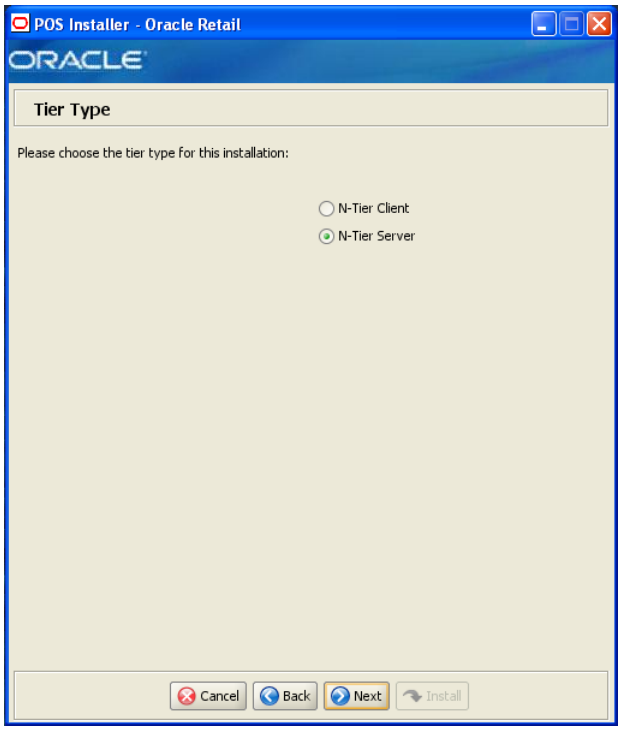
Field Title	Please enter the supported languages
Field Description	Select the languages that will be available for the Point-of-Service application. The languages selected on this screen determine the available choices on the Enter Default Locale screen.
Example	English

Figure A–5 Enter Default Locale

The field on this screen is described in the following table.

Field Title	Enter Default Locale
Field Description	Locale support in Point-of-Service enables the date, time, currency, calendar, address, and phone number to be displayed in the format for the selected default locale. The choices for default locale are dependent on the selections made on the Supported Languages screen. For each selected language, the default locale for that language is displayed on the Enter Default Locale screen. For example, if English and French are selected on the Supported Languages screen, en_US and fr_FR are the available choices for the default locale.
Example	en_US

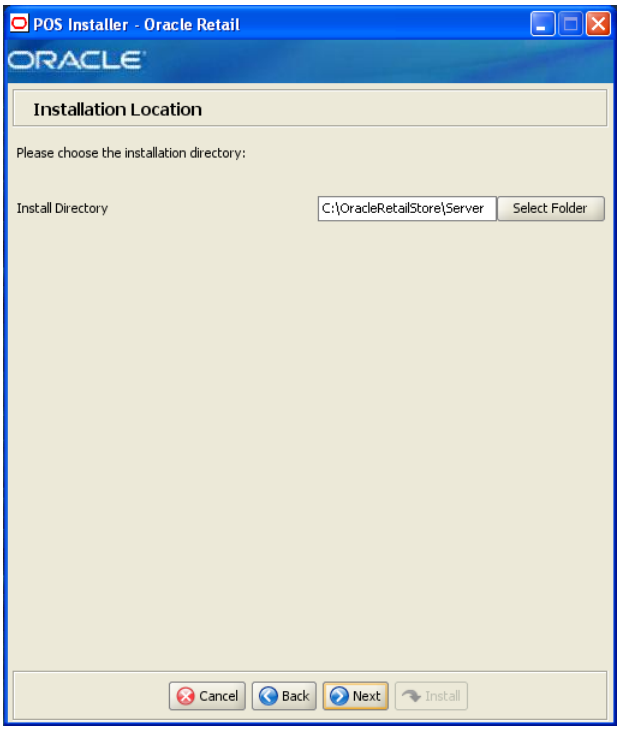
Figure A–6 Tier Type



The field on this screen is described in the following table.

Field Title	Tier Type
Field Description	Choose the server tier type for this installation. For more information, see "Determining Tier Type" in Chapter 2. To install the N-Tier version of the server, choose **N-Tier Server**.
Example	N-Tier Server

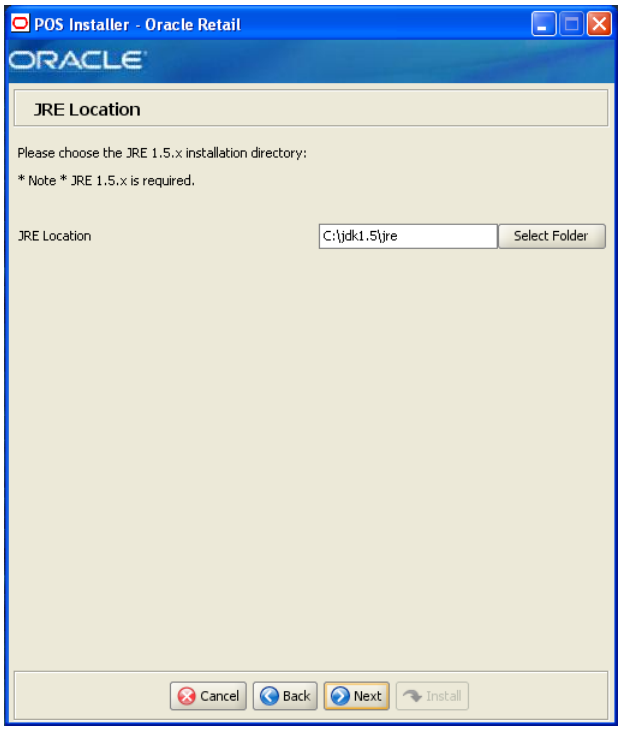
Figure A–7 Installation Location



The field on this screen is described in the following table.

Field Title	Install Directory
Field Description	Choose the directory into which the Point-of-Service files are copied. The default for the first directory in the path is `OracleRetailStore`. This directory should be the same for all Oracle Retail POS Suite products. When installing for Windows and **N-Tier Server** is selected for the Tier Type, the default installation directory is `OracleRetailStore\Server`. **Note:** The server and the client must not be installed into the same directory. In this guide, *<POS_install_directory>* refers to the selected installation directory for the server or client. Files specific to Point-of-Service are copied to the `\pos` subdirectory of `<POS_install_directory>`.
Example	`C:\OracleRetailStore\Server`

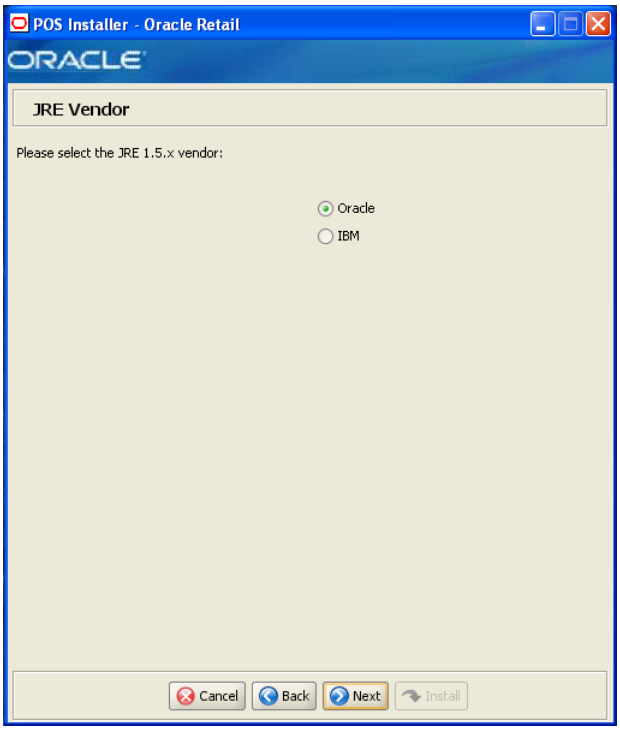
Figure A–8 JRE Location



The field on this screen is described in the following table.

Field Title	Folder
Field Description	Enter the location where the JRE is installed.
Example	`C:\jdk1.5\jre`

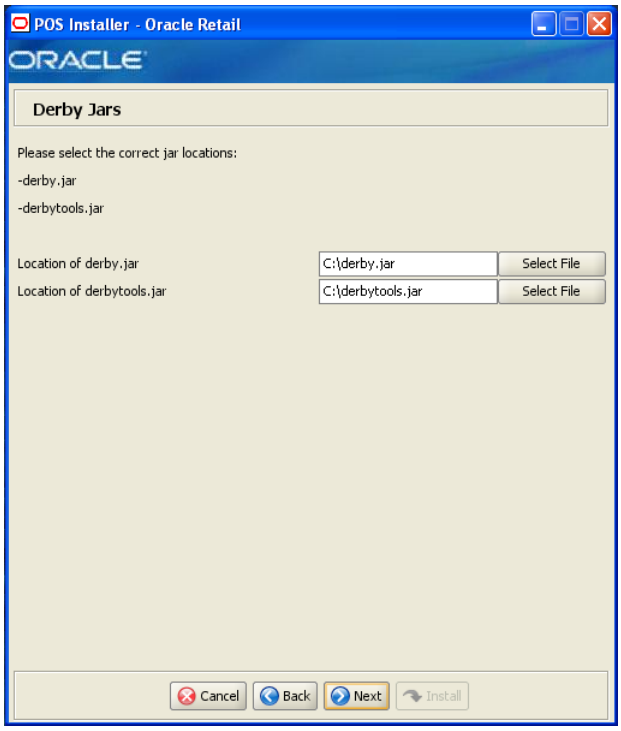
Figure A–9 JRE Vendor



The field on this screen is described in the following table.

Field Title	JRE Vendor
Field Description	Select the vendor for the JRE entered on the JRE Location screen: ▪ Oracle ▪ IBM Choose **Oracle**.

Figure A–10 Derby Jars

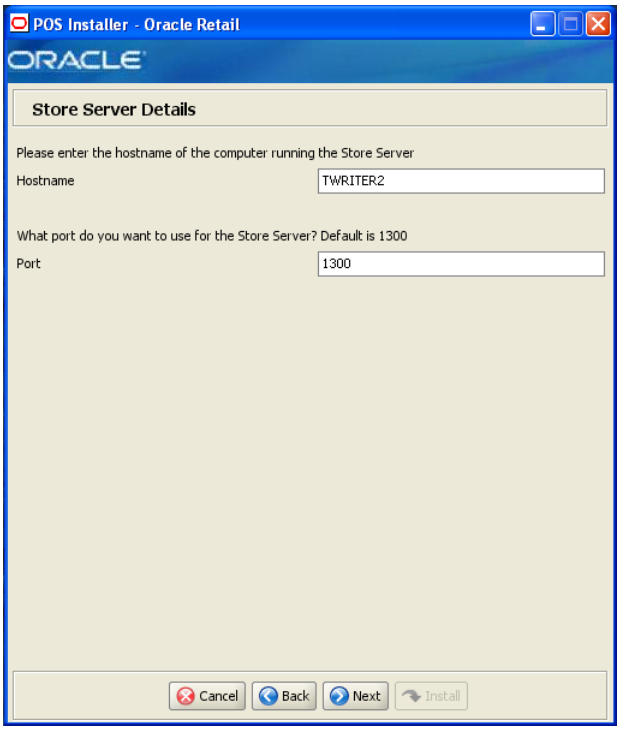


The fields on this screen are described in the following tables.

Field Title	Location of derby.jar
Field Description	Choose the location of the `derby.jar` file.
Example	`C:\derby.jar`

Field Title	Location of derbytools.jar
Field Description	Choose the location of the `derbytools.jar` file.
Example	`C:\derbytools.jar`

Figure A–11 Store Server Details

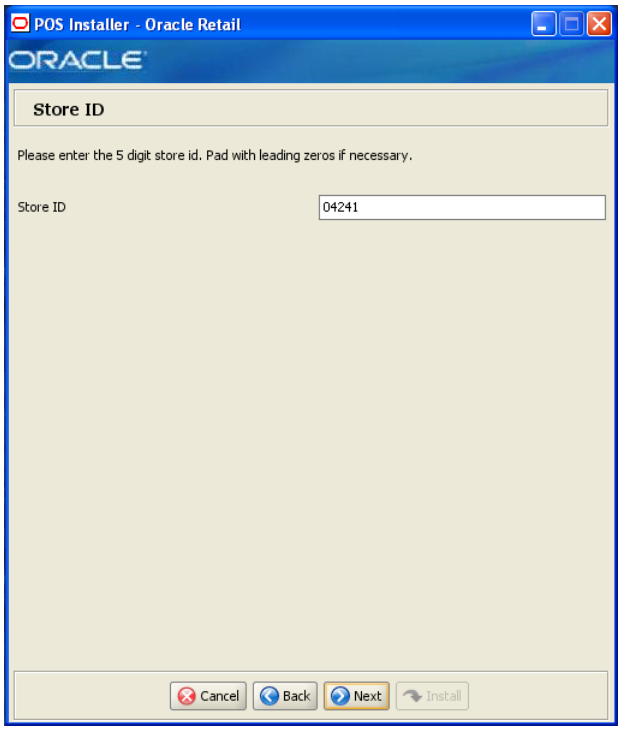


The fields on this screen are described in the following tables.

Field Title	Hostname
Field Description	Enter the host name of the store server.
Example	TWRITER2

Field Title	Port
Field Description	Enter the port number of the store server used for the communication between the store server and the host computer.
Example	1300

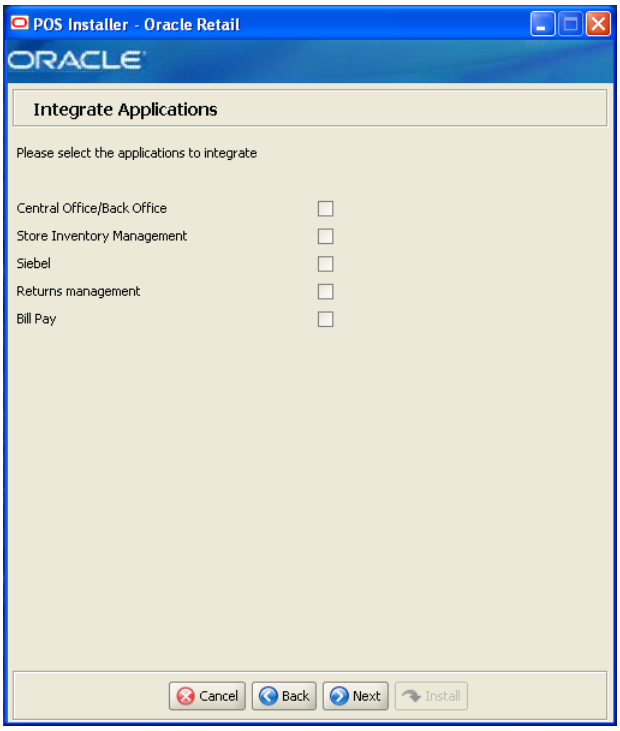
Figure A–12 Store ID



The field on this screen is described in the following table.

Field Title	Store ID
Field Description	Enter the store ID. **Note:** The store ID must be five digits. It can be padded with leading zeroes if necessary. The store ID can only contain the numeric characters 0 through 9.
Example	04241

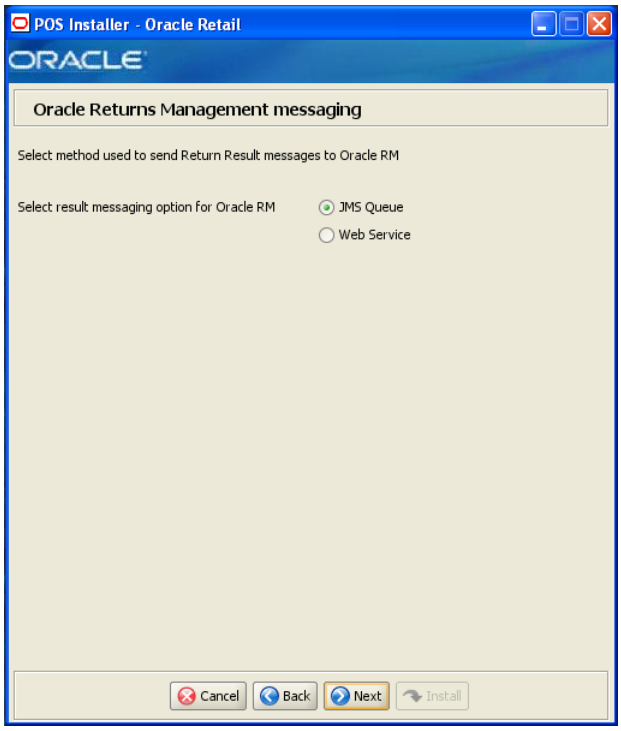
Figure A–13 Integrate Applications



The field on this screen is described in the following table.

Field Title	Applications
Field Description	Select the applications that Point-of-Service is integrated with. ▪ Central Office/Back Office ▪ Store Inventory Management ▪ Siebel ▪ Returns Management ▪ Bill Pay

Figure A–14 Oracle Returns Management Messaging



This screen is only displayed if **Returns Management** is selected on the Integrate Applications screen.

The field on this screen is described in the following table.

Field Title	Select result messaging option for Oracle Retail Returns Management
Field Description	Choose the method to use to send return result messages to Oracle Retail Returns Management. ▪ If you want messages sent to a JMS queue, choose **JMS Queue**. ▪ If you want to use a Web service to send the messages, choose **Web Service**.
Example	JMS Queue

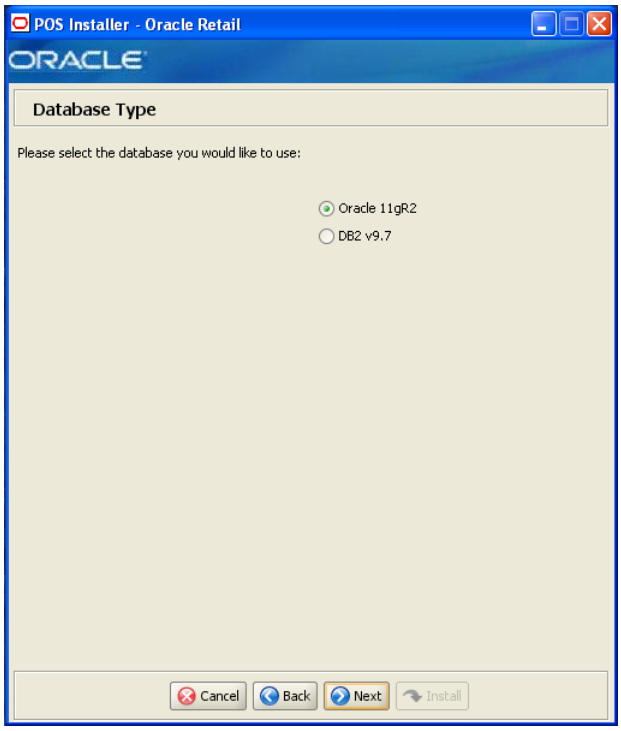
Figure A–15 Application Server Type

This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

The field on this screen is described in the following table.

Field Title	Application Server Type
Field Description	Select the application server to be used for the store server. ▪ WebLogicApplication Server ▪ Websphere Application Server Choose **WebLogic Application Server**.

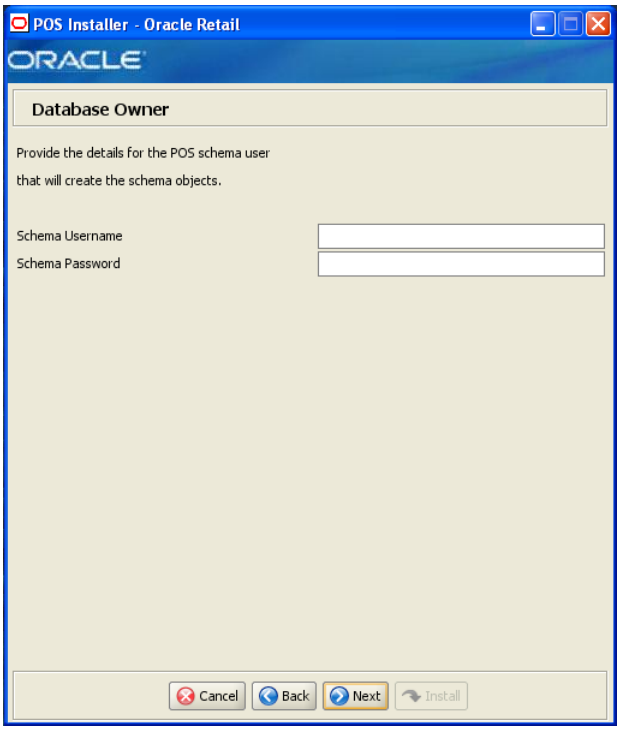
Figure A–16 Database Type



The field on this screen is described in the following table.

Field Title	Database Type
Field Description	Select the database provider that is used for the OracleRetailStore database. ■ Oracle 11gR2 ■ DB2 v9.7 Choose **Oracle 11gR2**.

Figure A–17 Database Owner

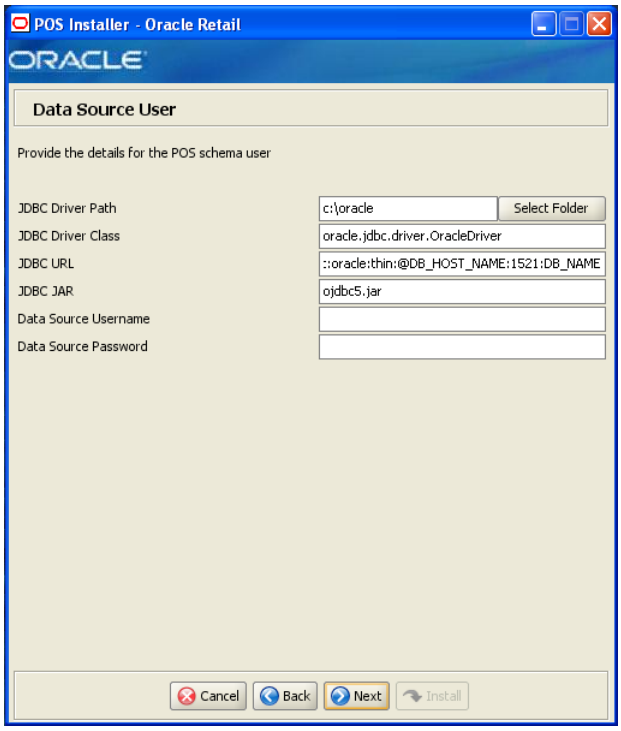


The fields on this screen are described in the following tables.

Field Title	Schema Username
Field Description	Schema user name that manages the objects in the schema. This user has Create, Drop, and Alter privileges in the schema, that is, Data Definition Language (DDL) execution privileges. For information on creating this user, see "Create the Database Schema Owner and Data Source Users" in Chapter 2. **Note:** This user creates the database objects used by Point-of-Service.
Example	DBOWNER

Field Title	Schema Password
Field Description	Enter the password for the database owner.

Figure A–18 Database Source User



The fields on this screen are described in the following tables.

Field Title	JDBC Driver Path
Field Description	Choose the path to the jar containing the database driver. This is the jar entered in the JDBC JAR field.
Example	`c:\oracle`

Field Title	JDBC Driver
Field Description	Enter the database driver class name.
Example	`oracle.jdbc.driver.OracleDriver`

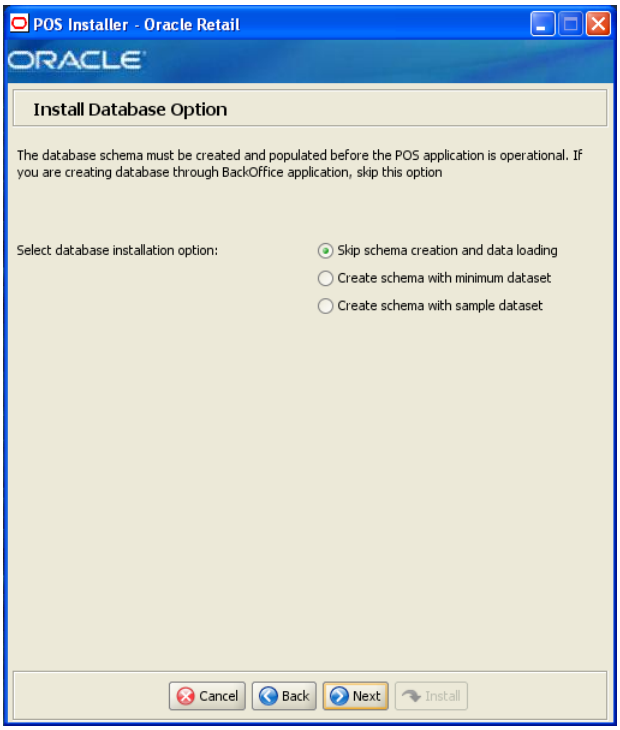
Field Title	JDBC URL
Field Description	Enter the URL used by the Point-of-Service application to access the database schema. For the expected syntax, see Appendix D.
Example	`jdbc:oracle:thin:@myhost:1521:mydatabase`

Field Title	JDBC JAR
Field Description	Enter the name of the jar containing the database driver.
Example	`ojdbc5.jar`

Field Title	Data Source Username
Field Description	Database user name that can access and manipulate the data in the schema. This user can have Select, Insert, Update, Delete, and Execute privileges on objects in the schema, that is, Data Manipulation Language (DML) execution privileges. For information on creating this user, see "Create the Database Schema Owner and Data Source Users" in Chapter 2. **Note:** This schema user is used by Point-of-Service to access the database.
Example	DBUSER

Field Title	Data Source Password
Field Description	Enter the password for the data source user.

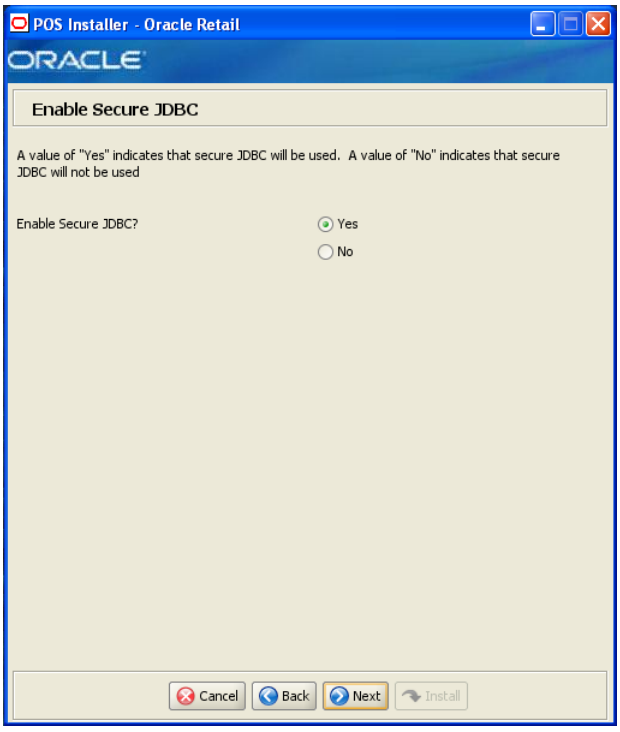
Figure A–19 Install Database Option



The field on this screen is described in the following table.

Field Title	Select database installation option
Field Description	The database schema must be created and populated before starting Point-of-Service. This screen gives you the option to have the installer create and populate the database schema or leave the database schema unmodified. **Caution:** If the database schema is already created and populated, select **Skip schema creation and data loading**. Selecting one of the other options will result in the loss of the data already in the database. If the database schema was created and populated using Back Office, Labels and Tags data, reports data, and Back Office parameters will be lost. ▪ To have the installer leave the database schema unchanged, select **Skip schema creation and data loading**. ▪ To have the installer create and populate the database schema with the minimum dataset, select **Create schema with minimum dataset**. ▪ To have the installer create and populate the database schema with the sample dataset, select **Create schema with sample dataset**. For more information, see "Database Install Options" in Chapter 2.
Example	Skip schema creation and data loading

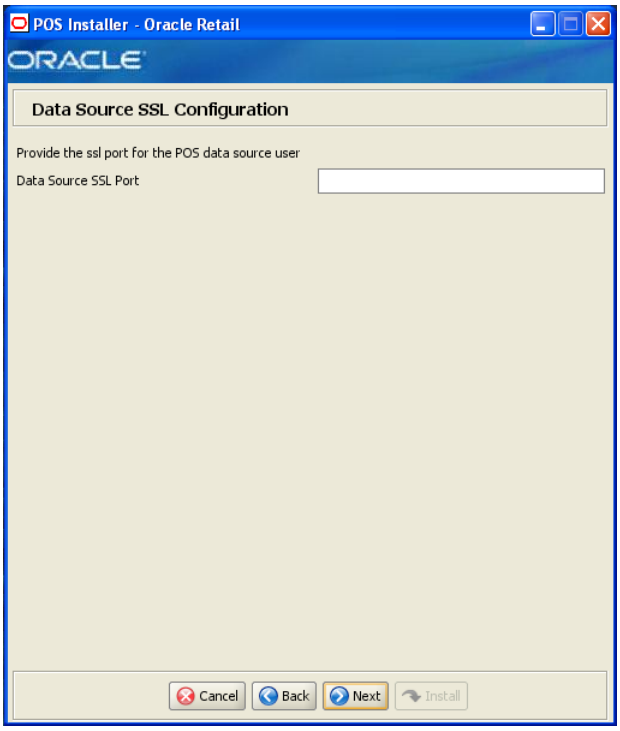
Figure A–20 Enable Secure JDBC



The field on this screen is described in the following table.

Field Title	Enable Secure JDBC?
Field Description	Select whether secure JDBC is to be used for communication with the database.
Example	Yes

Figure A–21 Data Source SSL Configuration

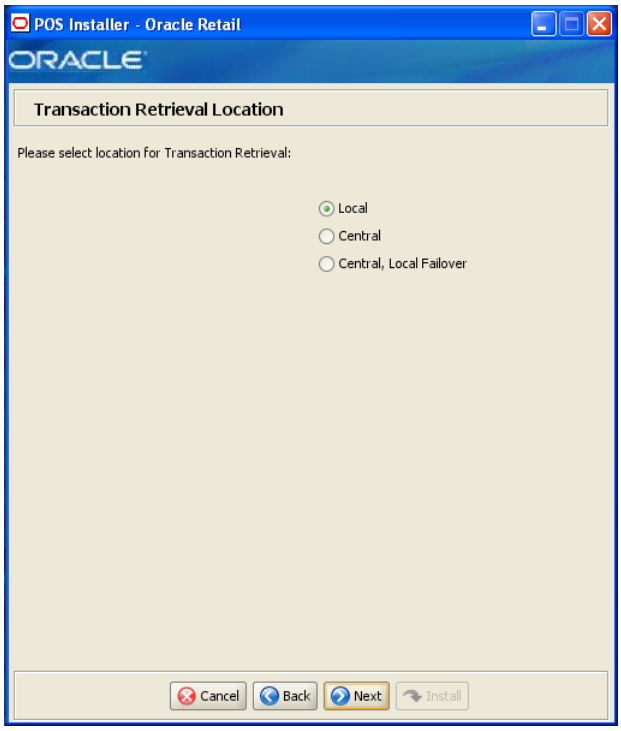


This screen is only displayed if **Yes** is selected on the Enable Secure JDBC screen.

The field on this screen is described in the following table.

Field Title	Data Source SSL Port
Field Description	SSL port used to access the database.
Example	7002

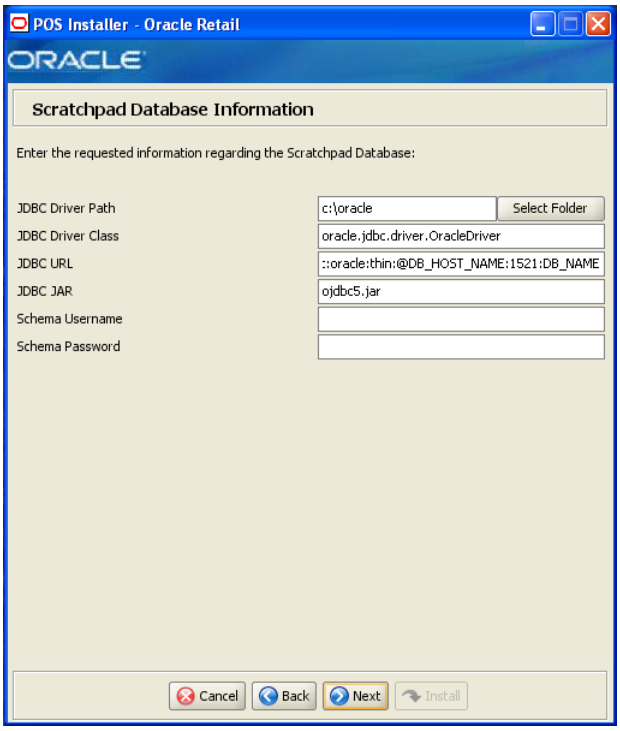
Figure A–22 Transaction Retrieval Location



The field on this screen is described in the following table.

Field Title	Transaction retrieval location
Field Description	Choose the location for retrieving transactions. ▪ If transactions should only be retrieved from the store database, choose **Local**. ▪ If transactions should only be retrieved from the corporate database, choose **Central**. ▪ If transactions should be retrieved from the corporate database, and if not found, then retrieved from the store database, choose **Central, Local Failover**. **Note:** You must choose the same location for both the store server and client installations.
Example	Local

Figure A–23 Scratchpad Database Information



This screen is only displayed if **Central** or **Central, Local Failover** is selected on the Transaction Retrieval Location screen.

The fields on this screen are described in the following tables.

Field Title	JDBC Driver Path
Field Description	Choose the path to the jar containing the database driver. This is the jar entered in the JDBC JAR field.
Example	`C:\oracle`

Field Title	JDBC Driver Class
Field Description	Enter the database driver class name.
Example	`oracle.jdbc.driver.OracleDriver`

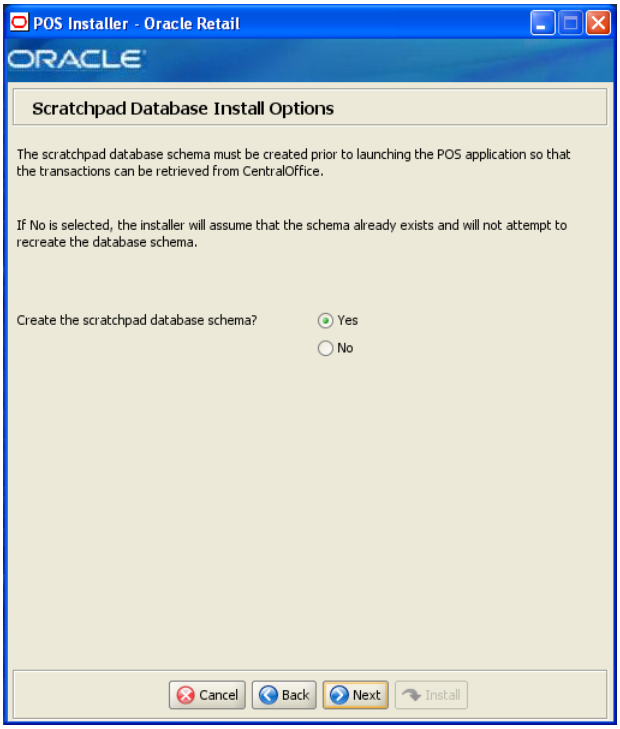
Field Title	JDBC URL
Field Description	Enter the URL used by the Point-of-Service application to access the database schema. For the expected syntax, see Appendix D.
Example	`jdbc:oracle:thin:@myhost:1521:mydatabase`

Field Title	JDBC JAR
Field Description	Enter the name of the jar containing the database driver.
Example	`ojdbc5.jar`

Field Title	Schema
Field Description	Enter the database user that owns the scratchpad database.
Example	DBUSER

Field Title	Schema Password
Field Description	Enter the password for the database user that owns the scratchpad database.

Figure A–24 Scratchpad Database Install Options

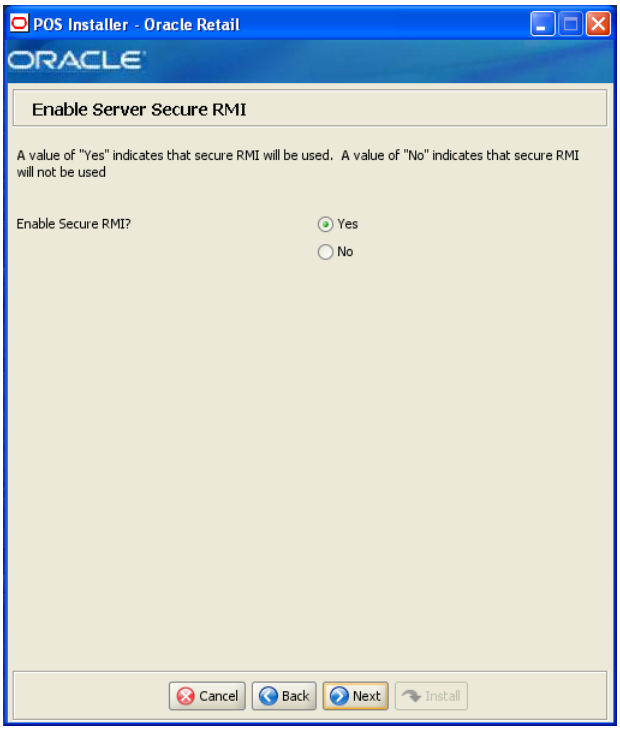


This screen is only displayed if **Central** or **Central, Local Failover** is selected on the Transaction Retrieval Location screen.

The field on this screen is described in the following table.

Field Title	Create the scratchpad database schema
Field Description	Choose whether the installer creates the scratchpad database schema.
Example	Yes

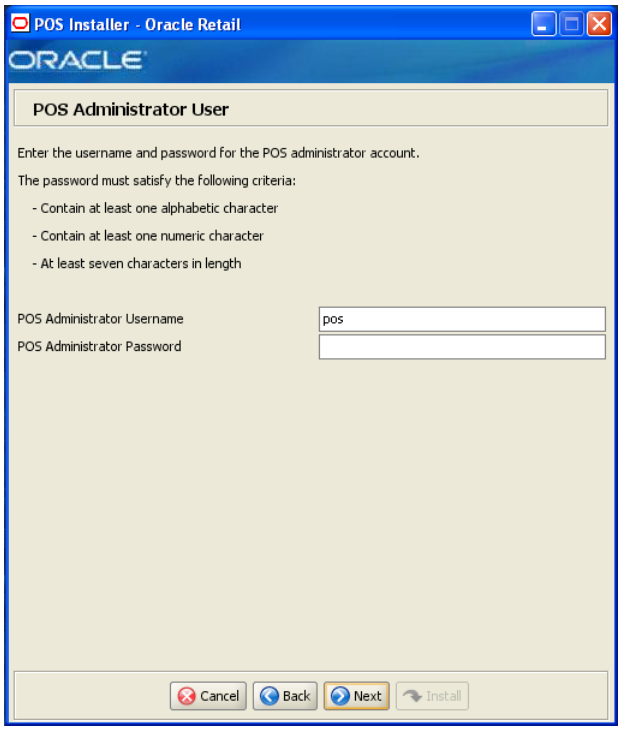
Figure A–25 Enable Server Secure RMI



The field on this screen is described in the following table.

Field Title	Enable Secure RMI?
Field Description	Select whether secure RMI is to be used for communication between the store server and registers.
Example	Yes

Figure A–26 POS Administrator User

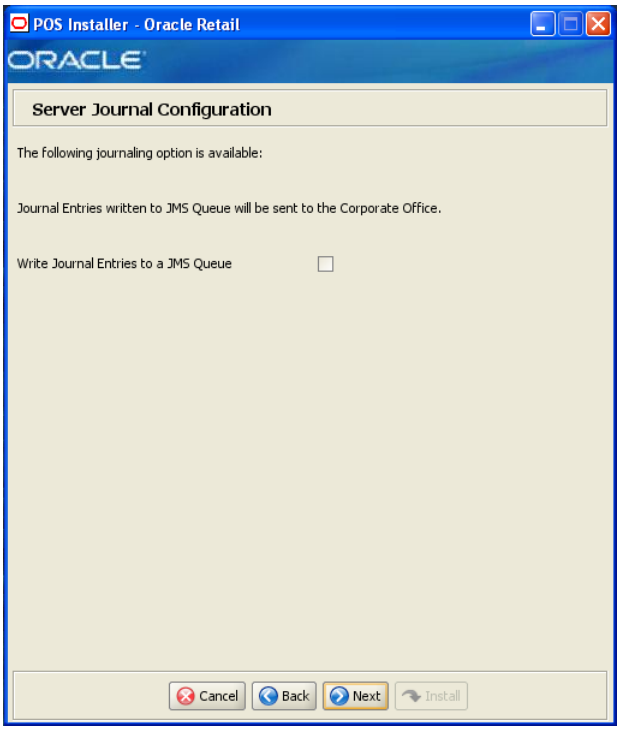


The fields on this screen are described in the following tables.

Field Title	POS Administrator Username
Field Description	Enter the user name used for performing Point-of-Service administrative functions.
Example	pos

Field Title	POS Administrator Password
Field Description	Enter the password for the administrator user.

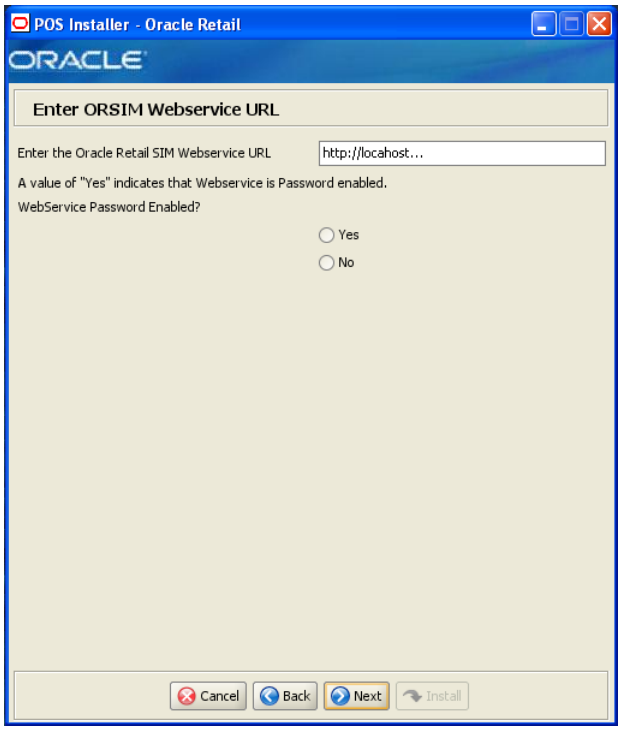
Figure A–27 Server Journal Configuration



The field on this screen is described in the following table.

Field Title	Write Journal Entries to a JMS Queue
Field Description	Check the box if the journal entries written to a JMS queue are sent to the corporate office.

Figure A–28 Enter ORSIM Webservice URL



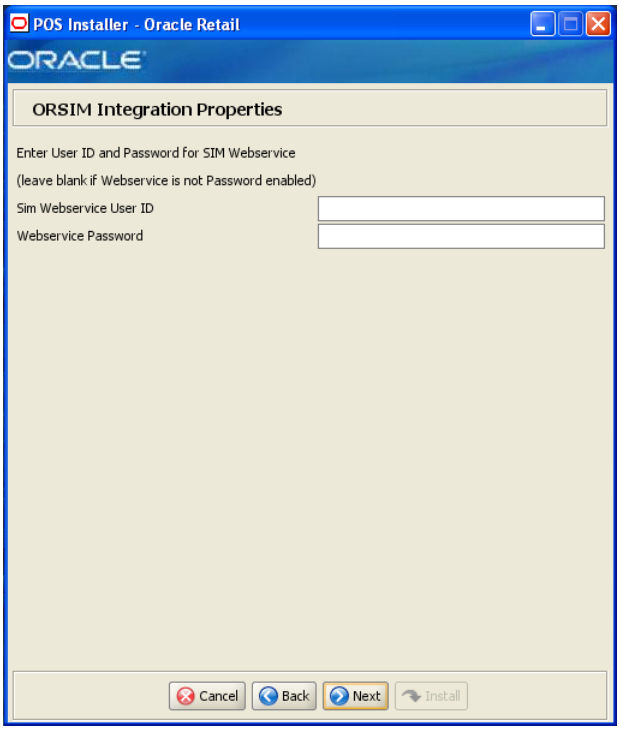
This screen is only displayed if **Store Inventory Management** is selected on the Integrate Applications screen.

The fields on this screen are described in the following tables.

Field Title	Enter the Oracle Retail Webservice URL
Field Description	Enter the URL used by the Point-of-Service application to access Oracle Retail Store Inventory Management.

Field Title	WebService Password Enabled
Field Description	Choose whether the Web service is password enabled.

Figure A–29 ORSIM Integration Properties



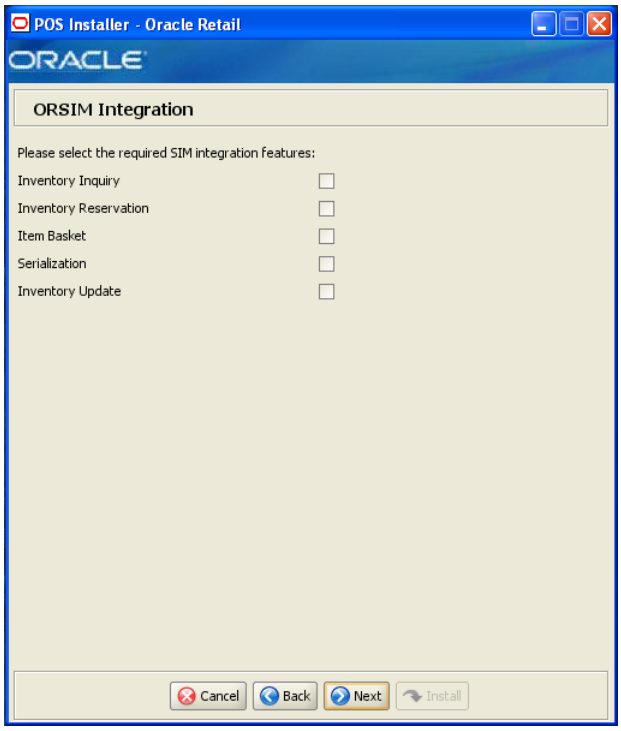
This screen is only displayed if **Store Inventory Management** is selected on the Integrate Applications screen.

The fields on this screen are described in the following tables.

Field Title	SIM Webservice User ID
Field Description	Enter the user ID used to access Oracle Retail Store Inventory Management.

Field Title	WebService Password
Field Description	Enter the password used to access Oracle Retail Store Inventory Management.

Figure A–30 ORSIM Integration

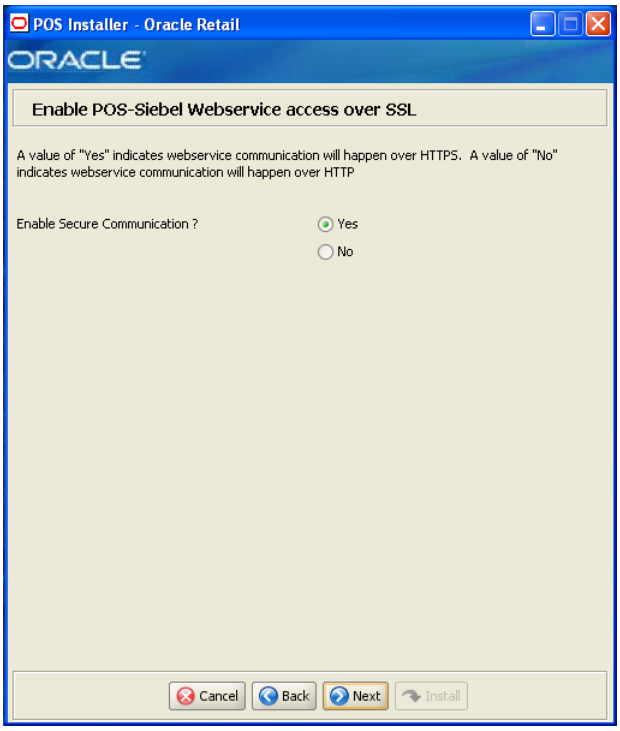


This screen is only displayed if **Store Inventory Management** is selected on the Integrate Applications screen.

The field on this screen is described in the following table.

Field Title	Please select the required SIM integration features
Field Description	Select the Oracle Retail Store Inventory Management (SIM) features that will be used in Point-of-Service: ▪ To inquire about inventory using SIM, select **Inventory Inquiry**. ▪ To reserve inventory using SIM, select **Inventory Reservation**. ▪ To enable item baskets created using SIM, select **Item Basket**. ▪ To enable serialization using SIM, select **Serialization**. ▪ To update inventory using SIM, select **Inventory Update**.
Example	Inventory Inquiry

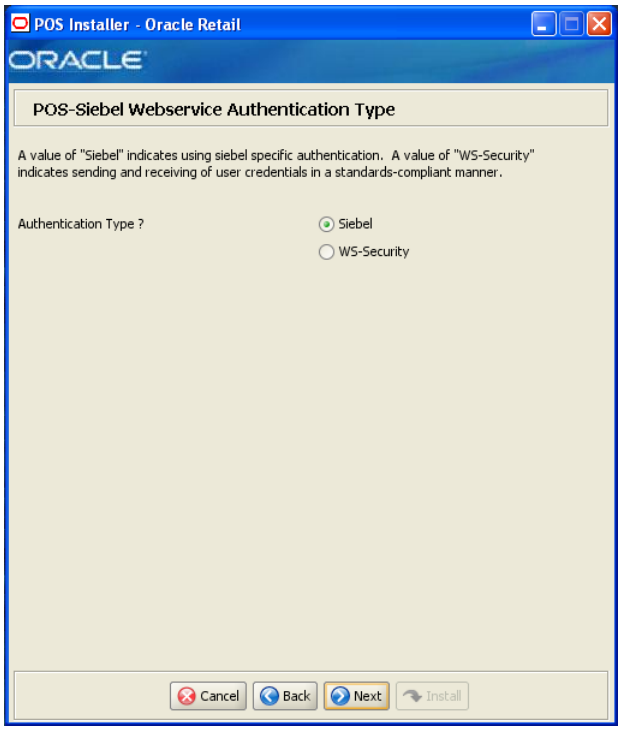
Figure A–31 Enable POS-Siebel Webservice Access Over SSL



This screen is only displayed if **Siebel** is selected on the Integrate Applications screen. The field on this screen is described in the following table.

Field Title	Enable Secure Communciation
Field Description	Select Yes if Web service communciation with Siebel using HTTPS.
Example	Yes

Figure A–32 POS-Siebel Webservice Authentication Type

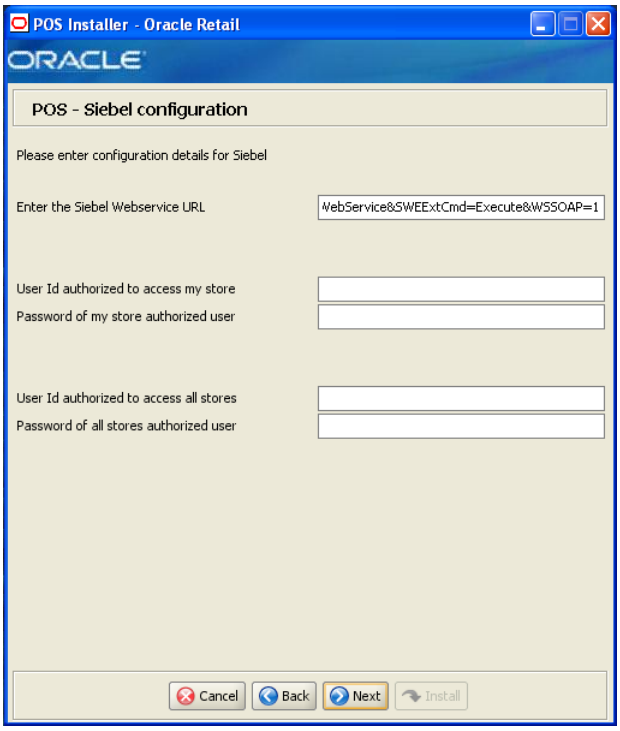


This screen is only displayed if **Siebel** is selected on the Integrate Applications screen.

The field on this screen is described in the following table.

Field Title	Enable Secure Communciation
Field Description	■ To use Siebel-specific authentication, select **Siebel**. ■ To send and receive user credentials in a standards-compliant manner, select **WS-Security**.
Example	Siebel

Figure A–33 POS-Siebel Configuration



This screen is only displayed if **Siebel** is selected on the Integrate Applications screen. The fields on this screen are described in the following tables.

Field Title	Enter the Siebel Webservice URL
Field Description	Enter the URL used by the Point-of-Service application to access Siebel.

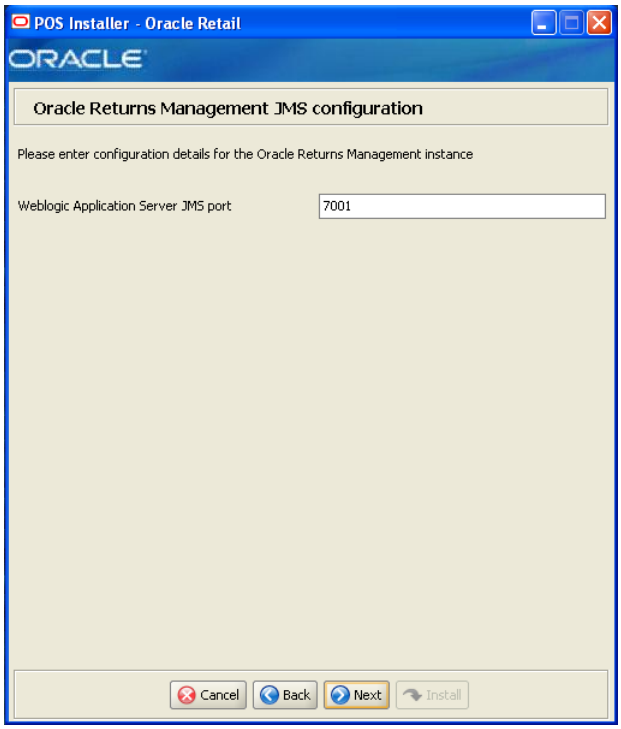
Field Title	User Id authorized to access my store
Field Description	Enter the user ID for the user authorized to access my store.

Field Title	Password of my store authorized user
Field Description	Enter the password for accessing my store.

Field Title	User Id authorized to access all stores
Field Description	Enter the user ID for the user authorized to access all stores.

Field Title	Password of all stores authorized user
Field Description	Enter the password for the accessing all stores.

Figure A–34 Oracle Returns Management JMS Configuration

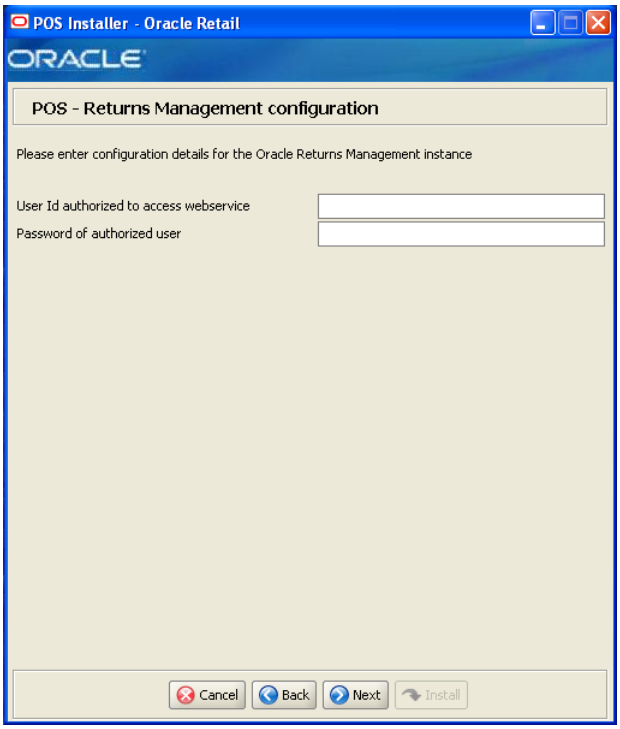


This screen is only displayed if **Returns Management** is selected on the Integrate Applications screen and **JMS Queue** is selected on the Oracle Returns Management Messaging screen.

The field on this screen is described in the following table.

Field Title	Weblogic Application Server JMS port
Field Description	Enter the port number of the JMS server to use to send return result messages to Oracle Retail Returns Management.
Example	7001

Figure A–35 POS - Returns Management Configuration



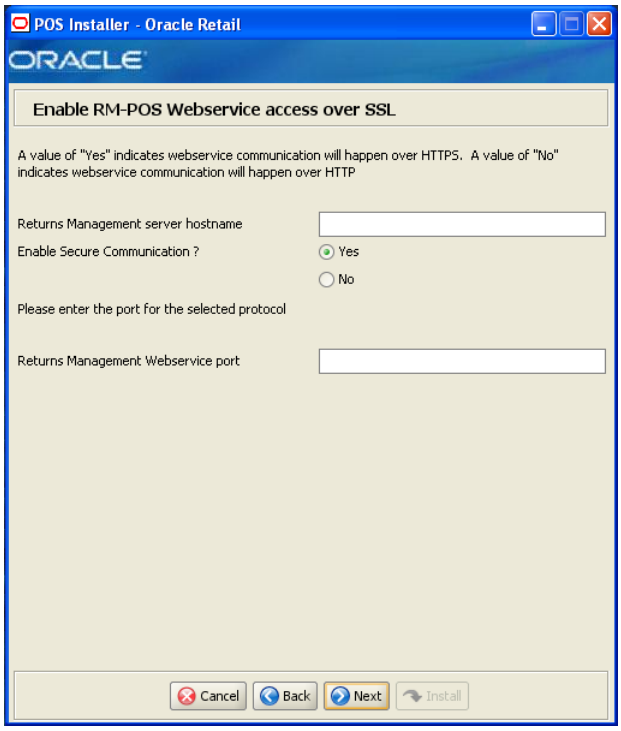
This screen is only displayed if **Returns Management** is selected on the Integrate Applications screen.

The fields on this screen are described in the following tables.

Field Title	User Id authorized to access webservice
Field Description	Enter the user ID which is used to access the Web service.

Field Title	Password of authorized user
Field Description	Enter the password of the authorized user.

Figure A–36 Enable RMPOS Webservice access over SSL



This screen is only displayed if **Returns Management** is selected on the Integrate Applications screen.

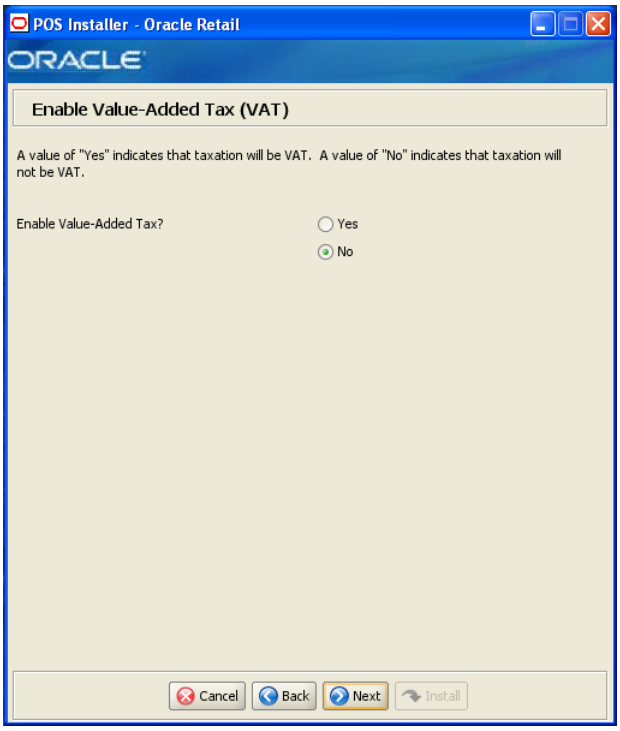
The fields on this screen are described in the following tables.

Field Title	Returns Management server hostname
Field Description	Enter the host name for the Oracle Retail Returns Management server.

Field Title	Enable Secure Communication
Field Description	Choose whether secure communication over HTTPS is used.

Field Title	Returns Management Webservice port
Field Description	Enter the port number for the Oracle Retail Returns Management Web service.

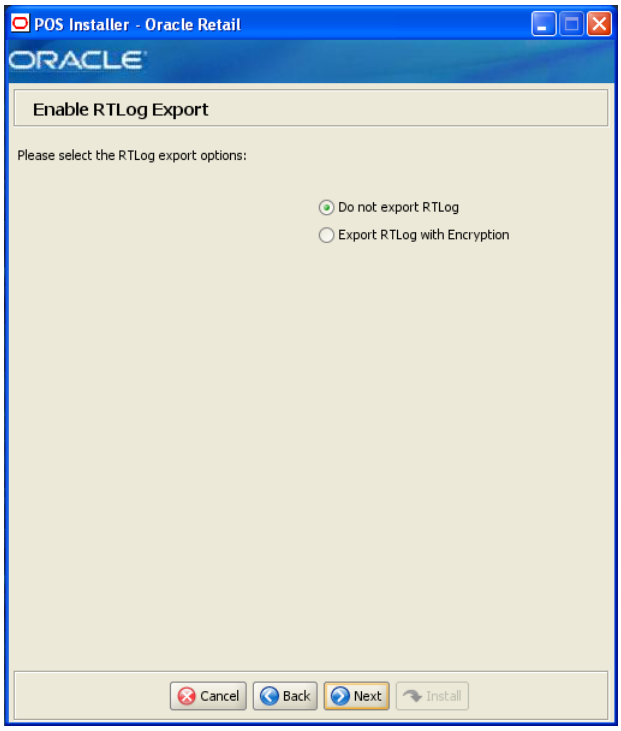
Figure A–37 Enable Value-Added Tax (VAT)



The field on this screen is described in the following table.

Field Title	Value-Added Tax
Field Description	Select Yes if Value-Added Tax is used.
Example	No

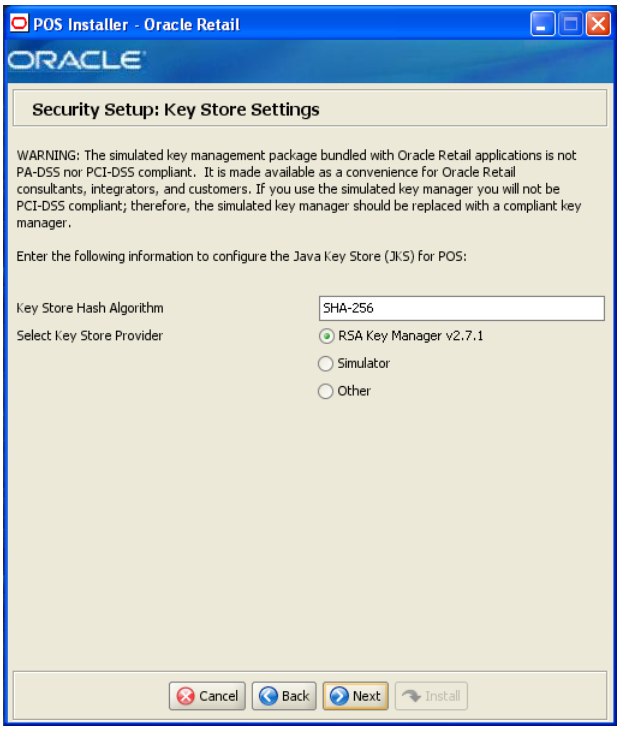
Figure A–38 Enable RTLog Export



The field on this screen is described in the following table.

Field Title	RTLog Export Options
Field Description	Choose how the RTLog is to be exported. ■ To not export the log, choose **Do not export RTLog**. ■ To export the log, choose **Export RTLog with Encryption**.
Example	Do not export RTLog

Figure A–39 Security Setup: Key Store Settings

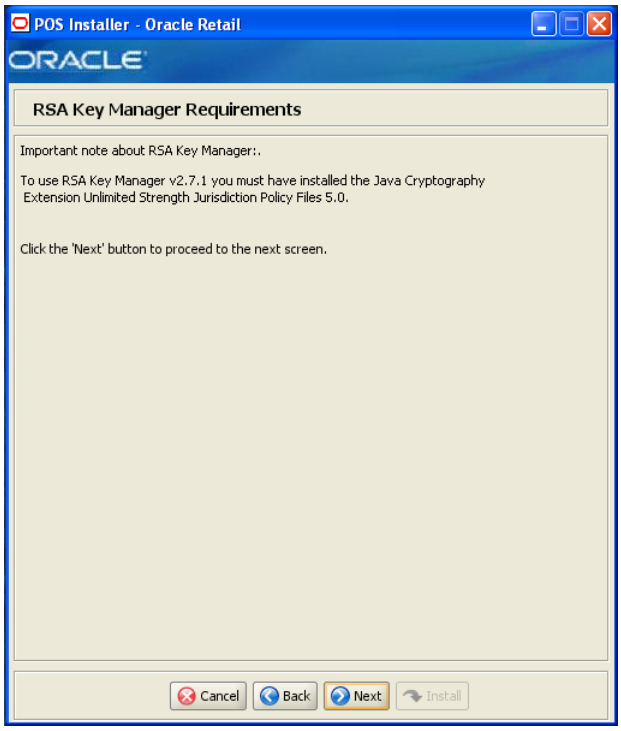


The fields on this screen are described in the following tables.

Field Title	Key Store Hash Algorithm
Field Description	Enter the name of the algorithm used by the Key Store to hash sensitive data.
Example	SHA-256

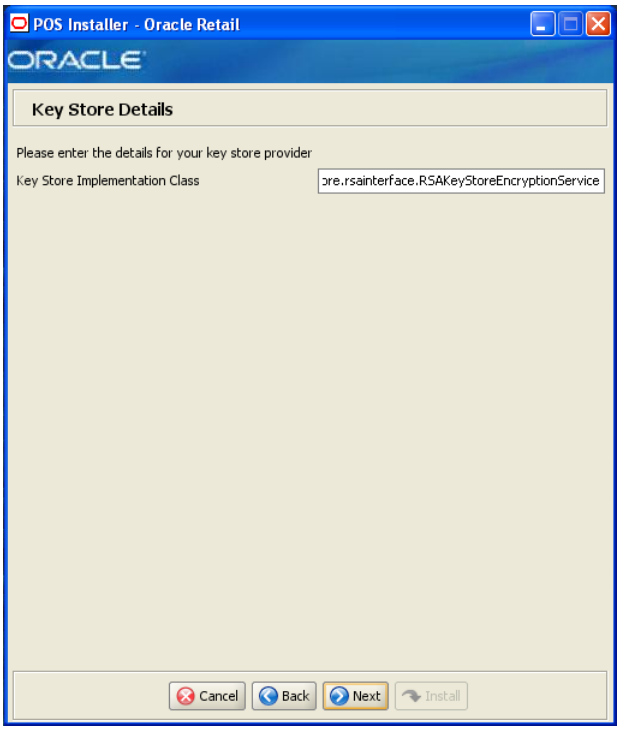
Field Title	Select Key Store Provider
Field Description	Provider for Key Store management. ▪ To use the RSA key management package, select **RSA Key Manager v2.7.1**. The next screen displayed is Figure A–40. ▪ To use the simulated key management package, select **Simulator**. The next screen displayed is Figure A–44. ▪ To use a different key management provider, select **Other**. The next screen displayed is Figure A–45.
Example	RSA Key Manager v2.7.1

Figure A–40 RSA Key Manager Requirements



This screen is only displayed if **RSA Key Manager v2.7.1** is selected for the Key Store provider on the Security Setup: Key Store screen. This informational screen explains the requirements to use the RSA Key Manager. Verify that you meet the requirements and then click **Next**.

Figure A–41 Key Store Details for RSA Key Manager 2.7.1

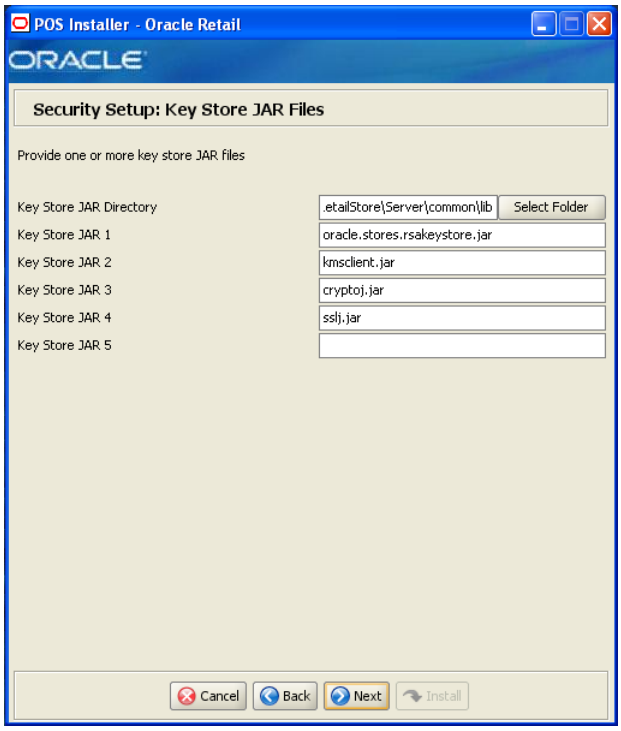


This screen is only displayed if **RSA Key Manager v2.7.1** is selected for the Key Store provider on the Security Setup: Key Store screen.

The field on this screen is described in the following table.

Field Title	Key Store Implementation Class
Field Description	Enter the class that invokes the RSA Key Manager interface.
Example	oracle.retail.stores.rsakeystore.rsainterface.RSAKeyStoreEncryptionService

Figure A–42 Security Setup: Key Store JAR Files for RSA Key Manager 2.7.1



This screen is only displayed if **RSA Key Manager v2.7.1** is selected for the Key Store provider on the Security Setup: Key Store screen.

The fields on this screen are described in the following tables. Up to five Key Store jar files may be entered.

Field Title	Key Store JAR Directory
Field Description	Choose the directory where the Key Store jar files are located.
Example	`C:\OracleRetailStore\Server\common\lib`

Field Title	Key Store JAR 1
Field Description	Enter the name of a Key Store jar file.
Example	rsakeystore.jar

Field Title	Key Store JAR 2
Field Description	Enter the name of a Key Store jar file.
Example	kmsclient.jar

Field Title	Key Store JAR 3
Field Description	Enter the name of a Key Store jar file.
Example	cryptoj.jar

Field Title	Key Store JAR 4
Field Description	Enter the name of a Key Store jar file.
Example	sslj.jar

Field Title	Key Store JAR 5
Field Description	Enter the name of a Key Store jar file.

Figure A–43 RSA Key Store Configuration

This screen is only displayed if **RSA Key Manager v2.7.1** is selected for the Key Store provider on the Security Setup: Key Store screen.

The fields on this screen are described in the following tables.

Field Title	Server Host Address
Field Description	Enter the IP address of the RSA server host.

Field Title	Server Host Port
Field Description	Enter the port number for the RSA server host.
Example	443 443 is the default used by the RSA Key Manager.

Field Title	Cipher Key Class
Field Description	Enter the RSA Key Manager cipher key class.

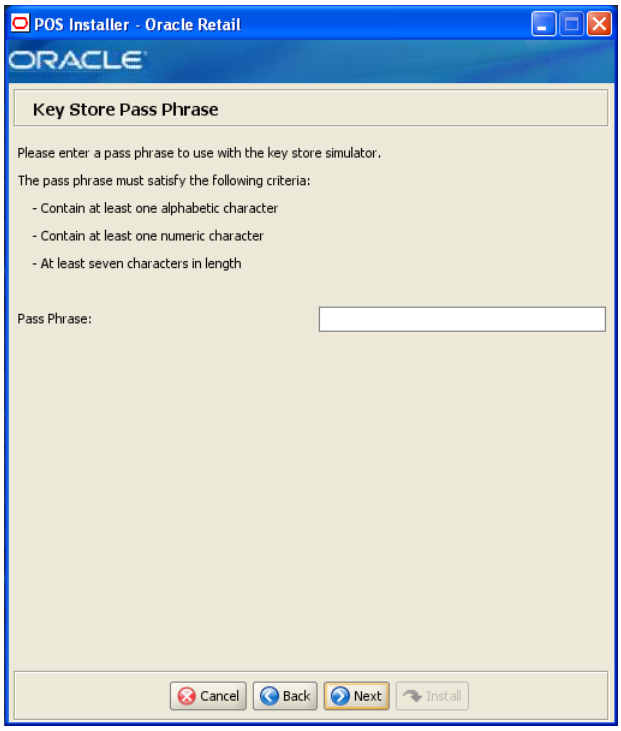
Field Title	Client Key Store File
Field Description	Select the location of the RSA Key Manager client Key Store file.

Field Title	Server Key Store File
Field Description	Select the location of the RSA Key Manager server Key Store file.

Field Title	Client Key Store Password
Field Description	Enter the password used to access the RSA Key Manager client Key Store.

Field Title	Cache Key Store Password
Field Description	Enter the password used to access the RSA Key Manager cache.

Figure A–44 Key Store Pass Phrase for Simulator Key Manager

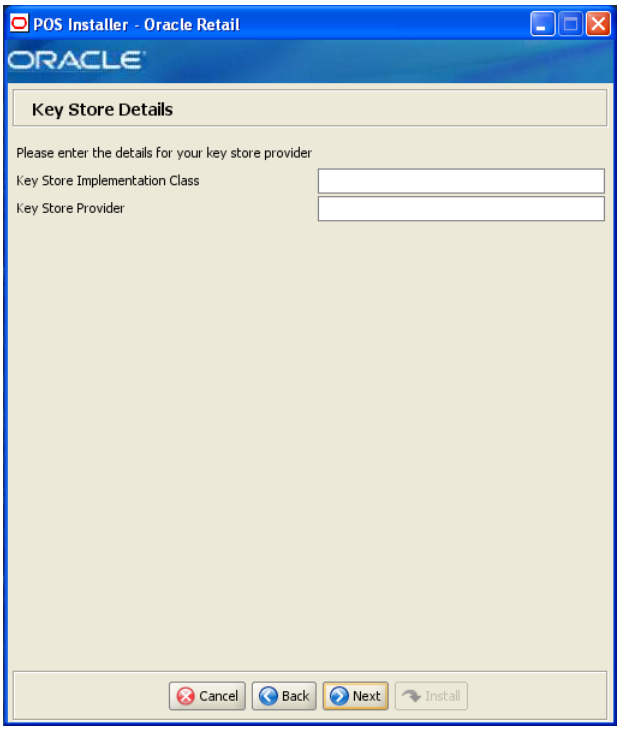


This screen is only displayed if **Simulator** is selected for the Key Store provider on the Security Setup: Key Store screen.

The field on this screen is described in the following table.

Field Title	Pass Phrase
Field Description	Enter the pass phrase used to access the Key Store simulator. **Note:** Use the same pass phrase for all Oracle Retail POS Suite applications in your configuration.

Figure A–45 Key Store Details for Other Key Manager



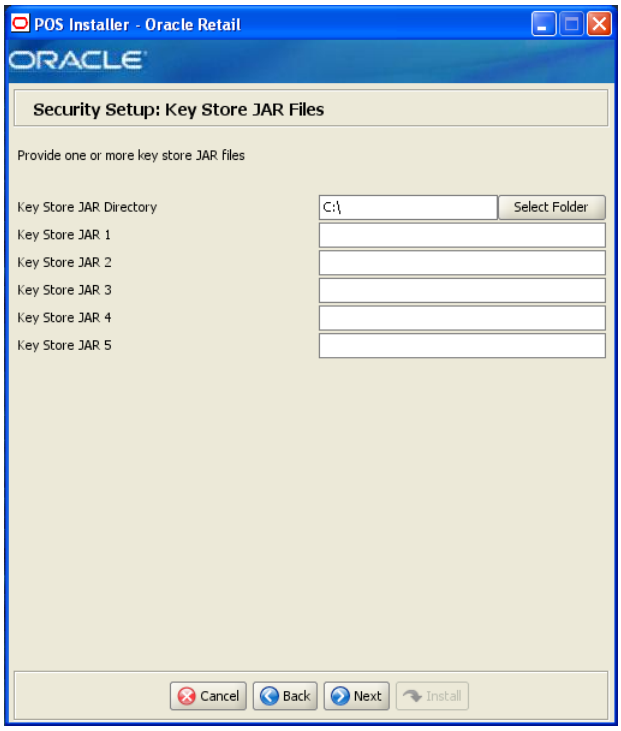
This screen is only displayed if **Other** is selected for the Key Store provider on the Security Setup: Key Store screen.

The fields on this screen are described in the following tables.

Field Title	Key Store Implementation Class
Field Description	Enter the class that invokes the key manager interface.

Field Title	Key Store Provider
Field Description	Enter the name of the provider for the Key Store.

Figure A–46 Security Setup: Key Store JAR Files for Other Key Manager



This screen is only displayed if **Other** is selected for the Key Store provider on the Security Setup: Key Store screen.

The fields on this screen are described in the following tables. Up to five Key Store jar files may be entered.

Field Title	Key Store JAR Directory
Field Description	Choose the directory where the Key Store jar files are located.

Field Title	Key Store JAR 1
Field Description	Enter the name of a Key Store jar file.

Field Title	Key Store JAR 2
Field Description	Enter the name of a Key Store jar file.

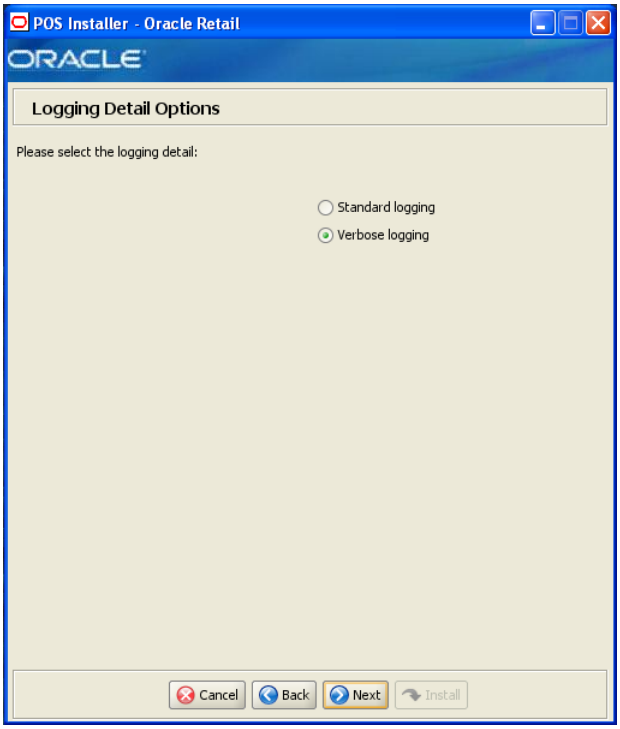
Field Title	Key Store JAR 3
Field Description	Enter the name of a Key Store jar file.

Field Title	Key Store JAR 4
Field Description	Enter the name of a Key Store jar file.

Field Title	Key Store JAR 5
Field Description	Enter the name of a Key Store jar file.

Field Title	TrustStore Password
Field Description	Enter the password for the truststore.

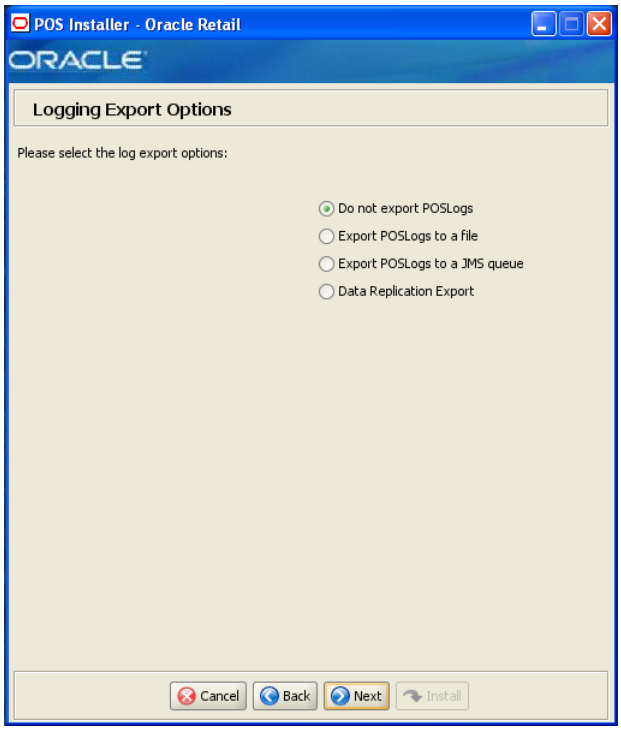
Figure A–47 Logging Detail Options



The field on this screen is described in the following table.

Field Title	Logging Detail Options
Field Description	Choose the level of client logging. ▪ To only log some of the messages, choose **Standard Logging**. ▪ To log all of the messages, choose **Verbose Logging**.
Example	Verbose logging

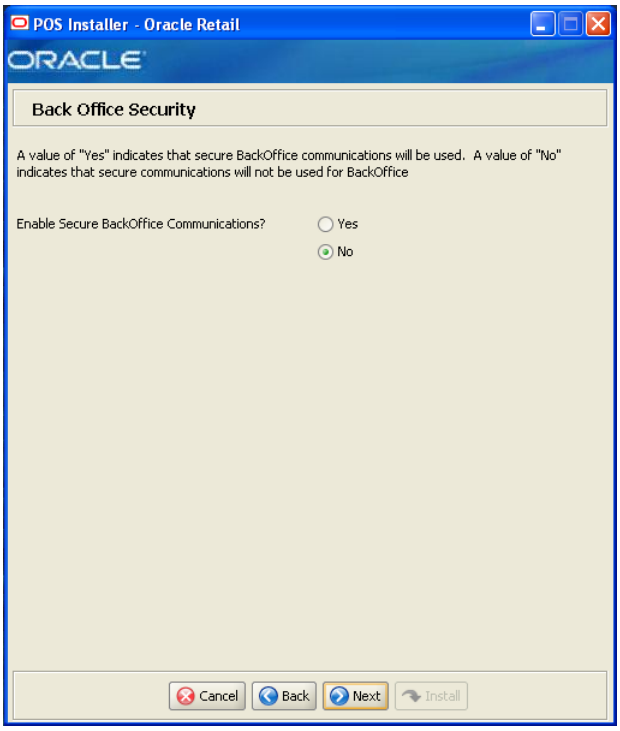
Figure A–48 Logging Export Options



The field on this screen is described in the following table.

Field Title	Logging Export Options
Field Description	Choose how the log is to be exported. ▪ To not generate any logs, choose **Do not export Point-of-Service logs**. ▪ To export the logs to a file, choose **Periodically export Point-of-Service logs to a file**. ▪ To export the logs to a JMS queue, choose **Periodically export Point-of-Service logs to a JMS queue**. ▪ To have the data pushed from the store to the corporate database using replication, choose **Data Replication Export**. **Note:** If you are using Centralized Transaction Retrieval, you must select **Data Replication Export**.
Example	Do not export Point-of-Service logs

Figure A–49 Back Office Security

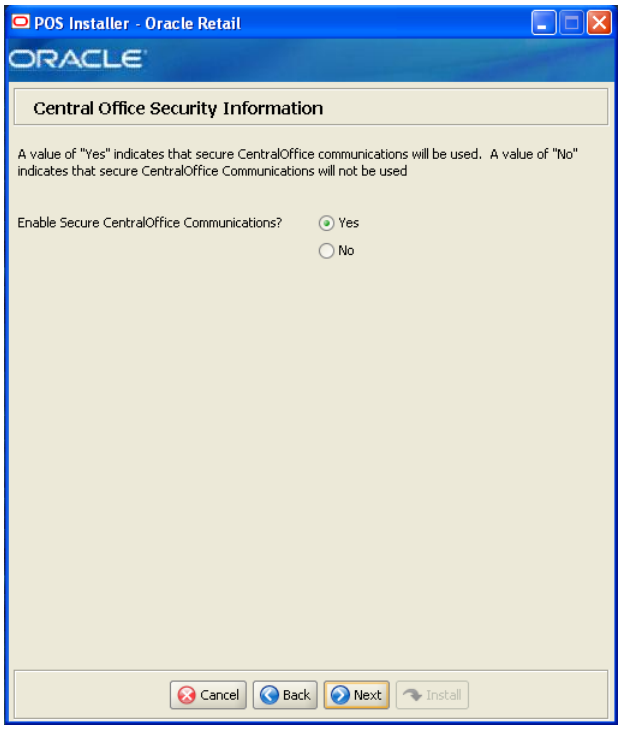


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

The field on this screen is described in the following table.

Field Title	Enable Secure Back Office Communications?
Field Description	Select Yes if secure communication with Back Office is required.
Example	Yes

Figure A–50 Central Office Security Information

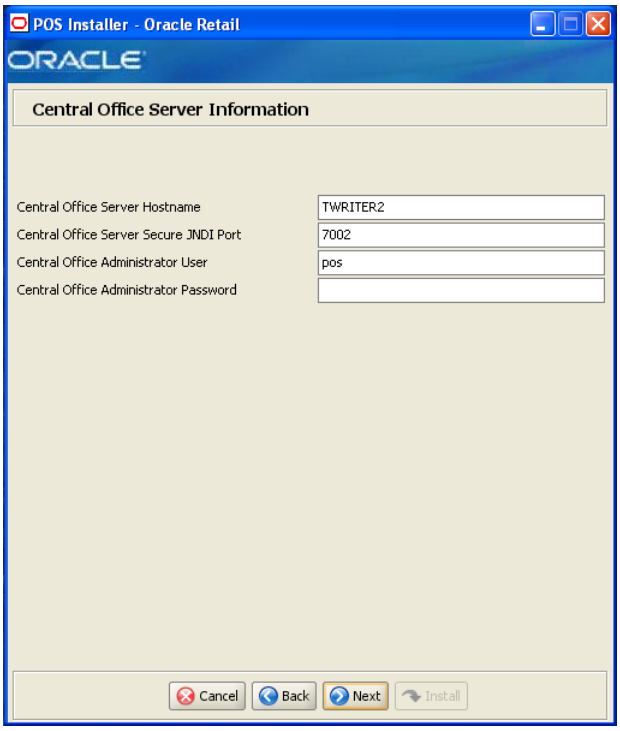


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

The field on this screen is described in the following table.

Field Title	Enable Secure Central Office Communications?
Field Description	Select Yes if secure communication with Central Office is required.
Example	Yes

Figure A–51 Central Office Server Information



This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

The fields on this screen are described in the following tables.

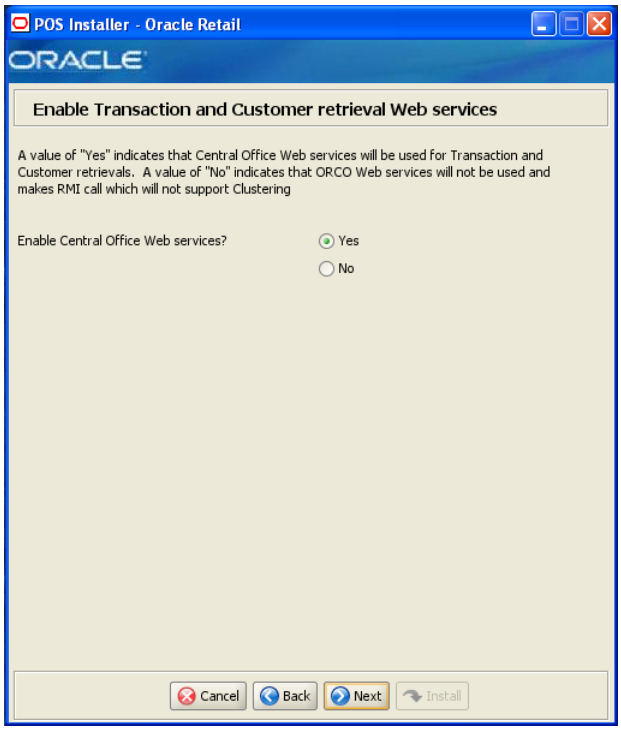
Field Title	Central Office Hostname
Field Description	Enter the hostname for the Central Office application.
Example	TWRITER2

Field Title	Central Office Server JNDI Port
Field Description	Enter the port number for the Central Office application. This is the port number that was selected when the Central Office domain was created.
Example	7002

Field Title	Central Office Administrator User
Field Description	Enter the user name used for performing Central Office administrative functions.
Example	coadmin

Field Title	Central Office Administrator Password
Field Description	Enter the password for the Central Office administrator user.

Figure A–52 Enable Transaction and Customer Retrieval Web Services

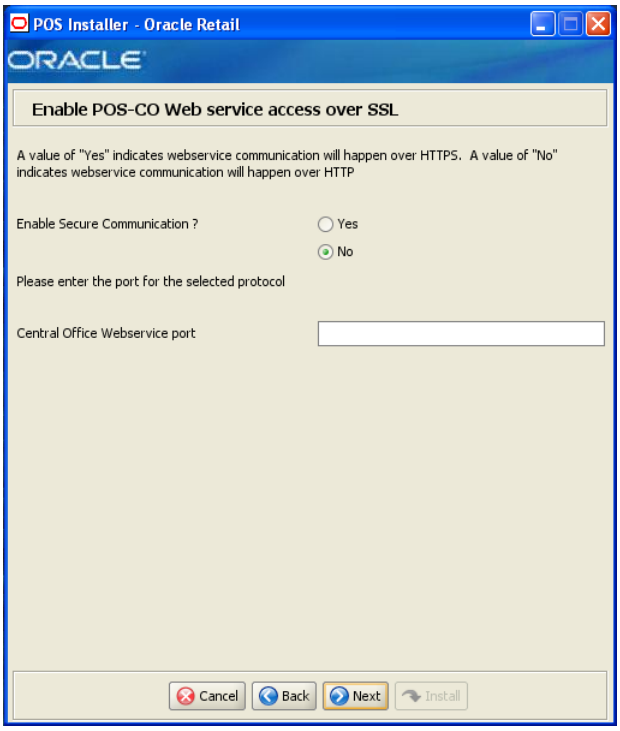


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen and **Central** or **Central, Local Failover** is selected on the Transaction Retrieval Location screen.

The field on this screen is described in the following table.

Field Title	Enable Central Office Webservices
Field Description	Select Yes if Oracle Retail Central Office is used for transaction and customer retrievals.
Example	Yes

Figure A–53 Enable POS-CO Web Service Access Over SSL



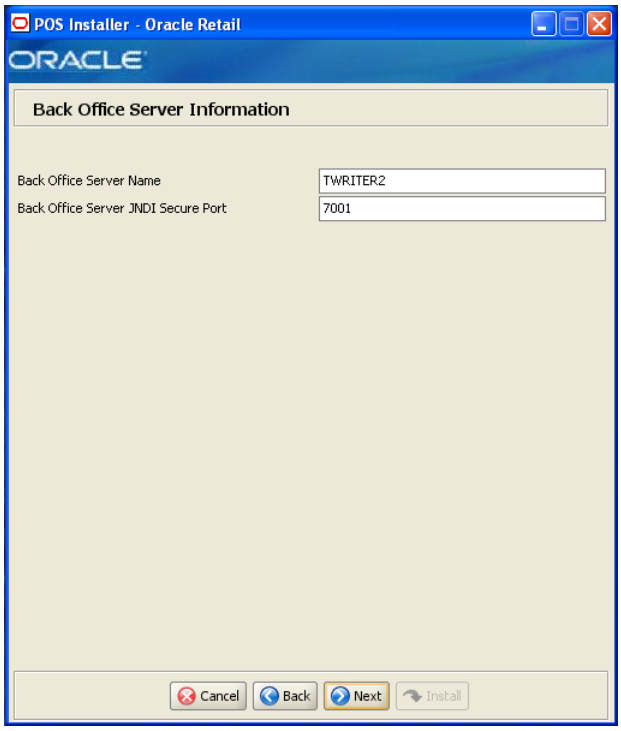
This screen is only displayed if **Yes** is selected on the Enable Transaction and Customer Retrieval Web Services screen.

The fields on this screen are described in the following tables.

Field Title	Enable Secure Communication
Field Description	Select Yes for Web service communication with Central Office using HTTPS.

Field Title	Central Office Webservice Port
Field Description	Enter the port number for the Central Office Web service.
Example	7001

Figure A–54 Back Office Server Information



This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

The fields on this screen are described in the following tables.

Field Title	Back Office Server Name
Field Description	Enter the host name for the Back Office application.
Example	TWRITER2

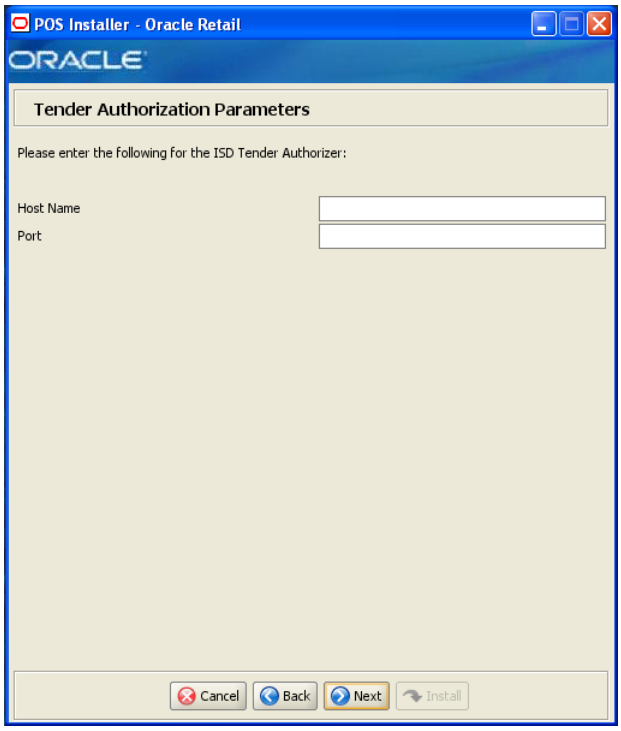
Field Title	Back Office Server JNDI Port
Field Description	Enter the port number for the Back Office application. This is the port number that was selected when the Back Office domain was created.
Example	7001

Figure A–55 Tender Authorization

The field on this screen is described in the following table.

Field Title	Select Tender Authorizer
Field Description	Choose where tender authorizations are sent. ▪ If approvals do not leave the store server and are based on values and certain numbers, choose **Simulated**. ▪ If approvals are sent to a third-party system to approve the authorizations, choose **ISD**. **Note:** Demo installations should use the Simulated option.
Example	Simulated

Figure A–56 Tender Authorization Parameters



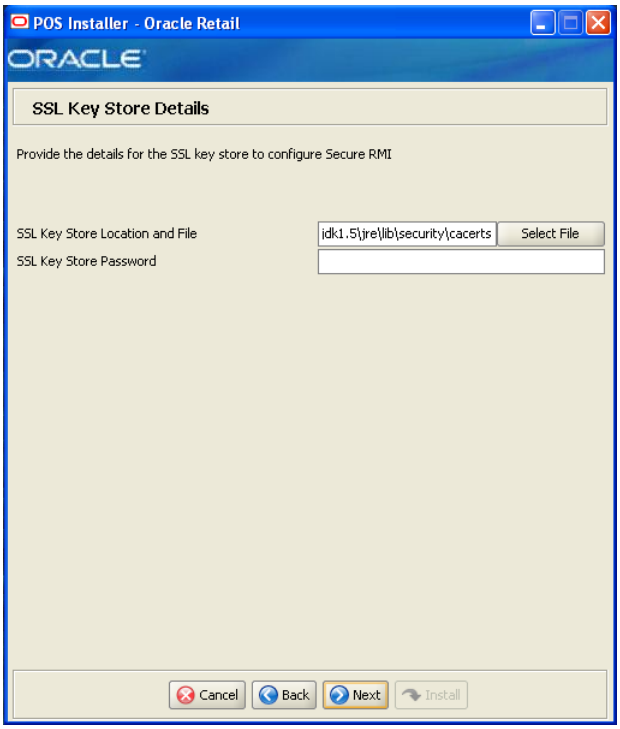
This screen is only displayed if **ISD** is selected for the Tender Authorization.

The fields on this screen are described in the following tables.

Field Title	Host Name
Field Description	Enter the host name of the tender authorizer.
Example	www.isdwhq.com

Field Title	Host Port
Field Description	Enter the port number used for the communication between the store server and the tender authorizer.
Example	15713

Figure A–57 SSL Key Store Details



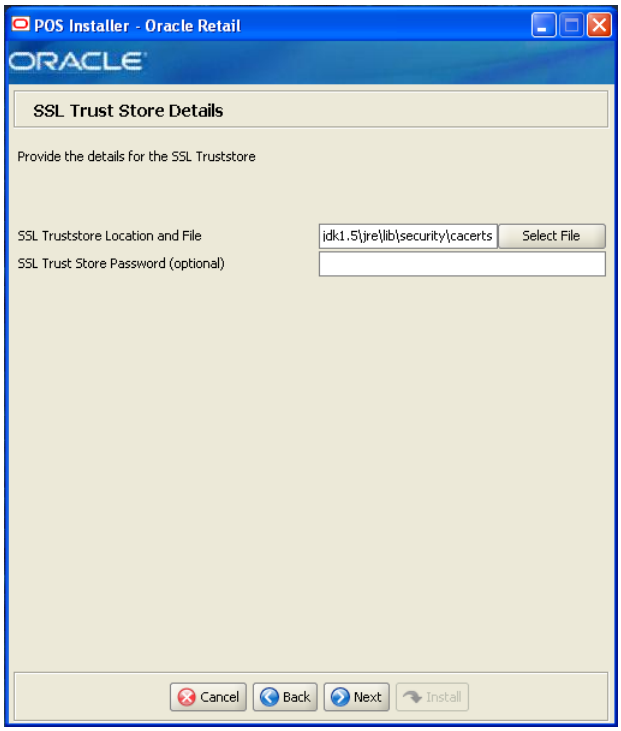
This screen is only displayed if **Yes** is selected on the Enable Secure RMI screen.

The fields on this screen are described in the following tables.

Field Title	SSL Key Store Location and File
Field Description	Enter the location and name of the Key Store.

Field Title	SSL Key Store Password
Field Description	Enter the password for the Key Store.

Figure A–58 SSL Trust Store Details



The fields on this screen are described in the following tables.

Field Title	SSL Truststore Location and File
Field Description	Enter the location and name of the truststore file.
Example	C:\jdk1.5\jre\lib\security\caerts

Field Title	SSL Trust Store Password (optional)
Field Description	Enter the password for the truststore.

Figure A–59 Installation Progress

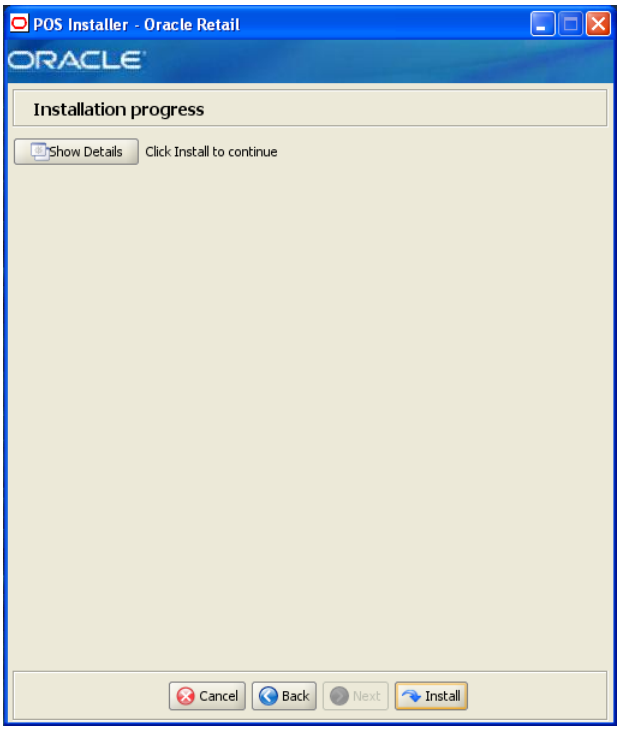
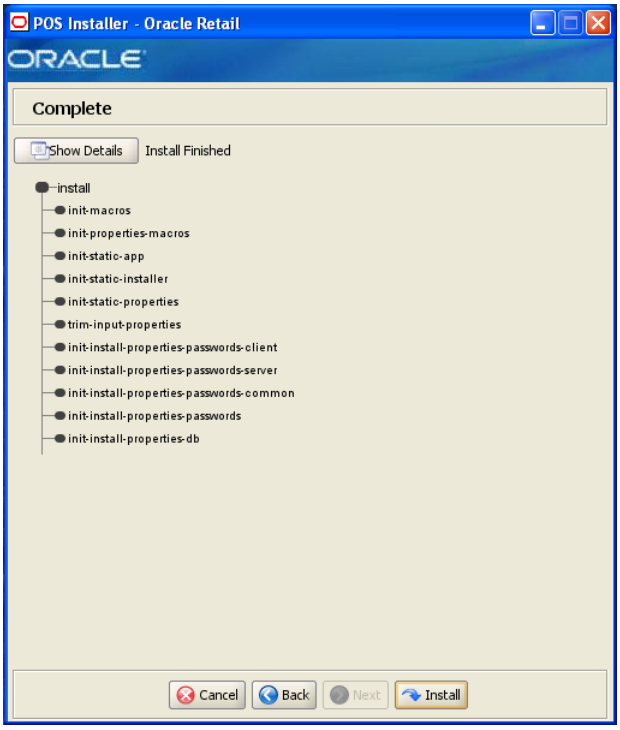


Figure A–60 Install Complete



B

Appendix: Installer Screens for Client Installation on the Oracle Stack

You need the following details about your environment for the installer to successfully install the Point-of-Service application. This appendix shows the screens that are displayed during the installation of the Point-of-Service client on the Oracle stack. Depending on the options you select, you may not see some screens or fields.

> **Note:** The flow of the screens and selections on the screens shown in this appendix follow the installation of the client using the supported software and hardware selections for the Oracle stack as shown in Chapter 1.

For each field on a screen, a table is included in this appendix that describes the field.

For the installer screens for a server installation on the Oracle stack, see Appendix A.

Figure B–1 Introduction

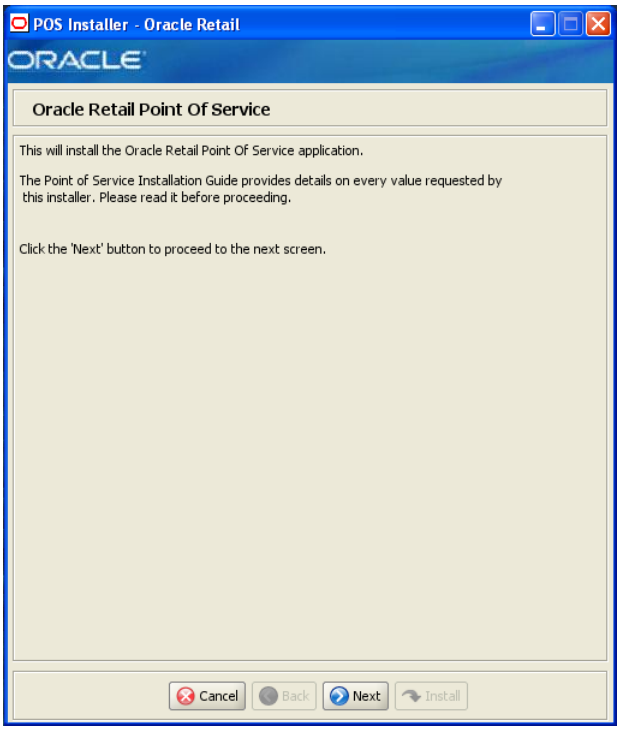
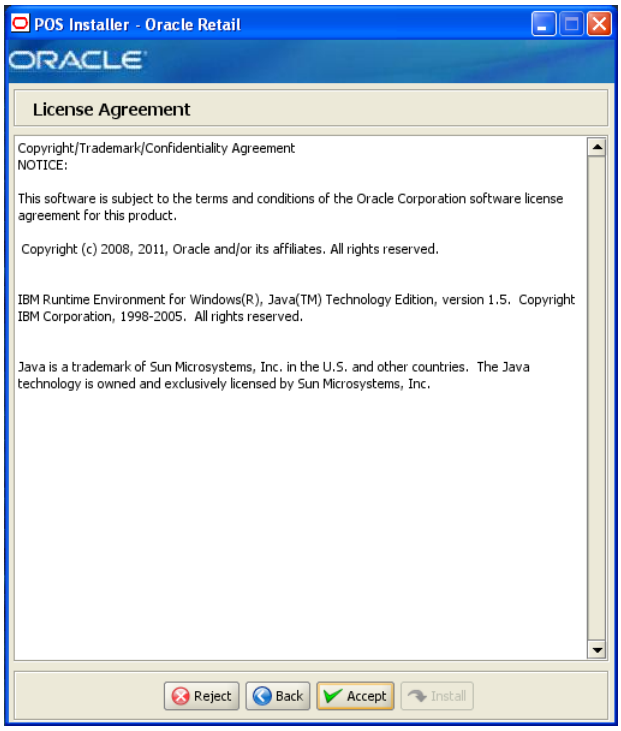


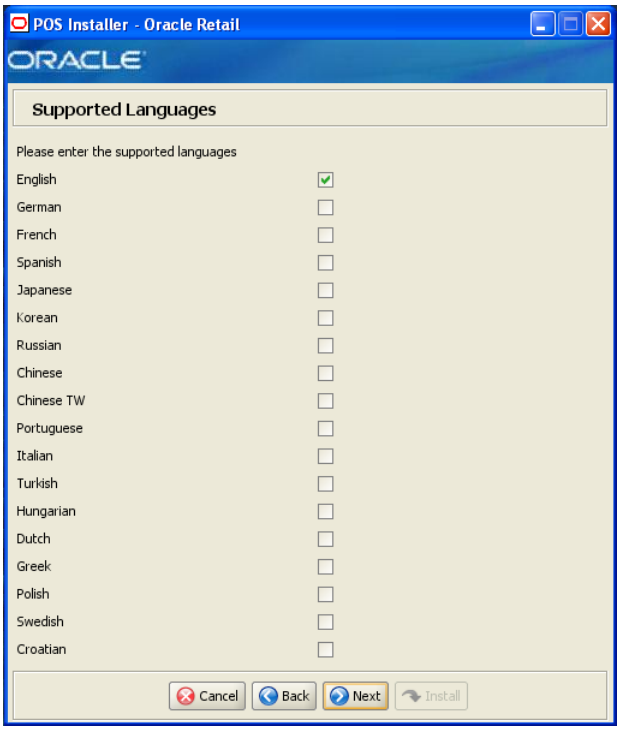
Figure B–2 Previous POS Install

Figure B–3 License Agreement



Note: You must choose to accept the terms of the license agreement in order for the installation to continue.

Figure B–4 Supported Languages



The field on this screen is described in the following table.

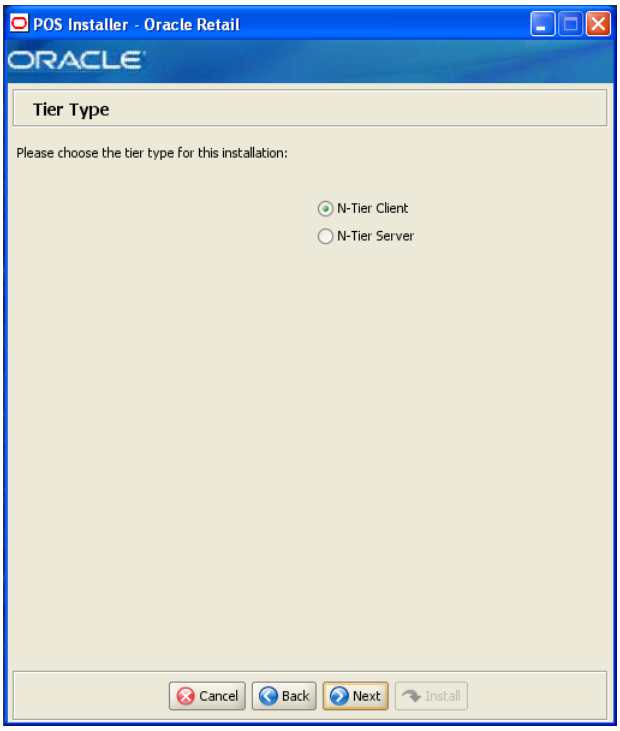
Field Title	Please enter the supported languages
Field Description	Select the languages that will be available for the Point-of-Service application. The languages selected on this screen determine the available choices on the Enter Default Locale screen.
Example	English

Figure B–5 Enter Default Locale

The field on this screen is described in the following table.

Field Title	Enter Default Locale
Field Description	Locale support in Point-of-Service enables the date, time, currency, calendar, address, and phone number to be displayed in the format for the selected default locale. The choices for default locale are dependent on the selections made on the Supported Languages screen. For each selected language, the default locale for that language is displayed on the Enter Default Locale screen. For example, if English and French are selected on the Supported Languages screen, en_US and fr_FR are the available choices for the default locale.
Example	en_US

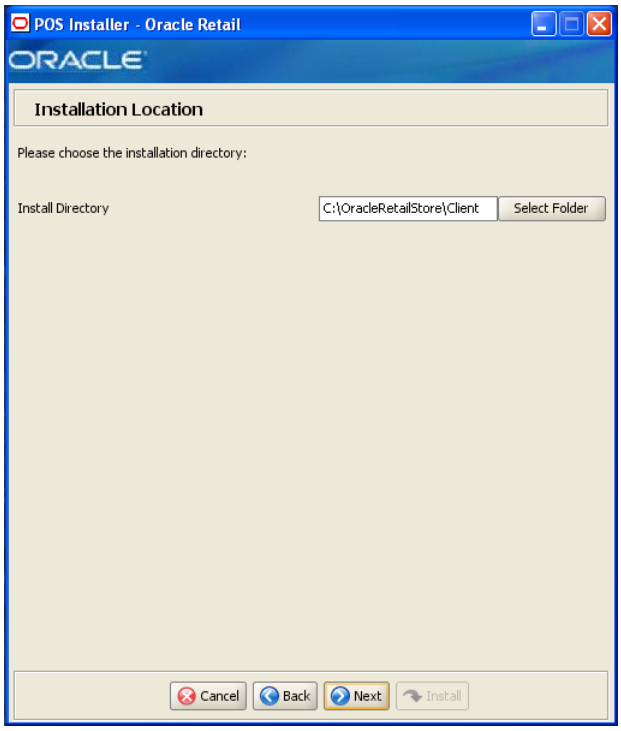
Figure B–6 Tier Type



The field on this screen is described in the following table.

Field Title	Tier Type
Field Description	Choose the server tier type for this installation. For more information, see "Determining Tier Type" in Chapter 2. To install the N-Tier version of the client, choose **N-Tier Client**.

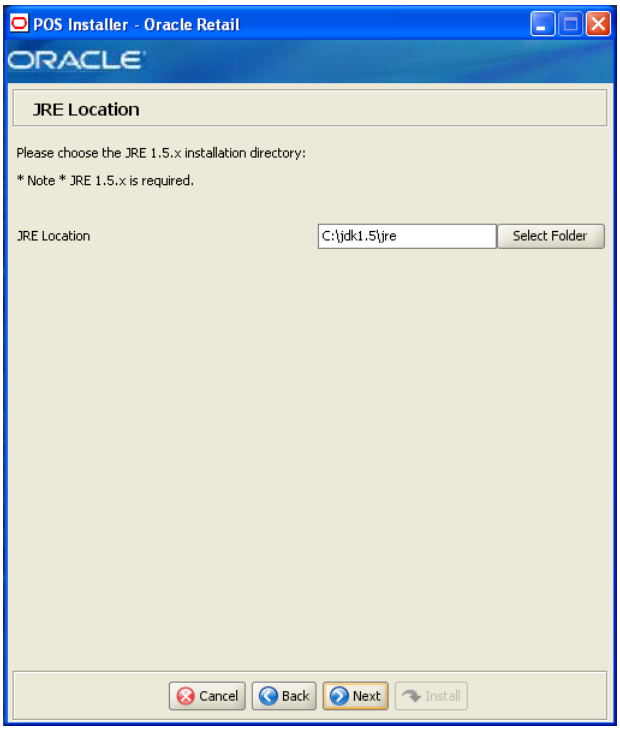
Figure B–7 Installation Location



The field on this screen is described in the following table.

Field Title	Install Directory
Field Description	Choose the directory into which the Point-of-Service files are copied. The default for the first directory in the path is `OracleRetailStore`. This directory should be the same for all Oracle Retail POS Suite products. When **N-Tier Client** is selected for the Tier Type, the default installation directory is `OracleRetailStore\Client`. **Note:** The server and the client must not be installed into the same directory. In this guide, *<POS_install_directory>* refers to the selected installation directory for the server or client. Files specific to Point-of-Service are copied to the `\pos` subdirectory of `<POS_install_directory>`.
Example	`C:\OracleRetailStore\Client`

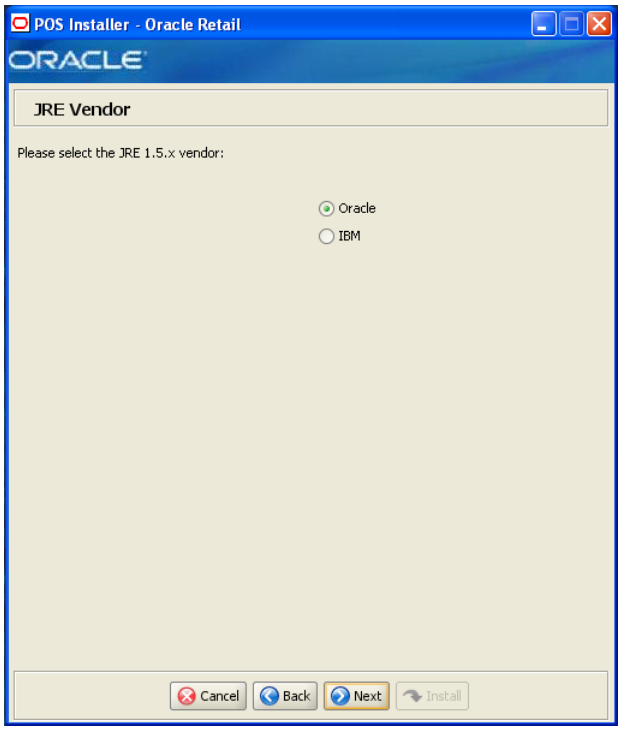
Figure B–8 JRE Location



The field on this screen is described in the following table.

Field Title	JRE Location
Field Description	Choose the location where the JRE is installed.
Example	`C:\jdk1.5\jre`

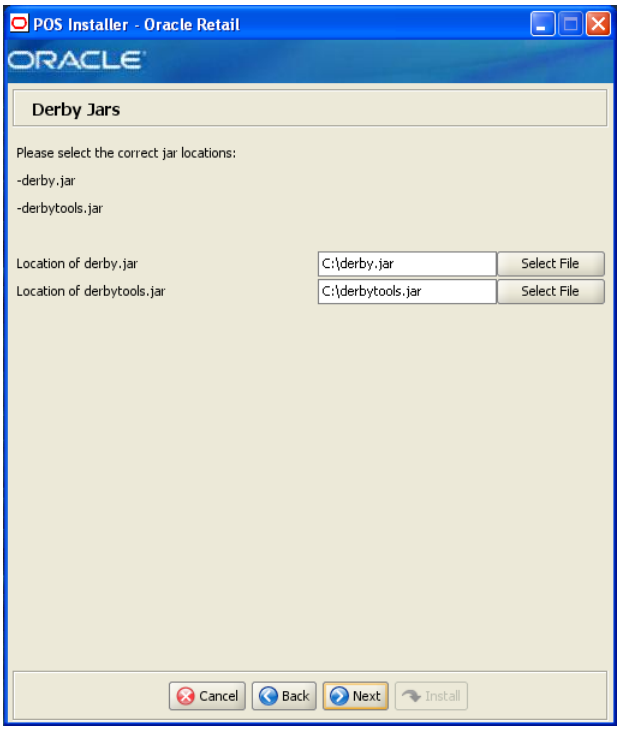
Figure B–9 JRE Vendor



The field on this screen is described in the following table.

Field Title	JRE Vendor
Field Description	Select the vendor for the JRE entered on the previous screen: ■ Oracle ■ IBM Choose **Oracle**.

Figure B–10 Derby Jars

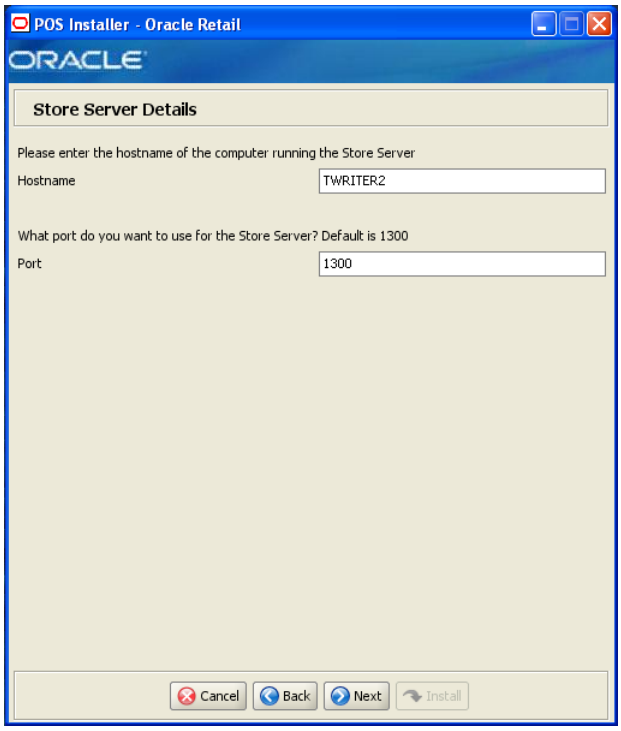


The fields on this screen are described in the following tables.

Field Title	Location of derby.jar
Field Description	Choose the location of the `derby.jar` file.
Example	`C:\derby.jar`

Field Title	Location of derbytools.jar
Field Description	Choose the location of the `derbytools.jar` file.
Example	`C:\derbytools.jar`

Figure B–11 Store Server Details

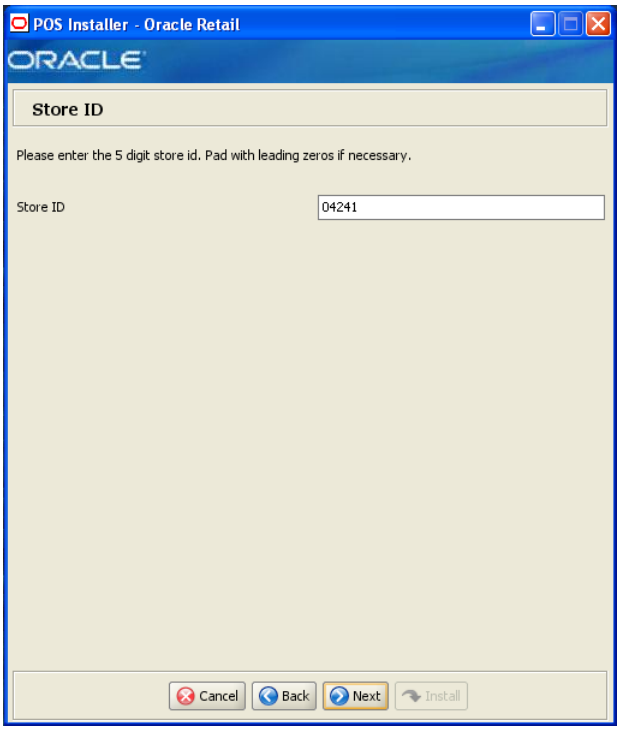


The fields on this screen are described in the following tables.

Field Title	Hostname
Field Description	Enter the host name of the store server.
Example	TWRITER2

Field Title	Port
Field Description	Enter the port number of the store server used for the communication between the store server and the host computer.
Example	1300

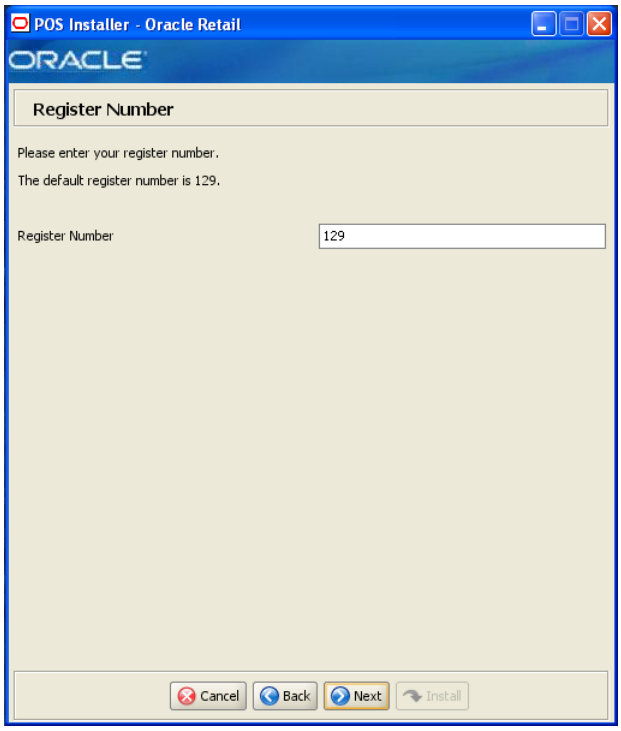
Figure B–12 Store ID



The field on this screen is described in the following table.

Field Title	Store ID
Field Description	Enter the store ID. **Note:** The store ID must be five digits. It can be padded with leading zeroes if necessary. The store ID can only contain the numeric characters 0 through 9.
Example	04241

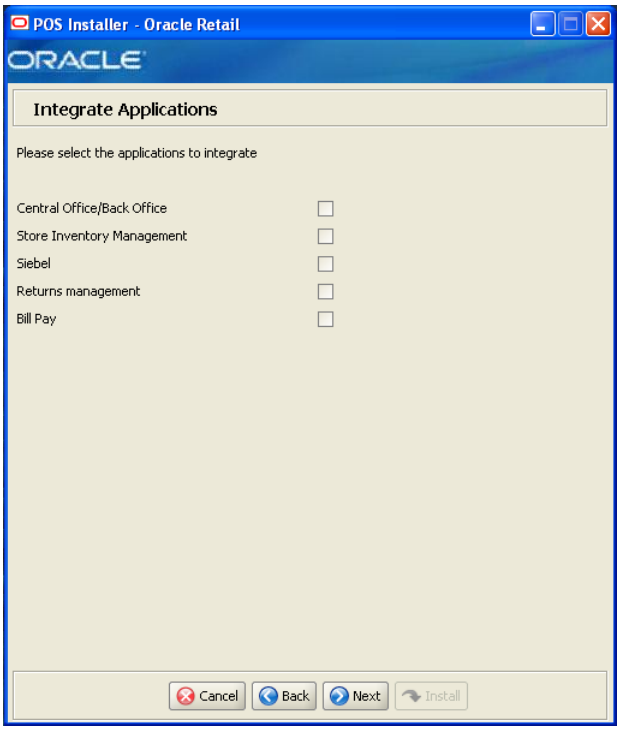
Figure B–13 Register Number



The field on this screen is described in the following table.

Field Title	Register Number
Field Description	Enter the register number for this installation.
Example	129 **Note:** 1 to 255 is supported for the register number. Do not install more than one client with the same register number at a store.

Figure B–14 Integrate Applications



The field on this screen is described in the following table.

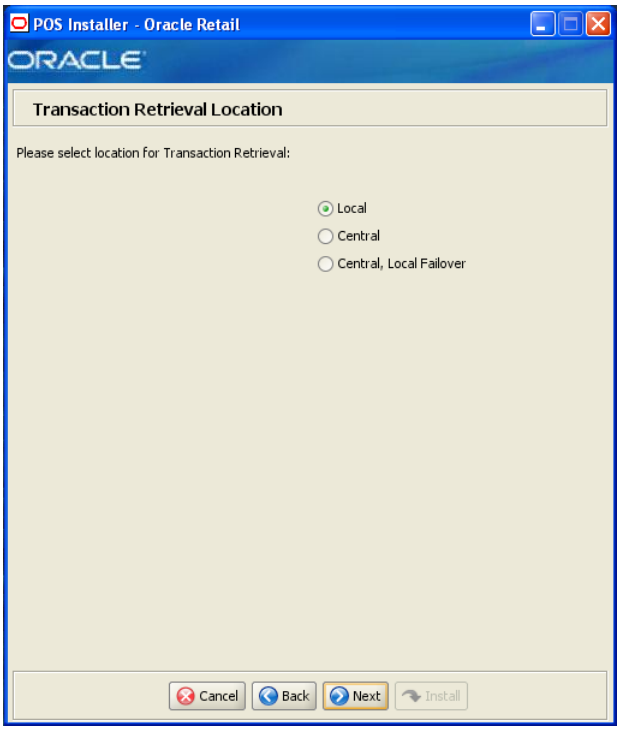
Field Title	Applications
Field Description	Select the applications that Point-of-Service is integrated with. ▪ Central Office/Back Office ▪ Store Inventory Management ▪ Siebel CMU Management ▪ Returns Management ▪ Bill Pay

Figure B–15 Application Server Type

The field on this screen is described in the following table.

Field Title	Application Server Type
Field Description	Select the application server to be used for the store server. ■ WebLogic Application Server ■ Websphere Application Server Choose **WebLogic Application Server**.

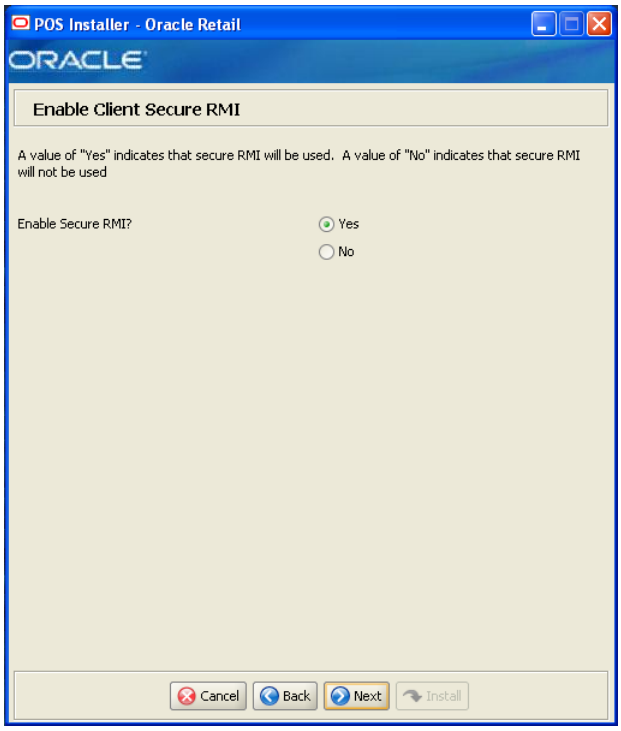
Figure B–16 Transaction Retrieval Location



The field on this screen is described in the following table.

Field Title	Transaction retrieval location
Field Description	Choose the location for retrieving transactions. ▪ If transactions should only be retrieved from the store database, choose **Local**. ▪ If transactions should only be retrieved from the corporate database, choose **Central**. ▪ If transactions should be retrieved from the corporate database, and if not found, then retrieved from the store database, choose **Central, Local Failover**. **Note:** You must choose the same location for both the store server and client installations.
Example	Local

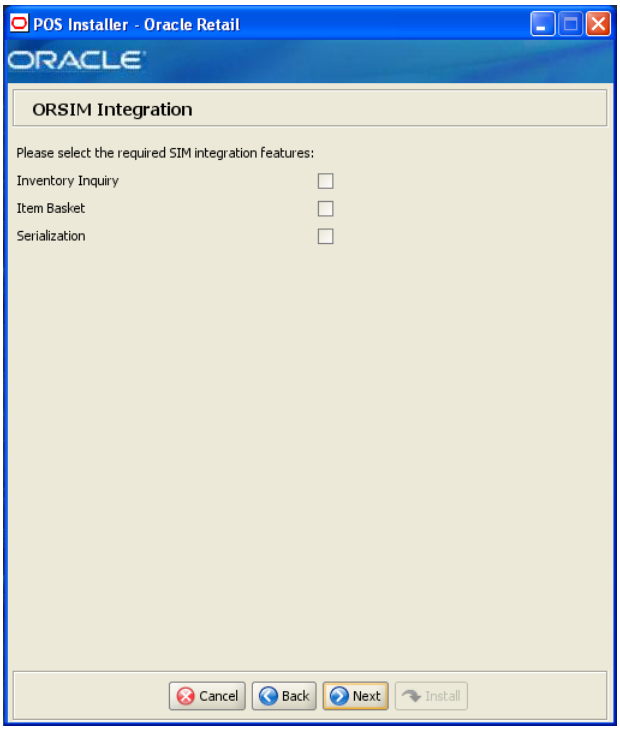
Figure B–17 Enable Client Secure RMI



The field on this screen is described in the following table.

Field Title	Enable SecureRMI?
Field Description	Select whether secure RMI is to be used for communication between the store server and registers.
Example	Yes

Figure B–18 ORSIM Integration

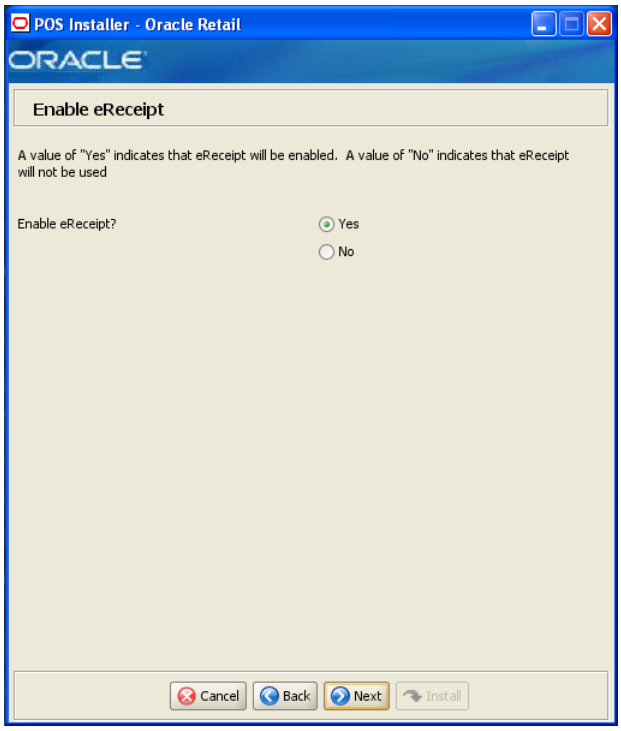


This screen is only displayed if **Store Inventory Management** is selected on the Integrate Applications screen.

The field on this screen is described in the following table.

Field Title	Select the required SIM integration features
Field Description	Select the Oracle Retail Store Inventory Management (SIM) features that will be used in Point-of-Service: ▪ To inquire about inventory using SIM, select **Inventory Inquiry**. ▪ To enable item baskets created using SIM, select **Item Basket**. ▪ To enable serialization using SIM, select **Serialization**.
Example	Inventory Inquiry

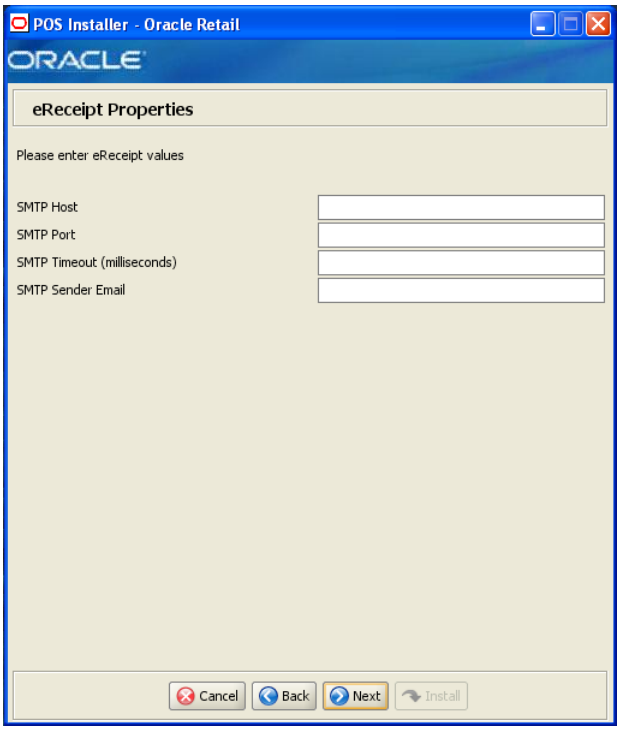
Figure B–19 Enable eReceipt



The field on this screen is described in the following table.

Field Title	Enable eReceipt?
Field Description	Choose whether the use of eReceipts is enabled.
Example	Yes

Figure B–20 eReceipt Properties



This screen is only displayed if **Yes** is selected on the Enable eReceipt screen.

The fields on this screen are described in the following tables.

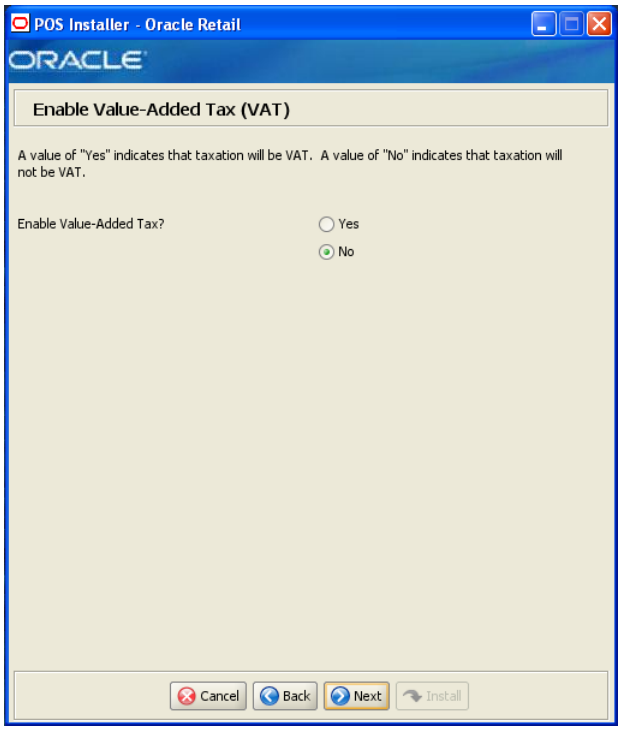
Field Title	SMTP Host
Field Description	Enter the host name for the SMTP server.

Field Title	SMTP Port
Field Description	Enter the port number for the SMTP server.

Field Title	SMTP Timeout (milliseconds)
Field Description	Enter the amount of time to wait for the SMTP server.

Field Title	SMTP Sender Email
Field Description	Enter the e-mail address to use for the from address in e-mails generated by Point-of-Service.

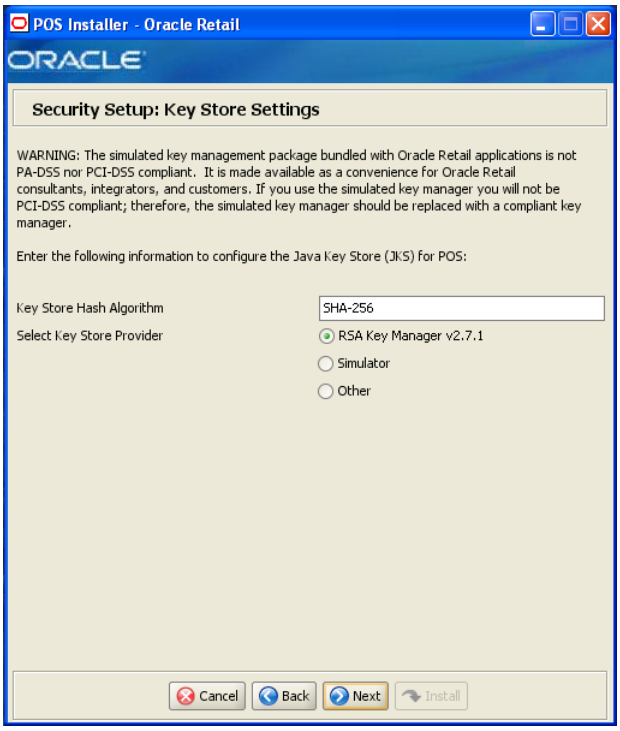
Figure B–21 Value-Added Tax (VAT)



The field on this screen is described in the following table.

Field Title	Value-Added Tax
Field Description	Select Yes if Value-added Tax is used.

Figure B–22 Security Setup: Key Store Settings

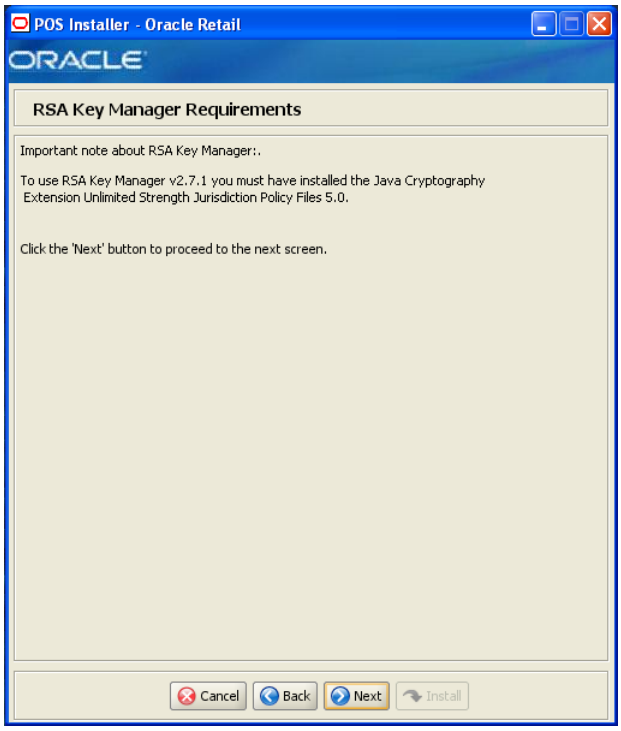


The fields on this screen are described in the following tables.

Field Title	Key Store Hash Algorithm
Field Description	Enter the name of the algorithm used by the Key Store to hash sensitive data.
Example	SHA-256

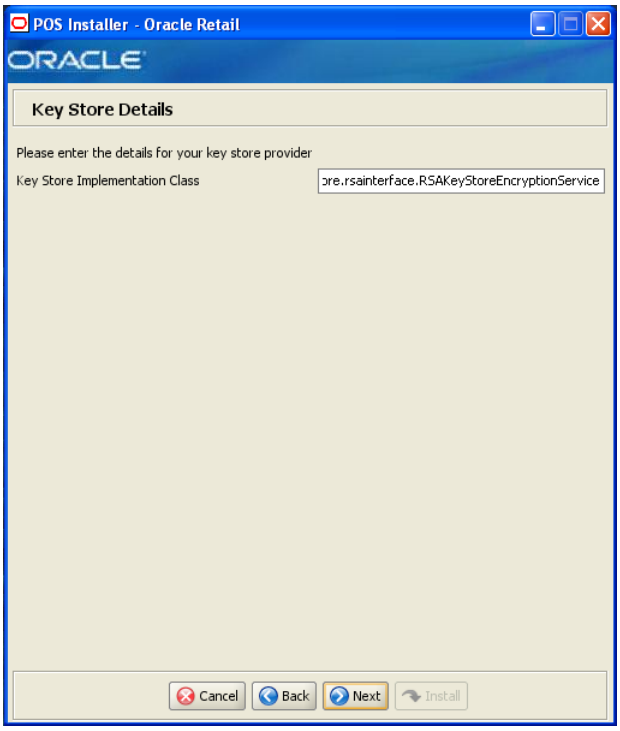
Field Title	Select Key Store Provider
Field Description	Provider for Key Store management. ▪ To use the RSA key management package, select **RSA Key Manager v2.7.1**. The next screen displayed is Figure B–23. ▪ To use the simulated key management package, select **Simulator**. The next screen displayed is Figure B–27. ▪ To use a different key management provider, select **Other**. The next screen displayed is Figure B–28.
Example	RSA Key Manager v2.7.1

Figure B–23 RSA Key Manager Requirements



This screen is only displayed if **RSA Key Manager v2.7.1** is selected for the Key Store provider on the Security Setup: Key Store screen. This informational screen explains the requirements to use the RSA Key Manager. Verify that you meet the requirements and then click **Next**.

Figure B–24 Key Store Details for RSA Key Manager 2.7.1

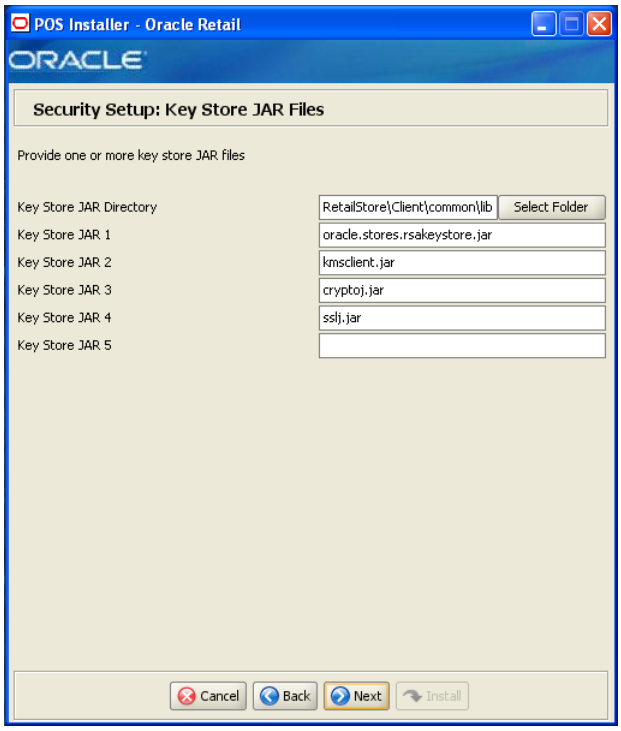


This screen is only displayed if **RSA Key Manager v2.7.1** is selected for the Key Store provider on the Security Setup: Key Store screen.

The field on this screen is described in the following table.

Field Title	Key Store Implementation Class
Field Description	Enter the class that invokes the RSA Key Manager interface.
Example	oracle.retail.stores.rsakeystore.rsainterface.RSAKeyStoreEncryptionService

Figure B–25 Security Setup: Key Store JAR Files for RSA Key Manager 2.7.1



This screen is only displayed if **RSA Key Manager v2.7.1** is selected for the Key Store provider on the Security Setup: Key Store screen.

The fields on this screen are described in the following tables. Up to five Key Store jar files may be entered.

Field Title	Key Store JAR Directory
Field Description	Choose the directory where the Key Store jar files are located.
Example	`C:\OracleRetailStore\Client\common\lib`

Field Title	Key Store JAR 1
Field Description	Enter the name of a Key Store jar file.
Example	rsakeystore.jar

Field Title	Key Store JAR 2
Field Description	Enter the name of a Key Store jar file.
Example	kmsclient.jar

Field Title	Key Store JAR 3
Field Description	Enter the name of a Key Store jar file.
Example	cryptoj.jar

Field Title	Key Store JAR 4
Field Description	Enter the name of a Key Store jar file.
Example	sslj.jar

Field Title	Key Store JAR 5
Field Description	Enter the name of a Key Store jar file.

Figure B–26 RSA Key Store Configuration

This screen is only displayed if **RSA Key Manager v2.7.1** is selected for the Key Store provider on the Security Setup: Key Store screen.

The fields on this screen are described in the following tables.

Field Title	Server Host Address
Field Description	Enter the IP address of the RSA server host.

Field Title	Server Host Port
Field Description	Enter the port number for the RSA server host.
Example	443 443 is the default used by the RSA Key Manager.

Field Title	Cipher Key Class
Field Description	Enter the RSA Key Manager cipher key class.

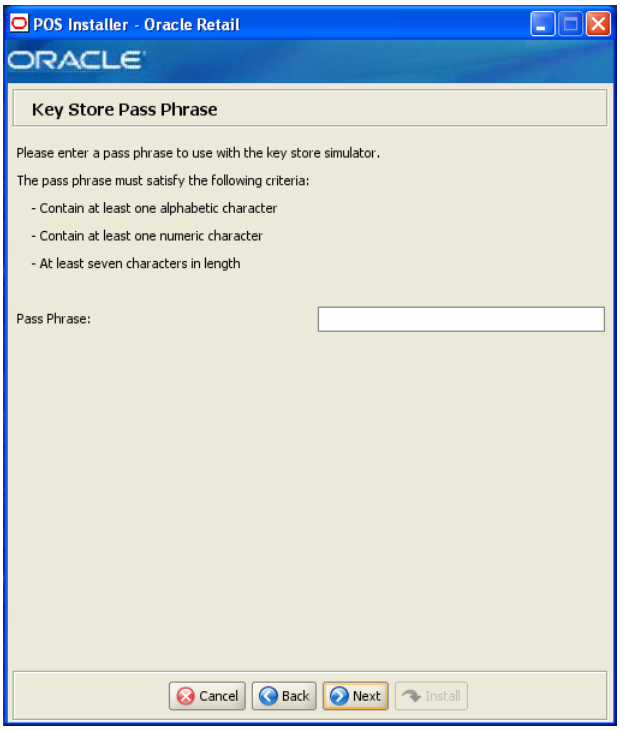
Field Title	Client Key Store File
Field Description	Select the location of the RSA Key Manager client Key Store file. **Note:** You must use forward slashes in the path name.

Field Title	Server Key Store File
Field Description	Select the location of the RSA Key Manager server Key Store file. **Note:** You must use forward slashes in the path name.

Field Title	Client Key Store Password
Field Description	Enter the password used to access the RSA Key Manager client Key Store.

Field Title	Cache Password
Field Description	Enter the password used to access the RSA Key Manager cache.

Figure B–27 Key Store Pass Phrase for Simulator Key Manager

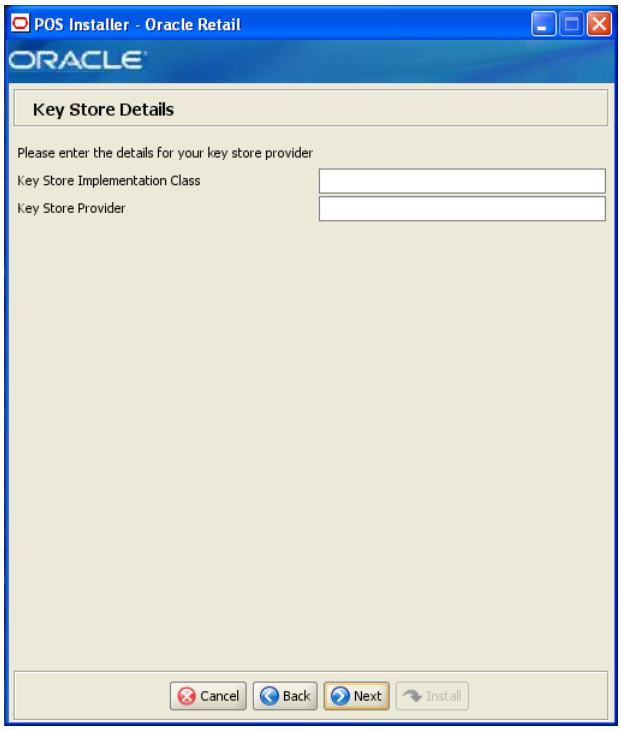


This screen is only displayed if **Simulator** is selected for the Key Store provider on the Security Setup: Key Store screen.

The field on this screen is described in the following table.

Field Title	Pass Phrase
Field Description	Enter the pass phrase used to access the Key Store simulator. **Note:** Use the same pass phrase for all Oracle Retail POS Suite applications in your configuration.

Figure B–28 Key Store Details for Other Key Manager



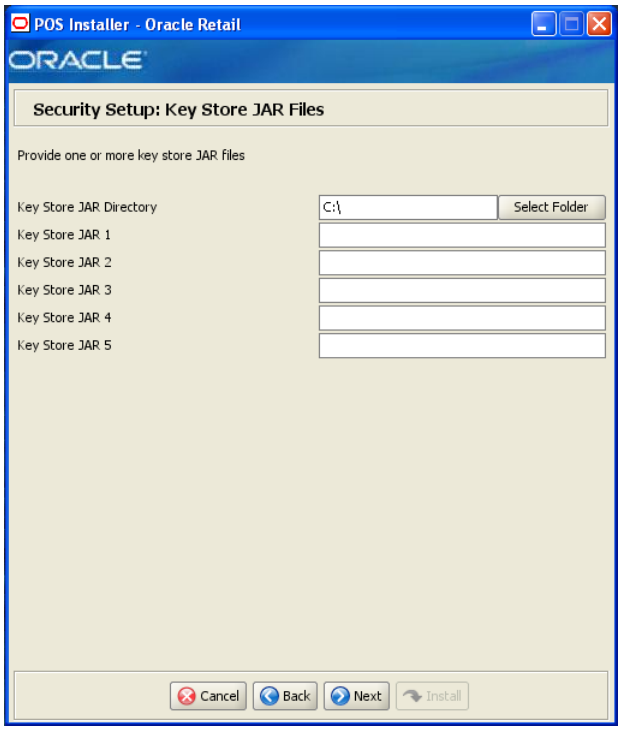
This screen is only displayed if **Other** is selected for the Key Store provider on the Security Setup: Key Store screen.

The fields on this screen are described in the following tables.

Field Title	Key Store Implementation Class
Field Description	Enter the class that invokes the key manager interface.

Field Title	Key Store Provider
Field Description	Enter the name of the provider for the Key Store.

Figure B–29 Security Setup: Key Store JAR Files for Other Key Manager



This screen is only displayed if **Other** is selected for the Key Store provider on the Security Setup: Key Store screen.

The fields on this screen are described in the following tables. Up to five Key Store jar files may be entered.

Field Title	Key Store JAR Directory
Field Description	Choose the directory where the Key Store jar files are located.

Field Title	Key Store JAR 1
Field Description	Enter the name of a Key Store jar file.

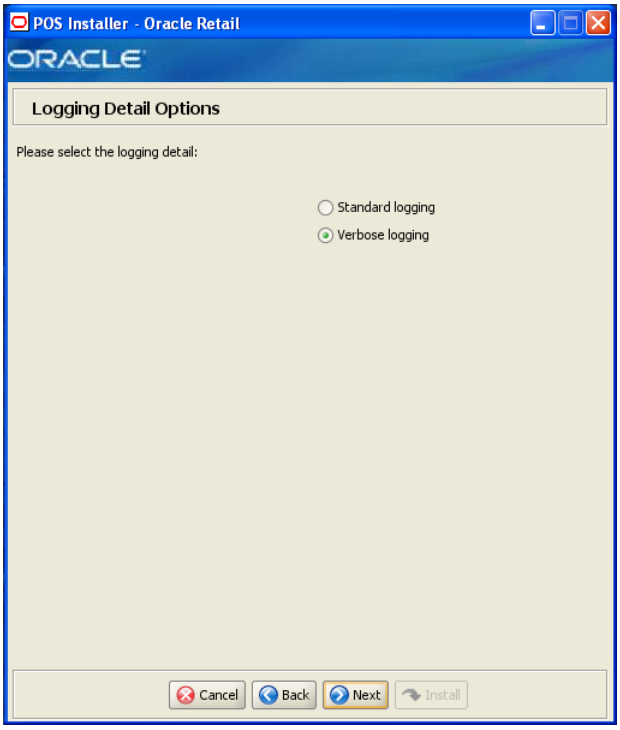
Field Title	Key Store JAR 2
Field Description	Enter the name of a Key Store jar file.

Field Title	Key Store JAR 3
Field Description	Enter the name of a Key Store jar file.

Field Title	Key Store JAR 4
Field Description	Enter the name of a Key Store jar file.

Field Title	Key Store JAR 5
Field Description	Enter the name of a Key Store jar file.

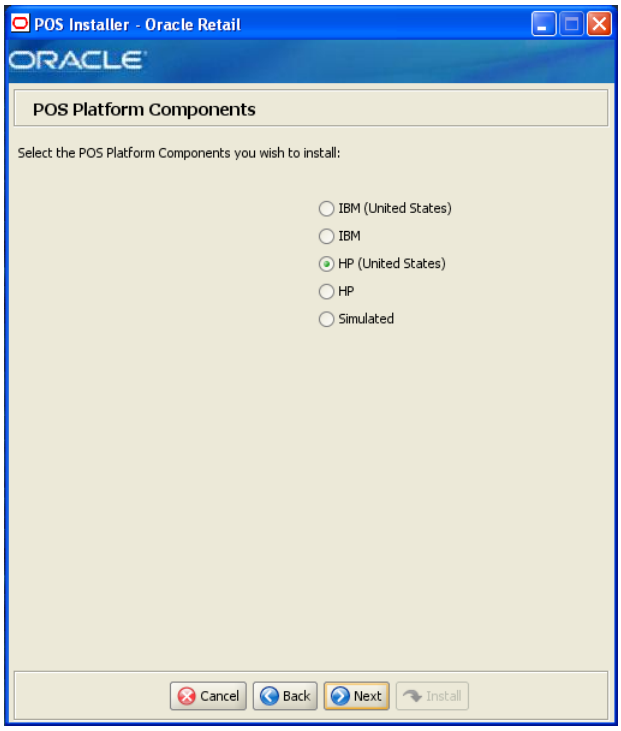
Figure B–30 Logging Detail Options



The field on this screen is described in the following table.

Field Title	Logging Detail Options
Field Description	Choose the level of client logging. ▪ To only log some of the messages, choose **Standard Logging**. ▪ To log all of the messages, choose **Verbose Logging**.
Example	Verbose logging

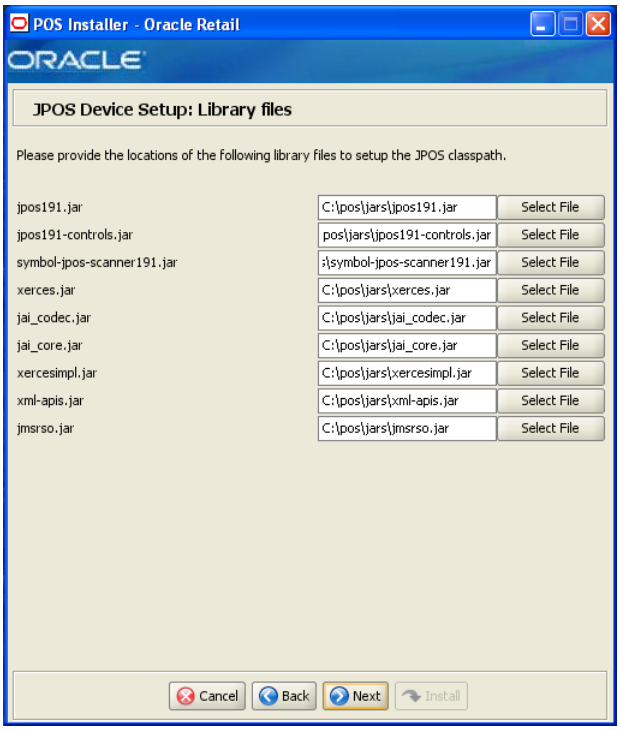
Figure B–31 POS Platform Components



The field on this screen is described in the following table.

Field Title	POS Platform Components
Field Description	From the platform components, choose the type of register and whether the devices are intended for use in or outside the United States: ▪ To use an HP register with devices intended for use in the United States, select **HP (United States)**. The next screen displayed is Figure B–32. ▪ To use an HP register with devices intended for use outside the United States, select **HP**. The next screen displayed is Figure B–32. ▪ To use a register with no devices, select **Simulated**. This should only be selected for a development environment. A network printer may be used. The next screen displayed is Figure B–40. **Note:** Only HP (United States), HP, and Simulated are supported on the Oracle stack.
Example	HP (United States)

Figure B–32 JPOS Device Setup: Library Files



This screen is only displayed if any component other than **Simulated** is selected on the POS Platform Components screen.

The fields on this screen are described in the following tables.

Field Title	**jpos191.jar**
Field Description	Enter the location of the jar file.
Example	C:\pos\jars\pos191.jar

Field Title	**jpos191-controls.jar**
Field Description	Enter the location of the jar file.
Example	C:\pos\jars\jpos191-controls.jar

Field Title	**symbol-jpos-scanner191.jar**
Field Description	Enter the location of the jar file.
Example	C:\pos\jars\symbol-jpos-scanner191.jar

Field Title	**xerces.jar**
Field Description	Enter the location of the jar file.
Example	C:\pos\jars\xerces.jar

Field Title	jai_codec.jar
Field Description	Enter the location of the jar file.
Example	C:\pos\jars\jai_codec.jar

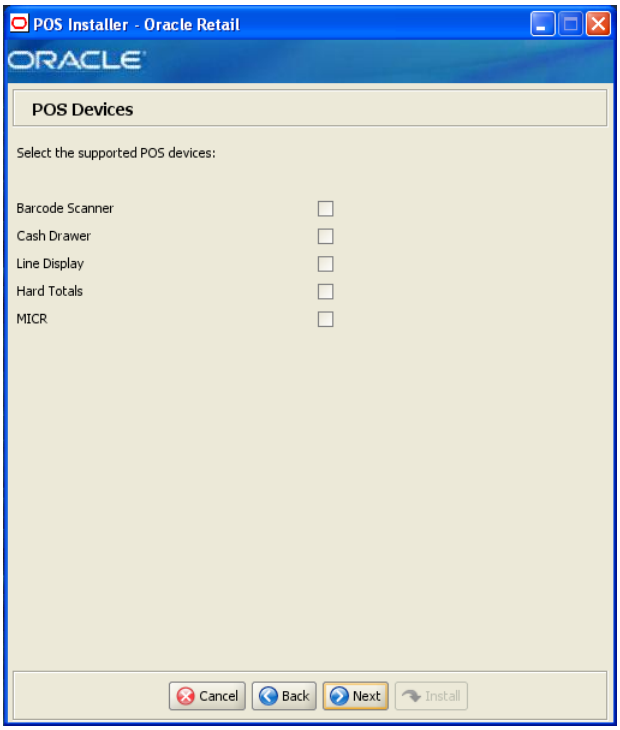
Field Title	jai_core.jar
Field Description	Enter the location of the jar file.
Example	C:\pos\jars\jai_core.jar

Field Title	xercesimpl.jar
Field Description	Enter the location of the jar file.
Example	C:\pos\jars\xercesimpl.jar

Field Title	xml-apis.jar
Field Description	Enter the location of the jar file.
Example	C:\pos\jars\xml-apis.jar

Field Title	jmsrso.jar
Field Description	Enter the location of the jar file.
Example	C:\pos\jars\jmsrso.jar

Figure B–33 POS Devices

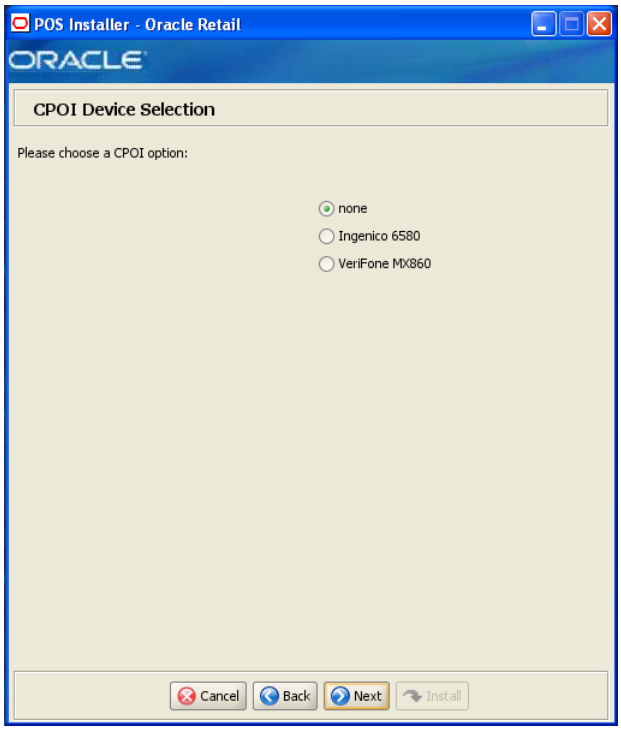


This screen is only displayed if any component other than **Simulated** is selected on the POS Platform Components screen.

The field on this screen is described in the following table.

Field Title	POS Devices
Field Description	Choose the devices to be attached to the client register.
Example	Cash Drawer

Figure B–34 CPOI Device Selection

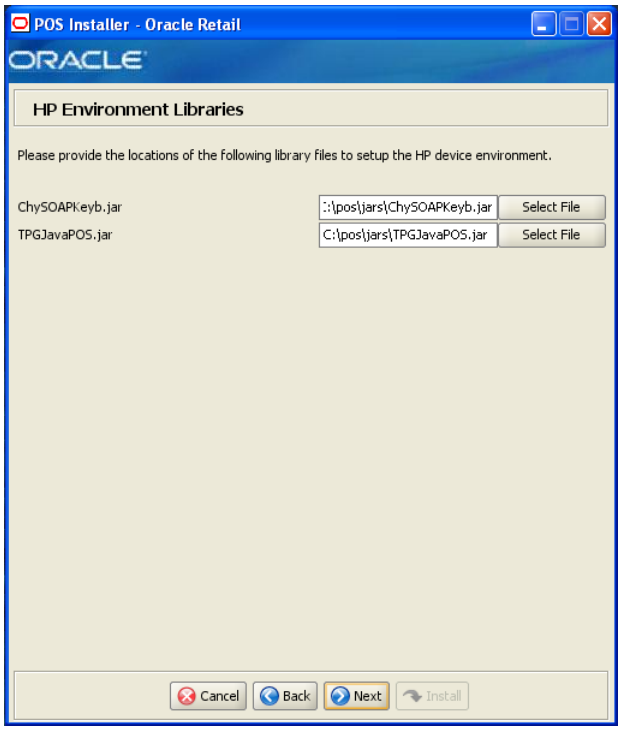


This screen is only displayed if any component other than **Simulated** is selected on the POS Platform Components screen.

The field on this screen is described in the following table.

Field Title	Please choose a CPOI option
Field Description	Choose the CPOI device to be used at the register. ■ To not use a CPOI device, choose **none**. ■ To use the VeriFone device, choose **Verifone MX860**. **Note:** Verifone MX860 is the CPOI device supported on the Oracle stack.
Example	none

Figure B–35 HP Environment Libraries



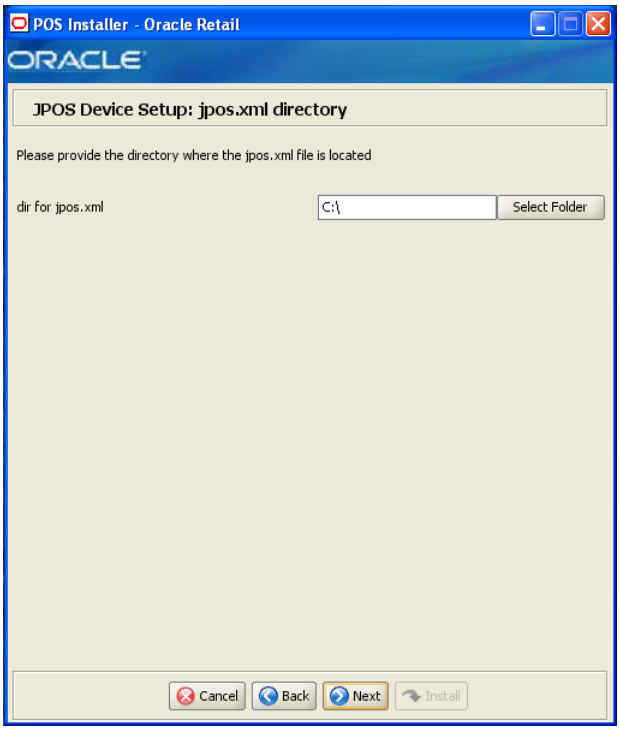
This screen is only displayed if **HP (United States)** or **HP** is selected on the POS Platform Components screen.

The fields on this screen are described in the following tables.

Field Title	ChySOAPKeyb.jar
Field Description	Enter the location of the jar file.
Example	C:\pos\jars\ChySOAPKeyb.jar

Field Title	TPGJavaPOS.jar
Field Description	Enter the location of the jar file.
Example	C:\pos\jars\TPGHJavaPOS.jar

Figure B–36 JPOS Device Setup: jpos.xml directory

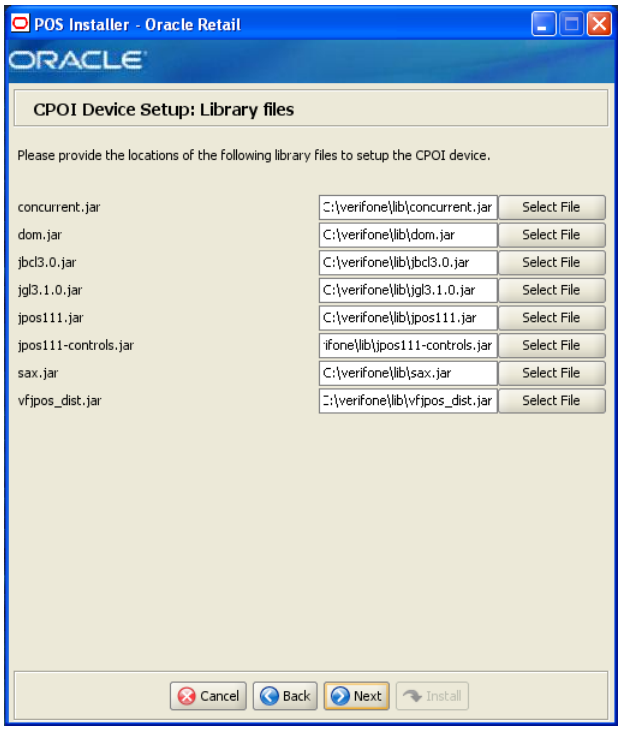


This screen is only displayed if any component other than **Simulated** is selected on the POS Platform Components screen.

The field on this screen is described in the following table.

Field Title	dir for jpos.xml
Field Description	Enter the location of the directory.

Figure B–37 CPOI Device Setup: Library files



This screen is only displayed if **Verifone MX6580** is selected on the CPOI Device Selection screen.

The fields on this screen are described in the following tables.

Field Title	concurrent.jar
Field Description	Enter the location of the jar file.
Example	C:\verifone\lib\concurrent.jar

Field Title	dom.jar
Field Description	Enter the location of the jar file.
Example	C:\verifone\lib\dom.jar

Field Title	jbcl3.0.jar
Field Description	Enter the location of the jar file.
Example	C:\verifone\lib\jbcl3.0.jar

Field Title	jgl3.1.0.jar
Field Description	Enter the location of the jar file.
Example	C:\verifone\lib\jgl3.1.0.jar

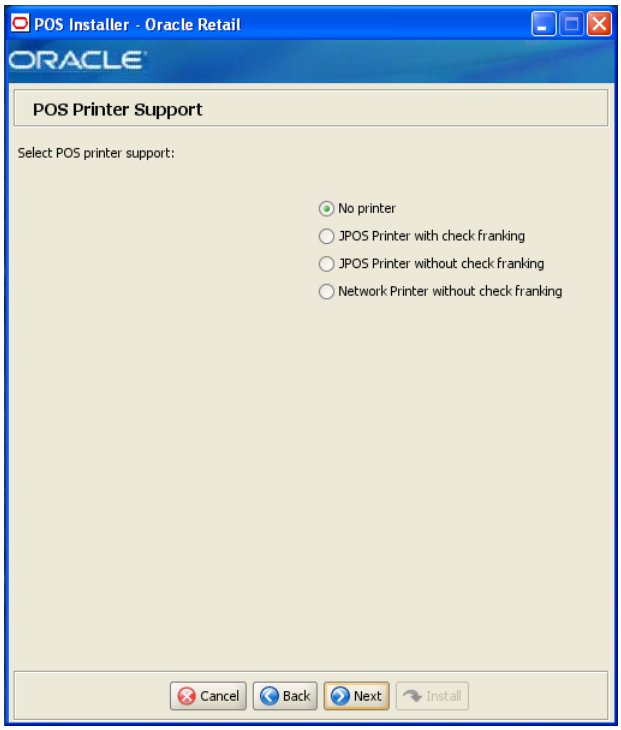
Field Title	jpos111.jar
Field Description	Enter the location of the jar file.
Example	C:\verifone\lib\jpos111.jar

Field Title	jpos111-controls.jar
Field Description	Enter the location of the jar file.
Example	C:\verifone\lib\jpos111-controls.jar

Field Title	sax.jar
Field Description	Enter the location of the jar file.
Example	C:\verifone\lib\sax.jar

Field Title	vfjpos_dist.jar
Field Description	Enter the location of the jar file.
Example	C:\verifone\lib\vfjpos_dist.jar

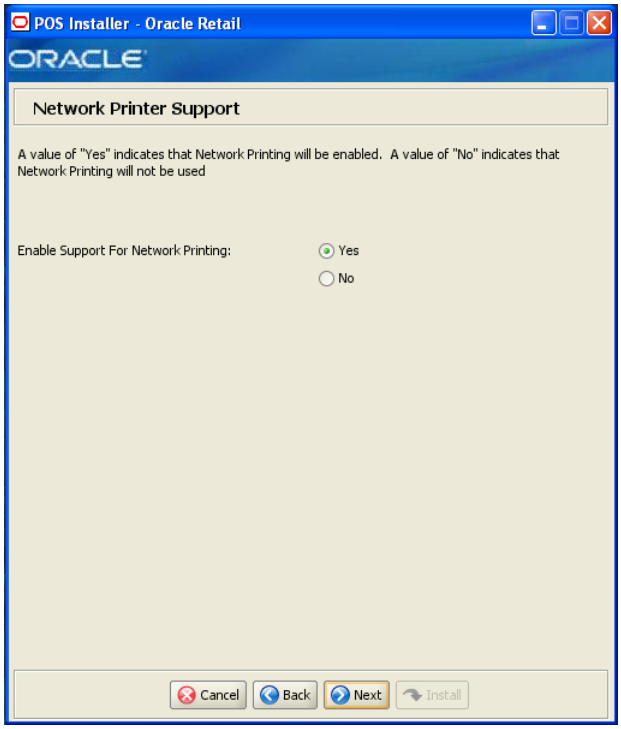
Figure B–38 POS Printer Support



The field on this screen is described in the following table.

Field Title	Select POS Printer Support
Field Description	Choose what is supported for a printer attached to the register or select a network printer.
Example	Printer with check franking

Figure B–39 Network Printer Support

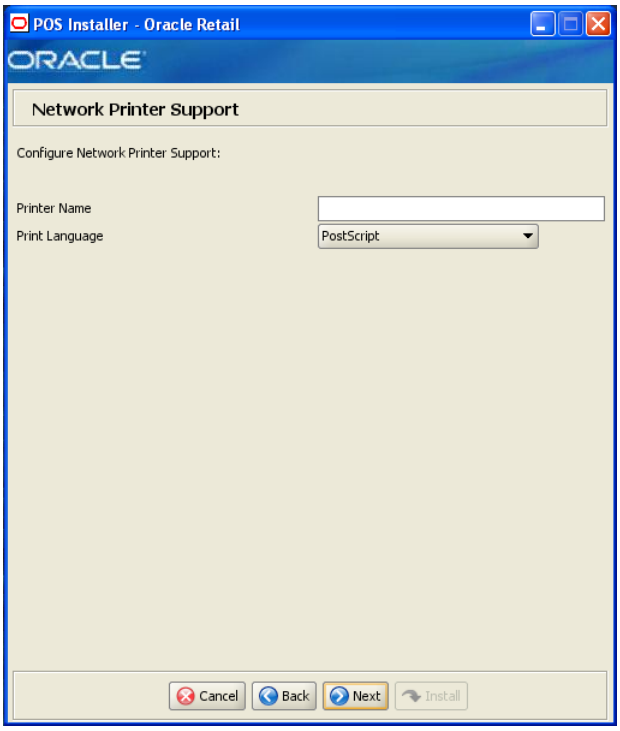


This screen is only displayed if **Network Printer without check franking** is selected on the POS Printer Support screen.

The field on this screen is described in the following table.

Field Title	Enable Support for Network Printing
Field Description	Select Yes to enable network printing.

Figure B–40 Network Printer Support Configuration

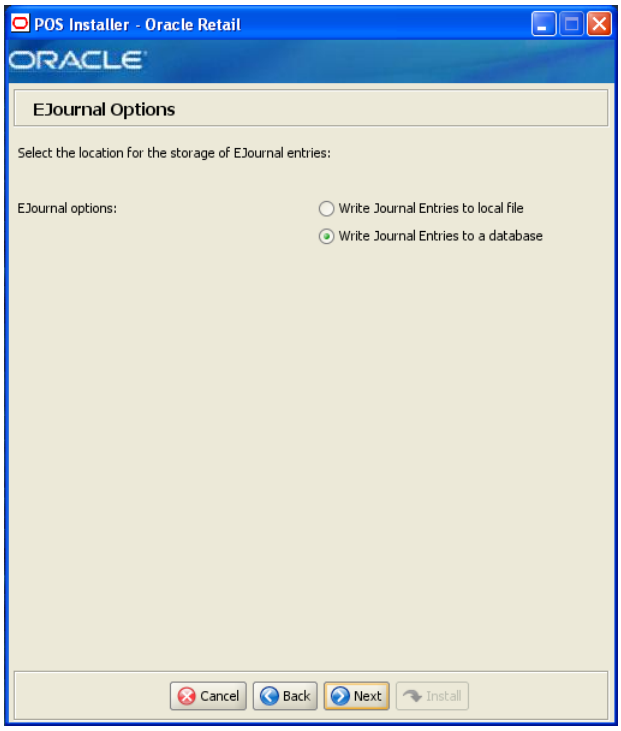


This screen is only displayed if **Yes** is selected on the Network Printer Support screen. The fields on this screen are described in the following tables.

Field Title	Printer Name
Field Description	Enter the network printer name.

Field Title	Printer Language
Field Description	Select the language for the network printer.
Example	PostScript

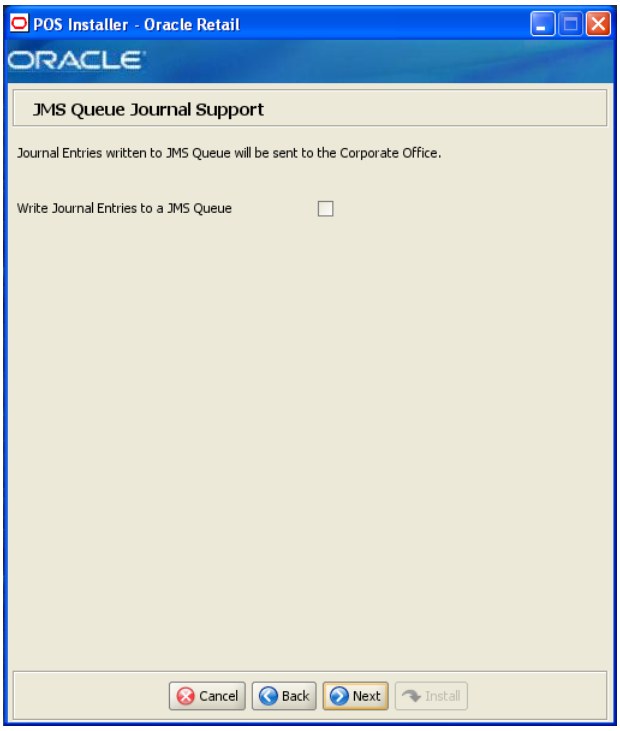
Figure B–41 EJournal Options



The field on this screen is described in the following table.

Field Title	EJournal Options
Field Description	Choose where the journal entries are to be written. ■ To write journal entries to a local file, choose **Write Journal Entries to local file**. ■ To write journal entries to a database, choose **Write Journal Entries to a database**.
Example	Write Journal Entries to a database

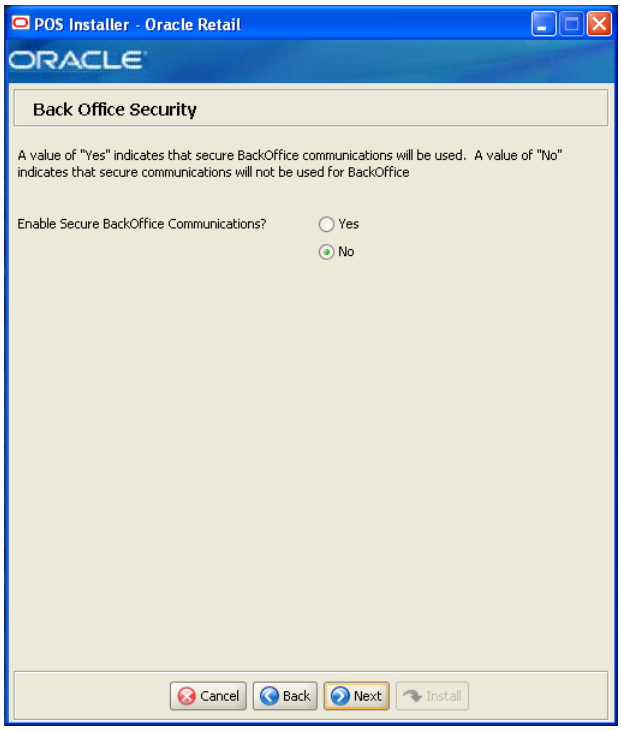
Figure B–42 JMS Queue Journal Support



The field on this screen is described in the following table.

Field Title	JMS Queue Journal Support
Field Description	Check the box if journal entries are to be written to a JMS queue and then sent to the corporate office.

Figure B–43 Back Office Security

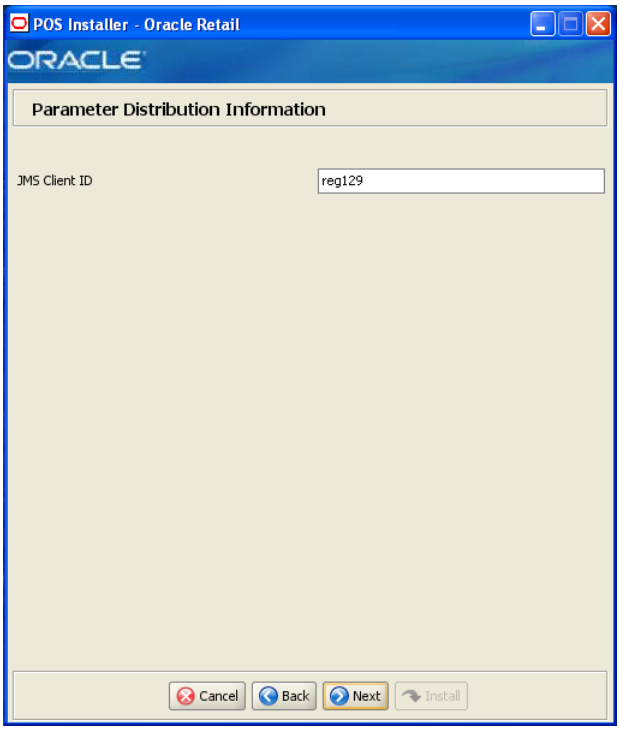


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

The field on this screen is described in the following table.

Field Title	Enable Secure Back Office Communications?
Field Description	Select Yes if secure communication with Back Office is required.
Example	Yes

Figure B–44 Parameter Distribution Information

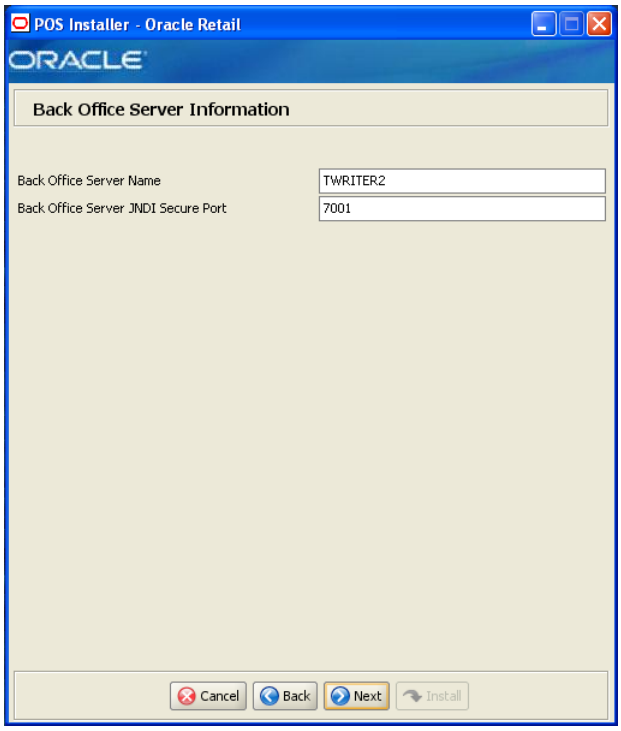


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

The fields on this screen are described in the following tables.

Field Title	JMS Client ID
Field Description	Identifier of the JMS client used for receiving parameter updates.
Example	`reg129`

Figure B–45 Back Office Server Information



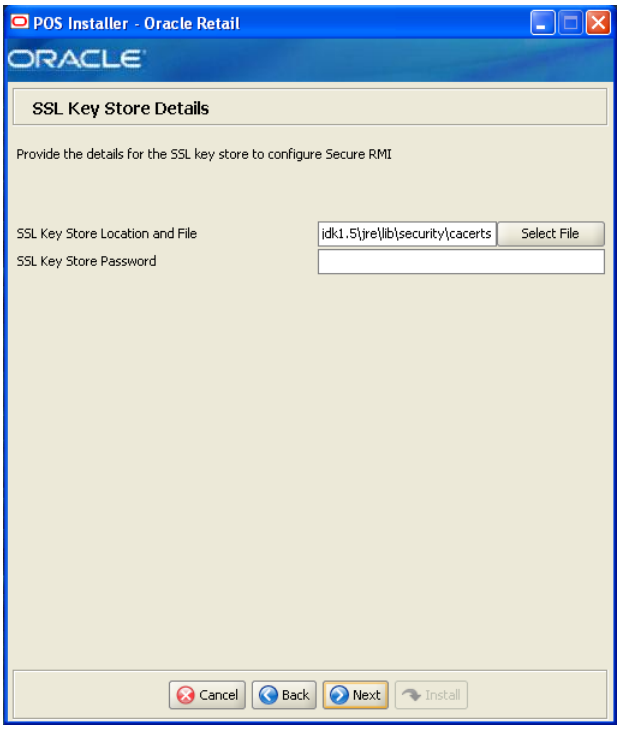
This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

The fields on this screen are described in the following tables.

Field Title	Back Office Server Name
Field Description	Enter the host name for the Back Office application.
Example	TWRITER2

Field Title	Back Office Server JNDI Port
Field Description	Enter the port number for the Back Office application. This is the port number that was entered when the Back Office domain was created.
Example	7001

Figure B–46 SSL Key Store Details



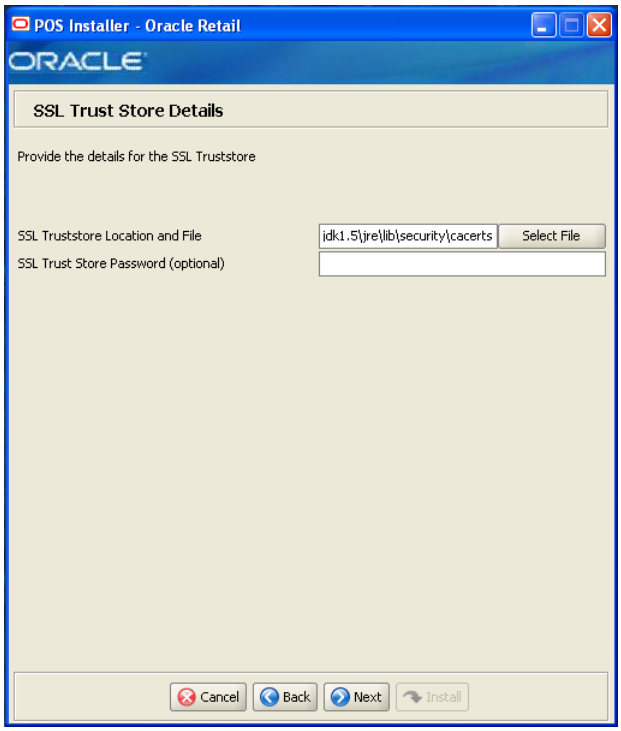
This screen is only displayed if **Yes** is selected on the Enable Secure RMI screen.

The fields on this screen are described in the following tables.

Field Title	SSL Key Store Location and File
Field Description	Enter the location and name of the Key Store.

Field Title	SSL Key Store Password
Field Description	Enter the password for the Key Store.

Figure B–47 SSL Trust Store Details

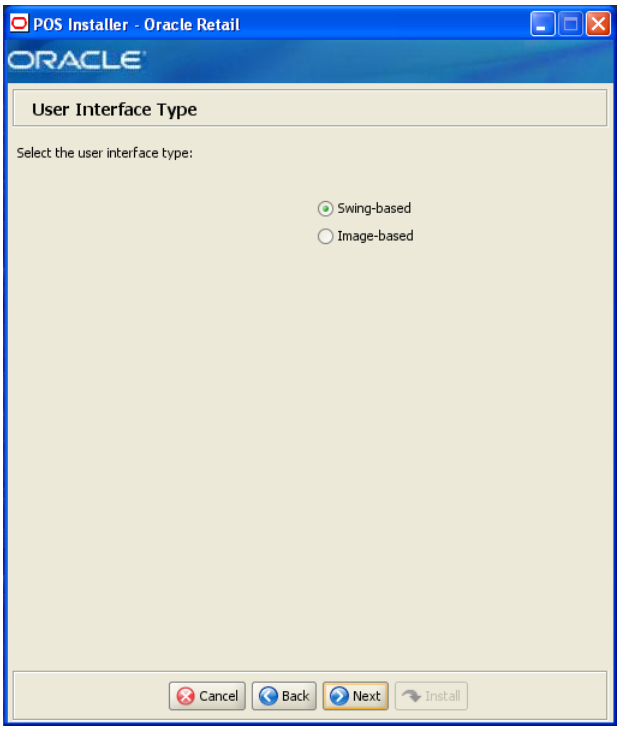


The fields on this screen are described in the following tables.

Field Title	SSL Truststore Location and File
Field Description	Enter the location and name of the truststore file.
Example	C:\jdk1.5\jre\lib\security\caerts

Field Title	SSL Trust Store Password (optional)
Field Description	Enter the password for the truststore.

Figure B–48 User Interface Type



The field on this screen is described in the following table.

Field Title	User Interface Type
Field Description	Choose the user interface look and feel. ▪ To use a standard swing interface, choose **Swing-based**. ▪ To use custom images for buttons and other graphics, choose **Image-based**.
Example	Swing-based

Figure B–49 Installation Progress

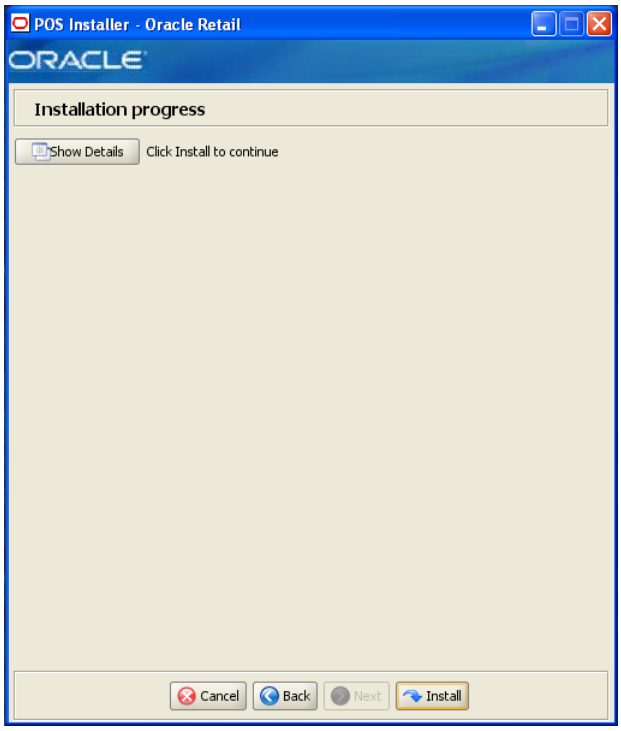
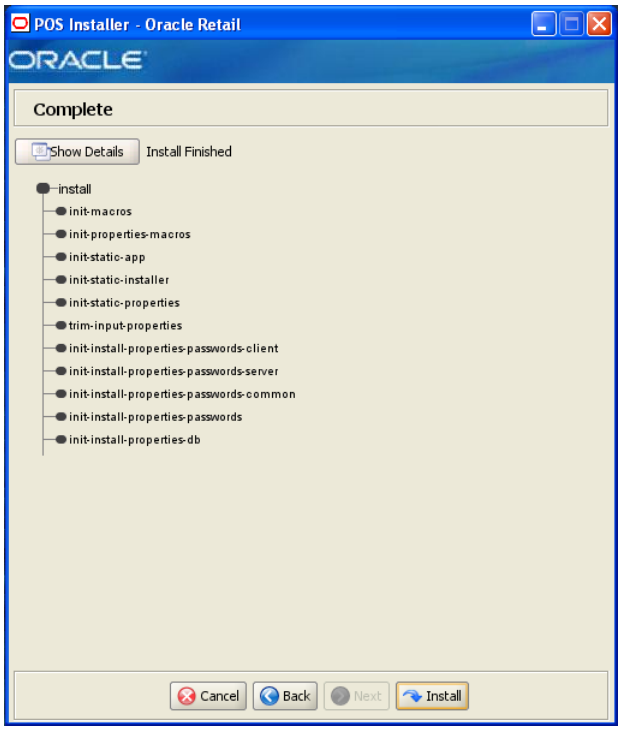


Figure B–50 Install Complete



C

Appendix: Installer Silent Mode

In addition to the GUI and text interfaces of the Point-of-Service installer, there is a silent mode that can be run. This mode is useful if you wish to run a new installation and use the settings you provided in a previous installation. It is also useful if you encounter errors during an installation and wish to continue after resolving them.

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 and the `cwallet.sso` file is created. In the second phase, this properties file is used to provide your settings for the installation.

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

1. If the installer failed in its previous run, edit the `ant.install.properties` file and correct any invalid settings that may have caused the failure.
2. If the previous install was successful, copy the wallet file from the previous installation to the staging area:
   - For the silent install of the server, copy the `cwallet.sso` file from the *<POS_install_directory>*`/`*<server>*`/pos/bin` directory to *<INSTALL_DIR>*.
   - For the silent install of a client, copy the `cwallet.sso` file from the *<POS_install_directory>*`/`*<client>*`/pos/bin` directory to *<INSTALL_DIR>*.
3. Run the installer again with the silent argument:

   ```
   install.cmd silent
   ```

D

Appendix: URL Reference

Both the database schema and application installers for the Point-of-Service product will ask for several different URLs. These include the following.

JDBC URL for an Oracle 11g Database

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

Syntax: `jdbc:oracle:thin:@<host>:<port>:<sid>`

- *<host>*: host name of the database server
- *<port>*: database listener port
- *<sid>*: system identifier for the database

For example, `jdbc:oracle:thin:@myhost:1521:mysid`

URL for the Siebel Web Service

Used by the Java application to access Siebel if integration with Siebel is enabled.

Syntax:

For most deployments, the URL will conform to one of the following patterns depending on the transport and Web service authentication being used.

- Using a transport method of HTTP and Siebel authentication:

  `http://<host>[:<port>]/eai_enu/start.swe?SWEExtSource=SecureWebService&SWEExtCmd=Execute&WSSOAP=1`

- Using a transport method of HTTP and WS-Security authentication:

  `http://<host>[:<port>]/eai_anon_enu/start.swe?SWEExtSource=SecureWebService&SWEExtCmd=Execute&WSSOAP=1`

- Using a transport method of HTTPS and Siebel authentication:

  `https://<host>[:<port>]/eai_secure_enu/start.swe?SWEExtSource=SecureWebService&SWEExtCmd=Execute&WSSOAP=1`

- Using a transport method of HTTPS and WS-Security authentication:

  `https://<host>[:<port>]/eai_secure_enu/start.swe?SWEExtSource=SecureWebService&SWEExtCmd=Execute&WSSOAP=1`

For example, `http://sdc78029svqe.corp.siebel.com/eai_enu/start.swe?SWEExtSource=SecureWebService&SWEExtCmd=Execute&WSSOAP=1`

E

Appendix: Common Installation Errors

This appendix describes some common errors encountered during installation of Point-of-Service.

"Pos installer finished with errors"

If you see this error message, there could be some settings incorrectly set or problems with the installer itself. For more information, check the *<POS_install_directory>*/pos/logs/installer_log.txt file.

"Dispatcher.main, Exception: java.security.AccessControlException: access denied (java.util.PropertyPermission * read,write)"

Symptom:

The application fails when starting up:

```
 [java] Dispatcher.main, Exception: java.security.AccessControlException: access
 denied (java.util.PropertyPermission * read,write)
     [java] java.security.AccessControlException: access denied
 (java.util.PropertyPermission * read,write)
     [java]     at java.security.AccessControlContext.checkPermission(Unknown
 Source)
     [java]     at java.security.AccessController.checkPermission(Unknown Source)
     [java]     at java.lang.SecurityManager.checkPermission(Unknown Source)
     [java]     at java.lang.SecurityManager.checkPropertiesAccess(Unknown Source)
     [java]     at java.lang.System.getProperties(Unknown Source)
     [java]     at
com.extendyourstore.foundation.tour.conduit.Dispatcher.<init>(Dispatcher.java:461)
     [java]     at
com.extendyourstore.foundation.tour.conduit.Dispatcher.getDispatcher(Dispatcher.ja
va:1301)
     [java]     at
com.extendyourstore.foundation.tour.conduit.Dispatcher.main(Dispatcher.java:2439)
     [java]     at
com.extendyourstore.foundation.config.TierLoader.main(TierLoader.java:359)
```

Solution:

This error usually occurs because the JRE that you are pointing to does not contain the `updated java.security` and `java.policy` files.

"java.lang.NullPointerException"

Symptom:

The application dies when starting up. Check the *<POS_install_directory>*/pos-install-yyyyMMddHHmm.log file, where yyyyMMddHHmm is the timestamp of the install. In the log file, search for **Database 'offlinedb' not found**.

```
ERROR 2007-07-29 15:54:49,608 4938
   (main:com.extendyourstore.foundation.manager.data.JdbcDataConnection):

[com.extendyourstore.foundation.manager.data.JdbcDataConnection.logSQLException
(JdbcDataConnection.java:1355)] Get Connection failed :Database 'offlinedb' not
found.
```

Solution:

This error occurs the first time the client is started after it is installed. The server was unable to establish a connection to the database. This prevented the offlinedb database from being created.

This error usually occurs because incorrect information was entered on the Database Configuration screen during the install. Reinstall the server with the correct database configuration information. Check that the IDDI folder was created for the server in *<POS_install_directory>*/pos/bin.

F

Appendix: Troubleshooting Problems on the Oracle Stack

This appendix contains information that may be useful if you encounter errors running Point-of-Service for the first time after an install.

The configuration steps enable Point-of-Service to communicate with Back Office and Central Office in order to receive parameter updates and to send EJournal and POSLogs up to Central Office. If you have problems, you may want to ensure the steps were successfully completed by the installer.

jndi.properties File Name

On the Central Office/Back Office Server Information screen, you enter the host name for the Central Office server. In the *<POS_install_directory>*/pos/config directory, there is a jndi.properties file for Central Office. When this file is created during installation, the name of the file includes the host name you entered for the Central Office server.

For example, if you enter centraloffice for the host name, the name of the created file is centraloffice.jndi.properties.

Secure RMI and Secure JDBC

Understanding SSL/TLS connection problems can be difficult, especially when it is not clear what messages are actually being sent and received. The SunJSSE has a built-in debug facility that is activated by the system property javax.net.debug.

- To enable SSL debugging for the Point-of-Service server, add -Djavax.net.debug=all to the StoreServerConduit.bat file and restart the server:

  ```
  set COMMAND "java %JAVA_OPTIONS% -Djavax.net.debug=all
  com.extendyourstore.foundation.config.TierLoader %CONDUIT_CONFIG%"
  ```

- To enable SSL debugging for the Point-of-Service client, add -Djavax.net.debug=all to the ClientConduit.bat file and start the client:

  ```
  set JAVA_OPTIONS=%JAVA_MEM_OPTIONS% %JAVA_OPTIONS%  -Djavax.net.debug=all
  ```

For information on understanding the debug output, see the following Web site:

http://java.sun.com/j2se/1.5.0/docs/guide/security/jsse/ReadDebug.html

In the log files for the server and client, look for HandshakeExceptions. The following examples list the most common exceptions:

- Certificates not yet active—This occurs when the date on the store server is ahead of the date on the client. Because of this dated discrepancy, the certificate exported from the server has not become active yet.
- Location for the Key Store or trust store is incorrect—For information about the files that are changed when enabling secure RMI, see Appendix J.
- KeyEncryptionService (RSA) is not located in the correct place—Due to this configuration error, the passwords in the XML files and `posfoundation.properties` file cannot be generated. An empty `posfoundation.properties` is created in in `OracleRetailStore\Server\pos\config` and `OracleRetailStore\Client\pos\config`.

  After fixing the KeyEncryptionService configuration issue, you either have to reinstall Point-of_Service or get a copy of the original `posfoundation.properties` file located in the *<INSTALL_DIR>*`\product\config` and update the file. To update the file, follow the steps in Appendix J to manually update the `posfoundation.properties` file.
- Type of the store server Key Store is different than the type of the client trust store—To check the type, use the following keytool commands:

  ```
  keytool -list -keystore <your_key_store_name_and_location>
  keytool -list -truststore <your_truststore_name_and_location>
  ```

  The above commands list the Key Store and trust store type and provider along with all the certificates that are stored in these files, as shown in the following example:

  ```
  Keystore type: jks

  Keystore provider: Oracle

  Your keystore contains 1 entry
  Oracle, Jul 9, 2009, keyEntry,
  Certificate fingerprint (MD5): EF:33:FE:13:0D:EC:8C:64:1B:C1:89:4C:86:62:6C:53
  ```

  Make sure that the Key Store type matches in both files.

G

Appendix: Best Practices for Passwords

This appendix has information on the practices that should be followed for passwords. The following topics are covered:

- "Password Guidelines"
- "Special Security Options for Oracle Databases"

Password Guidelines

To make sure users and their passwords are properly protected, follow these guidelines. The guidelines are based on the Payment Card Industry Data Security Standard (PCI-DSS):

- Verify the identity of the user before resetting any passwords.
- Set first-time passwords to a unique value for each user and require the password to be changed immediately after the first use.
- Immediately revoke access for any terminated users.
- Remove inactive user accounts at least every 90 days.
- Enable accounts used by vendors for remote maintenance only during the time period when access is needed.
- Communicate password procedures and policies to all users who have access to cardholder data.
- Do not use group, shared, or generic accounts and passwords.
- Require user passwords to be changed at least every 90 days.
- Require a minimum password length of at least seven characters.
- Require that passwords contain both numeric and alphabetic characters.
- Do not accept a new password that is the same as any of the last four passwords used by a user.
- Limit the number of repeated access attempts by locking out the user ID after not more than six attempts.
- Set the lockout duration to thirty minutes or until an administrator enables the user ID.

Special Security Options for Oracle Databases

The following information is based on Oracle Database version 11.2.0.1 and is found in the *Oracle Database Security Guide*.

Enforcing Password Policies Using Database Profiles

Password policies can be enforced using database profiles. The options can be changed using a SQL statement, for example:

```
alter profile appsample limit
```

Option	Setting	Description
FAILED_LOGIN_ATTEMPTS	4	Maximum number of login attempts before the account is locked.
PASSWORD_GRACE_TIME	3	Number of days a user has to change an expired password before the account is locked.
PASSWORD_LIFE_TIME	90	Number of days that the current password can be used.
PASSWORD_LOCK_TIME	30	Amount of time in minutes that the account is locked.
PASSWORD_REUSE_MAX	10	Number of unique passwords the user must supply before the first password can be reused.
PASSWORD_VERIFY_FUNCTION	<*routine_name*>	Name of the verification script that is used to ensure that the password meets the requirements of the password policy. See "Enforcing Password Policies Using a Verification Script".

Enforcing Password Policies Using a Verification Script

Password policies can be enforced using a password complexity verification script, for example:

```
UTLPWDMG.SQL
```

The password complexity verification routine ensures that the password meets the following requirements:

- Is at least four characters long
- Differs from the user name
- Has at least one alpha, one numeric, and one punctuation mark character
- Is not simple or obvious, such as welcome, account, database, or user
- Differs from the previous password by at least three characters

For example, to set the password to expire as soon as the user logs in for the first time:

```
CREATE USER jbrown
IDENTIFIED BY zX83yT
...
PASSWORD EXPIRE;
```

H

Appendix: Keytool Utility

The keytool utility is included with the JRE. It is used to create new keys, import digital certificates, export existing keys, and interact with the key management system.

Creating a Self-Signed Certificate

To create a self-signed certificate, use the following command. It creates a private key and a self-signed certificate that contains the corresponding public key:

```
keytool -genkey -keystore <your_keystore_name_and_location>
-alias <your_alias> -keyalg RSA
```

Note: If the provided Key Store does not exist on the file system, this command creates a new Key Store. It is recommended that you use your own Key Store file instead of using the default file, named `cacerts` provided by Java.

If no Key Store name is provided, the Key Store is, by default, stored in a file named `.keystore` in the user's home directory, as determined by the `user.home` system property. In this case, the default password for the Key Store is `changeit`.

Caution: The Key Store name and location is used by the Point-Of-Service installer to populate the `javax.net.ssl.keyStore` entry in the `posfoundation.properties` file. Make sure that the Key Store file and certificate are created before starting the installation.

Creating a Certificate Signing Request

To obtain a certificate signed by a real Certificate Authority, create a Certificate Signing Request.

1. Use the following command to generate the request:

   ```
   keytool -certreq -keystore <your_keystore_name_and_location>
   -alias <your_alias> -file <your_file.cer>
   ```

2. Once the Certificate Signing Request is saved in a file, send it to the Certificate Authority of your choice. To get a trial certificate, see the following Web site:

   https://www.thawte.com

3. When the response from the Certificate Authority is received, save the certificate in a file from which it can be imported. In order to import the certificate, the root certificate must be in your list of trusted certificate authorities, or you must accept the root certificate selected by the keytool utility.

4. To import the certificate, use the following command:

   ```
   keytool -import -keystore <your_keystore_name_and_location>
   -file <your_certificate_file.cer> -alias <your_alias> -trustcacerts
   ```

For development or testing purposes, it should not be necessary to get a trial certificate or have your certificate signed.

Exporting and Importing Certificates

The server in an SSL conversation must have a private key and a certificate that verifies its identity.

- The private key is used by the server as a part of the key exchange algorithm.
- The certificate is sent to the client to identify the server. This information is obtained from the Key Store.
- The truststore is used by the client to verify the certificate that is sent by the server.

To populate the truststore for the Point-of-Service client with the public certificate of a server:

1. Export the above generated certificate (without the private key) from the server Key Store. For information on creating the certificate, see Creating a Certificate Signing Request.

   ```
   keytool -export -keystore <your_keystore> -alias <your_alias>
   -file <your_file.cer>
   ```

2. Import the certificate into the truststore for the Point-of-Service client.

   ```
   keytool -import -alias <your_alias>
   -keystore <your_truststore_name_and_location> -file <your_file.cer>
   ```

   The Point-of-Service installer populates the `javax.net.ssl.trustStore` property in the `posfoundation.properties` file with the location and name of the truststore file.

Note: If the provided truststore does not exist on the file system, this command creates a new truststore. It is recommended that you use your own truststore file instead of using the default file, named `cacerts` provided by Java.

Caution: It is recommended that the certificate is added to your own truststore instead of the default `cacerts` truststore provided by Java.

The password for the default truststore is **changeit**. If you add it to a custom trust store, you need to communicate this to the JVM. The Point-of-Service installer sets the location and password for the truststore into the `javax.net.ssl.trustStore` and `javax.net.ssl.trustStorePassword` properties in the `posfoundation.properties` file.

Appendix: Secure JDBC with Oracle 11g Database

This appendix has information on setting up and communicating with a secured Oracle 11g database server based on the following assumptions:

- Client authentication is not needed.
- The Oracle wallet is used as a trust store on the database server.

SSL encryption for Oracle JDBC has been supported in the JDBC-OCI driver since Oracle JDBC 9.2.x, and is supported in the THIN driver starting in 10.2. SSL authentication has been supported in the JDBC-OCI driver since Oracle JDBC 9.2.x. The THIN driver supports Oracle Advanced Security SSL implementation in Oracle Database 11g Release 1 (11.2).

For more information, see the following Web sites:

- http://www.oracle.com/technetwork/database/enterprise-edition/wp-oracle-jdbc-thin-ssl-130128.pdf
- http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/toc.htm
- http://download.oracle.com/docs/cd/B28359_01/java.111/b31224/toc.htm

Creating the Oracle Wallet and Certificate for the Database Server

Note the following information:

- If you want have a user interface, run the server administration console.
- The wallet you create must support Auto Login. It must be enabled on the new wallet.
- The following is the wallet directory default:
  - For UNIX–`ORACLE_HOME/admin/ORACLE_SID`
  - For Microsoft Windows–`%USERPROFILE%\ORACLE\WALLETS`
  - Test server wallet information:
    * Wallet password: securedb11g
    * Wallet directory: `/u01/oracle/admin/SECURDB11G`

- When generating a self-signed certificate, note the following:
  - Do not use keytool to create a certificate for using Oracle wallets. They are incompatible.
  - Two wallets are needed to generate a self-signed certificate. One wallet is needed to sign the certificate and another wallet is needed to use the certificate.
  - For command line wallet access, use `orapki`.
  - For instructions on generating a self-signed certificate, see *APPENDIX B CREATING TRUSTSTORES AND KEYSTORES* in the following document:

    http://www.oracle.com/technetwork/database/enterprise-edition/wp-oracle-jdbc-thin-ssl-130128.pdf
  - The following are examples of `orapki` commands:
    * To create the wallet:

      ```
      orapki wallet create -wallet <wallet directory>
      ```

    * To add the self-signed certificate:

      ```
      orapki wallet add -wallet <wallet directory> -dn
      CN=<certificate name>,C-US -keysize 2048 -self_signed -validity 3650
      ```

    * To view the wallet:

      ```
      orapki wallet display -wallet <wallet directory>
      ```
- The Wallet Manager UI can also be used to import certificates.

Securing the Listener on the Server

The `listener.ora`, `tnsnames.ora`, and `sqlnet.ora` files are found in the `ORACLE_HOME/network/admin` directory. If the `sqlnet.ora` file does not exist, you need to create it.

To secure the listener on the server:

1. Add TCPS protocol to the `listener.ora` file.
2. Add TCPS protocol to the `tnsnames.ora` file.
3. Add the Oracle Wallet location to the `sqlnet.ora` and `listener.ora` files.
4. Add disabling of client authentication to the `sqlnet.ora` and `listener.ora` files.
5. Add encryption-only cipher suites to the `sqlnet.ora` file.
6. Bounce the listener once the file is updated.

Examples of Network Configuration Files

Examples of the following network configuration files are shown in this section:

- listener.ora
- sqlnet.ora
- tnsnames.ora

listener.ora

```
SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME = PLSExtProc)
      (ORACLE_HOME = /u01/oracle/11g)
      (PROGRAM = extproc)
    )
  )

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = 10.143.44.108)(PORT = 1521))
      (ADDRESS = (PROTOCOL = TCPS)(HOST = 10.143.44.108)(PORT = 2484))
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROCO))
    )
  )

WALLET_LOCATION=(SOURCE=(METHOD=FILE)
  (METHOD_DATA=(DIRECTORY=/u01/oracle/admin/SECURDB11G)))

SSL_CLIENT_AUTHENTICATION=FALSE
```

Caution: To generate a trace log, add the following entries to the `listener.ora` file:

```
TRACE_LEVEL_LISTENER = ADMIN
TRACE_DIRECTORY_LISTENER = /u01/oracle/11g/network/trace
TRACE_FILE_LISTENER = listener.trc
```

sqlnet.ora

```
SSL_CLIENT_AUTHENTICATION=FALSE

SSL_CIPHER_SUITES=(SSL_DH_anon_WITH_3DES_EDE_CBC_SHA, SSL_DH_anon_WITH_RC4_128_
MD5, SSL_DH_anon_WITH_DES_CBC_SHA)

WALLET_LOCATION=(SOURCE=(METHOD=FILE)
  (METHOD_DATA=(DIRECTORY=/u01/oracle/admin/SECURDB11G)))
```

tnsnames.ora

```
SECURDB11G =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = 10.143.44.108)(PORT = 1521))
      (ADDRESS = (PROTOCOL = TCPS)(HOST = 10.143.44.108)(PORT = 2484))
    )
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = SECURDB11G)
    )
  )
```

Securing Client Access

Caution: Ensure you are using `ojdbc.jar` version 10.2.x or later. Version 10.1.x or earlier will not connect over TCPS.

To secure client access:

1. Export the self-signed certificate from the server Oracle Wallet and import it into a local trust store. See "Exporting and Importing Certificates" in Appendix H.
2. Use the following URL format for the JDBC connection:

```
jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=tcps) (HOST=10.143.44.108)
(PORT=2484) ) (CONNECT_DATA= (SERVICE_NAME=SECURDB11G)))
```

3. The database connection call requires the following properties to be set, either as system properties or JDBC connection properties:

Property	Value
oracle.net.ssl_cipher_suites	(SSL_DH_anon_WITH_3DES_EDE_CBC_SHA, SSL_DH_anon_WITH_RC4_128_MD5, SSL_DH_anon_WITH_DES_CBC_SHA)
javax.net.ssl.trustStore	Path and file name of trust store For example: `/DevTools/Testing/Secure11g/truststore/truststore`
javax.net.ssl.trustStoreType	JKS
javax.net.ssl.trustStorePassword	Password for trust store

Specific Instructions for Point-of-Service

Note: This section applies to manual configuration of secure JDBC protocol. All the steps listed below are done automatically by the installer when **Yes** is selected on the Enable Secure JDBC screen.

To configure Oracle Retail Point-of-Service:

1. Configure the database server as shown above.
2. Copy the `ojdbc5.jar` file from the database server and replace in the `pos` library.

Note: The `ojdbc5.jar` file that comes with 11.2.0.1 version of database supports TCPS protocol.

3. Update the connection pool that is defined in the following files:
   - `server/pos/config/technician/DefaultDataTechnician.xml`
   - `server/pos/config/technician/EnterpriseDataTechnician.xml`

J

Appendix: Secure RMI

To enable secure RMI for register-to-store server communication:

1. Prepare the Key Store and trust stores using the keytool utility described in Appendix H.

   Note: If you are doing a manual configuration of secure RMI, follow Steps 2 and 3. If the installer is doing the configuration, the changes are made by the installer. If you do want to use different cipher suites, you must update the properties files.

2. For the store server, add the following properties to the *<pos_install_directory>*\server\pos\config\posfoundation.properties file:

   - EnabledCipherSuites=*<cipher_suites_to_use>*

     For example:

     EnabledCipherSuites=SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA

     If the EnabledCipherSuites property is not defined, the defaults are used.

     Note: It is recommended that the default cipher suites provided by Java are used.

   - EncryptValets=true

     This causes the RMI communication between Manager/Technician pairs to be secured.

   - javax.net.ssl.keyStore=$KEYSTORE_FILE$

     This points to the Key Store that contains the private keys and public certificates for the server. For example:

     javax.net.ssl.keyStore=%JAVA_HOME%\\jre\\lib\\security*<keystore_name>*

   - javax.net.ssl.keyStorePassword=!$KEYSTORE_PASSWORD$

     This is the encrypted password for the Key Store. For example:

     javax.net.ssl.keyStorePassword=!changeit

Note: The Key Store password follows the same convention for encryption as the other passwords.

3. For the register, add the following properties to the `<pos_install_directory>client\pos\config\posfoundation.properties` file:

   - `EnabledCipherSuites=<cipher_suites_to_use>`

     Note: The cipher suites selected for the register have to match the ones selected for the store server.

   - `EncryptValets=true`

     This causes the RMI communication between Manager/Technician pairs to be secured.

   - `javax.net.ssl.trustStore=$TRUSTSTORE_FILE$`

     This points to the trust store that contains the public certificates for the client. For example:

     `javax.net.ssl.trustStore=%JAVA_HOME%\jre\lib\security\<truststore_name>`

     Note: A trust store does not need to be defined in the `posfoundation.properties` file if certificates are imported into `cacerts` or `jssecacerts`. It is recommended that `cacerts` or `jssecacerts` is used.

K

Appendix: Device Configuration

Updates are made to the device configuration before running the installer. This appendix describes the updates.

The `jpos.xml` file needs to be updated to reflect the devices used on the machine. The typical location for this file is `C:\POS\IBMJPOS\jpos.xml`. For the updates for the devices, see the applicable section:

- "Configuring Devices for an HP Register"
- "Configuring a Verifone Customer Interaction Device"

Configuring Devices for an HP Register

To configure the devices for an HP register:

1. To configure the default scanner, copy the `JPOS_VendorInfo.xml` file into the *<POS_install_directory>*`\pos\bin` directory and replace the existing entry or add the following entry to the `jpos.xml` file:

```
<JposEntry logicalName="defaultScanner">
    <creation factoryClass="com.symbol.jpos.SymScannerSvc191Factory"
        serviceClass="com.symbol.jpos.SymScannerSvc191"/>
    <vendor name="Hewlett-Packard" url="http://www.hp.com"/>
    <jpos category="Scanner" version="1.9"/>
    <product description="Symbol Serial/USB Scanner" name="HP_USBSCANNER"
        url="http://www.hp.com"/>

    <!--Other non JavaPOS required properties-->
    <!--Comm port device name, must be 'USB' for USB scanner-->
    <prop name="port" value="USB"/>
    <!--Scanner type, default=0, valid values are: 0=Any,
        18944=TableTop(0x4A00), 19200=HandHeld(0x4B00)-->
    <prop name="ScannerType" value="0"/>
</JposEntry>
```

2. To configure the default printer, replace the existing entry or add the following entry to the `jpos.xml` file:

```
<JposEntry logicalName="defaultPrinter">
    <creation
        factoryClass="com.tpg.javapos.jpos.TPGJposServiceInstanceFactory"
  serviceClass="com.tpg.javapos.jpos.services.posprinter.POSPrinterService"/>
    <vendor name="HP" url="http://www.hp.com"/>
    <jpos category="POSPrinter" version="1.8"/>
    <product description="HP POS Printer Service" name="HP Services for
        JavaPOS(TM) Standard" url="http://www.hp.com"/>
```

```
    <!--Other non JavaPOS required property (mostly vendor properties and bus
        specific properties i.e. RS232 )-->
    <prop name="sModelClassName" value="com.tpg.javapos.models.hydra.ptr_cd_
micr.tpg7xx.TPG7xxPtrCDMICRModelLoader"/>
    <!--prop name="commChannel" value="ethernet"/-->
    <prop name="Img_PortNumber" value="9001"/>
    <!--prop name="Ret_PortNumber" value="9000"/-->
    <prop name="dualClientImager" value ="false"/>
    <prop name="Img_IPAddress" value="10.1.2.33"/>
    <prop name="CloseOnTransmit" value="true"/>
    <!--prop name="commChannel" value="serial"/-->
    <!--prop name="portName" value="ethernet"/-->
    <prop name="commChannel" value="nativeusb"/>
    <!--prop name="portName" value="COM2"/-->
    <prop name="portName" value="nativeusb"/>
    <prop name="baudRate" value="115200"/>
    <prop name="dataBits" value="8"/>
    <prop name="stopBits" value="1"/>
    <prop name="parity" value="N"/>
    <prop name="flowControl" value="RTS"/>
    <!--prop name="ImagerCommChannel" value="ethernetserver"/-->
    <!--prop name="ImagerCommChannel" value="serial"/-->
    <prop name="ImagerCommChannel" value="nativeusb"/>
    <prop name="AutoLineFeed" value="true"/>
    <prop name="sModel" value="7176"/>
    <prop name="asciiBarCode" value="true"/>
</JposEntry>
```

3. To configure the default MICR device, replace the existing entry or add the following entry to the `jpos.xml` file:

```
<JposEntry logicalName="defaultMICR">
    <creation
        factoryClass="com.tpg.javapos.jpos.TPGJposServiceInstanceFactory"
        serviceClass="com.tpg.javapos.jpos.services.micr.MICRService"/>
    <vendor name="HP" url="http://www.hp.com"/>
    <jpos category="MICR" version="1.8"/>
    <product description="HP MICR Service" name="HP Services for JavaPOS(TM)
        Standard" url="http://www.hp.com"/>

    <!--Other non JavaPOS required property (mostly vendor properties and bus
        specific properties i.e. RS232 )-->
    <prop name="sModelClassName" value="com.tpg.javapos.models.hydra.ptr_cd_
micr.tpg7xx.TPG7xxPtrCDMICRModelLoader"/>
    <!--prop name="removeMICRSpaces" value="true"/-->
    <prop name="sHydraProfileName" value="defaultPrinter"/>
</JposEntry>
```

4. To configure the default MSR:

   a. Obtain the keyboard JPOS drivers from HP at the following Web site:

      http://h20000.www2.hp.com/bizsupport/TechSupport/SoftwareDescription.jsp?lang=en&cc=us&prodTypeId=12454&prodSeriesId=3791663&prodNameId=3791664&swEnvOID=4047&swLang=13&mode=2&taskId=135&swItem=vc-64938-1

   b. Install the drivers.

      The installer will seem to install twice. The first install will explode the `JPOS for HP POS with MSR Keyboard.exe` into the chosen directory.

The second install will execute that file. The directory choice for the second install is not honored, so the location of the files is `C:\Program Files\HP\HookJavaPOS`.

c. Copy the `libchyjpos2.dll` file into the JRE bin directory for the client install.

d. Replace the existing entry or add the following entry to the `jpos.xml` file:

```
<JposEntry logicalName="defaultMSR">
    <creation
        factoryClass="com.cherry.jpos.CherryMSRServiceInstanceFactory"
        serviceClass="com.cherry.jpos.CherryMSRService"/>
    <vendor name="Cherry GmbH" url="http://www.cherry.de"/>
    <jpos category="MSR" version="1.10"/>
    <product description="POS MSR from HP" name="POS MSR AP series"
        url="http://www.cherry.de"/>
    <!--<prop name="LibPath" type="String"
    value="/usr/local/CherryJavaPOS-Linux.1.6.0.3/jar/libchyjpos.so"/>-->
    <prop name="LibName" type="String" value="libchyjpos2"/>
    <prop name="DeviceName" type="String" value=""/>
    <!--<prop name="DeviceName" type="String" value="ChyMSRUSB"/>-->
    <!--<prop name="DeviceName" type="String" value="MSR8000"/>-->
    <!-- The property "BuzzerGoodRead" is only valid for Cherry
        MultiBoard USB keyboard on LINUX -->
    <prop name="BuzzerGoodRead" type="String" value="100"/>
    <prop name="Debug" type="String" value="false"/>
</JposEntry>
```

5. To configure the default cash drawer, replace the existing entry or add the following entry to the `jpos.xml` file:

```
<JposEntry logicalName="defaultCashDrawer">
    <creation
        factoryClass="com.tpg.javapos.jpos.TPGJposServiceInstanceFactory"
    serviceClass="com.tpg.javapos.jpos.services.cashdrawer.CashDrawerService"/>
    <vendor name="HP" url="http://www.hp.com"/>
    <jpos category="CashDrawer" version="1.8"/>
    <product description="HP CashDrawer Service" name="HP Services for
        JavaPOS(TM) Standard" url="http://www.hp.com"/>

    <!--Other non JavaPOS required property (mostly vendor properties and bus
        specific properties i.e. RS232 )-->
    <prop name="sModelClassName" value="com.tpg.javapos.models.hydra.ptr_cd_
micr.tpg7xx.TPG7xxPtrCDMICRModelLoader"/>
    <prop name="sHydraProfileName" value="defaultPrinter"/>
</JposEntry>
```

6. To configure the default line display, replace the existing entry or add the following entry to the `jpos.xml` file:

```
<JposEntry logicalName="defaultLineDisplay">
    <creation
        factoryClass="VFD.DeviceServiceInstanceFactory"
        serviceClass="VFD.HP_POLE_DISPLAY"/>
    <vendor name="Hewlett-Packard" url="http://www.HP.com"/>
    <jpos category="LineDisplay" version="1.5"/>
    <product description="Example LineDisplay " name="LineDisplay Service for
        JavaPOS(TM) Standard" url="http://www.HP.com"/>
    <prop name="portName3" type="String" value="COM3"/>
    <prop name="baudRate" type="String" value="9600"/>
    <!--Other non JavaPOS required property (mostly vendor properties and bus
```

```
        specific properties i.e. RS232 )-->
</JposEntry>
```

Configuring a Verifone Customer Interaction Device

To prepare the device with the necessary forms and images, refer to the instructions in the following file:

<POS_install_directory>\config\device\verifone\mx860\InstallationInstructions.txt

To configure a Verifone Customer Interaction device:

1. To configure the Verifone device for signature capture, replace the existing entry or add the following entry to the `jpos.xml` file. Set the `portName` value to the appropriate COM port. In the following example, this change is shown in bold:

```
<JposEntry logicalName="cpoiSignatureCapture">
    <creation
     factoryClass="com.verifone.javapos.services.VFJposServiceInstanceFactory"
 serviceClass="com.verifone.javapos.services.mx8xx.SignatureCaptureService"/>
   <vendor name="VeriFone" url="http://www.verifone.com"/>
   <jpos category="Signature Capture" version="1.11"/>
   <product description="VeriFone mx8xx SignatureCaptureService"
      name="VeriFone Signature Capture" url="http://www.javapos.com"/>
   <!--Other non JavaPOS required property (mostly vendor properties and
      bus specific properties i.e. RS232 )-->
   <prop name="CommTimeout" type="Integer" value="2000"/>
   <prop name="portName" type="String" value="COM3"/>
   <prop name="SIGCAP_FORM" type="String" value="FA_SIGN"/>
   <prop name="PROXYIPADDRESS" type="String" value="127.0.0.1"/>
   <prop name="dataBits" type="String" value="8"/>
   <prop name="EndY" type="String" value="240"/>
   <prop name="PROTCLASSNAME" type="String"
      value="com.verifone.javapos.devices.PP201DeviceManager"/>
   <prop name="deviceName" type="String" value="mx8xx"/>
   <prop name="EndX" type="String" value="435"/>
   <prop name="PROXYSTARTUP" type="String" value="local"/>
   <prop name="TERMTYPE" type="String" value="MX8XX"/>
   <prop name="parity" type="String" value="None"/>
   <prop name="stopBits" type="String" value="1"/>
   <prop name="serviceType" type="String"
      value="SignatureCaptureService"/>
   <prop name="PASSTENABLE" type="String" value="FALSE"/>
   <prop name="PROXYPORTNUMBER" type="Integer" value="9800"/>
   <prop name="StartY" type="String" value="180"/>
   <prop name="StartX" type="String" value="60"/>
   <prop name="StartTimeOut" type="String" value="0"/>
   <prop name="configName" type="String" value="MX8XX"/>
   <prop name="baudRate" type="String" value="115200"/>
</JposEntry>
```

2. To configure the Verifone device for customer interaction device screens, replace the existing entry or add the following entry to the `jpos.xml` file. Set the `portName` value to the appropriate COM port. In the following example, this change is shown in bold:

```
<JposEntry logicalName="cpoiGUI">
    <creation
      factoryClass="com.verifone.javapos.services.VFJposServiceInstanceFactory"
      serviceClass="com.verifone.javapos.services.mx8xx.LineDisplayService"/>
    <vendor name="VeriFone" url="http://www.verifone.com"/>
```

```
    <jpos category="Line Display" version="1.11"/>
    <product description="VeriFone mx8xx LineDisplayService" name="VeriFone
        Line Display" url="http://www.javapos.com"/>
    <!--Other non JavaPOS required property (mostly vendor properties and
        bus specific properties i.e. RS232 )-->
    <prop name="CommTimeout" type="Integer" value="3000"/>
    <prop name="portName" type="String" value="COM3"/>
    <prop name="PROXYIPADDRESS" type="String" value="127.0.0.1"/>
    <prop name="dataBits" type="String" value="8"/>
    <prop name="PROTCLASSNAME" type="String"
        value="com.verifone.javapos.devices.PP201DeviceManager"/>
    <prop name="deviceName" type="String" value="mx8xx"/>
    <prop name="PROXYSTARTUP" type="String" value="local"/>
    <prop name="FontSizeList" type="String" value="10,11,12,13,14,15"/>
    <prop name="TERMTYPE" type="String" value="MX8XX"/>
    <prop name="XDTXOptions" type="String" value="49409"/>
    <prop name="DeviceWindows" type="String" value="10"/>
    <prop name="FontName" type="String"
        value="VeraMono|VeraMoBd|VeraMoIt|VeraMoBI"/>
    <prop name="parity" type="String" value="None"/>
    <prop name="stopBits" type="String" value="1"/>
    <prop name="serviceType" type="String" value="LineDisplayService"/>
    <prop name="PASSTENABLE" type="String" value="FALSE"/>
    <prop name="PROXYPORTNUMBER" type="Integer" value="9800"/>
    <prop name="ColorOptions" type="String" value="E4E1AE|000000|FF0000"/>
    <prop name="ScreenModeList" type="String"
        value="19x53,18x45,16x40,14x40,14x35,13x35"/>
    <prop name="configName" type="String" value="MX8XX"/>
    <prop name="baudRate" type="String" value="115200"/>
</JposEntry>
```

3. To configure the Verifone device for the PIN Pad device, replace the existing entry or add the following entry to the `jpos.xml` file. Set the `portName` value to the appropriate COM port. In the following example, this change is shown in bold:

```
<JposEntry logicalName="cpoiPINPad">
    <creation
      factoryClass="com.verifone.javapos.services.VFJposServiceInstanceFactory"
      serviceClass="com.verifone.javapos.services.mx8xx.VFFormService"/>
   <vendor name="VeriFone" url="http://www.verifone.com"/>
   <jpos category="Form" version="1.11"/>
   <product description="VeriFone mx8xx VFFormService" name="VeriFone
      Form" url="http://www.javapos.com"/>
   <!--Other non JavaPOS required property (mostly vendor properties and
      bus specific properties i.e. RS232 )-->
   <prop name="CommTimeout" type="Integer" value="2000"/>
   <prop name="portName" type="String" value="COM3"/>
   <prop name="PROXYIPADDRESS" type="String" value="127.0.0.1"/>
   <prop name="dataBits" type="String" value="8"/>
   <prop name="PROTCLASSNAME" type="String"
      value="com.verifone.javapos.devices.PP201DeviceManager"/>
   <prop name="deviceName" type="String" value="mx8xx"/>
   <prop name="PROXYSTARTUP" type="String" value="local"/>
   <prop name="PINPAD_FORM" type="String" value="860_FA_PINE"/>
   <prop name="TERMTYPE" type="String" value="MX8XX"/>
   <prop name="parity" type="String" value="None"/>
   <prop name="stopBits" type="String" value="1"/>
   <prop name="serviceType" type="String" value="VFFormService"/>
   <prop name="PASSTENABLE" type="String" value="FALSE"/>
   <prop name="PROXYPORTNUMBER" type="Integer" value="9800"/>
```

```
   <prop name="configName" type="String" value="MX8XX"/>
   <prop name="baudRate" type="String" value="115200"/>
</JposEntry>
```

4. To configure the Verifone device for the MSR device, replace the existing entry or add the following entry to the `jpos.xml` file. Set the `portName` value to the appropriate COM port. In the following example, this change is shown in bold:

```
<JposEntry logicalName="cpoiMSR">
    <creation
      factoryClass="com.verifone.javapos.services.VFJposServiceInstanceFactory"
      serviceClass="com.verifone.javapos.services.mx8xx.MSRService"/>
    <vendor name="VeriFone" url="http://www.verifone.com"/>
    <jpos category="Magnetic Stripe Reader" version="1.11"/>
    <product description="VeriFone mx8xx MSRService" name="VeriFone
        Magnetic Stripe Reader" url="http://www.javapos.com"/>
    <!--Other non JavaPOS required property (mostly vendor properties and
        bus specific properties i.e. RS232 )-->
    <prop name="CommTimeout" type="Integer" value="2000"/>
    <prop name="portName" type="String" value="COM3"/>
    <prop name="PROXYIPADDRESS" type="String" value="127.0.0.1"/>
    <prop name="dataBits" type="String" value="8"/>
    <prop name="PROTCLASSNAME" type="String"
        value="com.verifone.javapos.devices.PP201DeviceManager"/>
    <prop name="deviceName" type="String" value="mx8xx"/>
    <prop name="PROXYSTARTUP" type="String" value="local"/>
    <prop name="TERMTYPE" type="String" value="MX8XX"/>
    <prop name="parity" type="String" value="None"/>
    <prop name="stopBits" type="String" value="1"/>
    <prop name="serviceType" type="String" value="MSRService"/>
    <prop name="PASSTENABLE" type="String" value="FALSE"/>
    <prop name="PROXYPORTNUMBER" type="Integer" value="9800"/>
    <prop name="configName" type="String" value="MX8XX"/>
    <prop name="baudRate" type="String" value="115200"/>
</JposEntry>
```

L

Appendix: Installation Order

This section provides a guideline for the order in which the Oracle Retail applications should be installed. If a retailer has chosen to use only some of the applications, the order is still valid, less the applications not being installed.

> **Note:** The installation order is not meant to imply integration between products.

Enterprise Installation Order

1. Oracle Retail Merchandising System (RMS), Oracle Retail Trade Management (RTM), Oracle Retail Sales Audit (ReSA), Optional: Oracle Retail Fiscal Management (ORFM)

   > **Note:** ORFM is an optional application for RMS if you are implementing Brazil localization.

2. Oracle Retail Service Layer (RSL)
3. Oracle Retail Extract, Transform, Load (RETL)
4. Oracle Retail Active Retail Intelligence (ARI)
5. Oracle Retail Warehouse Management System (RWMS)
6. Oracle Retail Allocation
7. Oracle Retail Invoice Matching (ReIM)
8. Oracle Retail Price Management (RPM)

   > **Note:** During installation of RPM, you are asked for the RIBforRPM provider URL. Since RIB is installed after RPM, make a note of the URL you enter. If you need to change the RIBforRPM provider URL after you install RIB, you can do so by editing the remote_service_locator_info_ribserver.xml file.

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. Since RIB is installed after SIM, make a note of the URL you enter. If you need to change the RIB provider URL after you install RIB, you can do so by editing 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 Optimzation (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 Workspace (ORW)