Oracle® Retail Point-of-Service

Installation Guide, Volume 2 - IBM Stack

Release 13.4.9

E71411-01

March 2016

ORACLE®

Oracle Retail Point-of-Service Installation Guide, Volume 2 - IBM Stack, Release 13.4.9

E71411-01

Copyright © 2016, 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 is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

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

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

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

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

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

Value-Added Reseller (VAR) Language

Oracle Retail VAR Applications

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

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

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

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

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

You acknowledge and confirm that Oracle grants you use of only the object code of the VAR Applications. Oracle will not deliver source code to the VAR Applications to you. Notwithstanding any other term or condition of the agreement and this ordering document, you shall not cause or permit alteration of any VAR Applications. For purposes of this section, "alteration" refers to all alterations, translations, upgrades, enhancements, customizations or modifications of all or any portion of the VAR Applications including all

reconfigurations, reassembly or reverse assembly, re-engineering or reverse engineering and recompilations or reverse compilations of the VAR Applications or any derivatives of the VAR Applications. You acknowledge that it shall be a breach of the agreement to utilize the relationship, and/or confidential information of the VAR Applications for purposes of competitive discovery.

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

Contents

Send Us Your Comments xi

Preface xiii

Audience xiii
Documentation Accessibility xiii
Related Documents xiii
Customer Support xiii
Review Patch Documentation xiv
Improved Process for Oracle Retail Documentation Corrections xiv
Oracle Retail Documentation on the Oracle Technology Network xiv
Conventions xv

1 Preinstallation Tasks

Requesting Infrastructure Software 1-1
Check Supported Store Server Software Requirements 1-1
Check Supported Client Hardware and Software Requirements 1-1
Check Oracle Retail Software Dependencies 1-2
Check Third-Party Software Dependencies 1-2
Check Additional Oracle Technologies 1-3
Integration with Other Applications 1-3
Oracle Retail Central Office and Back Office 1-3
Oracle Retail Store Inventory Management 1-3
Siebel CMU Management 1-4
Oracle Retail Returns Management 1-4
Bill Payment 1-4
Tender Authorization 1-4
Hardware Requirements 1-5
Store Server 1-5
Client 1-5
Peripheral Devices for Clients 1-6
Check Java Key Manager Requirement 1-6
Check Secure JDBC and Secure RMI 1-6
Tender Authorization Testing 1-6
ACI PIN Comm 1-7

PXP Solutions ANYpay POS 1-8
Implementation Guidelines for Security 1-10

2 Secure Configuration

Operating System 2-1
Additional Resource 2-2
Infrastructure/Middleware 2-2
Database 2-2
Messaging 2-2
RSA Key Manager 2-2
Java Cryptography Extension (JCE) 2-3
Network Considerations 2-3
Oracle Retail POS Suite Application Configuration 2-3
Technology Considerations 2-3
Credential Store Framework 2-3
Wireless Technology 2-4
Application Specific Settings 2-4
Application Runtime Settings 2-5
Application Parameters 2-5
Temporary Password Length 2-5
Database Configuration 2-5
Integration with Other Applications 2-5
Scripts and Command Line Utilities 2-5
Wallet Management Tool 2-5
Purge Scripts 2-6

3 Installation on the IBM Stack

Create the Database Schema Owner and Data Source Users 3-1
Installing Point-of-Service 3-2
Determining Tier Type 3-2
Installing the Database 3-3
Required Settings for the Database 3-3
Installing Point-of-Service on Machines 3-3
Updating Device Configuration 3-3
Expand the Point-of-Service Distribution 3-3
Obtain the Third-Party Library Files Required by Point-of-Service 3-4
Obtain the DB2 Files 3-4
Obtain the WebSphere Files 3-5
Obtain the WebSphere MQ Files 3-5
Obtain the JRE Required for Client Install 3-5
Obtain the IBM JRE Required for Client Install 3-5
Secure Communication 3-6
Database Install Options 3-6
Create the Database Schema with Oracle Retail Back Office 3-7
Obtain the Files Needed for RSA Data Protection Manager 3-7
Obtain the RSA Data Protection Manager Version 3.1 Jar Files 3-7
Install the Java Cryptography Extension (JCE) 3-7

Run the Point-of-Service Application Installer ... 3-8
Resolve Errors Encountered During Application Installation ... 3-8
Create the Database Schema ... 3-9
Create without Oracle Retail Back Office ... 3-9
Resolve Issues with Misprinted Characters in eReceipts and Network Printed Reports and Receipts ... 3-10
Resolve Misprinted Character Problems in eReceipts ... 3-10
Resolve Misprinted Character Problems in Network Printed Receipts and Reports ... 3-11
Set up the Store Server for Tender Authorization ... 3-12
Results of a Point-of-Service Installation ... 3-12
Running Point-of-Service ... 3-13
Creating a Custom Installation ... 3-13

A Appendix: Installer Screens Server Installation on SLEPOS

B Appendix: Installer Screens for Client Installation on SLEPOS

C Appendix: Installer Silent Mode

D Appendix: URL Reference

JDBC URL for an IBM DB2 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 IBM Stack

jndi.properties File Name ... F-1
Performing a Manual Integration ... F-1
Client Configuration ... F-1
Store Server Configuration ... F-2
Secure RMI and Secure JDBC ... F-5

G Appendix: Device Configuration

Configuring Devices for an IBM SurePOS Register ... G-1
Configuring a Device for ACI PIN Comm ... G-5

H Appendix: Installation Order

Enterprise Installation Order ... H-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 Application Owner ... A-6
A–8 Installation Location ... A-7
A–9 JRE Location ... A-8
A–10 JRE Vendor ... 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 Websphere Application Server: Third Party Jars ... A-15
A–17 Database Type ... A-16
A–18 Database Owner ... A-17
A–19 Database Source User ... A-18
A–20 Install Database Option ... A-20
A–21 Sample Dataset ... A-21
A–22 Secure Options ... A-22
A–23 Data Source SSL Configuration ... A-23
A–24 Transaction Retrieval Location ... A-24
A–25 Scratchpad Database Information ... A-25
A–26 Scratchpad Database Install Options ... A-27
A–27 POS Administrator User ... A-28
A–28 Enable Transaction and Customer Retrieval Web Services ... A-29
A–29 POS-CO WebService Details ... A-30
A–30 Server Journal Configuration ... A-31
A–31 Select JMS SSL Level ... A-32
A–32 Enter ORSIM Webservice URL ... A-33
A–33 ORSIM Integration Properties ... A-34
A–34 ORSIM Integration ... A-35
A–35 Enable POS-Siebel Webservice Access Over SSL ... A-36
A–36 POS-Siebel Webservice Authentication Type ... A-37
A–37 POS-Siebel Configuration ... A-38
A–38 Oracle Returns Management JMS Configuration ... A-39
A–39 RM-POS WebService Details ... A-41
A–40 Enable Value-Added Tax (VAT) ... A-42
A–41 Enable RTLog Export ... A-43
A–42 Security Setup: Key Manager Settings ... A-44
A–43 RSA Data Protection Manager Requirements ... A-45
A–44 Security Setup: Key Store RSA JAR Files ... A-46
A–45 RSA Client Configuration ... A-47
A–46 Key Store Pass Phrase for Simulator Key Manager ... A-48
A–47 Logging Detail Options ... A-49
A–48 Logging Export Options ... A-50
A–49 Data Replication Options ... A-51
A–50 E-mail Notification for Communication Failures ... A-52
A–51 Data Replication Transport JMS Options ... A-53
A–52 Central Office Server Information ... A-54
A–53 Back Office Server Information ... A-55
A–54 Tender Authorization ... A-56

A–55 Tender Authorization: ISD PIN Comm A-57
A–56 SSL Key Store Details A-59
A–57 SSL Trust Store Details A-60
A–58 Installation Progress A-61
A–59 Install Complete A-62
B–1 Introduction B-1
B–2 Previous POS Install B-2
B–3 License Agreement B-2
B–4 Supported Languages B-3
B–5 Enter Default Locale B-4
B–6 Tier Type B-5
B–7 Application Owner B-6
B–8 Installation Location B-7
B–9 JRE Location B-8
B–10 JRE Vendor B-9
B–11 Store Server Details B-10
B–12 Store ID B-11
B–13 Register Number B-12
B–14 Integrate Applications B-13
B–15 Application Server Type B-14
B–16 Websphere Application Server: Third Party Jars B-15
B–17 Transaction Retrieval Location B-16
B–18 Enable Client Secure RMI B-17
B–19 Select JMS SSL Level B-18
B–20 ORSIM Integration B-19
B–21 Enable eReceipt B-20
B–22 eReceipt Properties B-21
B–23 Enable Value-Added Tax (VAT) B-22
B–24 Security Setup: Key Manager Settings B-23
B–25 RSA Data Protection Manager Requirements B-24
B–26 Security Setup: Key Store RSA JAR Files B-25
B–27 RSA Client Configuration B-26
B–28 Key Store Pass Phrase for Simulator Key Manager B-27
B–29 Logging Detail Options B-28
B–30 POS Platform Components B-29
B–31 JPOS Device Setup: Library Files B-30
B–32 POS Devices B-31
B–33 IBM Environment Libraries B-32
B–34 JPOS Device Setup: jpos.xml directory B-35
B–35 POS Printer Support B-36
B–36 Network Printer Support Configuration B-37
B–37 EJournal Options B-38
B–38 JMS/Webservice Queue Journal Support B-39
B–39 Parameter Distribution Information B-40
B–40 Back Office Server Information B-41
B–41 Tender Authorization B-42
B–42 Tender Authorization: ISD PIN Comm B-43
B–43 Tender Authorization: Servebase PC-EFT B-44
B–44 SSL Key Store Details B-45
B–45 SSL Trust Store Details B-46
B–46 User Interface Type B-47
B–47 Installation Progress B-48
B–48 Install Complete B-48

List of Tables

1–1 Store Server Requirements 1-1
1–2 Client Requirements 1-2
1–3 Supported Oracle Retail Products 1-2
1–4 Additional Oracle Technologies 1-3
1–5 ACI PIN Comm Authorization Transaction Set Tested 1-7
1–6 PXP Solutions ANYpay POS Authorization Transaction Set Tested 1-8
3–1 Server Tier Logical Components 3-2
3–2 <POS_install_directory> Subdirectories 3-12
3–3 <POS_install_directory>/pos Subdirectories 3-12

Send Us Your Comments

Oracle Retail Point-of-Service Installation Guide, Volume 2 - IBM Stack, Release 13.4.9

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

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

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

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

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

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

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

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

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

- System administrators and operations personnel
- Database administrators
- System analysts and programmers
- Integrators and implementation staff personnel

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Retail Point-of-Service Release 13.4.9 documentation set:

- *Oracle Retail Point-of-Service Installation Guide, Volume 1 - Oracle Stack*
- *Oracle Retail Point-of-Service Release Notes*
- *Oracle Retail POS Suite Data Model Data Dictionary*

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, 13.4) or a later patch release (for example, 13.4.9). If you are installing the base release or additional patch releases, read the documentation for all releases that have occurred since the base release before you begin installation. Documentation for patch releases can contain critical information related to the base release, as well as information about code changes since the base release.

Improved Process for Oracle Retail Documentation Corrections

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

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

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

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

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

Oracle Retail Documentation on the Oracle Technology Network

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

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

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

Conventions

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 IBM stack that must be met before Oracle Retail Point-of-Service can be installed.

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

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

Requesting Infrastructure Software

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

Check Supported 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	SLEPOS 11 SP2
Database	IBM DB2 9.7 (64-bit)
JDK/JRE	IBM JRE 1.6 or later within the Jave 1.6 code line

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. A computer mouse is 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	Versions Supported
Register	IBM SurePOS 700 (742/743)
Operating System	SLEPOS 11 SP2
JVM	IBM JRE 1.6 (JPOS 1.13) or later within the Java 1.6 code line
Persistent Storage	Apache Derby 10.5.3
Cash drawer	IBM cash drawer
Pole Display	IBM pole display
Keyboard	IBM keyboard
Scanner	Symbol Scanner LS2208 and LS4208
PIN Pad	▪ Verifone MX860 ▪ Verifone VX810 (EMV)
Receipt Printer	IBM printer
Biometric Device	Not supported

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	13.4.9
Oracle Retail Central Office	13.4.9
Oracle Retail Merchandising System	13.2.9
Oracle Retail Price Management	13.2.9
Oracle Retail Returns Management	2.4.9
Oracle Retail Sales Audit	13.2.9
Oracle Retail Store Inventory Management	13.2.9 (on Oracle WebLogic)

Check Third-Party Software Dependencies

The following third-party software must be obtained:

- The `db2jcc.jar` file must be obtained from your IBM DB2 database server installation. For more information, see "Obtain the Third-Party Library Files Required by Point-of-Service" in Chapter 3.
- WebSphere jar files must be obtained from your WebSphere server installation. For more information, see "Obtain the Third-Party Library Files Required by Point-of-Service" in Chapter 3.

- If you are using the RSA Data Protection Manager, you must download specific jar files. For more information, see "Check Java Key Manager Requirement".

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 CMU	8.1.1.3

Integration with Other Applications

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 a payment application for tender authorization. See Figure A–54.

See the following sections for more information.

- "Oracle Retail Central Office and Back Office"
- "Oracle Retail Store Inventory Management"
- "Siebel CMU Management"
- "Oracle Retail Returns Management"
- "Bill Payment"
- "Tender Authorization"

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 Management features to be integrated

Siebel CMU Management

Siebel Communications, Media, and Utilities (CMU) 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 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*.

Tender Authorization

If Oracle Retail Point-of-Service is integrated with a payment application for tender authorization, you provide the details required for the payment application selected.

If the payment application selected is ACI PIN Comm, the following details are required:

- Location of the ISD ToolKit JAR file
- Name of the IMSRTRIBSpecSDK JAR file
- Name of the isdcrypt JAR file
- Name of the MSPCommAPI JAR file
- Four digit numeric value for the location
- Primary IP address and port number used for the communication between the store server and the tender authorizer

- Secondary IP address and port number used for the communication between the store server and the tender authorizer
- Tertiary IP address and port number used for the communication between the store server and the tender authorizer
- Address of the Image Capture Web service

If the payment application selected is PXP Solutions ANYpay POS (selected as Servebase PC-EFT POS on the installer screen), the following details are required:

- Host name of the machine running ANYpay POS
- Port number at which ANYpay POS is listening
- Merchant ID provided by the bank
- Customer Code provided by the bank
- Store's site identification
- ANYpay POS user name and password

For additional information:

- For the steps performed after the server installation, see "Set up the Store Server for Tender Authorization" in Chapter 3.
- For the list of transactions tested for this release, see "Tender Authorization 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.

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 Java Key Manager Requirement

Oracle Retail Point-of-Service requires that a Java Key Manager system is available 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 Data Proctection Manager, you must use version 3.1. You must obtain specific jar files for version 3.1 and install the Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files 6.0. See "Obtain the Files Needed for RSA Data Protection Manager" in Chapter 3.

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 "Secure Communication" in Chapter 3.

Tender Authorization Testing

Tender authorization testing was done with ACI PIN Comm and PXP Solutions ANYpay POS. For each payment application, the version used for the testing and the transaction types and messages that were tested are listed.

ACI PIN Comm

The following ACI versions were used for testing:

- PIN Comm 6.4.4.008 and toolkit (ITK) version 335b
- SAF/TOR 6.4.2.005 and toolkit (ITK) version 335b

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

Table 1–5 ACI PIN Comm Authorization Transaction Set Tested

Transaction Type	Transaction Type Message Sent from ACI PIN Comm to Point-of-Service
Check Tender	■ Check Sale Approval ■ Check Sale Authorization Offline ■ Check Sale Authorization Timeout ■ Check Sale Decline ■ Check Sale Post Void ■ Check Sale Referral
Credit Card Tender	■ Credit Card Return Approval ■ Credit Card Return Authorization Offline ■ Credit Card Return Authorization Timeout ■ Credit Card Return Decline ■ Credit Card Return Post Void ■ Credit Card Return Referral ■ Credit Card Sale Approval ■ Credit Card Sale Authorization Offline ■ Credit Card Sale Authorization Timeout ■ Credit Card Sale Decline ■ Credit Card Sale Partial Approval ■ Credit Card Sale Post Void ■ Credit Card Sale Referral
Debit Card Tender	■ Debit Card Sale Approval ■ Debit Card Sale Authorization Offline ■ Debit Card Sale Authorization Timeout ■ Debit Card Sale Decline ■ Debit Card Sale Partial Approval ■ Debit Card Post Void
Gift Card Issue	■ Gift Card Issue Approval ■ Gift Card Issue Authorization Offline ■ Gift Card Issue Authorization Timeout ■ Gift Card Issue Decline
Gift Card Redeem	■ Gift Card Redeem Approval ■ Gift Card Redeem Authorization Offline ■ Gift Card Redeem Authorization Timeout

Table 1–5 (Cont.) ACI PIN Comm Authorization Transaction Set Tested

Transaction Type	Transaction Type Message Sent from ACI PIN Comm to Point-of-Service
Gift Card Refund Issue new gift card or reload to existing gift card	■ Gift Card Issue Approval ■ Gift Card Issue Authorization Offline ■ Gift Card Issue Authorization Timeout ■ Gift Card Issue Decline ■ Gift Card Reload Approval ■ Gift Card Reload Authorization Offline ■ Gift Card Reload Authorization Timeout ■ Gift Card Reload Decline
Gift Card Reload	■ Gift Card Reload Approval ■ Gift Card Reload Authorization Offline ■ Gift Card Reload Authorization Timeout ■ Gift Card Reload Decline
Gift Card Tender	■ Gift Card Sale Approval ■ Gift Card Sale Authorization Offline ■ Gift Card Sale Authorization Timeout ■ Gift Card Sale Decline ■ Gift Card Post Void ■ Gift Card Sale Referral
House Account Tender	■ House Account Return Approval ■ House Account Return Authorization Offline ■ House Account Return Authorization Timeout ■ House Account Return Decline ■ House Account Sale Approval ■ House Account Sale Authorization Offline ■ House Account Sale Authorization Timeout ■ House Account Sale Decline ■ House Account Sale Post Void ■ House Account Sale Referral

PXP Solutions ANYpay POS

The version used for testing was 2.0.0.52.

Table 1–6 shows the transaction types and messages that were tested.

Table 1–6 PXP Solutions ANYpay POS Authorization Transaction Set Tested

Transaction Type	Transaction Type Message Sent from PXP Solutions ANYpay POS to Point-of-Service
Check Tender	■ Check Sale Decline **Note:** Tendering with a check is declined when PXP Solutions is the payment application.

Table 1–6 (Cont.) PXP Solutions ANYpay POS Authorization Transaction Set Tested

Transaction Type	Transaction Type Message Sent from PXP Solutions ANYpay POS to Point-of-Service
Chip and Pin Credit Card and Debit Card Tender	■ Chip and Pin Card Return Approval ■ Chip and Pin Card Return Authorization Offline ■ Chip and Pin Card Return Authorization Timeout ■ Chip and Pin Card Return Post Void ■ Chip and Pin Card Return Referral ■ Chip and Pin Card Sale Approval ■ Chip and Pin Card Sale Authorization Offline ■ Chip and Pin Card Sale Authorization Timeout ■ Chip and Pin Card Sale Decline ■ Chip and Pin Card Sale Post Void ■ Chip and Pin Card Sale Referral
Credit Card Tender	■ Credit Card Return Approval ■ Credit Card Return Authorization Offline ■ Credit Card Return Authorization Timeout ■ Credit Card Return Post Void ■ Credit Card Return Referral ■ Credit Card Sale Approval ■ Credit Card Sale Authorization Offline ■ Credit Card Sale Authorization Timeout ■ Credit Card Sale Decline ■ Credit Card Sale Post Void ■ Credit Card Sale Referral
Debit Card Tender	■ Debit Card Return Approval ■ Debit Card Return Authorization Offline ■ Debit Card Return Authorization Timeout ■ Debit Card Return Post Void ■ Debit Card Return Referral ■ Debit Card Sale Approval ■ Debit Card Sale Authorization Offline ■ Debit Card Sale Authorization Timeout ■ Debit Card Sale Decline ■ Debit Card Sale Post Void ■ Debit Card Sale Referral
Gift Card Tender	■ Gift Card Sale Decline **Note:** Tendering with a gift card is declined when PXP Solutions is the payment application.
House Account Tender	■ House Account Sale Decline **Note:** Tendering with a house account is declined when PXP Solutions is the payment application.
Check Tender	■ Check Sale Decline **Note:** Tendering with a check is declined when PXP Solutions is the payment application.

Table 1–6 (Cont.) PXP Solutions ANYpay POS Authorization Transaction Set Tested

Transaction Type	Transaction Type Message Sent from PXP Solutions ANYpay POS to Point-of-Service
Chip and Pin Credit Card and Debit Card Tender	■ Chip and Pin Card Return Approval ■ Chip and Pin Card Return Authorization Offline ■ Chip and Pin Card Return Authorization Timeout ■ Chip and Pin Card Return Post Void ■ Chip and Pin Card Return Referral ■ Chip and Pin Card Sale Approval ■ Chip and Pin Card Sale Authorization Offline ■ Chip and Pin Card Sale Authorization Timeout ■ Chip and Pin Card Sale Decline ■ Chip and Pin Card Sale Post Void ■ Chip and Pin Card Sale Referral
Credit Card Tender	■ Credit Card Return Approval ■ Credit Card Return Authorization Offline ■ Credit Card Return Authorization Timeout ■ Credit Card Return Post Void ■ Credit Card Return Referral ■ Credit Card Sale Approval ■ Credit Card Sale Authorization Offline ■ Credit Card Sale Authorization Timeout ■ Credit Card Sale Decline ■ Credit Card Sale Post Void ■ Credit Card Sale Referral

Implementation Guidelines for Security

Note: It is recommended that the passwords for key stores and trust stores are changed from the values set by default. If this is not done, the system could be vulnerable to access by any unauthorized user with knowledge of the default passwords.

For information on implementing security, see the *Oracle Retail POS Suite Security Guide*. This guide describes specific security features and implementation guidelines for the POS Suite products.

2

Secure Configuration

This chapter serves as a guide for administrators and people installing the product to securely configure Oracle Retail Point-of-Service. To see a broader spectrum of suggested security-related practices for this application, see the *Oracle Retail POS Suite Security Guide*.

> **Note:** All the Oracle Retail POS Suite applications should follow the same practices for configuring a secure environment.

This chapter is intended for security administrators and people installing the products who will deploy and configure the Oracle Retail POS Suite applications. These users perform the following tasks:

- Install and deploy the applications
- Configure the applications
- Apply patches to the applications

It is assumed that the readers of this chapter have a general knowledge of administering the underlying technologies and the application.

This chapter begins with the operating system and moves through the supporting middleware to the application, and its connections with other resources.

> **Note:** The options set by default for the installer are the most secure selection. If you choose to not use any of the default selections, you need to consider the implications of that change on the security of your installed product.

Any references to Payment Card Industry Data Security Standard (PCI-DSS) requirements are from PCI-DSS version 2.0.

Operating System

To see the operating systems and browsers supported for this release of Point-of-Service, see Chapter 1.

The Oracle Retail POS Suite applications do not rely on insecure services or protocols. If the retailer or systems integrator customizes or extends the applications, these extensions must not rely on insecure services or protocols.

For more information about securing services and protocols, see the *Oracle Retail POS Suite Security Guide*.

Additional Resource

The Center for Internet Security has published benchmarks for securing your systems at the operating system level. You can find the benchmark for SUSE Linux (SLEPOS) at the following link:

http://benchmarks.cisecurity.org/en-us/?route=downloads.browse.category.benchmarks.os.linux.suse

Infrastructure/Middleware

To see the database and application server supported for this release of Point-of-Service, see Chapter 1.

Database

For recommendations on securing the database as well as JDBC communications between the POS Suite applications and the database, see the *Oracle Retail POS Suite Security Guide*.

Do not store sensitive data on Internet-accessible systems. For example, your Web server and database server must not be on the same physical server. Oracle Retail POS Suite applications do not require the database server and Web server to be hosted on the same physical server machine.

For information about secure configuration of IBM DB2, see the *IBM DB2 9.7 Database Security Guide* at the following Web site:

ftp://public.dhe.ibm.com/ps/products/db2/info/vr97/pdf/en_US/DB2Security-db2sece971.pdf

Messaging

Secure JMS messaging configuration is specific to the application server. For information about securing the JMS messaging, see the *Oracle Retail POS Suite Security Guide*.

The Oracle Retail POS Suite applications do not permit a user to send unencrypted sensitive data by end-user messaging technologies, such as e-mail. If you customize an application to permit sending sensitive data, by end-user messaging technologies, you must use a solution that renders the sensitive data unreadable or implements strong cryptography.

The embedded Browser feature in Point-of-Service provides the facility to access a Web URL within the application. Care must be taken that the URL set in the Point-of-Service Browser URL parameter is not a public e-mail Web site.

RSA Key Manager

The Oracle Retail POS Suite applications are designed to be easily integrated with an external key management service selected by the retailer. The applications perform no encryption, decryption, or key management. Many enterprise applications are available to perform those functions. Because of this, the applications require integration with a key management service in order to start properly.

The applications are designed to plug into a key management service with the addition of a thin layer that wraps the interface to a key manager of your choice, such as RSA and so on. The adaptor can be instantiated by an application framework such as Spring, so that it is easy to write and deploy an adaptor for a different key manager without modifying application code. Point-of-Service provides an adapter for RSA Key Manager Java Client, version 3.1. See the following file:

```
oracle.retail.stores.rsakeystore.rsainterface.RSAKeyStoreEncryptionService.java
```

This does not create a dependency on the RSA product, as a similar adapter could be developed for a different key management product. However, Point-of-Service is a *Secured by RSA Certified Partner Solution*, certified with RSA Key Manager, as documented at the following Web site:

```
https://gallery.emc.com/community/marketplace/rsa?view=overview
```

For information on installing Point-of-Service with the RSA Key Manager, see "Check Java Key Manager Requirement" in Chapter 1.

Java Cryptography Extension (JCE)

For information on JCE, see "Install the Java Cryptography Extension (JCE)" in Chapter 3.

Network Considerations

For recommendations on securing the network and other enterprise security considerations, see the *Oracle Retail POS Suite Security Guide*.

Oracle Retail POS Suite Application Configuration

This section covers secure configuration that is recommended for all Oracle Retail POS Suite applications.

Technology Considerations

These technologies should be considered.

Credential Store Framework

A credential store is used for the secure storage of application-to-application credentials. It is not used for storing user credentials. The credential store framework (CSF) API is used to access and perform operations on the credential store. CSF provides the following capabilities:

- Enables the secure management of credentials.
- Provides an API for the storage, retrieval, and maintenance of credentials.
- Supports file-based, such as Oracle wallet, and LDAP-based credential management.

For information about the design of the credential store framework, see the *Oracle Retail POS Suite Security Guide*.

Wireless Technology

Oracle Retail POS Suite applications are not designed as wireless applications. If wireless technology is used, you must adhere to PCI-DSS compliant wireless settings, per PCI-DSS Requirements 1.2.3, 2.1.1, and 4.1.1.

Application Specific Settings

The Release 13.4.9 Oracle Retail POS Suite applications enable out-of-the-box audit logging by default. These logs should not be disabled.

Application log files are configurable. If you modify the settings, you must ensure they are compliant with PCI-DSS requirements 10.2 and 10.3.

The POS Suite applications implement automated audit trails for all system components to reconstruct the following events:

- All actions taken by any individual with administrative privileges as assigned in the application
- Access to application audit trails managed by or within the application
- Invalid logical access attempts
- Use of application's identification and authentication mechanisms
- Initialization of the application audit logs
- Creation and deletion of system-level objects within or by the application

The Release 13.4.9 Oracle Retail POS Suite applications implement an automated audit trail logging of various events happening on the system. The audit trail logging is configured in the log4j configuration file maintained for each application. The various events that need to be logged and the file where the audit logging information will be captured are configured in the log4j configuration file.

Caution: Do not comment out any of the entries or prevent the logging from occurring.

For each event, the Oracle Retail Audit log service logs the point of Origination of the event. In addition, the audit log framework logs the Initialization of the Audit log itself.

The log files are created with the following names and in following locations:

File Name: audit.log

Location (in each register):

<POS_install_directory>/*<client>*/pos/logs

The following events should be captured at the system level:

- Login or logoff
- Start or stop a process
- Use of user rights
- Account administration
- Change the security policy
- Restart and shut down the system

- USB events and Mount andUnmount events
- Access a file or directory (create a file, remove a file, read a file, or change file descriptors)

Various tools are available to collect audit trail information. Audit trails should be maintained for the applications and for external system events.

Application Runtime Settings

After installation, these settings should be used.

Application Parameters

Set these application parameters before running Point-of-Service.

Temporary Password Length The Temporary Password Length parameter is used to determine the length of system generated temporary passwords. This parameter resides in the application XML parameter file.

> **Caution:** This parameter can be set to generate passwords to have a length between 7 and 12 characters. In order to comply with PCI-DSS section 8.5.10, the Oracle Retail POS Suite applications must not be modified to allow fewer than 7 characters.

Database Configuration Password policy settings are configured through the database. By default, the password policy is compliant with PCI-DSS section 8.5.

> **Caution:** If you change the password policy, ensure the modified settings comply with the PCI-DSS.

Integration with Other Applications

The Oracle Retail POS Suite applications integrate through the use of Web services and Java RMI. For information about securing these interface protocols, see the *Oracle Retail POS Suite Security Guide*.

Scripts and Command Line Utilities

This section covers scripts and utilities used after installation.

Wallet Management Tool

When installing an Oracle Retail POS Suite application, the installer creates the cwallet.sso file and stores application-to-application credentials that were entered on the installer screens in the file. If the credentials change once the application is installed, the cwallet.sso file must be updated with the new passwords.

The Wallet Management Tool is provided to update an existing credential and add a new credential in the wallet file. It prompts for the required information.

For information on using the Wallet Management Tool, see the *Oracle Retail POS Suite Security Guide*.

Purge Scripts

The Oracle Retail POS Suite applications come with stored procedures and scripts that permit a DBA to purge the databases of data that the retailer determines are no longer necessary to store. Access to these scripts should be restricted. For more information about the purge scripts, see the *Oracle Retail POS Suite Security Guide*.

3

Installation on the IBM Stack

This chapter provides information about the installation procedures for Oracle Retail Point-of-Service on the IBM Stack. For a list of tested components and supported versions for the IBM 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".

> **Note:** Do not include spaces in directory names. The installer or Point-of-Service application may be unable to locate a directory that has spaces in its name.

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 is 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 the *Oracle Retail POS Suite Security Guide*.

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 the schema owner user.

```
CREATE SCHEMA <schema_name> AUTHORIZATION <schema_username>
```

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

```
GRANT CREATETAB, BINDADD, CONNECT, IMPLICIT_SCHEMA ON DATABASE TO USER
<schema_username>
```

4. Grant the following object level privileges to the schema owner user.

```
GRANT CREATEIN, DROPIN, ALTERIN ON SCHEMA <schema_name> TO USER
<schema_username> WITH GRANT OPTION
```

To create the data source user:

1. If not already logged in, log in using the database administrator user ID.
2. Create the data source user.

```
CREATE SCHEMA <data_source_schema_name> AUTHORIZATION <data_source_username>
```

3. Grant the privileges, shown in the following example, to the data source user.

```
GRANT CONNECT, IMPLICIT_SCHEMA ON DATABASE TO USER <data_source_username>
```

4. Grant the following object level privileges to the data source user.

```
GRANT CREATEIN ON SCHEMA <data_source_schema_name> TO USER <data_source_
username> WITH GRANT OPTION
```

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

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 3–1:

Table 3–1 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 POS Suite Operations Guide*.

Required Settings for the Database

During database creation, the database must be set to UTF8.

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 `/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 G:

- "Configuring Devices for an IBM SurePOS Register"
- "Configuring a Device for ACI PIN Comm"

Expand the Point-of-Service Distribution

To extract the Point-of-Service files:

1. Extract the Point-of-Service 13.4.9 distribution zip file.
2. Create a new staging directory for the Point-of-Service application distribution `ORPOS-13.4.9.zip` file, for example, `/tmp/orpos/orpos-staging`.

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

3. Copy or upload `ORPOS-13.4.9.zip` to *<staging_directory>* and extract its contents. The following files and directories should be created under *<staging_directory>*`/ORPOS-13.4.9`:

```
ant/
ant-ext/
antinstall/
installer-resources/
installer-templates/
product/
antinstall-config.xml
build.xml
build-antinstall.xml
build-common.xml
build-common-esapi.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-13.4.9` is referred to as *<INSTALL_DIR>*.

Obtain the Third-Party Library Files Required by Point-of-Service

The Point-of-Service application uses specific files for the DB2 drivers from IBM, IBM WebSphere jar files, and IBM WebSphere MQ jar files. Before running the Point-of-Service application installer, you must obtain the DB2 file from your database server, obtain the WebSphere jar files from your WebSphere installation, and obtain the WebSphere MQ jar files from your WebSphere MQ installation. Copy these jar files to folders accessible by the operating system user running the installer. The installer prompts for the location of the jar files on the WebSphere Application Server: Third Party Jars screen. See Figure A–16 and Figure B–16.

Obtain the DB2 Files

To obtain the DB2 files:

1. Obtain the `db2jcc.jar` and `db2jcc_license_cu.jar` files from your database server at <*IBM_DB2_INSTALL_DIR*>.
2. Copy the jar files to `/opt/IBM/SQLLIB/java/`.

Obtain the WebSphere Files

To obtain the WebSphere jar files:

1. Copy the required jar files from the following locations:
   - *<WAS_INSTALL_DIR>*/WebSphere/AppServer/deploytool/itp/plugins/com.ibm.websphere.v7_7.0.1.v20100710_0411/wasJars/runtime.jar
   - *<WAS_INSTALL_DIR>*/WebSphere/AppServer/runtimes/com.ibm.ws.admin.client_7.0.0.jar
   - *<WAS_INSTALL_DIR>*/WebSphere/AppServer/runtimes/com.ibm.ws.ejb.thinclient_7.0.0.jar
   - *<WAS_INSTALL_DIR>*/plugins/com.ibm.ws.runtime.jar
   - *<WAS_INSTALL_DIR>*/WebSphere/AppServer/plugins/com.ibm.ws.sib.server.jar
   - *<WAS_INSTALL_DIR>*/WebSphere/AppServer/plugins/com.ibm.ws.security.crypto.jar
2. Extract the jar files from the following rar file:

   unrar *<WAS_INSTALL_DIR>*/WebSphere/AppServer/runtimes/sibc.jmsra.jar
3. Copy the jar files to /opt/was-jars.

Obtain the WebSphere MQ Files

To obtain the WebSphere MQ jar files:

1. Copy the required jar files from /opt/mqm/java/lib:
   - com.ibm.mq.commservices.jar
   - com.ibm.mq.headers.jar
   - com.ibm.mq.jar
   - com.ibm.mq.jmqi.jar
   - com.ibm.mq.mqjms.jar
   - connector.jar
   - dhbcore.jar
   - jms.jar
2. Copy the jar files to /opt/mq-jars.

Obtain the JRE Required for Client Install

Depending on the type of register, obtain the required JRE for the client install.

Obtain the IBM JRE Required for Client Install

This release requires IBM JRE 1.7 for client installs on IBM SurePOS registers. It is distributed by IBM with JavaPOS 113.

Secure Communication

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

- When running the installer for a server, you select whether secure JDBC will be used for communication with the database and whether secure RMI will be used for communication between the store server and registers on the Secure Options screen. See Figure A–22.
  - If **Enable Secure JDBC** is selected, the installer sets up the secure JDBC. If you do not select this and you want to manually set up the secure JDBC after the installer completes, see the *Oracle Retail POS Suite Security Guide*.
  - If **Enable Secure RMI** is selected, the installer sets up the secure RMI. If you do not select this and you want to manually set up the secure JDBC after the installer completes, see the *Oracle Retail POS Suite Security Guide*.
- When running the installer for a client, you select whether secure RMI will be used for communication between the store server and register on the Enable Client Secure RMI screen. See Figure B–18.
  - 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 the *Oracle Retail POS Suite Security Guide*.

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. See Figure A–20.

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, reports data, and Back Office parameters will be lost.

- If you choose **Create schema with sample dataset**, the installer creates and populates the database schema 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.

  To use this option, you must provide the location of the zip file containing the sample dataset on the Sample Dataset installer screen. See Figure A–21. You can obtain the `sample-dataset-13.4.1.zip` file from the Oracle Software Delivery Cloud at the following Web site:

  `https://edelivery.oracle.com/`

- If you choose **Create schema with minimum dataset**, the installer creates and populates the database schema 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 "Create the Database Schema".

Note: If Point-of-Service is being installed for the first time and a clean schema is being used, do not select the **Skip schema creation and data loading** option. The installer will fail at some point if there is no data available in the database. You must populate the database schema before running the installer by selecting one of the other options.

If the schema is already populated and you want to manually restore or update the data, select the **Skip schema creation and data loading** option.

Create 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.

Obtain the Files Needed for RSA Data Protection Manager

If you are using the RSA Data Protection Manager, you must do the following:

- "Obtain the RSA Data Protection Manager Version 3.1 Jar Files"
- "Install the Java Cryptography Extension (JCE)"

Obtain the RSA Data Protection Manager Version 3.1 Jar Files

You must obtain the required jar files from your RSA Data Protection Manager provider.

1. Obtain the following jar files from your RSA Data Protection Manager provider:
   - certj.jar
   - cryptojce.jar
   - cryptojcommon.jar
   - jcm.jar
   - kmsclient.jar
   - sslj.jar
2. Copy the jar files into a directory accessible to the installer, for example, `<INSTALL_DIR>/rsa-jars`.

Install the Java Cryptography Extension (JCE)

If a payment application or RSA Data Protection Manager version 3.1 will be used, you must update the security for your JRE. You need to obtain version 1.4.2 of the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files. The 1.4.2 version for the JCE Unlimited Strength Encryption is compatible with the IBM Java 6 JRE.

1. Make a backup copy of `local_policy.jar` and `US_export_policy.jar`.

```
cd $JRE_HOME/lib/security
mv local_policy.jar local_policy.jar.bak
mv US_export_policy.jar US_export_policy.jar.bak
```

2. Download version 1.4.2 of JCE.
   a. Go to the following Web site:

      http://www.ibm.com/developerworks/java/jdk/security/50/

   b. Click **IBM SDK Policy Files**. You are prompted to log in.
   c. After you log in, follow the instructions to download the 1.4.2+ version JCE.
3. Copy the jar files into the JRE security directory. The files are bundled as `unrestrict142.zip`.

Run 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 on SLEPOS, see Appendix B.

1. Change to the *<INSTALL_DIR>* directory.
2. Set the `JAVA_HOME` environment variable to the location of the Java JRE.

> **Note:** The installer is not compatible with versions of Java earlier than 1.6.

3. Run the `install.sh` 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.sh`

   The installer leaves behind the `ant.install.properties` and `cwallet.sso` files for repeat installations.

Resolve 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.

Create the Database Schema

The scripts that create the database schema can be run from the *<INSTALL_DIR>* directory. The database server can be on the same system as the application server or on a different system.

Create without Oracle Retail Back Office

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

1. Change to the *<INSTALL_DIR>* 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.

   ```
   PATH=$JAVA_HOME/bin:$ANT_HOME/bin:$PATH; export PATH
   ```

4. Run ant targets to create the database schema and load data:

   - no: no action occurs.
   - schema: creates the schema but does not load any data.
   - sample: creates the database schema containing the sample dataset. The sample dataset includes the minimum dataset.

     To use this option, you must provide the location of the zip file containing the sample dataset on the Sample Dataset installer screen. You can obtain the `sample-dataset-13.4.1.zip` file from the Oracle Software Delivery Cloud.
   - minimum: creates the database schema containing the minimum dataset.

   To create the database schema:

   a. In the `ant.install.properties` file, set the database information and set the `input.install.database` property to one of the above values.

   b. Run `install.sh ant install-database`.

5. If you are using Centralized Transaction Retrieval, create the Scratchpad database schema 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 schema already exists and does not create it.

   To create the Scratchpad database schema:

   a. In the `ant.install.properties` file, set the scratchpad database information and set the `input.install.scratchpad.database` property to true.

   b. Run `install.sh ant install-scratchpad`.

6. To load the purge procedures:

   For information on the procedures provided for purging aged data, see the *Oracle Retail POS Suite Operations Guide*.

   a. Change to the *<POS_install_directory>* directory.

   b. In the `ant.install.properties` file, set the `input.install.database` property to load_purge_procedures.

c. Run `install.sh ant install-database`.

Resolve Issues with Misprinted Characters in eReceipts and Network Printed Reports and Receipts

Fonts are not included in the installation of Point-of-Service. They are provided by the operating system and specialty font vendors. Common problems encountered with eReceipts and network printed receipts and reports include misprinted characters (such as a pound sign instead of a multibyte character), illegible characters, and incorrect text alignment. These issues are often resolved by insuring that the Point-of-Service client is configured for the best font available for the language on the operating system.

To resolve issues with misprinted characters, see the following sections:

- "Resolve Issues with Misprinted Characters in eReceipts and Network Printed Reports and Receipts"
- "Resolve Misprinted Character Problems in eReceipts"

Resolve Misprinted Character Problems in eReceipts

To resolve misprinted character problems in eReceipts:

1. Verify that the operating system is installed with a fixed-width font capable of cleanly displaying the misprinted character.

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

2. If the client is running, shut down the client.
3. In the style-sheet used by the Point-of-Service client for eReceipts, specify the best font available for the language on the operating system. Point-of-Service uses Extensible Style-sheet Language Formatting Objects (XSL-FO) to transform each line of receipt data into PDF output. The following file contains the style-sheet:

   <POS_install_directory>/*<client>*/pos/receipts/printing/templates/xsl/ipp_default.xsl

   The style-sheet used for eReceipts specifies the Courier font family. To specify a different font, such as MS Gothic or Courier New, replace the reference to Courier with the new font name as shown in the following example:

   ```
   <xsl:template match="text">
       <fo:block text-align="left" font-family="MS Gothic" font-size="10pt"
           linefeed-treatment="preserve" white-space-collapse="false"
           white-space-treatment="preserve" wrap-option="no-wrap">
   ```

4. Set the receipt line size in the following file:

   <POS_install_directory>/*<client>*/config/context/DeviceContext.xml

   Change the value of receiptLineSize to a number that results in the correct alignment of the text. There are four occurrences of receiptLineSize in the file. Make the same change to all the occurrences. In the following example, the value is changed to 44:

```
<property name="receiptLineSize" value="44" />
```

5. Set the printing of line feeds in the following file:

   <POS_install_directory>/*<client>*/pos/config/technician/PosDeviceTechnician.xml

   Set the value of the alwaysPrintLineFeeds property to true:

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

Point-of-Service is configured to automatically search for fonts in the default paths for your operating system. Point-of-Service uses the Apache Formatting Objects Processor (FOP) to generate eReceipt PDF files. If the font identified in the style-sheet used for eReceipts cannot be automatically found, it can be manually registered in the Apache FOP advanced configuration file:

<POS_install_directory>/*<client>*/pos/receipts/printing/templates/fonts/FopFontConfig.xml

For more information about Apache FOP fonts, see the following Web site:

http://xmlgraphics.apache.org/fop/1.0/fonts.html

Resolve Misprinted Character Problems in Network Printed Receipts and Reports

To resolve misprinted character problems in network printed receipts and reports:

1. Verify that the operating system is installed with a fixed-width font capable of cleanly displaying the misprinted character.

   Note: Point-of-Service assumes fonts are fixed-width for receipts and reports. If variable-width fonts are used, the fields in a network printed receipt or report will not align properly.

2. If the client is running, shut down the client.
3. In the style-sheet used by the Point-of-Service client for network printing, specify the best font available for the language on the operating system. Point-of-Service uses Extensible Style-sheet Language Formatting Objects (XSL-FO) to transform each line receipt or report data into the type of output designated for the configured network printer. The following file contains the style-sheet:

   <POS_install_directory>/*<client>*/pos/receipts/printing/templates/xsl/ipp_default.xsl

   The style-sheet used for network printing specifies the Courier font family. To specify a different font, such as MS Gothic or Courier New, replace the reference to Courier with the new font name as shown in the following example:

   ```
   <xsl:template match="text">
       <fo:block text-align="left" font-family="MS Gothic" font-size="10pt"
           linefeed-treatment="preserve" white-space-collapse="false"
           white-space-treatment="preserve" wrap-option="no-wrap">
   ```

4. Set the receipt line size in the following file:

   <POS_install_directory>/*<client>*/config/context/DeviceContext.xml

Change the value of receiptLineSize to a number that results in the correct alignment of the text. There are four occurrences of receiptLineSize in the file. Make the same change to all the occurrences. In the following example, the value is changed to 44:

```
<property name="receiptLineSize" value="44" />
```

5. Set the printing of line feeds in the following file:

   <POS_install_directory>/*<client>*/pos/config/technician/PosDeviceTechnician.xml

   Set the value of the alwaysPrintLineFeeds property to true:

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

Set up the Store Server for Tender Authorization

If ACI PIN Comm was selected on the Tender Authorization screen, you must update the security for your store server JRE. For more information, see "Install the Java Cryptography Extension (JCE)".

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

Results of a Point-of-Service Installation

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

Table 3–2 <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 3–3:

Table 3–3 <POS_install_directory>/pos Subdirectories

Name	Contents
bin	Startup 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 shell script (such as `dbstart.sh`) exists.

To run Point-of-Service:

1. Start the store server:

   `StoreServerConduit.sh`

   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:

   `ClientConduit.sh`

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 POS Suite Implementation Guide, Volume 2 - Extension Solutions* 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.

A

Appendix: Installer Screens Server Installation on SLEPOS

You need specific details about your environment for the installer to successfully install the Point-of-Service application on the IBM Stack on SLEPOS. 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 on SLEPOS, see Appendix B.

Figure A–1 Introduction

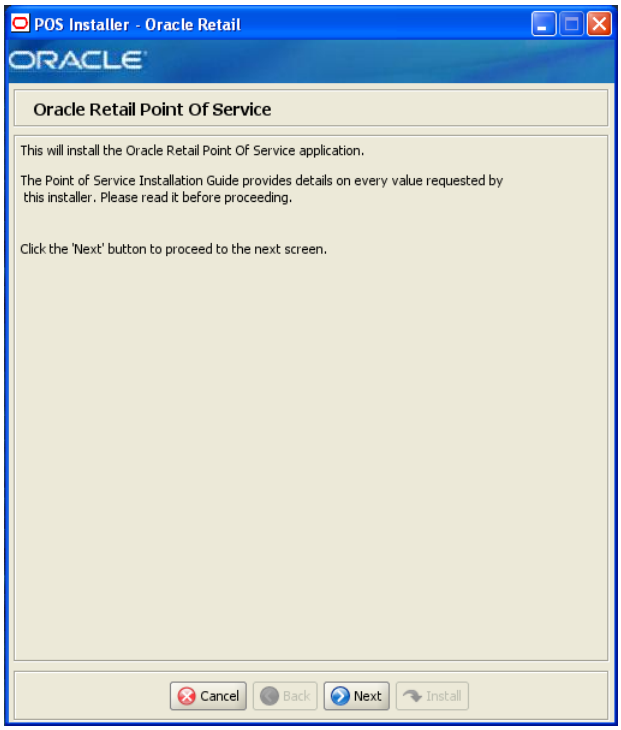


Figure A–2 Previous POS Install

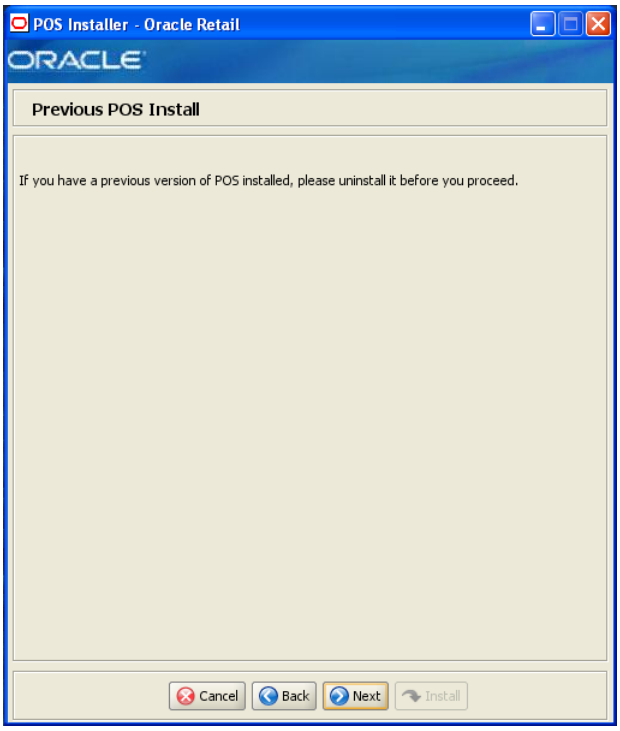
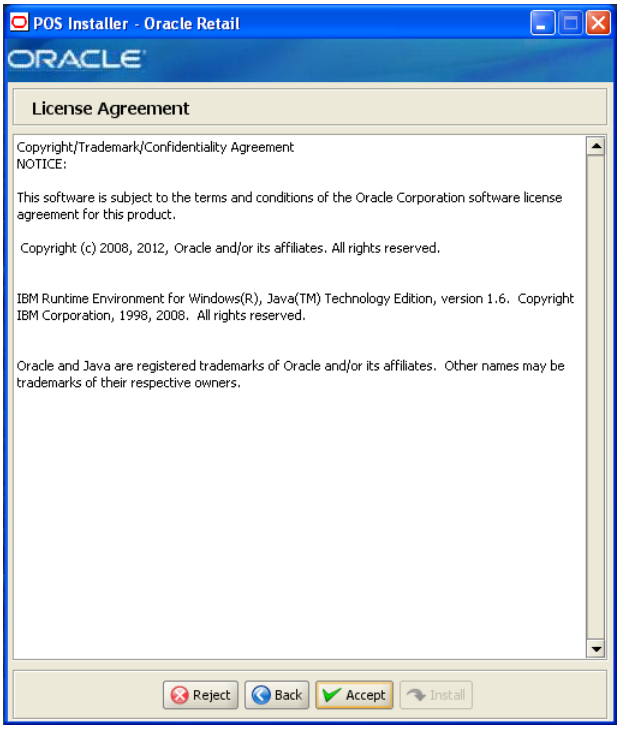
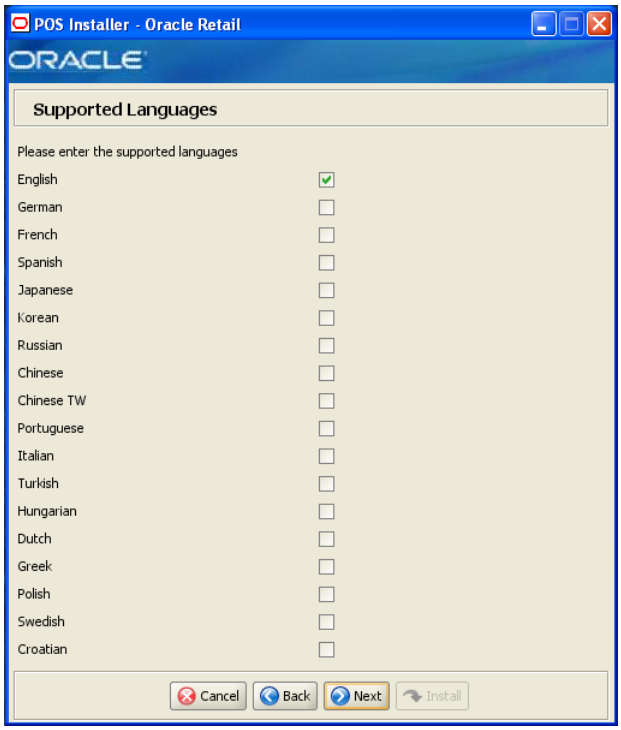


Figure A–3 License Agreement



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.

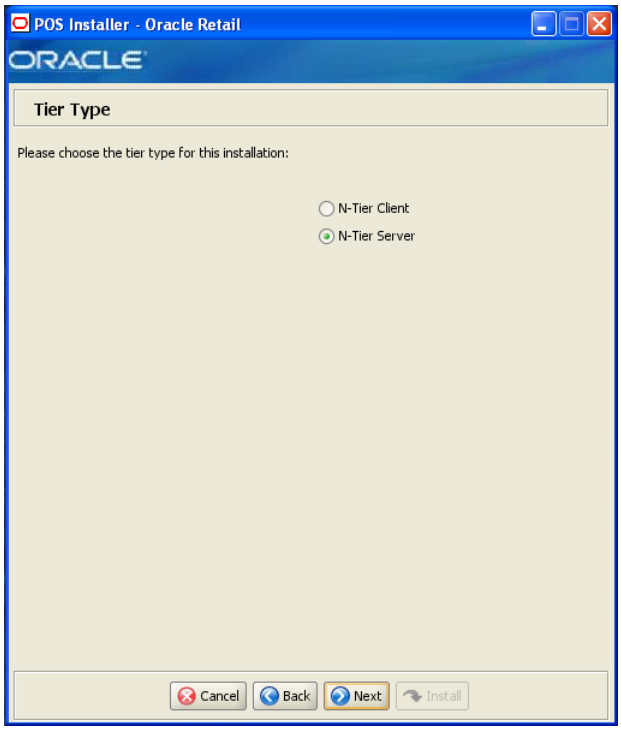
Details	Content
Field Title	Please enter the supported languages
Field Description	Select the languages that will be available for the Point-of-Service application. The languages selected on this screen determine the available choices on the Enter Default Locale screen.
Example	English

Figure A–5 Enter Default Locale

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

Details	Content
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

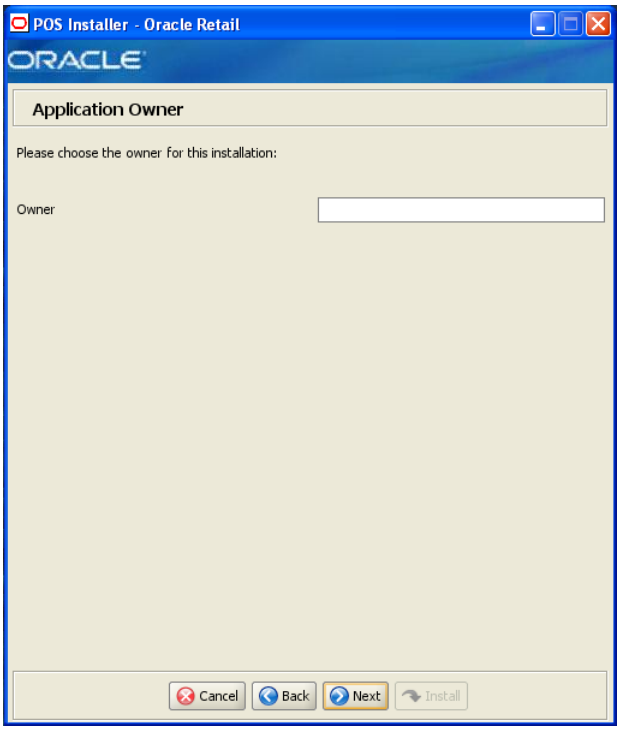
Figure A–6 Tier Type



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

Details	Content
Field Title	Tier Type
Field Description	Choose the server tier type for this installation. For more information, see "Determining Tier Type" in Chapter 3. To install the N-Tier version of the server, choose **N-Tier Server**.
Example	N-Tier Server

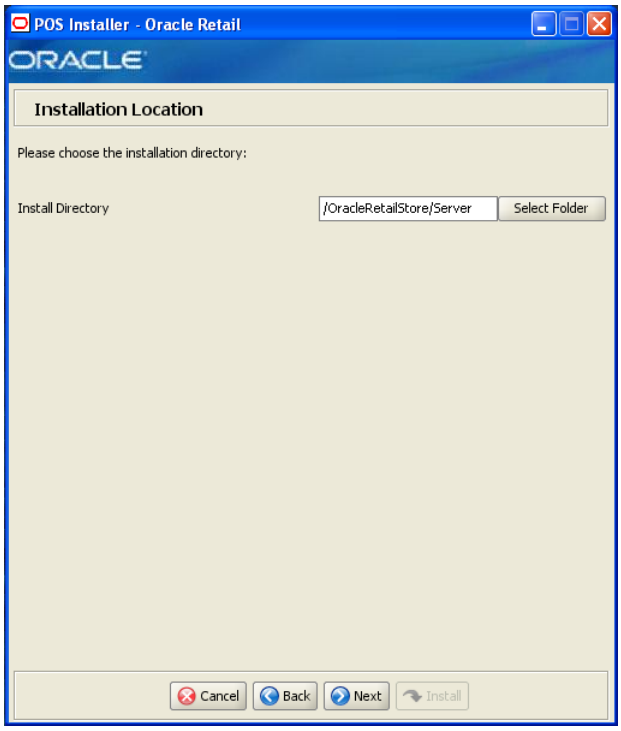
Figure A–7 Application Owner



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

Details	Content
Field Title	Owner
Field Description	Enter the operating system user who will be the owner for this installation.

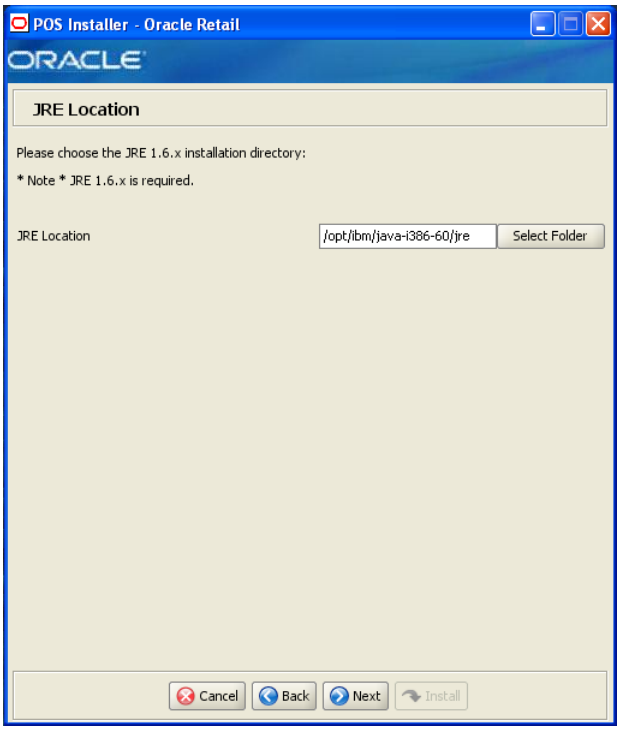
Figure A–8 Installation Location



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

Details	Content
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 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	`/OracleRetailStore/Server`

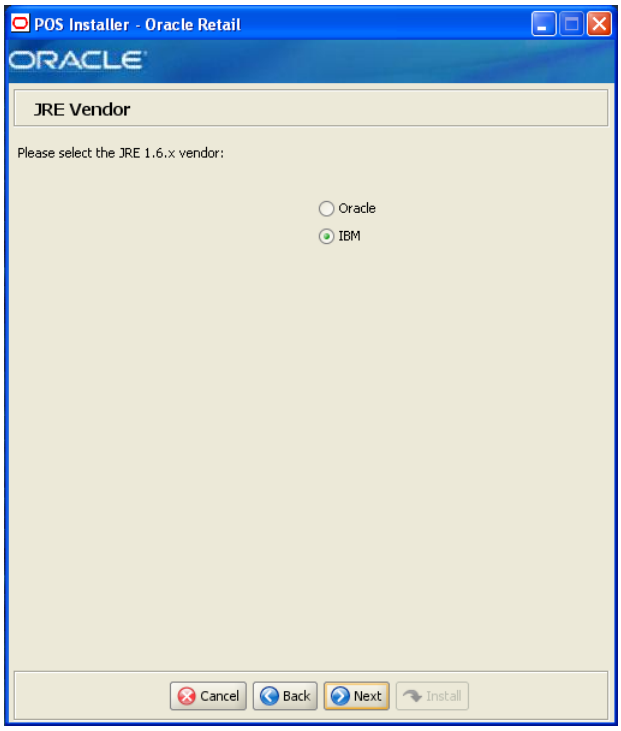
Figure A–9 JRE Location



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

Details	Content
Field Title	JRE Location
Field Description	Enter the location where the JRE is installed.
Example	`/opt/ibm/java-i386-60/jre6`

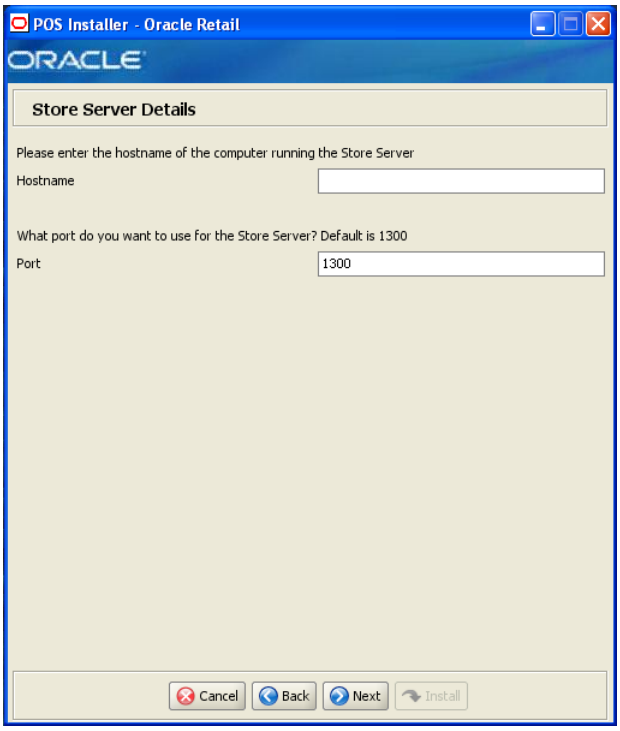
Figure A–10 JRE Vendor



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

Details	Content
Field Title	Please select the JRE 1.6.x vendor
Field Description	Select the vendor for the JRE entered on the JRE Location screen: ■ Oracle ■ IBM Choose **IBM**.

Figure A–11 Store Server Details

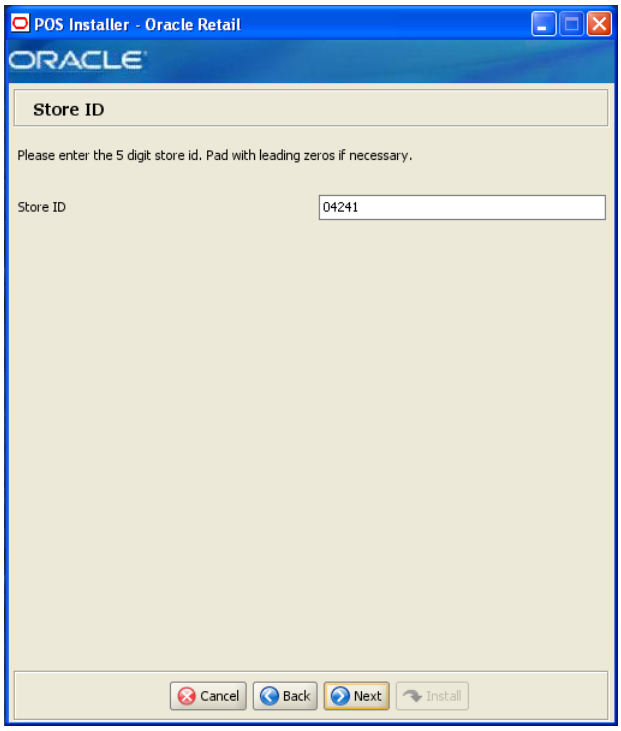


The fields on this screen are described in the following tables.

Details	Content
Field Title	Hostname
Field Description	Enter the host name of the store server.

Details	Content
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

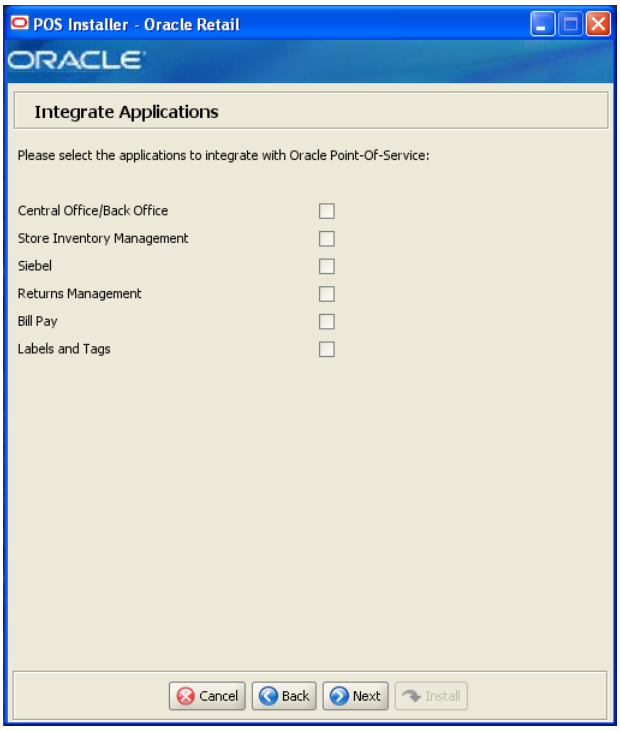
Figure A–12 Store ID



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

Details	Content
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

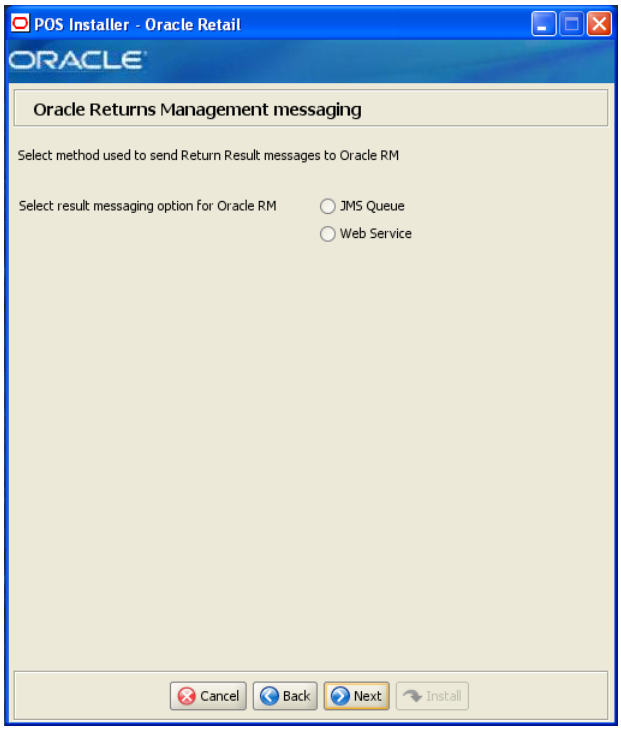
Figure A–13 Integrate Applications



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

Details	Content
Field Title	Please select the applications to integrate with Oracle Point-of-Service
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.

Details	Content
Field Title	Select result messaging option for Oracle RM
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**.

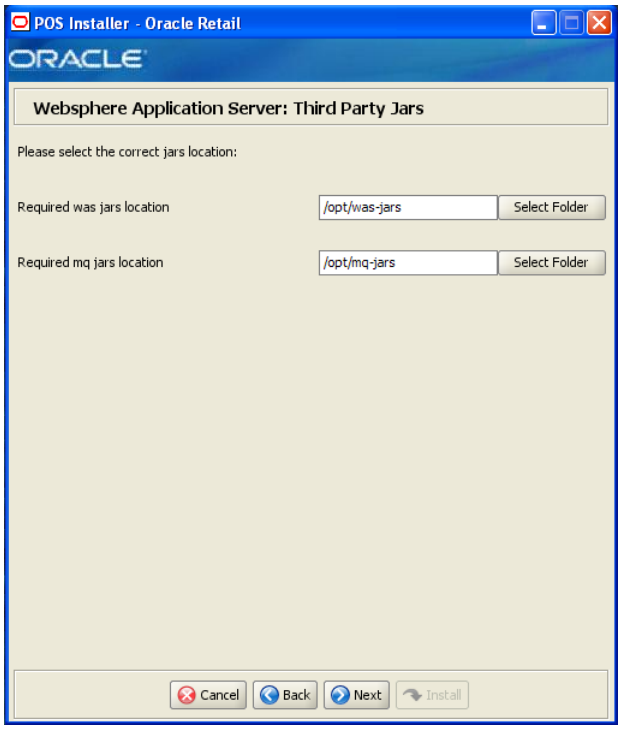
Figure A–15 Application Server Type

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.

Details	Content
Field Title	Please select the application server you would like to user
Field Description	Select the application server to be used for the store server. ▪ WebLogic Application Server ▪ Websphere Application Server Choose **Websphere Application Server**.

Figure A–16 Websphere Application Server: Third Party Jars



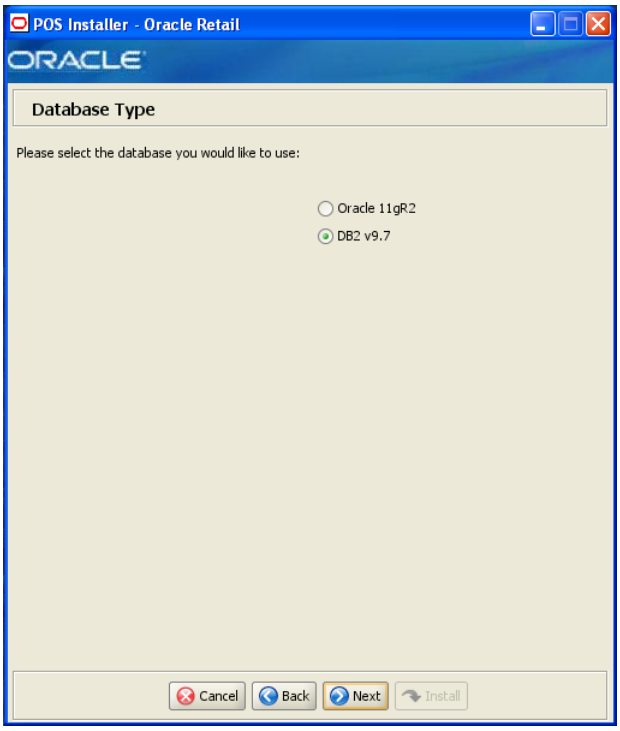
This screen is only displayed if **WebSphere Application Server** is selected on the Application Server Type screen.

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

Details	Content
Field Title	Required was jars location
Field Description	Choose the location of the was jar files. See "Obtain the Third-Party Library Files Required by Point-of-Service" in Chapter 3 for the list of required jar files.
Example	`/opt/was-jars`

Details	Content
Field Title	Required mq jars location
Field Description	Choose the location of the mq jar files. See "Obtain the Third-Party Library Files Required by Point-of-Service" in Chapter 3 for the list of required jar files.
Example	`/opt/mq-jars`

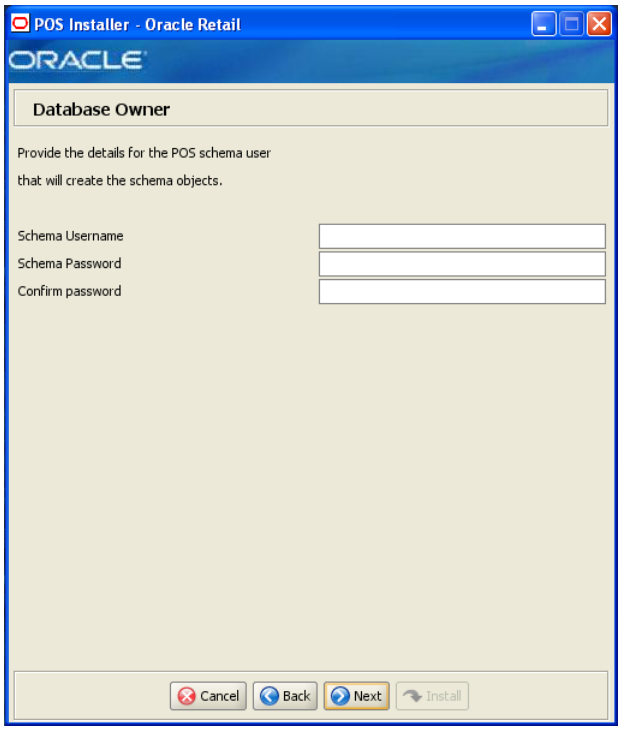
Figure A–17 Database Type



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

Details	Content
Field Title	Please select the database you would like to use
Field Description	Select the database provider that is used for the OracleRetailStore database. ▪ Oracle 11gR2 ▪ DB2 v9.7 Choose **DB2 v9.7**.

Figure A–18 Database Owner



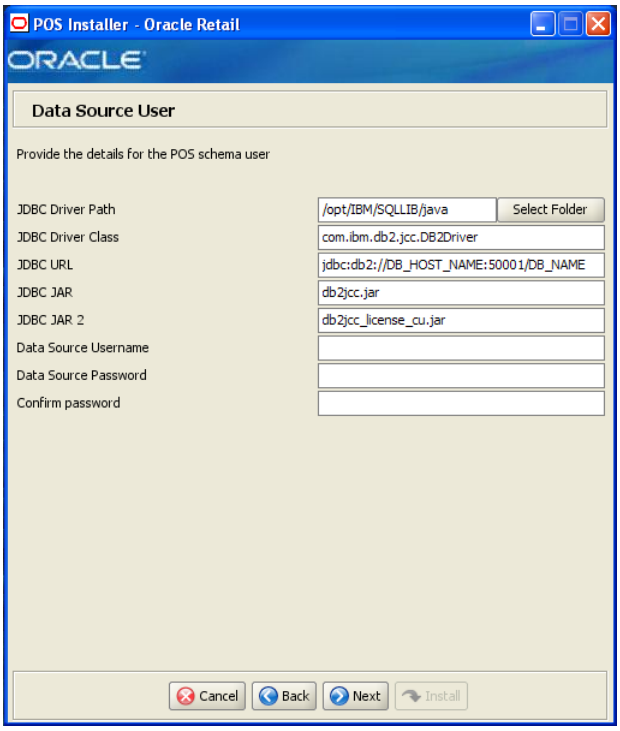
The fields on this screen are described in the following tables.

Details	Content
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 3. **Note:** This user creates the database objects used by Point-of-Service.

Details	Content
Field Title	Schema Password
Field Description	Password for the database owner.

Details	Content
Field Title	Confirm Password
Field Description	Reentered Schema Password used to confirm the password. **Note:** The passwords in the Schema Password and Confirm Password fields must match.

Figure A–19 Database Source User



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

For information on obtaining the jar files, see "Obtain the DB2 Files" in Chapter 3.

Details	Content
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	`/opt/IBM/SQLLIB/java/`

Details	Content
Field Title	JDBC Driver
Field Description	Enter the database driver class name.
Example	`com.ibm.db2.jcc.DB2Driver`

Details	Content
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:db2://DB_HOST_NAME:500001/DB_NAME`

Details	Content
Field Title	JDBC JAR
Field Description	Enter the name of the jar containing the database driver.
Example	`db2jcc.jar`

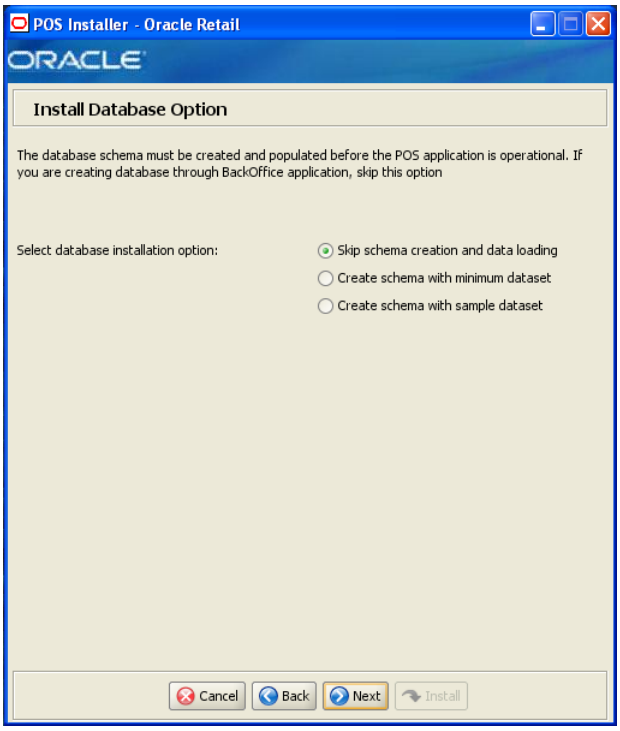
Details	Content
Field Title	JDBC JAR2
Field Description	Enter the name of the jar containing the database licensing.
Example	`db2jcc_license_cu.jar`

Details	Content
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 3. **Note:** This schema user is used by Point-of-Service to access the database.

Details	Content
Field Title	Data Source Password
Field Description	Password for the data source user.

Details	Content
Field Title	Confirm Password
Field Description	Reentered Data Source Password used to confirm the password. **Note:** The passwords in the Data Source Password and Confirm Password fields must match.

Figure A–20 Install Database Option



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

Details	Content
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, 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 3.
Example	Skip schema creation and data loading

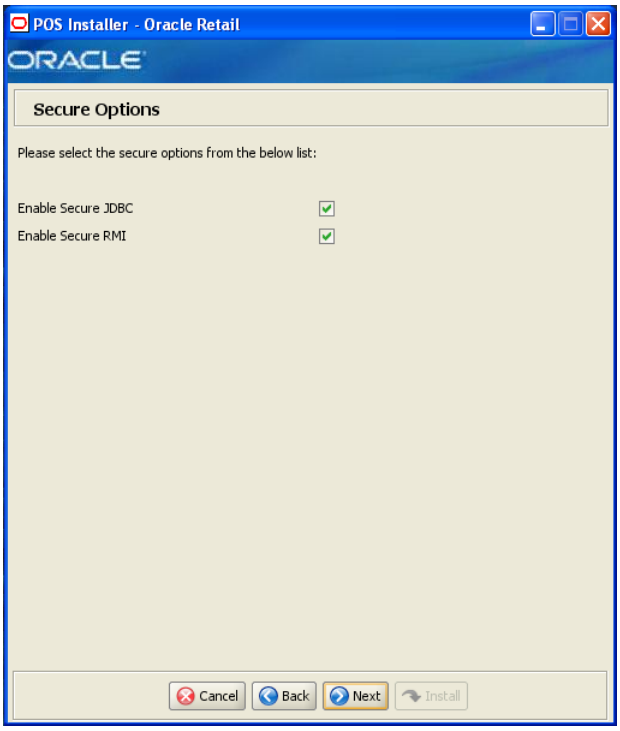
Figure A–21 Sample Dataset

This screen is only displayed when **Create schema with sample dataset** is selected on the Install Database Option screen.

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

Details	Content
Field Title	Sample dataset file
Field Description	Enter the path to the sample dataset to be loaded into the database schema. You can obtain the `sample-dataset-13.4.1.zip` file from the Oracle Software Delivery Cloud at the following Web site: `https://edelivery.oracle.com/` For more information on the sample dataset, see "Database Install Options" in Chapter 3.
Example	`/oracle/retail/samples/sample-db.zip`

Figure A–22 Secure Options

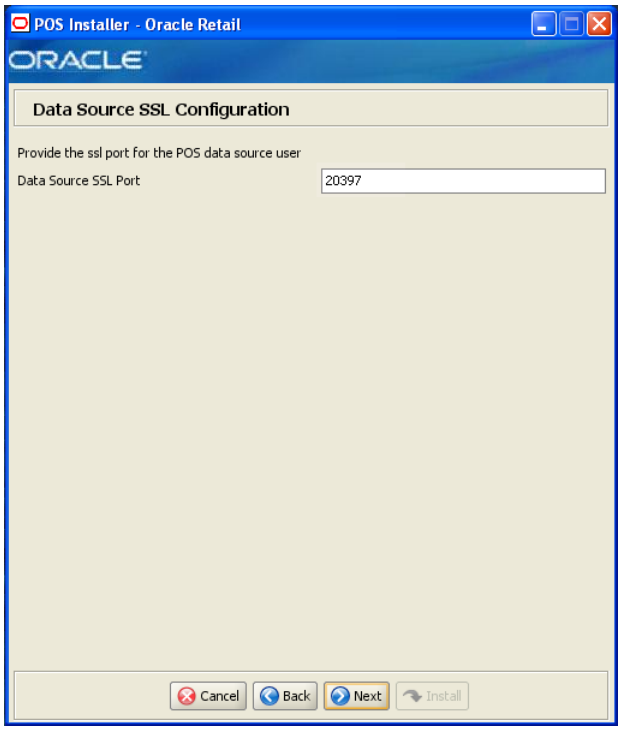


The fields on this screen are described in the following tables.

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

Details	Content
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–23 Data Source SSL Configuration

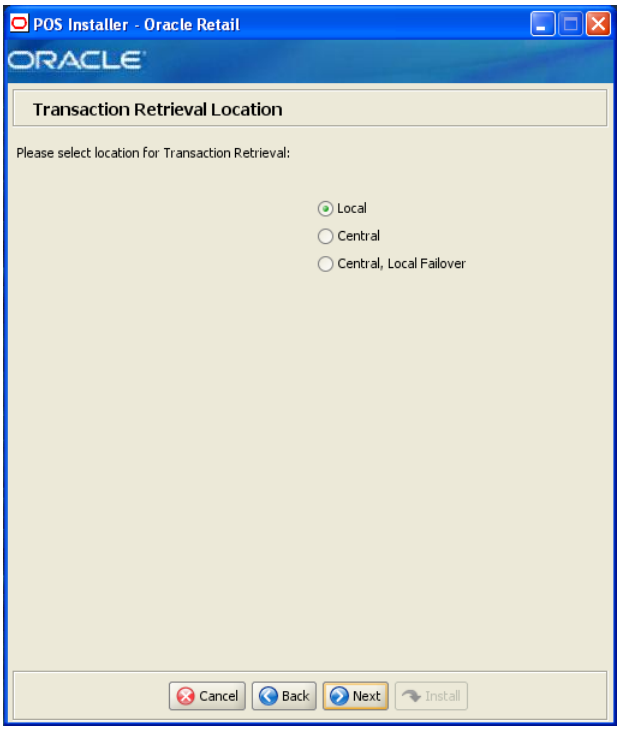


This screen is only displayed if **Enable Secure JDBC** is selected on the Secure Options screen.

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

Details	Content
Field Title	Data Source SSL Port
Field Description	SSL port used to access the database.
Example	20397

Figure A–24 Transaction Retrieval Location

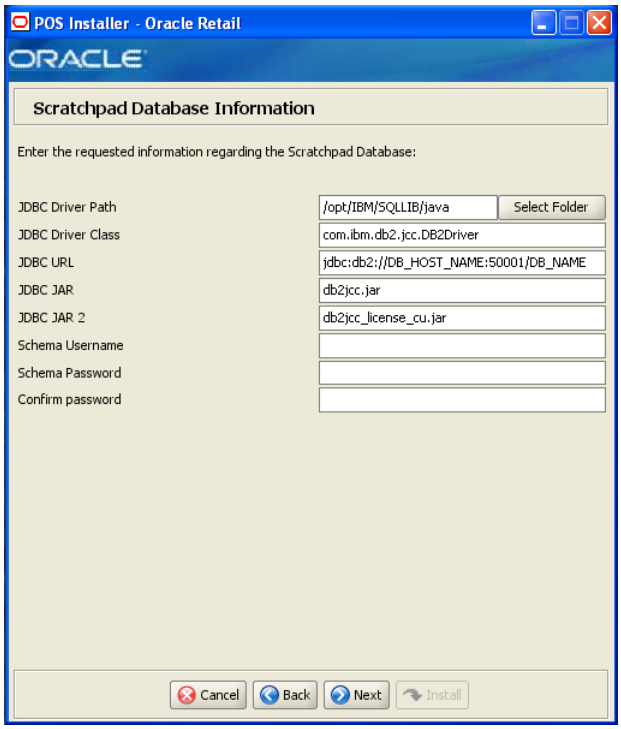


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

Details	Content
Field Title	Please select location for Transaction Retrieval
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–25 Scratchpad Database Information



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

For information on obtaining the jar files, see "Obtain the DB2 Files" in Chapter 3.

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

Details	Content
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	`/opt/IBM/SQLLIB/java`

Details	Content
Field Title	JDBC Driver Class
Field Description	Enter the database driver class name.
Example	`com.ibm.db2.jdbc.DB2Driver`

Details	Content
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:db2://DB_HOST_NAME:50001/DB_NAME`

Details	Content
Field Title	JDBC JAR
Field Description	Enter the name of the jar containing the database driver.
Example	`db2jcc.jar`

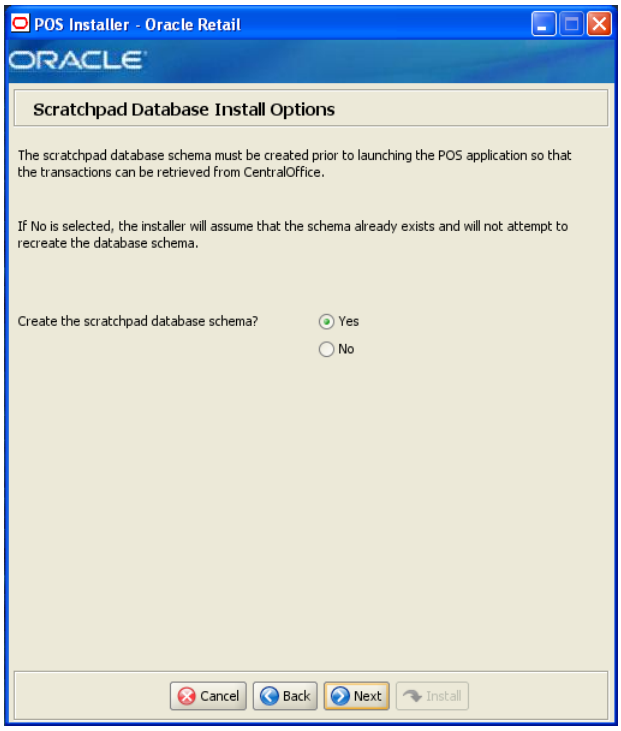
Details	Content
Field Title	JDBC JAR 2
Field Description	Enter the name of the jar containing the database licensing.
Example	`db2jcc_license_cu.jar`

Details	Content
Field Title	Schema Username
Field Description	Enter the database user that owns the scratchpad database.

Details	Content
Field Title	Schema Password
Field Description	Password for the database owner.

Details	Content
Field Title	Confirm Password
Field Description	Reentered Schema Password used to confirm the password. **Note:** The passwords in the Schema Password and Confirm Password fields must match.

Figure A–26 Scratchpad Database Install Options

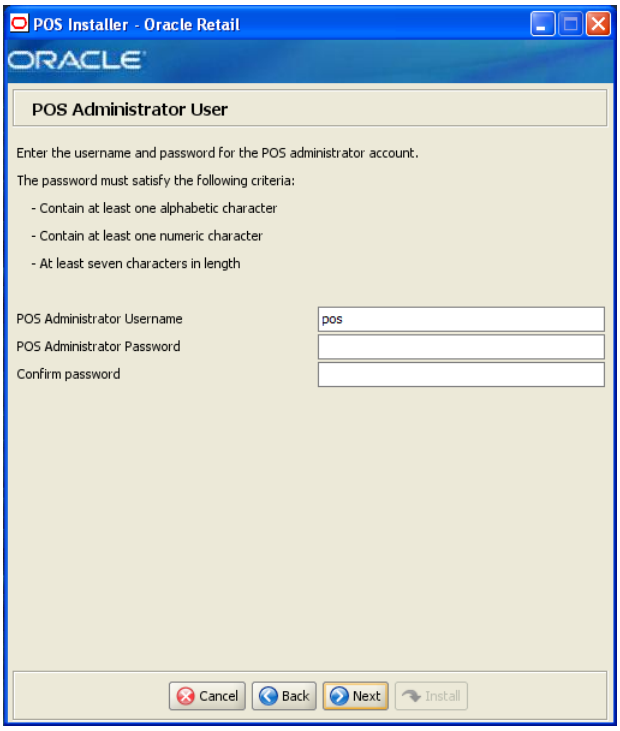


This screen is only displayed if **Central** or **Central, Local Failover** is selected on the Transaction Retrieval Location screen.

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

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

Figure A–27 POS Administrator User



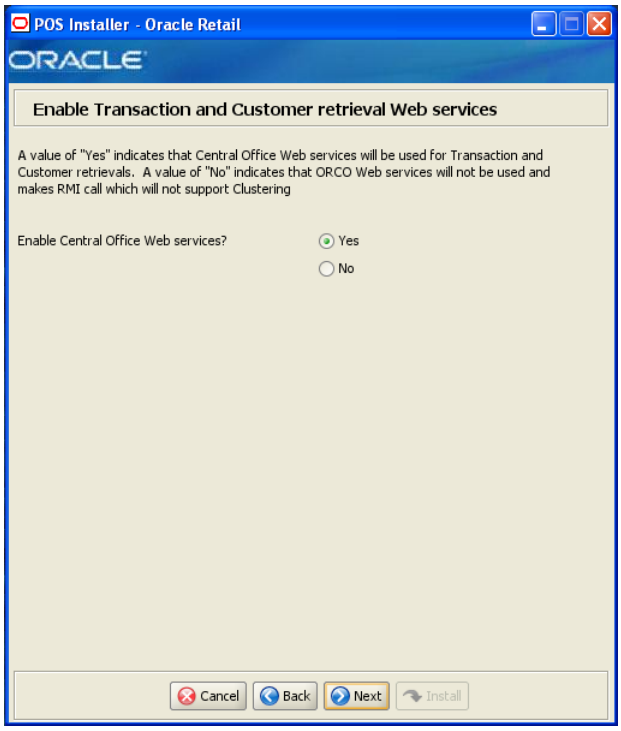
The fields on this screen are described in the following tables.

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

Details	Content
Field Title	POS Administrator Username
Field Description	Enter the password for the administrator user.

Details	Content
Field Title	Confirm Password
Field Description	Reentered POS Administrator Password used to confirm the password. **Note:** The passwords in the POS Administrator Password and Confirm Password fields must match.

Figure A–28 Enable Transaction and Customer Retrieval Web Services

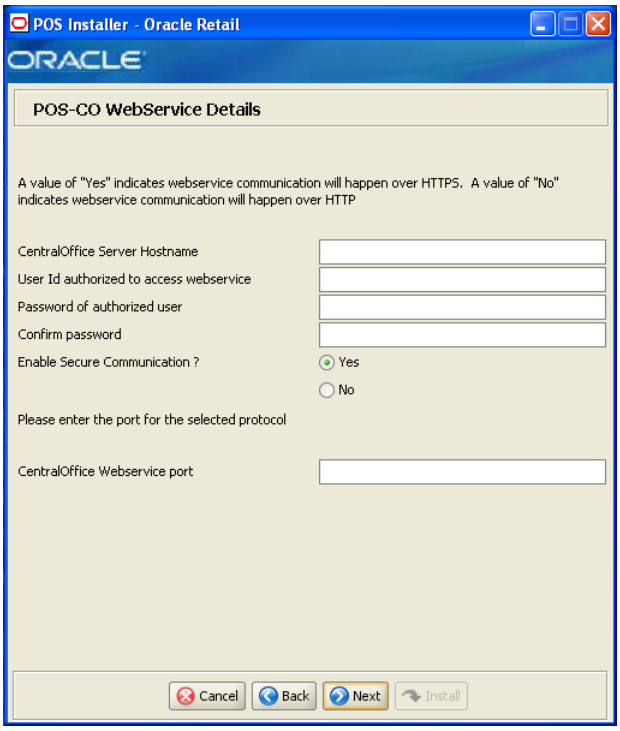


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

Details	Content
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–29 POS-CO WebService Details



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.

Details	Content
Field Title	Central Office Server Hostname
Field Description	Enter the host name for the Central Office Web service.

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

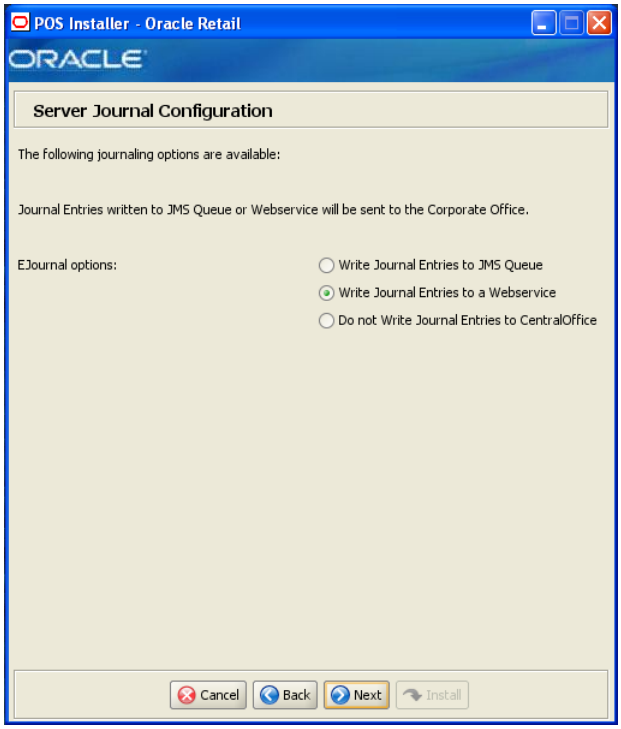
Details	Content
Field Title	Password of authorized user
Field Description	Enter the password of the authorized user.

Details	Content
Field Title	Confirm Password
Field Description	Reentered Password of authorized user used to confirm the password. **Note:** The passwords in the Password of authorized user and Confirm Password fields must match.

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

Details	Content
Field Title	Central Office Webservice Port
Field Description	Enter the port number for the Central Office Web service.

Figure A–30 Server Journal Configuration

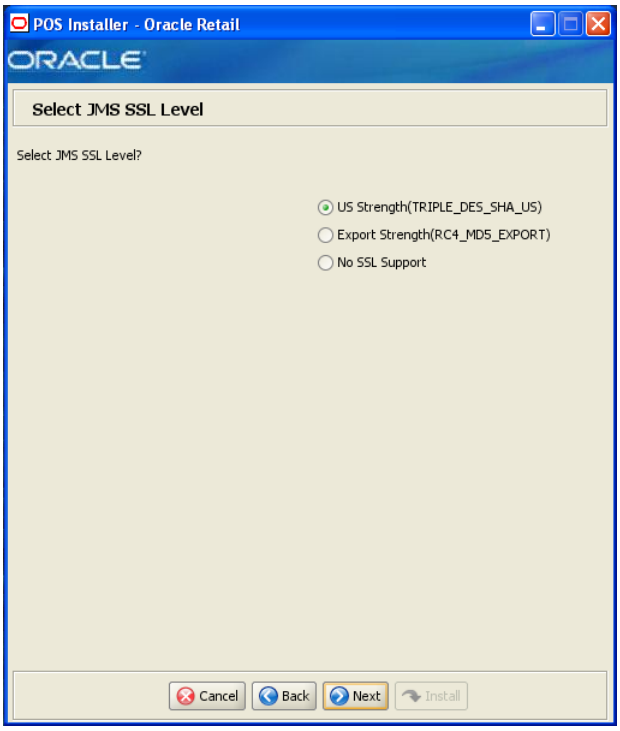


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

Details	Content
Field Title	EJounal options
Field Description	Select an option for journaling. Journal entries written to a JMS queue or Web service are sent to the corporate office. ▪ Write Journal Entries to JMS Queue ▪ Write Journal Entries to a Webservice ▪ Do not Write Journal Entries to CentralOffice
Example	Write Journal Entries to a Webservice

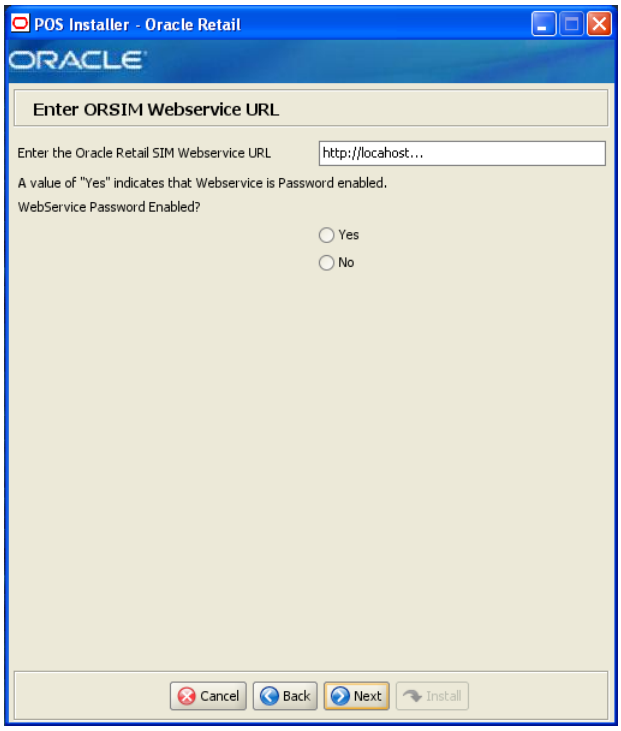
Figure A–31 Select JMS SSL Level



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

Details	Content
Field Title	Select JMS SSL Level
Field Description	JMS SSL level to be used. ▪ To use US strength, select **US Strength(TRIPLE_DES_SHA_US)**. US Strength requires that the JCE policy jar files are installed. See "Install the Java Cryptography Extension (JCE)". ▪ To use export strength, select **Export Strength(RC4_MDS_EXPORT)**. ▪ To not use ssl support, select **No SSL Support**.
Example	US Strength(TRIPLE_DES_SHA_US)

Figure A–32 Enter ORSIM Webservice URL



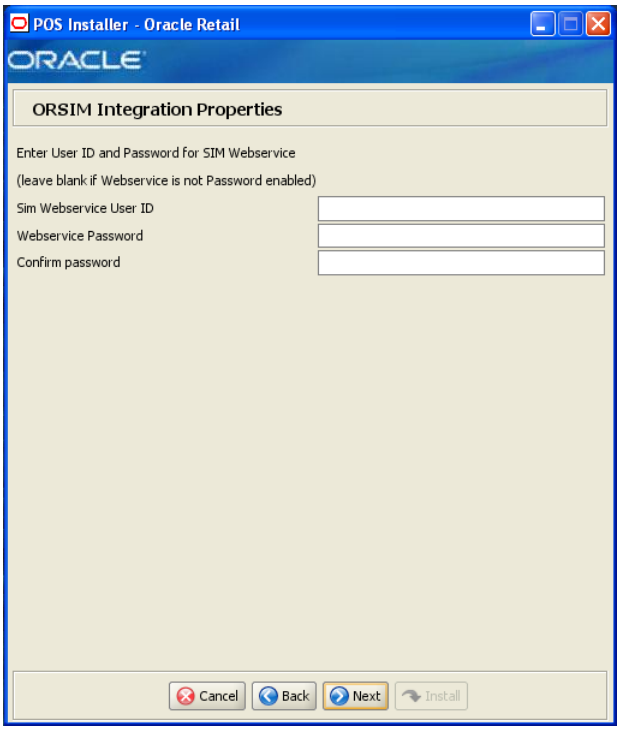
This screen is only displayed if **Store Inventory Management** is selected on the Integrate Applications screen.

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

Details	Content
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.

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

Figure A–33 ORSIM Integration Properties



This screen is only displayed if **Yes** is selected for the Webservice Password Enabled field on the Enter ORSIM Webservice URL screen.

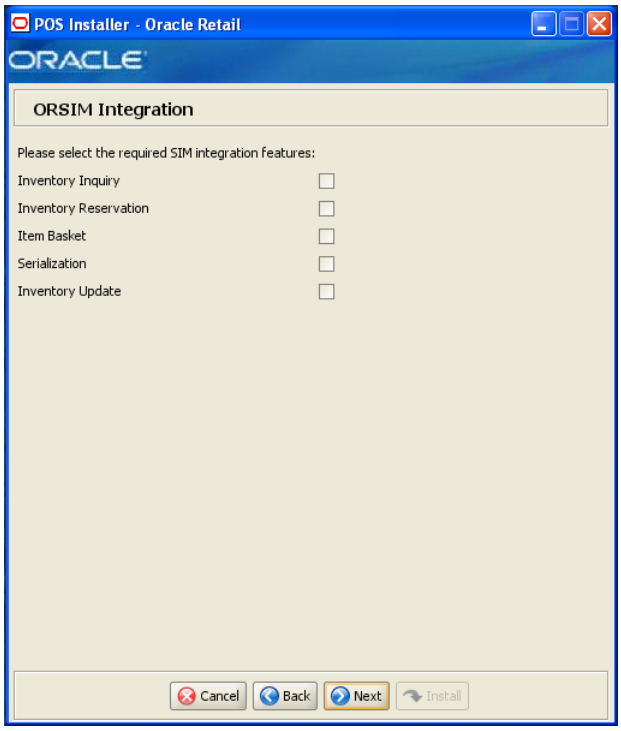
The fields on this screen are described in the following tables.

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

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

Details	Content
Field Title	Confirm Password
Field Description	Reentered WebService Password used to confirm the password. **Note:** The passwords in the WebService Password and Confirm Password fields must match.

Figure A–34 ORSIM Integration

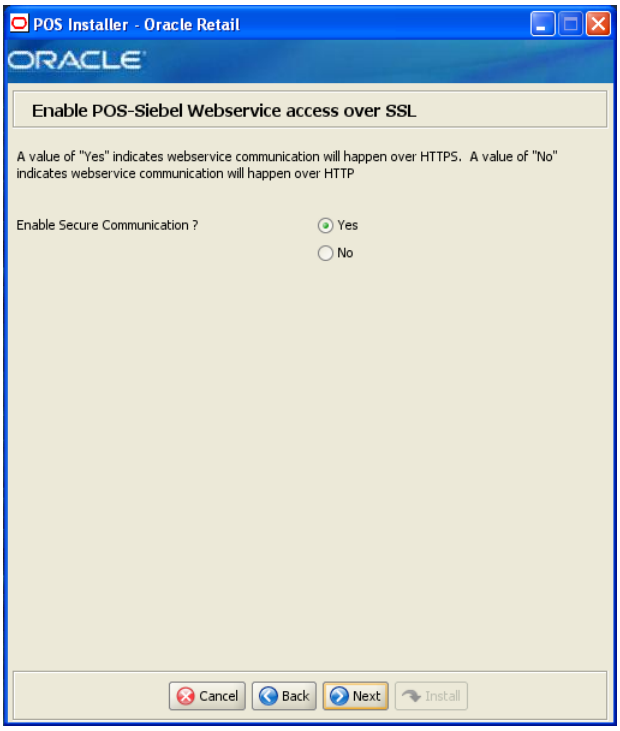


This screen is only displayed if **Store Inventory Management** is selected on the Integrate Applications screen.

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

Details	Content
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**.

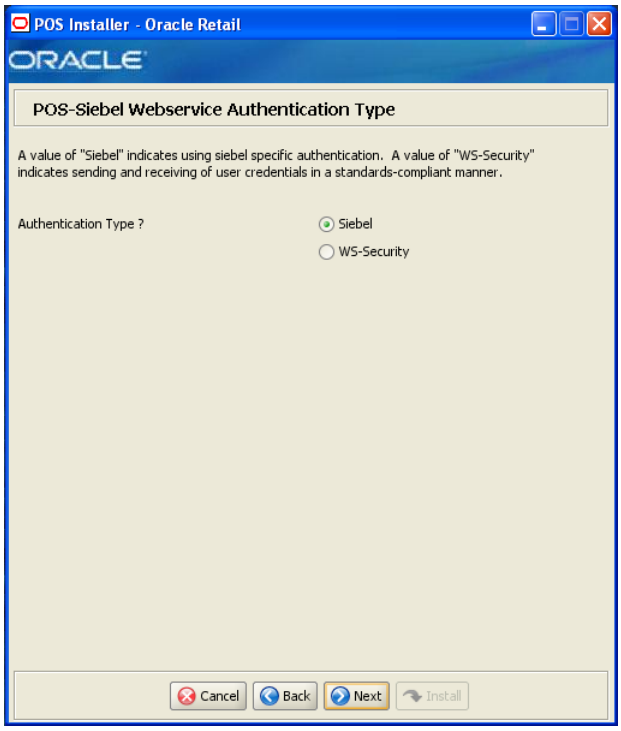
Figure A–35 Enable POS-Siebel Webservice Access Over SSL



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.

Details	Content
Field Title	Enable Secure Communication?
Field Description	Select Yes if Web service communication with Siebel using HTTPS.
Example	Yes

Figure A–36 POS-Siebel Webservice Authentication Type

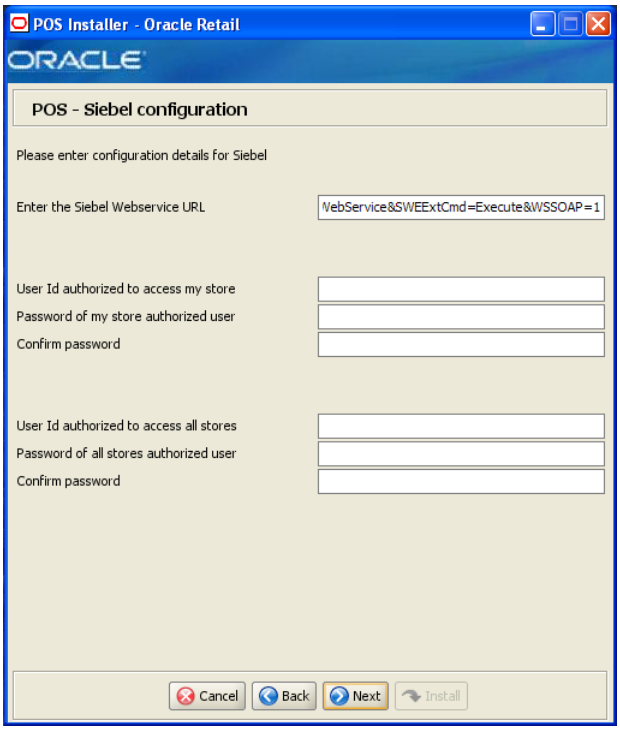


This screen is only displayed if **Siebel** is selected on the Integrate Applications screen.

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

Details	Content
Field Title	Authentication Type?
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–37 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.

Details	Content
Field Title	Enter the Siebel Webservice URL
Field Description	Enter the URL used by the Point-of-Service application to access Siebel.
Example	`https://HOST[:PORT]/eai_secure_enu/start.swe?SWEExtSource=SecureWebService&SWEExtCmd=Execute&WSSOAP=1`

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

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

Details	Content
Field Title	Confirm Password

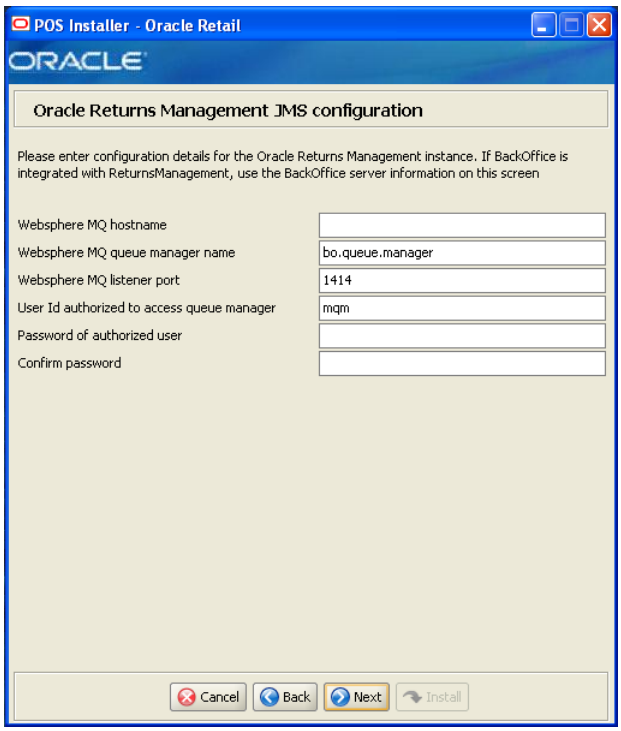
Details	Content
Field Description	Reentered password of my store authorized user used to confirm the password. **Note:** The passwords in the Password of my store authorized user and Confirm Password fields must match.

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

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

Details	Content
Field Title	Confirm Password
Field Description	Reentered password of all stores authorized user used to confirm the password. **Note:** The passwords in the Password of all stores authorized user and Confirm Password fields must match.

Figure A–38 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 fields on this screen are described in the following tables.

Details	Content
Field Title	Websphere MQ Hostname
Field Description	Enter the name for the IBM WebSphere MQ host.

Details	Content
Field Title	Websphere MQ Queue Manager Name
Field Description	Enter the name of the IBM WebSphere MQ queue manager.
Example	bo.queue.manager

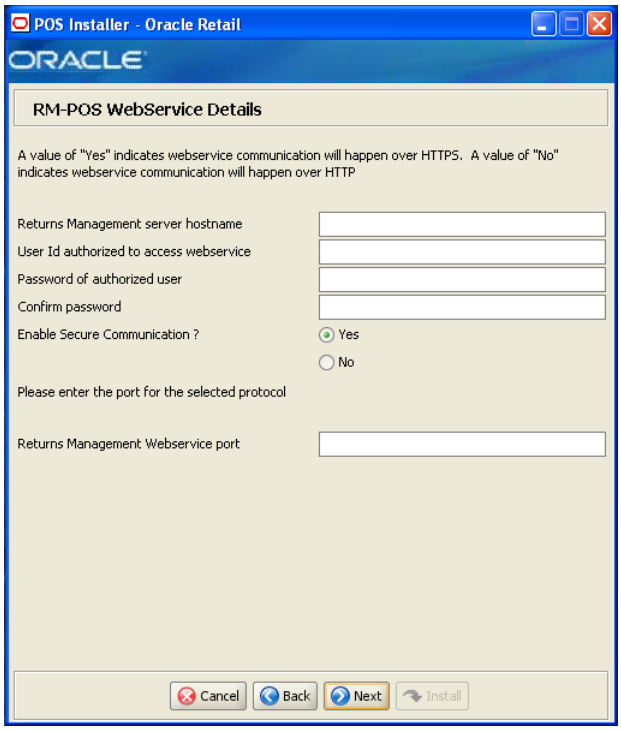
Details	Content
Field Title	Websphere MQ Listener Port
Field Description	Enter the port number for the IBM WebSphere MQ listener.
Example	1414

Details	Content
Field Title	User ID Authorized to Access Queue Manager
Field Description	Enter the user ID used to access the IBM WebSphere MQ manager.
Example	mqm

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

Details	Content
Field Title	Confirm Password
Field Description	Reentered Password of authorized user used to confirm the password. **Note:** The passwords in the Password of authorized user and Confirm Password fields must match.

Figure A–39 RM-POS WebService Details



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

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

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

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

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

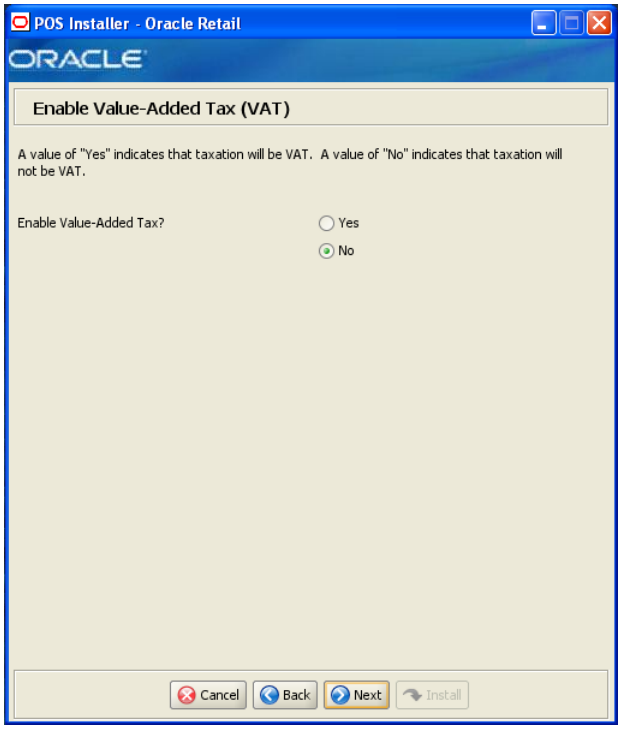
Details	Content
Field Title	Confirm Password

Details	Content
Field Description	Reentered Password of authorized user used to confirm the password. **Note:** The passwords in the Password of authorized user and Confirm Password fields must match.

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

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

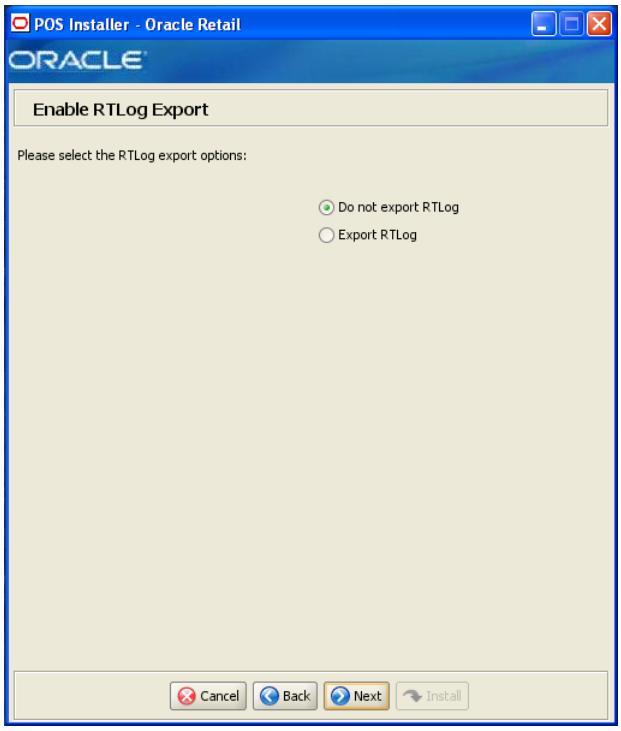
Figure A–40 Enable Value-Added Tax (VAT)



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

Details	Content
Field Title	Enable Value-Added Tax?
Field Description	Select Yes if Value-Added Tax is used.
Example	No

Figure A–41 Enable RTLog Export



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

Details	Content
Field Title	Please select 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**.
Example	Do not export RTLog

Figure A–42 Security Setup: Key Manager Settings

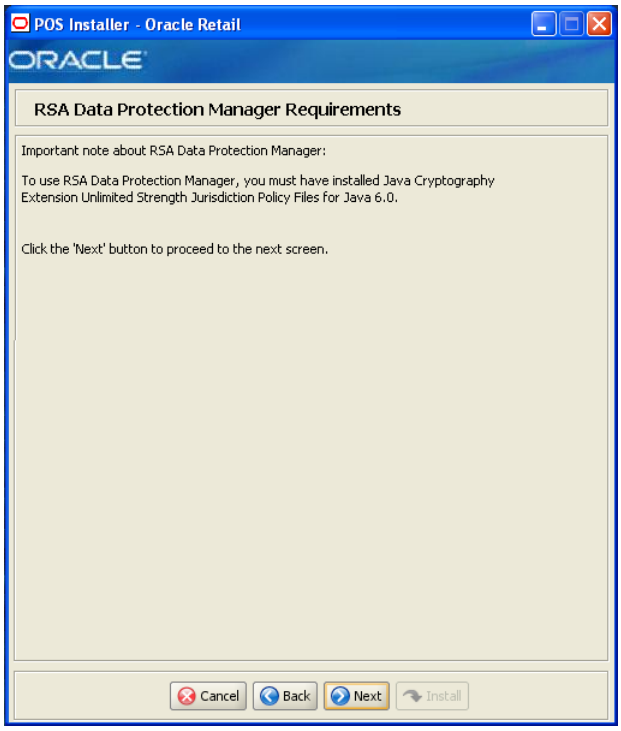
This screen is used to configure the Encryption Key Manager.

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

Details	Content
Field Title	Hash Algorithm
Field Description	Name of the algorithm used by the Key Manager to hash sensitive data.
Example	SHA-256

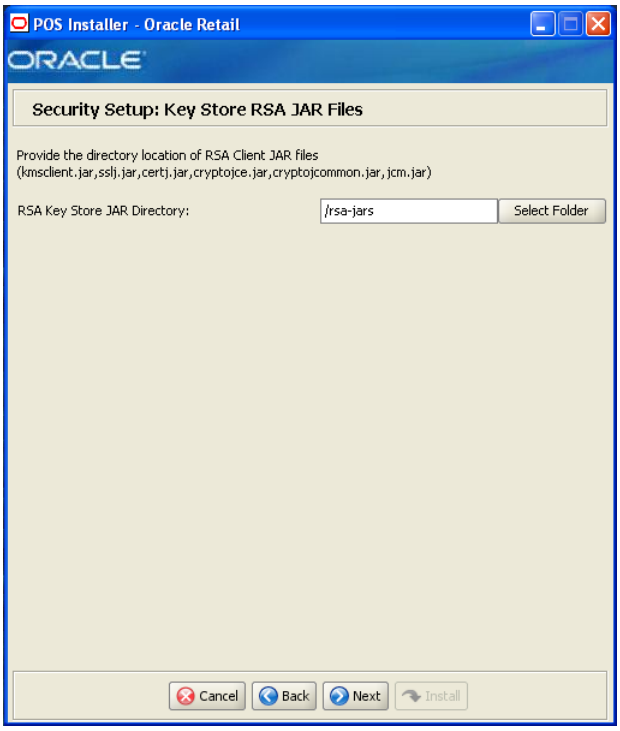
Details	Content
Field Title	Select Key Manager
Field Description	Provider for Key Manager: ■ To use the RSA Data Protection Manager, select **RSA Data Protection Manager**. The next screen displayed is Figure A–43. ■ To use the simulated key management package, select **Simulator**. The next screen displayed is Figure A–46.
Example	RSA Data Protection Manager

Figure A–43 RSA Data Protection Manager Requirements



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

Figure A–44 Security Setup: Key Store RSA JAR Files



This screen is only displayed if **RSA Data Protection Manager** is selected for the Key Manager on the Security Setup: Key Manager Settings screen.

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

Details	Content
Field Title	RSA Key Store JAR Directory
Field Description	Choose the directory where the following Key Store jar files are located: ▪ certj.jar ▪ cryptojce.jar ▪ cryptojcommon.jar ▪ jcm.jar ▪ kmsclient.jar ▪ sslj.jar
Example	`/rsa-jars`

Figure A–45 RSA Client Configuration

This screen is only displayed if **RSA Data Protection Manager** is selected for the Key Manager on the Security Setup: Key Manager Settings screen.

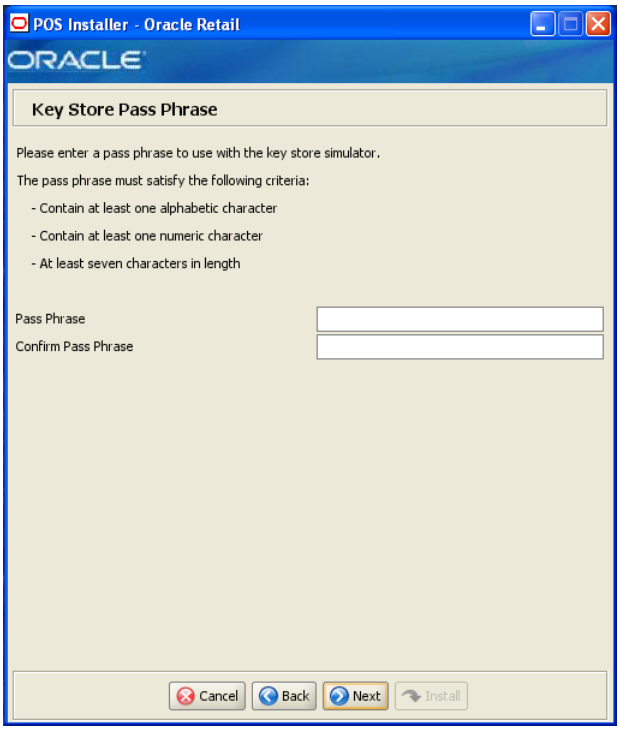
The fields on this screen are described in the following tables.

Details	Content
Field Title	Cipher Key Class
Field Description	Enter the name of the cipher suite that defines the authentication and encryption algorithms that will be used by RSA to negotiate the security settings for the network connection.

Details	Content
Field Title	RSA Client Configuration File
Field Description	Select the location of the RSA client configuration file. This file contains the details for configuring the RSA client.

Details	Content
Field Title	Generate a new client.app.name value
Field Description	To have the installer generate a unique name for the client.app.name value in the RSA client configuration file, select **Yes**. To not change the value in the configuration file, select **No**.
Example	No

Figure A–46 Key Store Pass Phrase for Simulator Key Manager



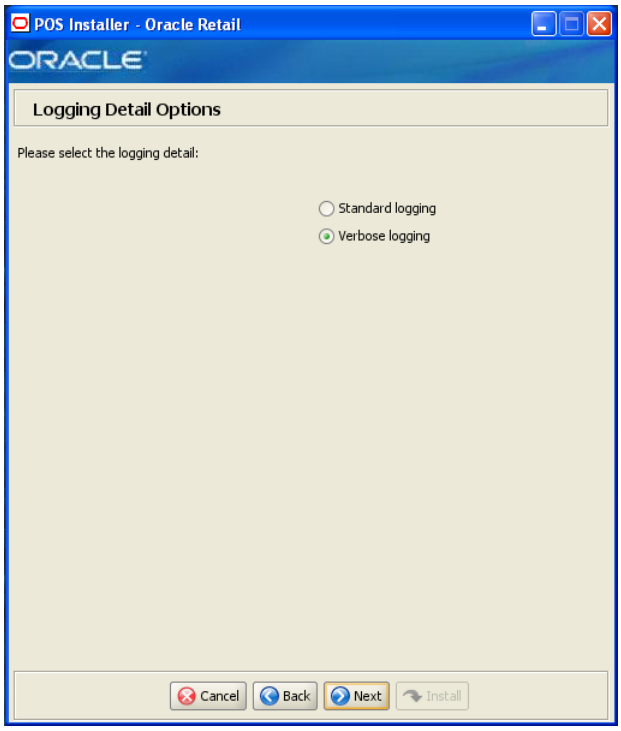
This screen is only displayed if **Simulator** is selected for the Key Manager on the Security Setup: Key Manager Settings screen.

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

Details	Content
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.

Details	Content
Field Title	Confirm Pass Phrase
Field Description	Reentered Pass Phrase used to confirm the pass phrase. **Note:** The pass phrases in the Pass Phrase and Confirm Pass Phrase fields must match.

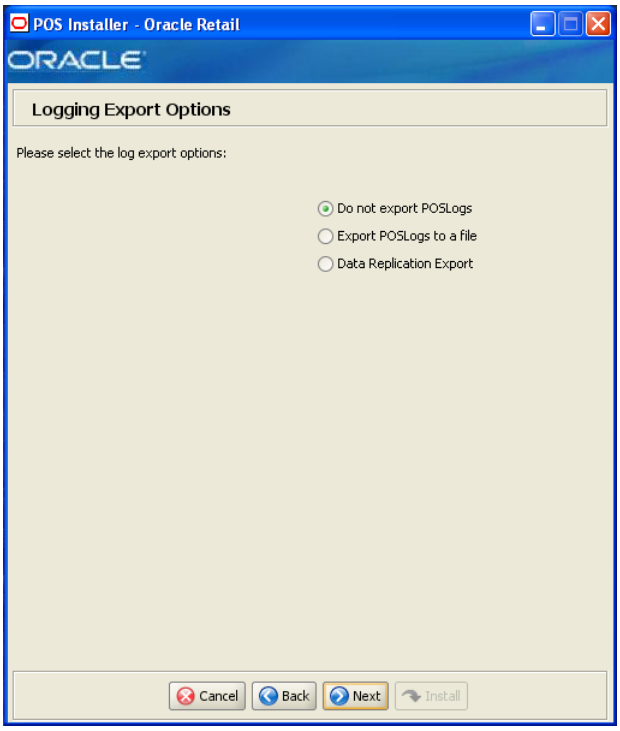
Figure A–47 Logging Detail Options



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

Details	Content
Field Title	Please select the logging detail
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

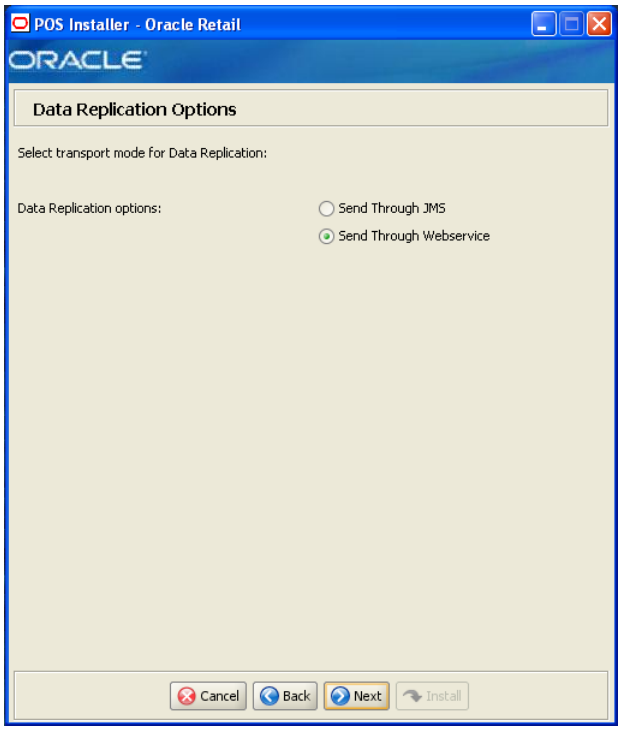


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

Details	Content
Field Title	Please select 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 **Export Point-of-Service logs to a file**. ▪ 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 Data Replication Options

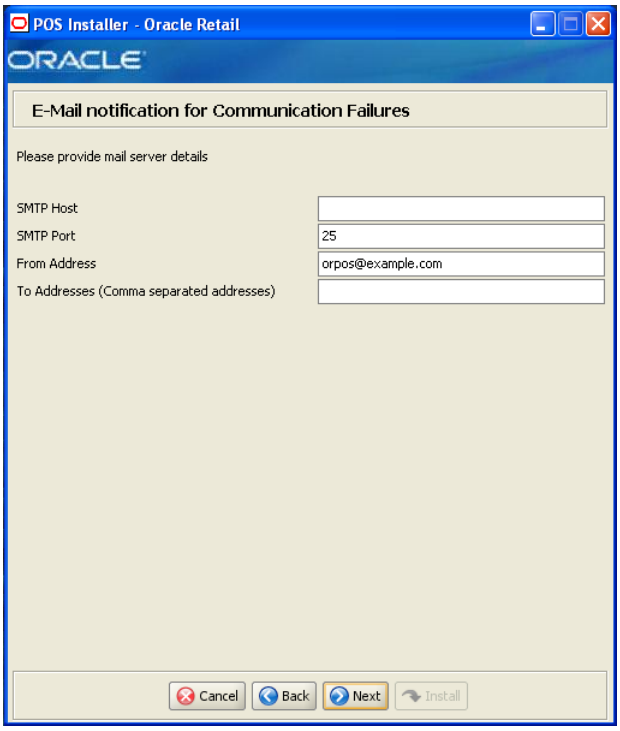


This screen is only displayed if **Data Replication Export** is selected on the Logging Export Options screen.

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

Details	Content
Field Title	Select transport mode for Data Replication
Field Description	Select the transport mode for data replication. ■ To use a JMS queue, choose **Send through JMS**. ■ To use a Web service, choose **Send through Webservice**.
Example	Send through Webservice

Figure A–50 E-mail Notification for Communication Failures



This screen is only displayed if **Send through Webservice** is selected on the Data Replication Options screen.

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

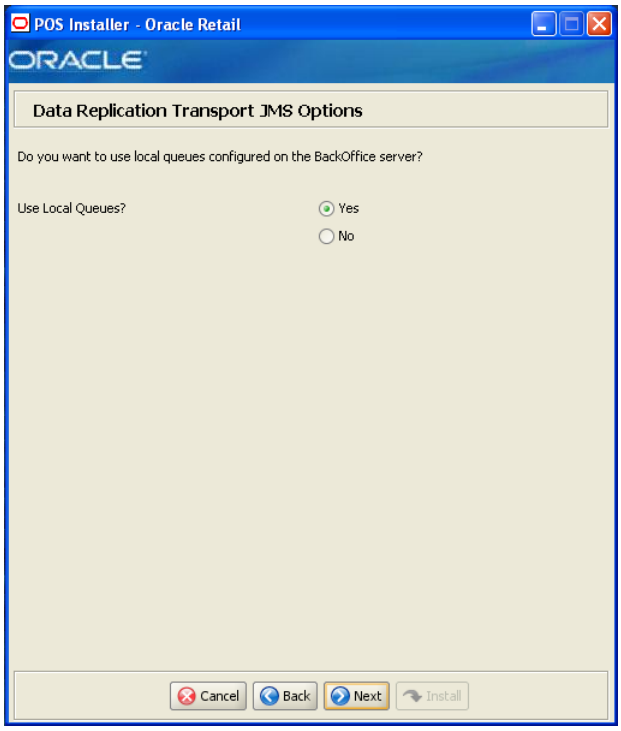
Details	Content
Field Title	SMTP host
Field Description	Host where the SMTP server is running.

Details	Content
Field Title	SMTP Port
Field Description	Enter the SMTP port number.
Example	25

Details	Content
Field Title	From Address
Field Description	Enter the address for sender of the e-mail.
Example	orpos@example.com

Details	Content
Field Title	To Address (Comma Separated Addresses)
Field Description	Enter the addresses for the recipients of the e-mail.

Figure A–51 Data Replication Transport JMS Options

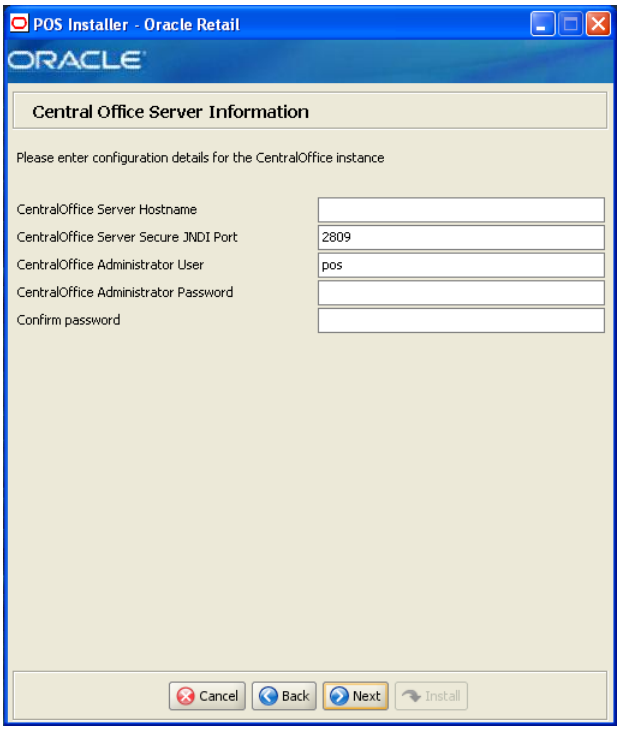


This screen is only displayed if **Send through JMS** is selected on the Data Replication Options screen.

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

Details	Content
Field Title	Use Local Queues?
Field Description	Select whether local queues are used for JMS transport. ■ To use a local queue, choose **Yes**. ■ To not use a local queue, choose **No**.
Example	Yes

Figure A–52 Central Office Server Information



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

To find the JNDI port number, the information is available in:

<WebSphere Application Server install>/profiles/*<profile name>*/logs/AboutThisProfile.txt. BOOTSTRAP_ADDRESS is the port number.

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

Details	Content
Field Title	Central Office Server Hostname
Field Description	Enter the host name for the Central Office application.

Details	Content
Field Title	Central Office Server Secure 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	2809

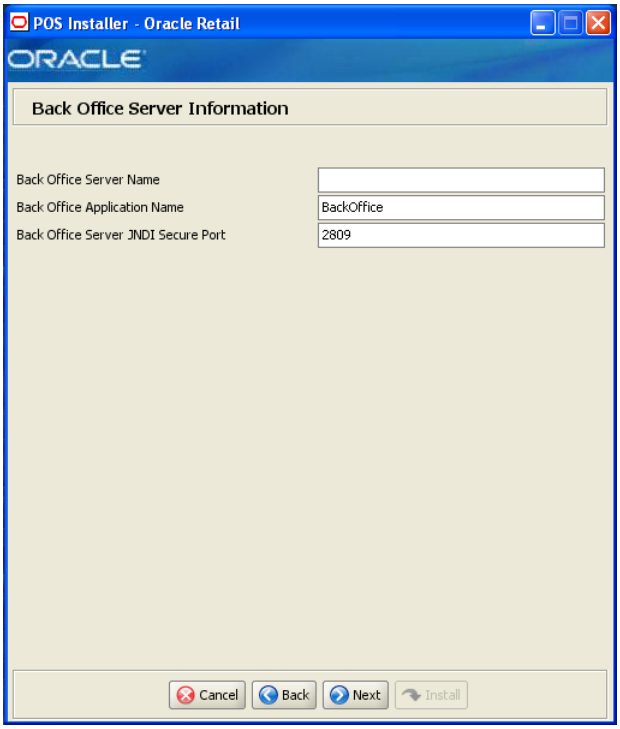
Details	Content
Field Title	Central Office Administrator User

Details	Content
Field Description	Enter the user name for the integration with Central Office. This user does not have to be a user with administration privileges.
Example	pos

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

Details	Content
Field Title	Confirm Password
Field Description	Reentered Central Office Administrator Password used to confirm the password. **Note:** The passwords in the Central Office Administrator Password and Confirm Password fields must match.

Figure A–53 Back Office Server Information



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

To find the JNDI port number, the information is available in:

`<WebSphere Application Server install>/profiles/<profile name>/logs/AboutThisProfile.txt.`
`BOOTSTRAP_ADDRESS` is the port number.

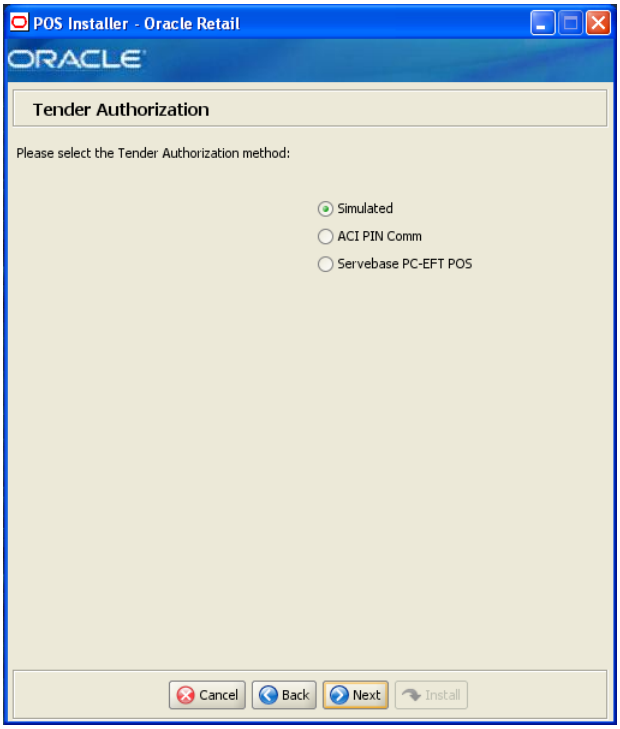
The fields on this screen are described in the following tables.

Details	Content
Field Title	Back Office Server Name
Field Description	Enter the host name for the Back Office application.

Details	Content
Field Title	Back Office Application Name
Field Description	Enter the name for the Back Office application.
Example	BackOffice

Details	Content
Field Title	Back Office Server JNDI Secure Port
Field Description	Enter the port number for the Back Office application.
Example	2809

Figure A–54 Tender Authorization

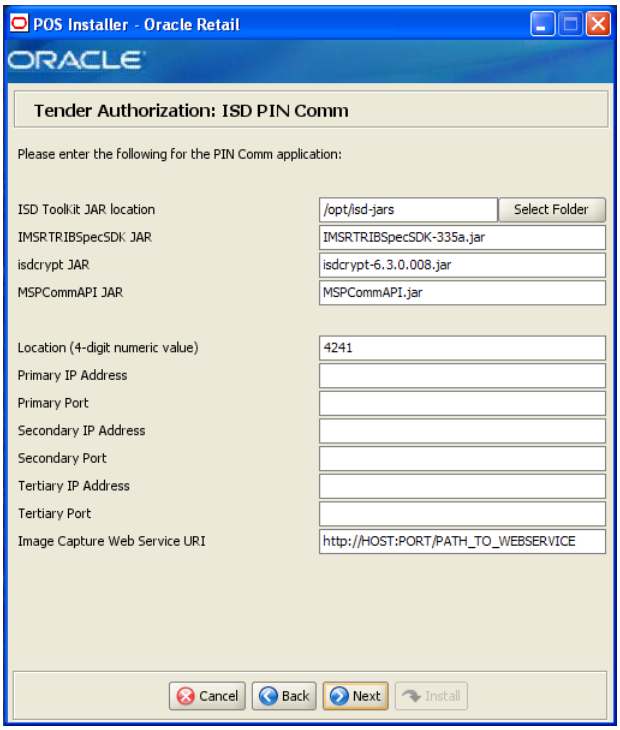


The field on this screen is described in the following table.

Details	Content
Field Title	Please select the tender authorization method

Details	Content
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 **ACI PIN Comm** or **Servebase PC_EFT POS**. **Note:** Demo installations should use the Simulated option.
Example	Simulated

Figure A–55 Tender Authorization: ISD PIN Comm



This screen is only displayed if **ACI PIN Comm** is selected for the Tender Authorization.

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

Details	Content
Field Title	ISD ToolKit JAR Location
Field Description	Enter the path to the ISD ToolKit JAR file.
Example	`/opt/isd-jars`

Details	Content
Field Title	IMSRTRIBSpecSDK JAR
Field Description	Enter the name of the IMSRTRIBSpecSDK JAR file.

Details	Content
Example	`IMSRTRIBSpecSDK-335a.jar`

Details	Content
Field Title	isdcrypt JAR
Field Description	Enter the name of the isdcrypt JAR file.
Example	`isdcrypt-6.3.0.008.jar`

Details	Content
Field Title	MSPCommAPI JAR
Field Description	Enter the name of the MSPCommAPI JAR file.
Example	MSPCommAPI.jar

Details	Content
Field Title	Location (4-digit numeric value)
Field Description	Enter the four digit numeric value for the location.
Example	4241

Details	Content
Field Title	Primary IP Address
Field Description	Enter the primary IP address used for the communication between the store server and the tender authorizer.

Details	Content
Field Title	Primary Port
Field Description	Enter the primary port number used for the communication between the store server and the tender authorizer.

Details	Content
Field Title	Secondary IP Address
Field Description	Enter the secondary IP address used for the communication between the store server and the tender authorizer.

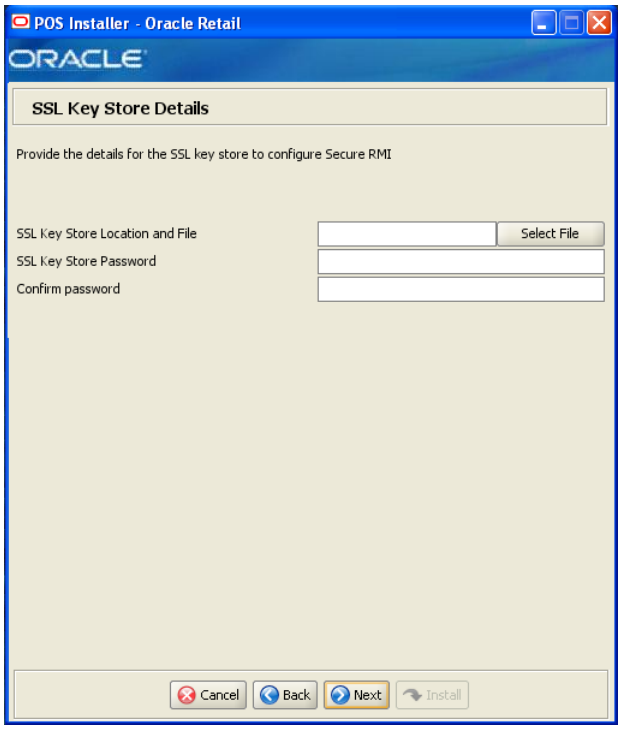
Details	Content
Field Title	Secondary Port
Field Description	Enter the secondary port number used for the communication between the store server and the tender authorizer.

Details	Content
Field Title	Tertiary IP Address
Field Description	Enter the tertiary IP address used for the communication between the store server and the tender authorizer.

Details	Content
Field Title	Tertiary Port
Field Description	Enter the tertiary port number used for the communication between the store server and the tender authorizer.

Details	Content
Field Title	Image Capture Web Service URI
Field Description	Enter the address of the Image Capture Web service.
Example	`http://HOST:PORT/PATH_TO_WEBSERVICE`

Figure A–56 SSL Key Store Details



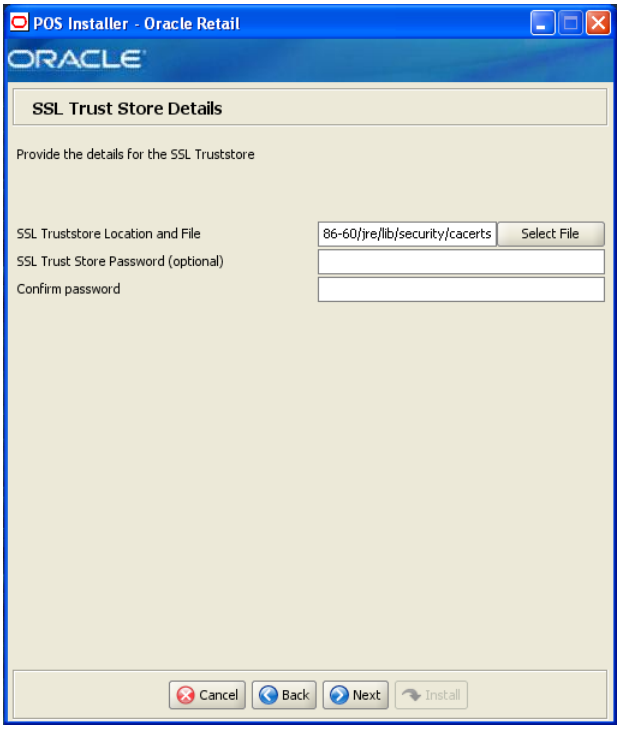
The fields on this screen are described in the following tables.

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

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

Details	Content
Field Title	Confirm Password
Field Description	Reentered SSL Key Store Password used to confirm the password. **Note:** The passwords in the SSL Key Store Password and Confirm Password fields must match.

Figure A–57 SSL Trust Store Details



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

Details	Content
Field Title	SSL Truststore Location and File
Field Description	Enter the location and name of the truststore file.
Example	`/opt/ibm/java-i386-60/security/cacerts`

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

Details	Content
Field Title	Confirm Password
Field Description	Reentered SSL Trust Store Password used to confirm the password. **Note:** The passwords in the SSL Trust Store Password and Confirm Password fields must match.

Figure A–58 Installation Progress

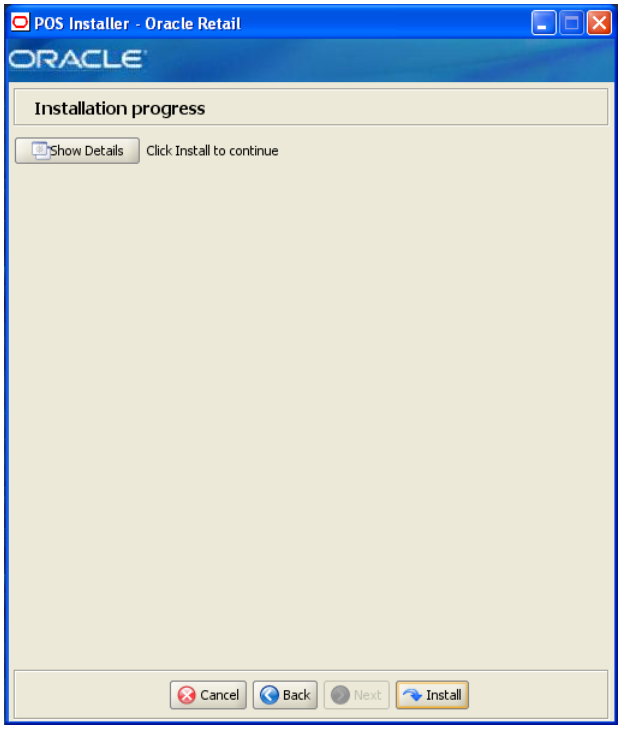
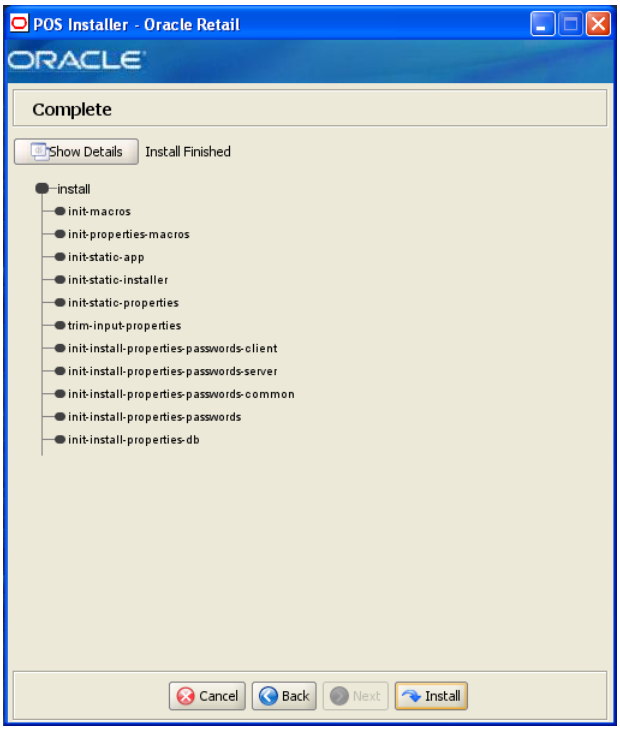


Figure A–59 Install Complete



B

Appendix: Installer Screens for Client Installation on SLEPOS

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 IBM stack. 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 server installation on the IBM stack, see Appendix A.

Figure B–1 Introduction

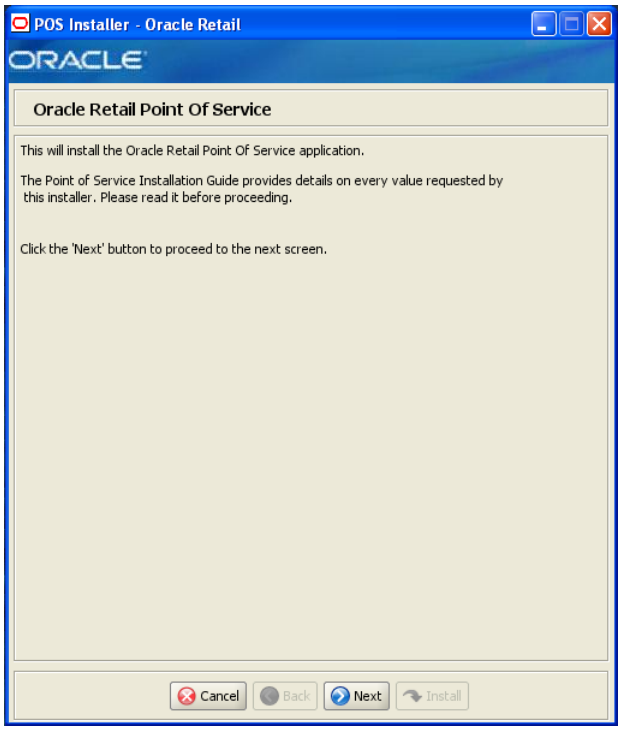


Figure B–2 Previous POS Install

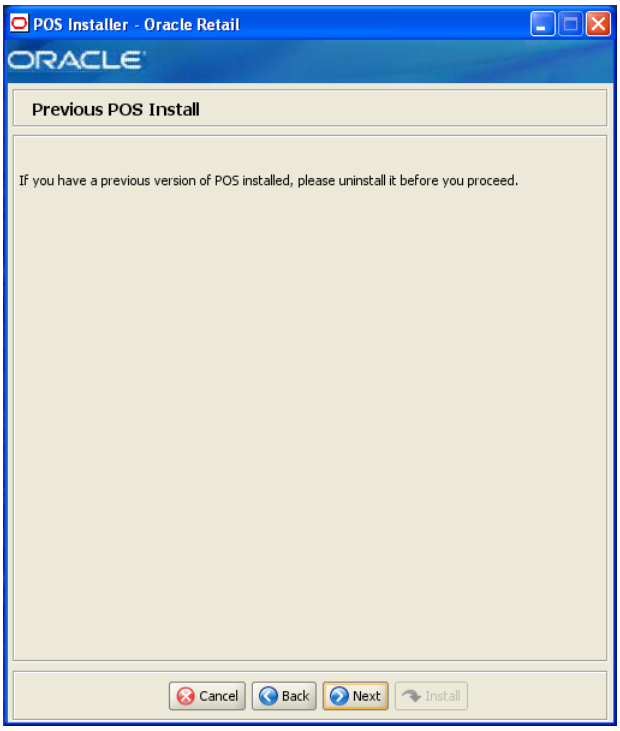
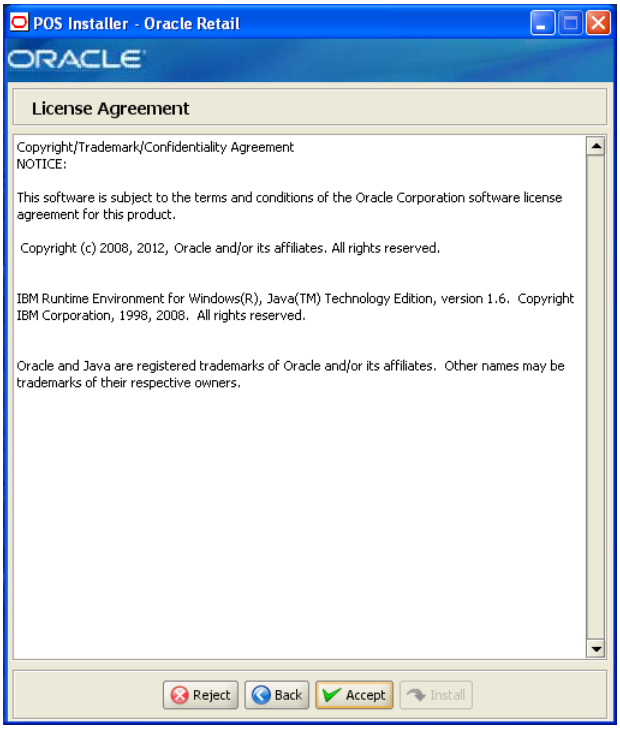
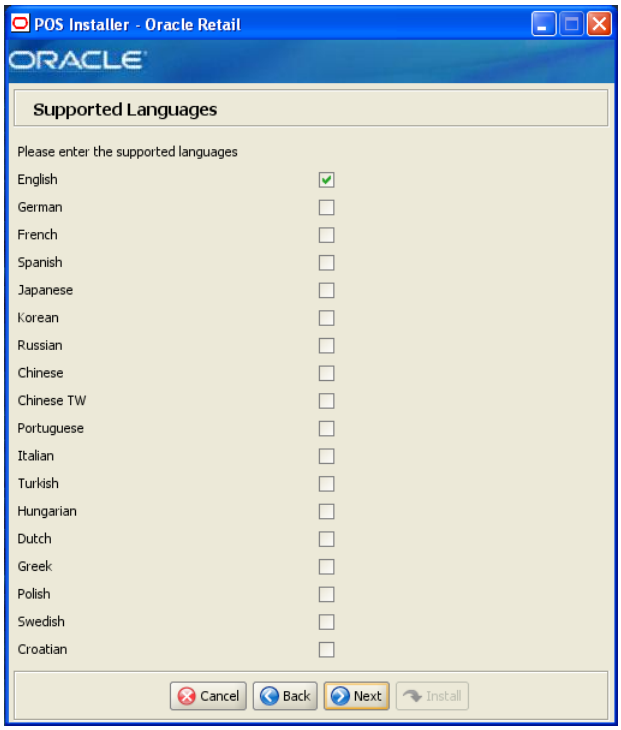


Figure B–3 License Agreement



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.

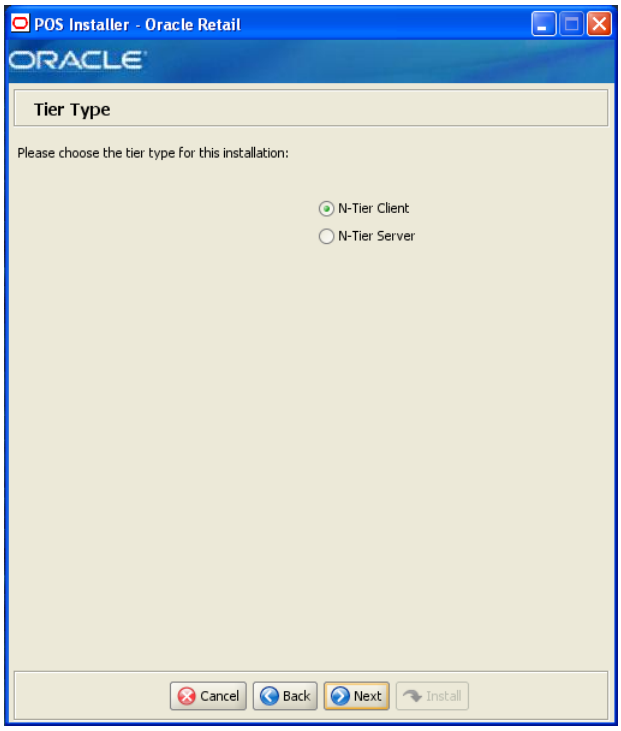
Details	Content
Field Title	Please enter the supported languages
Field Description	Select the languages that will be available for the Point-of-Service application. The languages selected on this screen determine the available choices on the Enter Default Locale screen.
Example	English

Figure B–5 Enter Default Locale

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

Details	Content
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

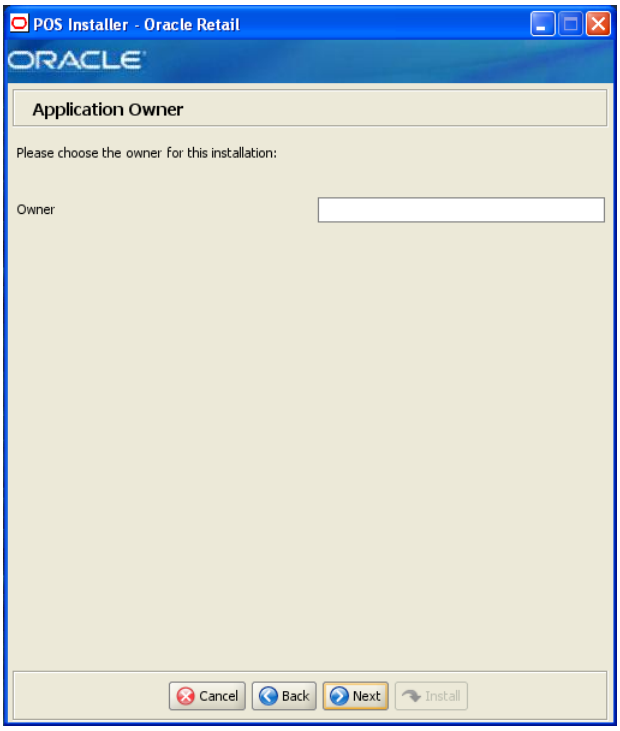
Figure B–6 Tier Type



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

Details	Content
Field Title	Tier Type
Field Description	Choose the server tier type for this installation. For more information, see "Determining Tier Type" in Chapter 3. To install the N-Tier version of the client, choose **N-Tier Client**.
Example	N-Tier Client

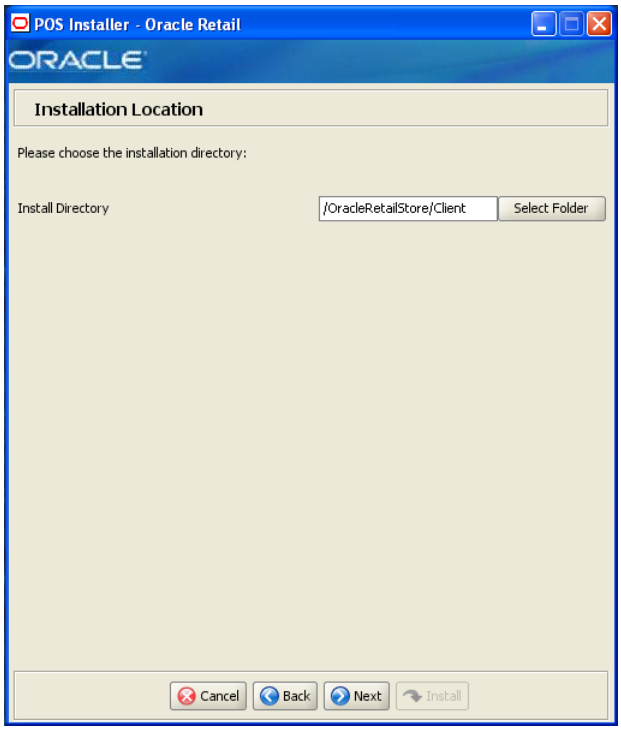
Figure B–7 Application Owner



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

Details	Content
Field Title	Owner
Field Description	Enter the operating system user who will be the owner for this installation.

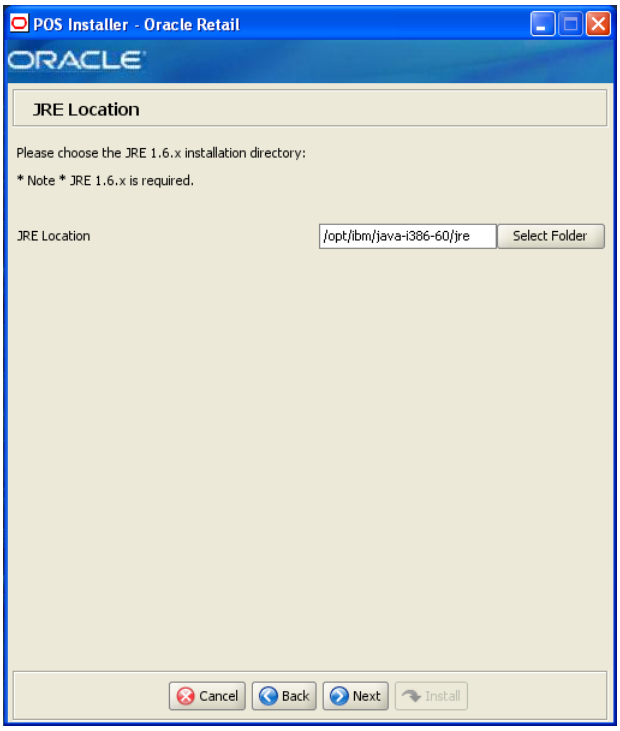
Figure B–8 Installation Location



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

Details	Content
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	`/OracleRetailStore/Client`

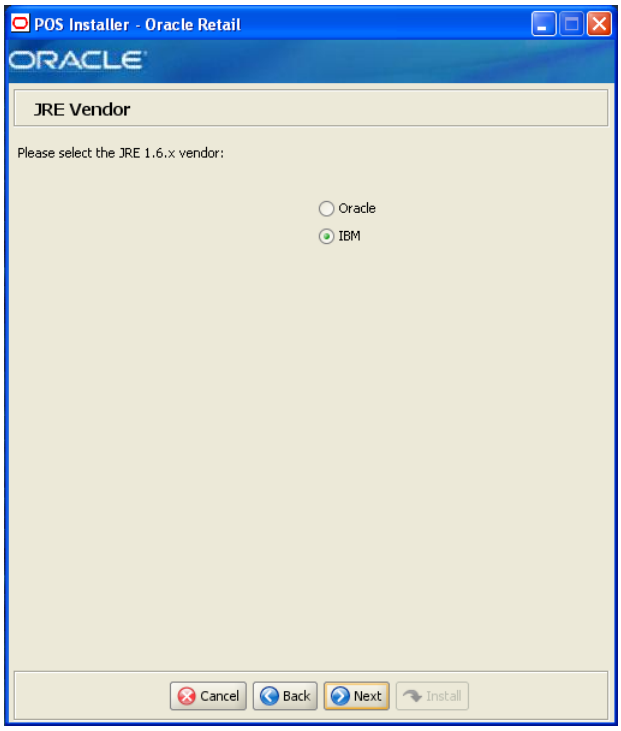
Figure B–9 JRE Location



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

Details	Content
Field Title	JRE Location
Field Description	Enter the location where the JRE is installed.
Example	`/opt/ibm/java-i386-60/jre6`

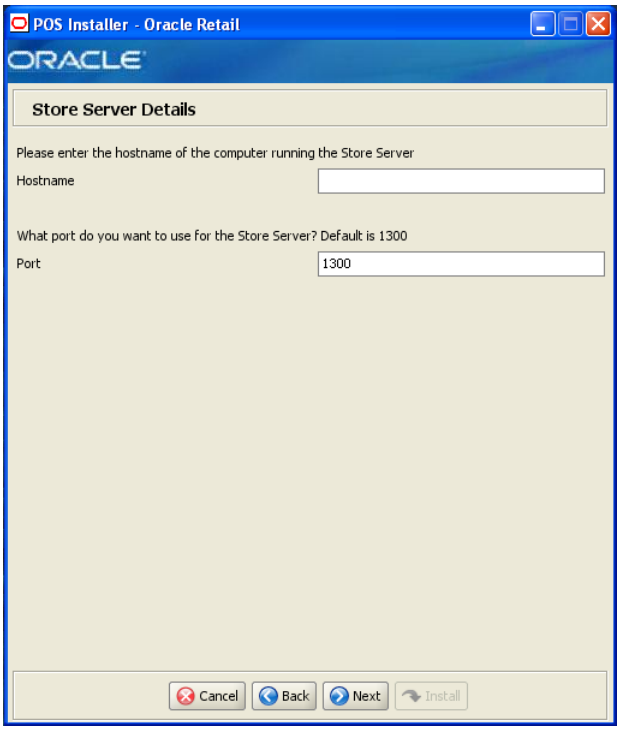
Figure B–10 JRE Vendor



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

Details	Content
Field Title	Please select the JRE 1.6.x vendor
Field Description	Select the vendor for the JRE entered on the JRE Location screen: ■ Oracle ■ IBM Choose **IBM**.

Figure B–11 Store Server Details

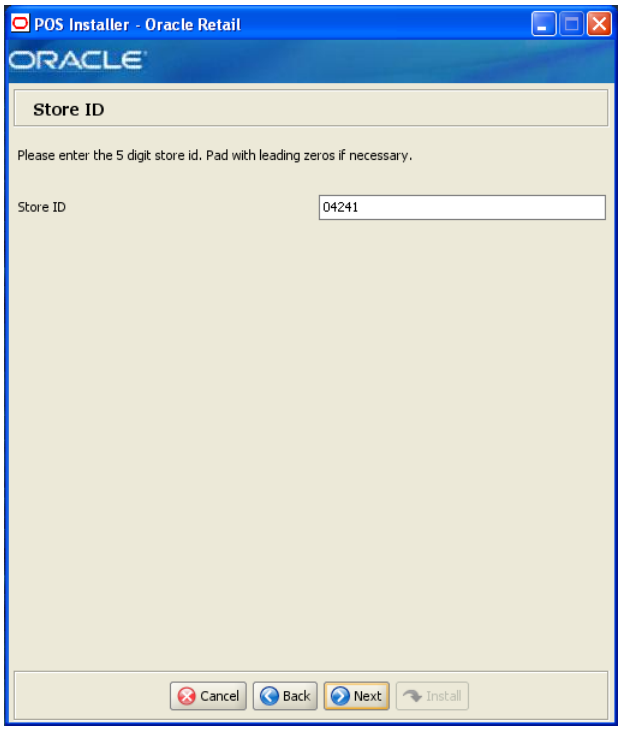


The fields on this screen are described in the following tables.

Details	Content
Field Title	Hostname
Field Description	Enter the host name of the store server.

Details	Content
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

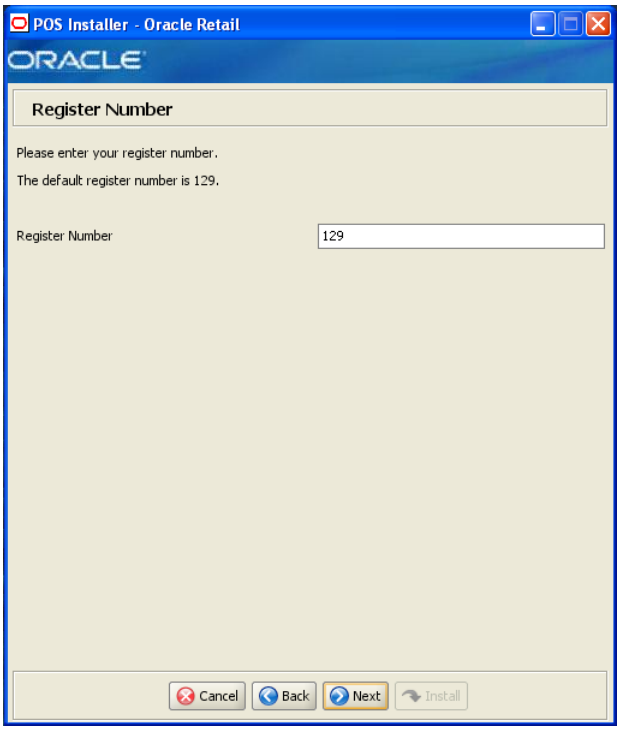
Figure B–12 Store ID



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

Details	Content
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

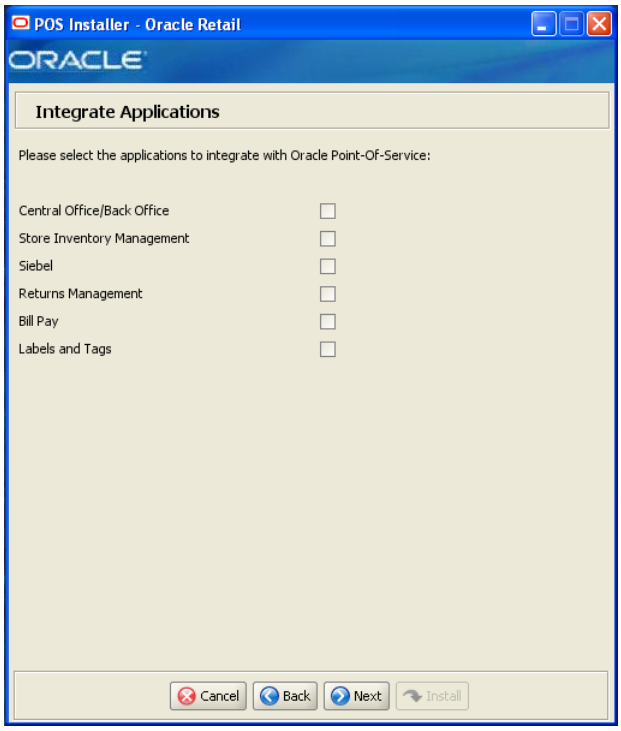
Figure B–13 Register Number



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

Details	Content
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.

Details	Content
Field Title	Please select the applications to integrate with Oracle Point-of-Service
Field Description	Select the applications that Point-of-Service is integrated with. ■ Central Office/Back Office ■ Store Inventory Management ■ Siebel ■ Returns Management ■ Bill Pay

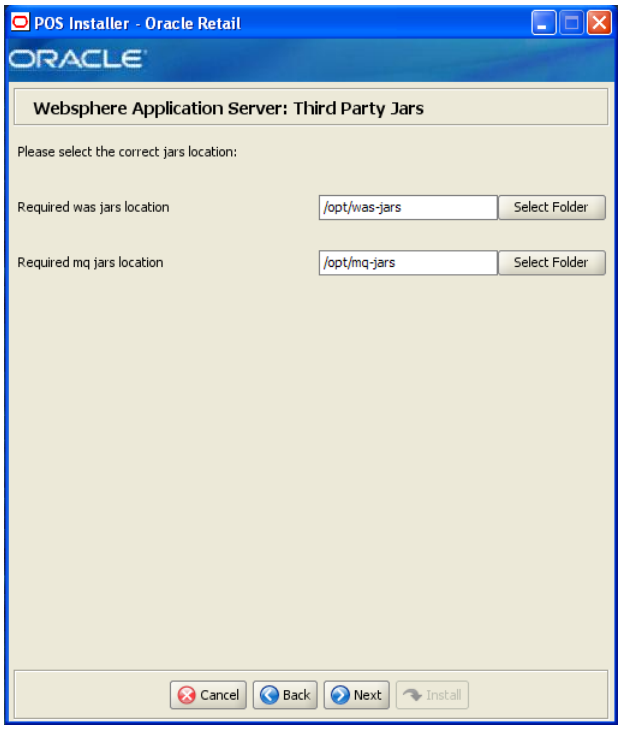
Figure B–15 Application Server Type

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.

Details	Content
Field Title	Please select the application server you would like to user
Field Description	Select the application server to be used for the store server. ▪ WebLogic Application Server ▪ Websphere Application Server Choose **Websphere Application Server**.

Figure B–16 Websphere Application Server: Third Party Jars



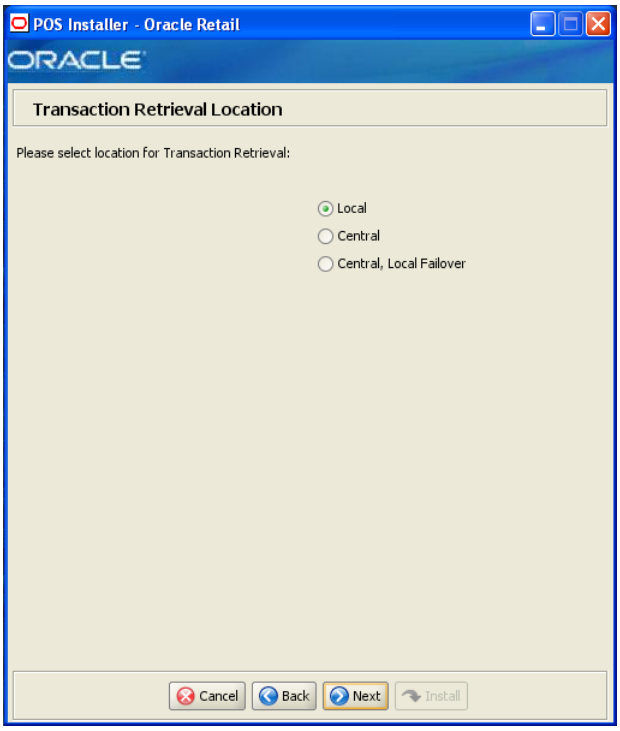
This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

Details	Content
Field Title	Required was jars location
Field Description	Choose the location of the was jars file. See "Obtain the Third-Party Library Files Required by Point-of-Service" in Chapter 3 for the list of required jar files.
Example	`/opt/was-jars`

Details	Content
Field Title	Required mq jars location
Field Description	Choose the location of the mq jars file. See "Obtain the Third-Party Library Files Required by Point-of-Service" in Chapter 3 for the list of required jar files.
Example	`/opt/mq-jars`

Figure B–17 Transaction Retrieval Location

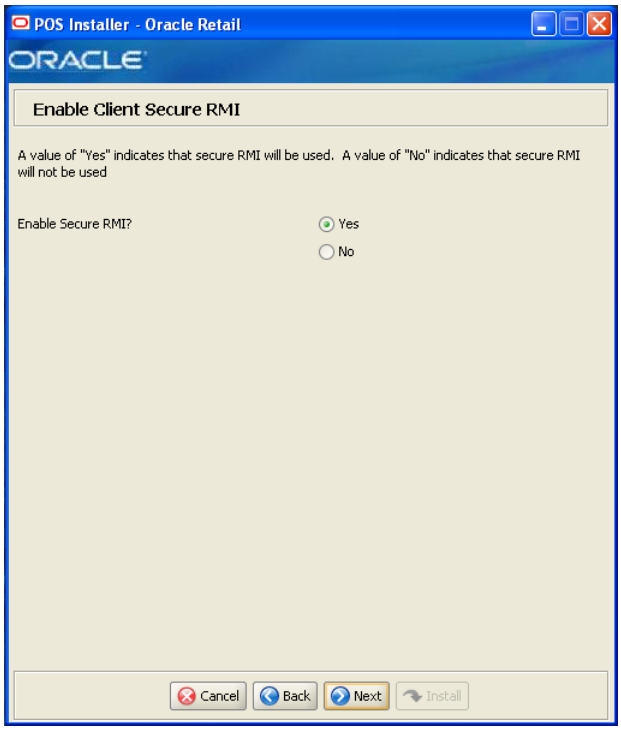


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

Details	Content
Field Title	Please select location for Transaction Retrieval
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

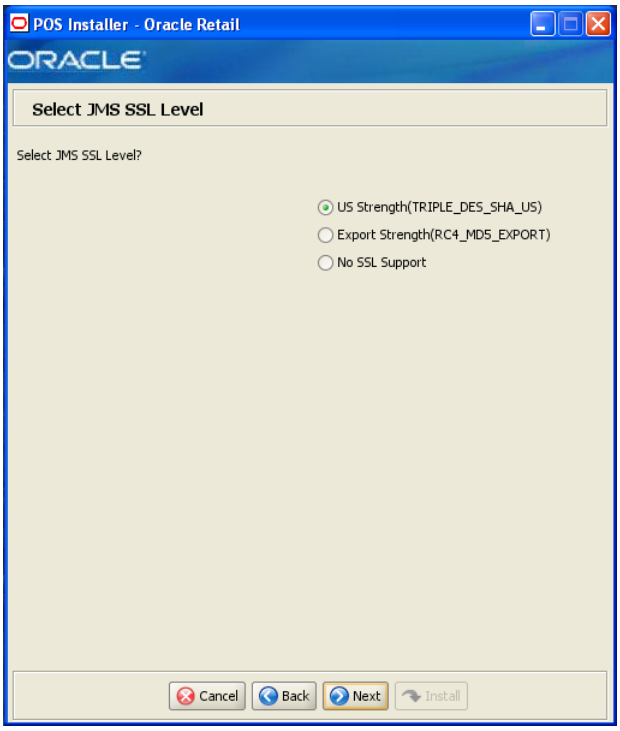
Figure B–18 Enable Client Secure RMI



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

Details	Content
Field Title	Enable SecureRMI?
Field Description	Select whether secure RMI is to be used for communication between the store server and registers. **Note:** If **Yes** is selected, secure RMI must also have been configured for the store server.
Example	Yes

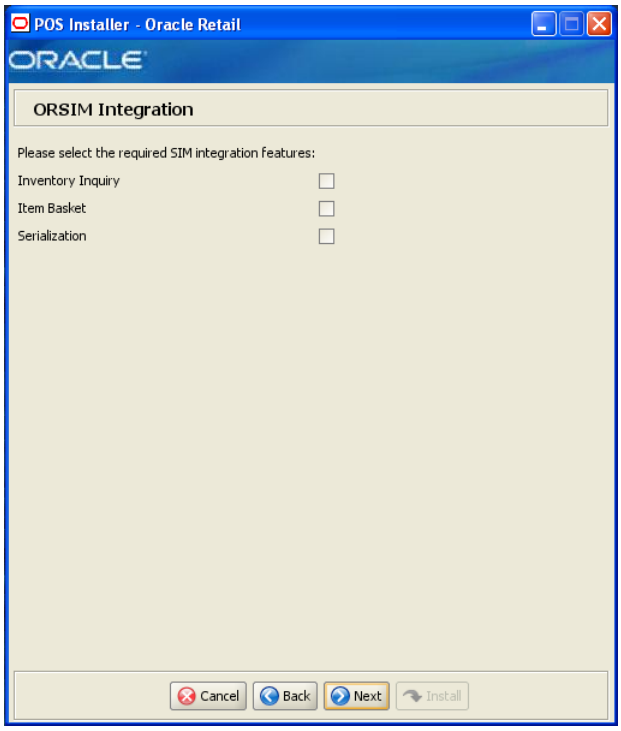
Figure B–19 Select JMS SSL Level



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

Details	Content
Field Title	Select JMS SSL Level
Field Description	JMS SSL level to be used. ■ To use US strength, select **US Strength(TRIPLE_DES_SHA_US)**. US Strength requires that the JCE policy jar files are installed. See "Install the Java Cryptography Extension (JCE)". ■ To use export strength, select **Export Strength(RC4_MDS_EXPORT)**. ■ To not use ssl support, select **No SSL Support**.
Example	US Strength(TRIPLE_DES_SHA_US)

Figure B–20 ORSIM Integration

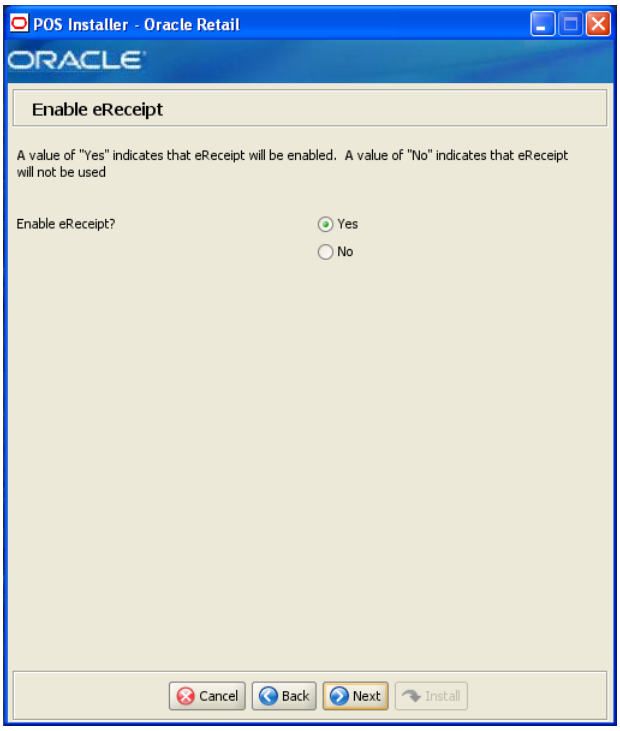


This screen is only displayed if **Store Inventory Management** is selected on the Integrate Applications screen.

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

Details	Content
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 enable item baskets created using SIM, select **Item Basket**. ■ To enable serialization using SIM, select **Serialization**.

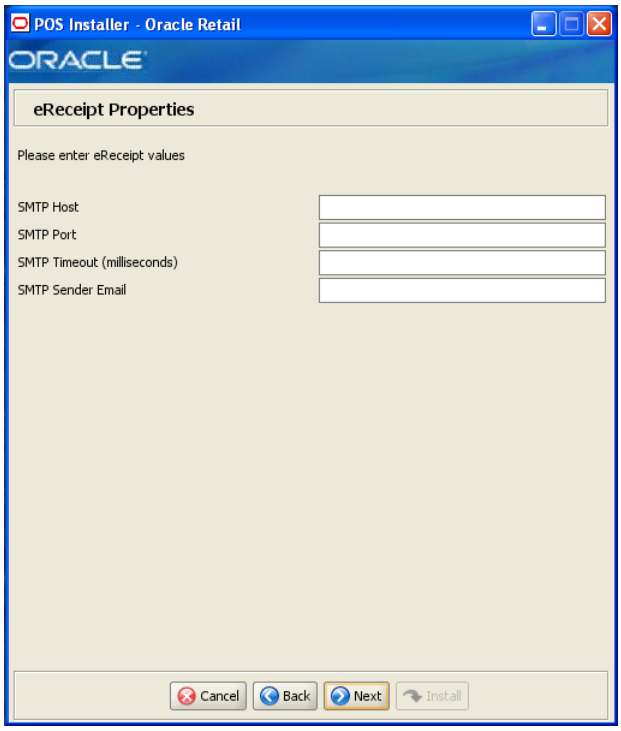
Figure B–21 Enable eReceipt



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

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

Figure B–22 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.

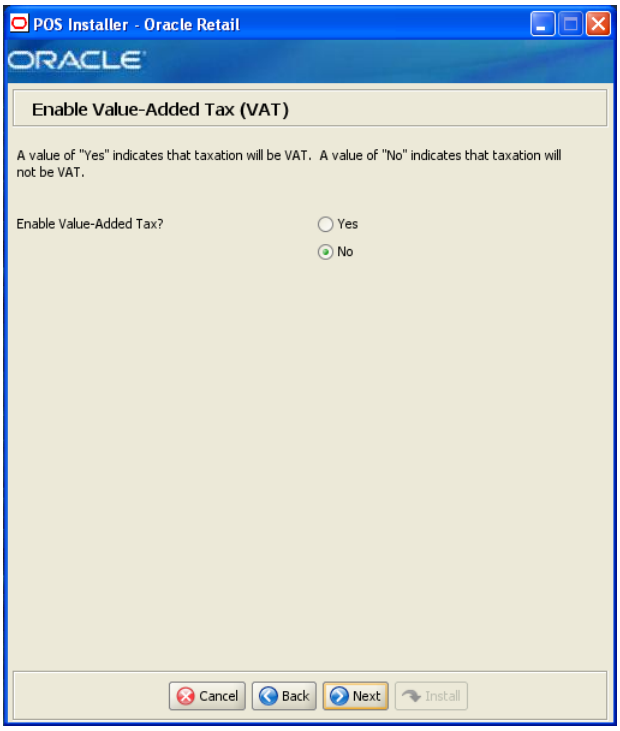
Details	Content
Field Title	SMTP Host
Field Description	Enter the host name for the SMTP server.

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

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

Details	Content
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–23 Enable Value-Added Tax (VAT)



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

Details	Content
Field Title	Enable Value-Added Tax?
Field Description	Select Yes if Value-Added Tax is used.
Example	No

Figure B–24 Security Setup: Key Manager Settings

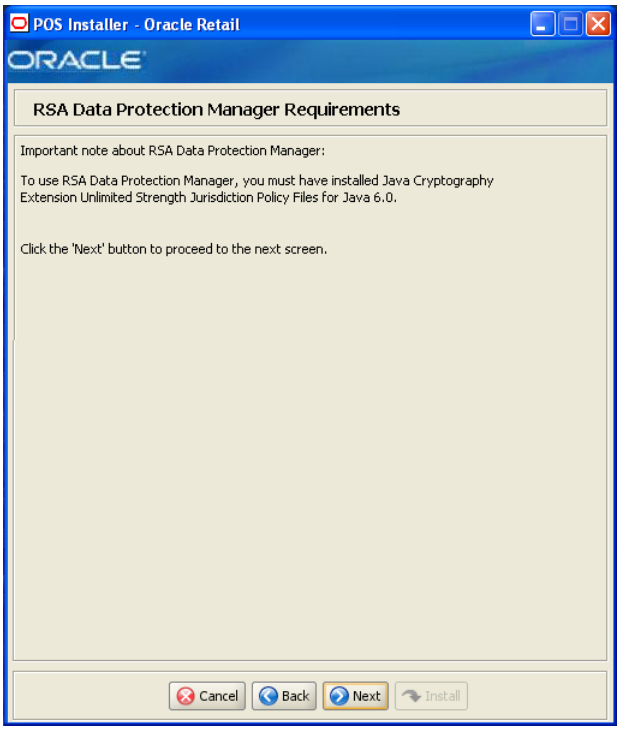
This screen is used to configure the Encryption Key Manager.

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

Details	Content
Field Title	Hash Algorithm
Field Description	Name of the algorithm used by the Key Manager to hash sensitive data.
Example	SHA-256

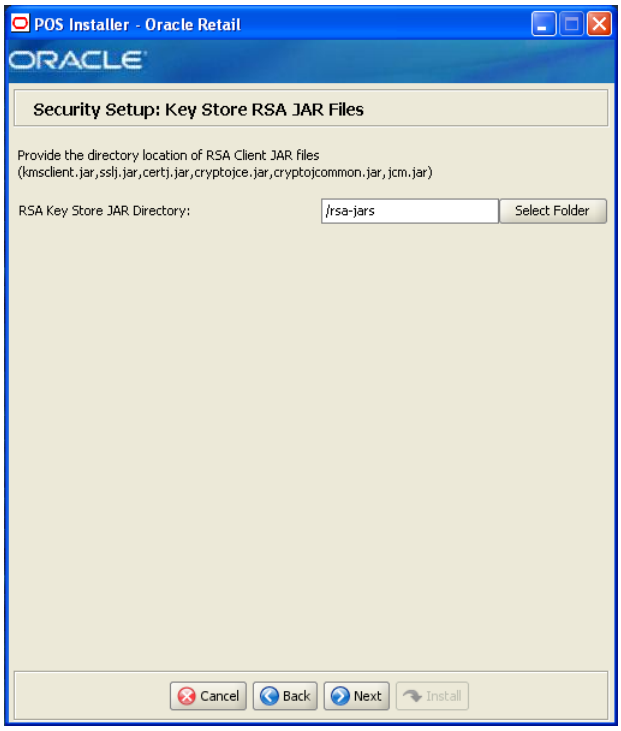
Details	Content
Field Title	Select Key Manager
Field Description	Provider for Key Manager: ■ To use the RSA Data Protection Manager, select **RSA Data Protection Manager**. The next screen displayed is Figure B–25. ■ To use the simulated key management package, select **Simulator**. The next screen displayed is Figure B–28.
Example	RSA Data Protection Manager

Figure B–25 RSA Data Protection Manager Requirements



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

Figure B–26 Security Setup: Key Store RSA JAR Files



This screen is only displayed if **RSA Data Protection Manager** is selected for the Key Manager on the Security Setup: Key Manager Settings screen.

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

Details	Content
Field Title	RSA Key Store JAR Directory
Field Description	Choose the directory where the following Key Store jar files are located: ■ certj.jar ■ cryptojce.jar ■ cryptojcommon.jar ■ jcm.jar ■ kmsclient.jar ■ sslj.jar
Example	`/rsa-jars`

Figure B–27 RSA Client Configuration

This screen is only displayed if **RSA Data Protection Manager** is selected for the Key Manager on the Security Setup: Key Manager Settings screen.

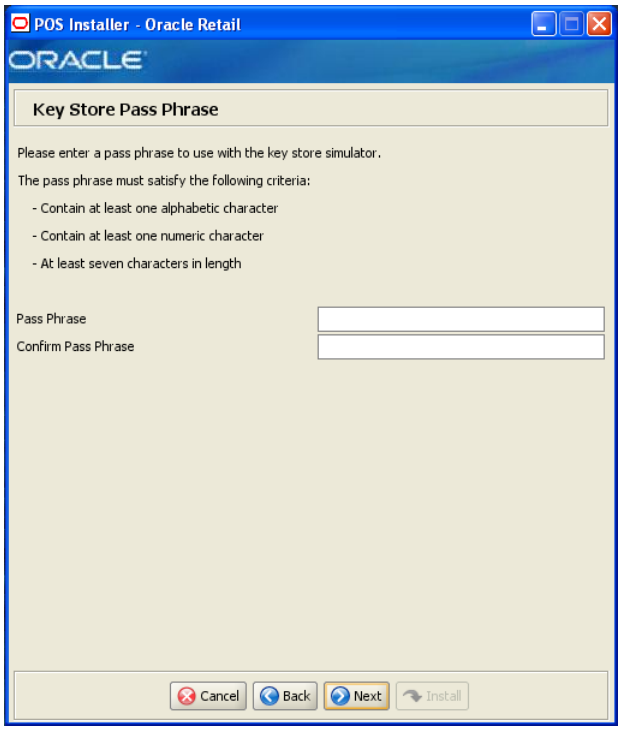
The fields on this screen are described in the following tables.

Details	Content
Field Title	Cipher Key Class
Field Description	Enter the name of the cipher suite that defines the authentication and encryption algorithms that will be used by RSA to negotiate the security settings for the network connection.

Details	Content
Field Title	RSA Client Configuration File
Field Description	Select the location of the RSA client configuration file. This file contains the details for configuring the RSA client.

Details	Content
Field Title	Generate a new client.app.name value
Field Description	To have the installer generate a unique name for the client.app.name value in the RSA client configuration file, select **Yes**. To not change the value in the configuration file, select **No**.
Example	No

Figure B–28 Key Store Pass Phrase for Simulator Key Manager



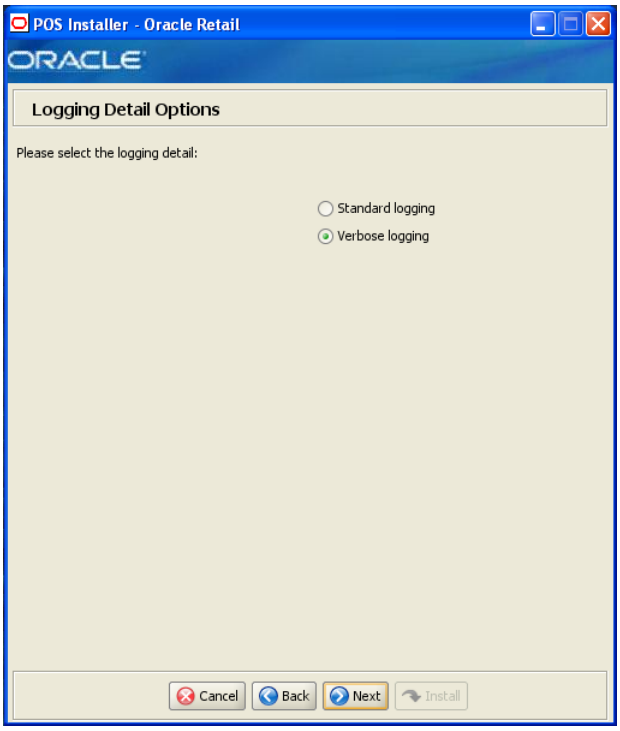
This screen is only displayed if **Simulator** is selected for the Key Manager on the Security Setup: Key Manager Settings screen.

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

Details	Content
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.

Details	Content
Field Title	Confirm Pass Phrase
Field Description	Reentered Pass Phrase used to confirm the pass phrase. **Note:** The pass phrases in the Pass Phrase and Confirm Pass Phrase fields must match.

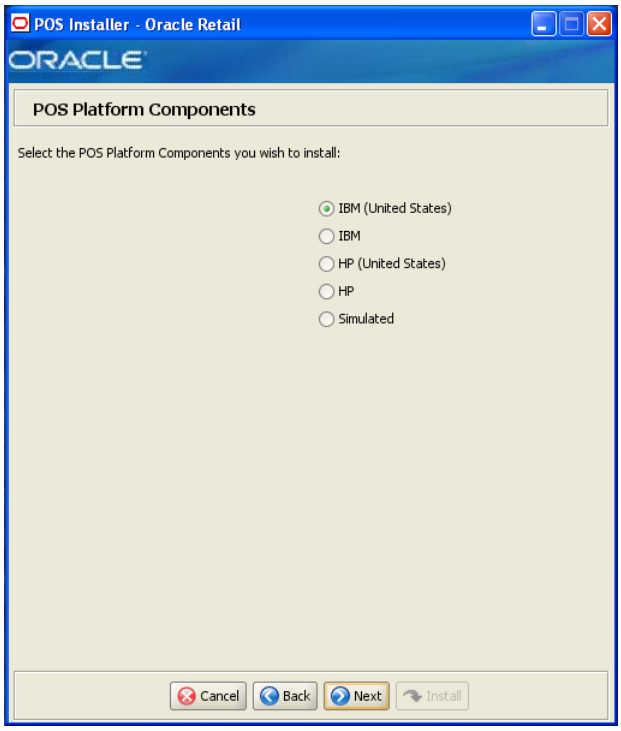
Figure B–29 Logging Detail Options



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

Details	Content
Field Title	Please select the logging detail
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

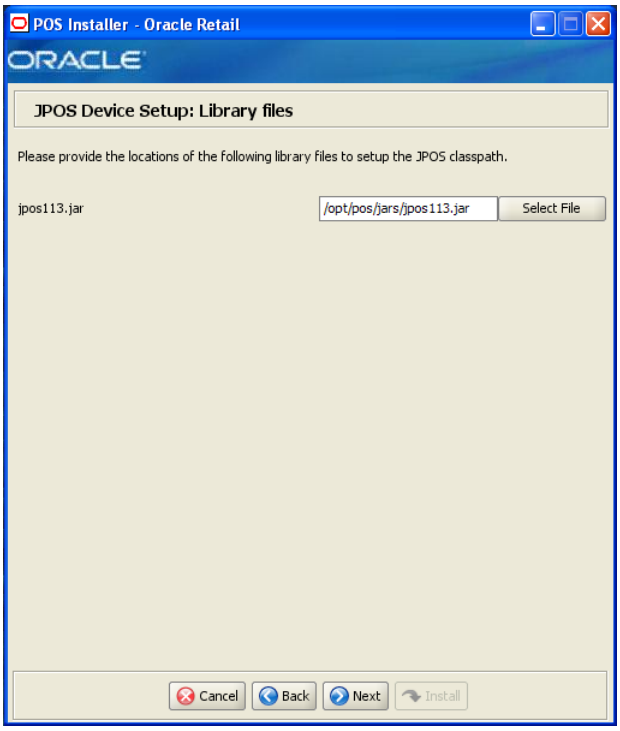
Figure B–30 POS Platform Components



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

Details	Content
Field Title	Select the POS Platform Components you wish to install
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 IBM register with devices intended for use in the United States, select **IBM (United States)**. ▪ To use an IBM register with devices intended for use outside the United States, select **IBM**. ▪ To use an HP register with devices intended for use in the United States, select **HP (United States)**. ▪ To use an HP register with devices intended for use outside the United States, select **HP**. ▪ To use a register with no devices, select **Simulated**. This should only be selected for a development environment. A network printer may be used. **Note:** Only IBM (United States), IBM, and Simulated are supported when running SLEPOS on the IBM stack.
Example	IBM (United States)

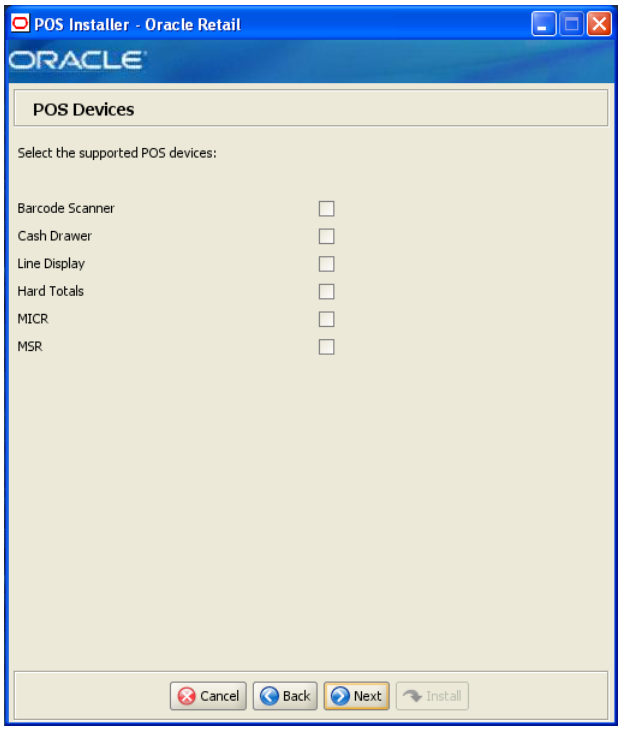
Figure B–31 JPOS Device Setup: Library Files



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

Details	Content
Field Title	jpos113.jar
Field Description	Enter the location of the jar file.
Example	`/opt/pos/jars/pos113.jar`

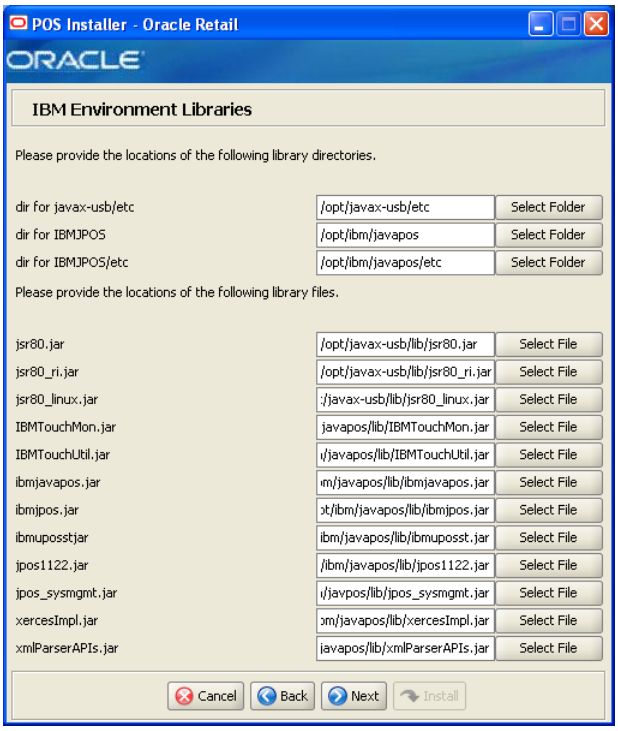
Figure B–32 POS Devices



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

Details	Content
Field Title	POS Devices
Field Description	Choose the devices to be attached to the client register.

Figure B–33 IBM Environment Libraries



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

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

Details	Content
Field Title	dir for javax-usb/etc
Field Description	Enter the location of the jar file.
Example	`/opt/javax-usb/etc`

Details	Content
Field Title	dir for IBMJPOS
Field Description	Enter the location of the jar file.
Example	`/opt/ibm/javapos`

Details	Content
Field Title	dir for IBMJPOS/etc
Field Description	Enter the location of the jar file.
Example	`/opt/ibm/javapos/etc`

Details	Content
Field Title	jsr80.jar

Details	Content
Field Description	Enter the location of the jar file.
Example	`/opt/javax-usb/lib/jsr80.jar`

Details	Content
Field Title	jsr80_ri.jar
Field Description	Enter the location of the jar file.
Example	`/opt/javax-usb/lib/jsr80_ri.jar`

Details	Content
Field Title	jsr80_linux.jar
Field Description	Enter the location of the jar file.
Example	`/opt/javax-usb/lib/jsr80_linux.jar`

Details	Content
Field Title	IBMTouchMon.jar
Field Description	Enter the location of the jar file.
Example	`/opt/ibm/javapos/lib/IBMTouchMon.jar`

Details	Content
Field Title	IBMTouchUtil.jar
Field Description	Enter the location of the jar file.
Example	`/opt/ibm/javapos/lib/IBMTouchUtil.jar`

Details	Content
Field Title	ibmjavapos.jar
Field Description	Enter the location of the jar file.
Example	`/opt/ibm/javapos/lib/ibmjavapos.jar`

Details	Content
Field Title	ibmjpos.jar
Field Description	Enter the location of the jar file.
Example	`/opt/ibm/javapos/lib/ibmjpos.jar`

Details	Content
Field Title	ibmupposst.jar
Field Description	Enter the location of the jar file.

Details	Content
Example	`/opt/ibm/javapos/lib/ibmuposst.jar`

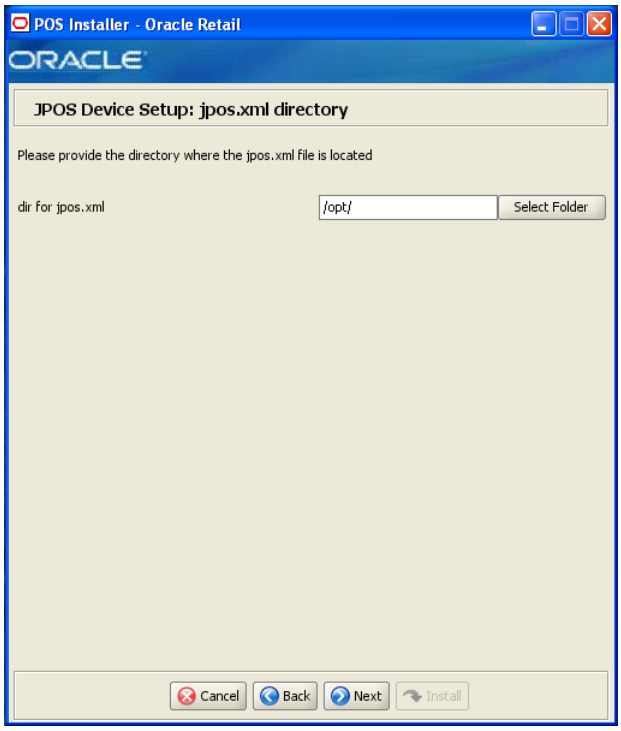
Details	Content
Field Title	jpos1122.jar
Field Description	Enter the location of the jar file.
Example	`/opt/ibm/javapos/lib/jpos1122.jar`

Details	Content
Field Title	jpos_sysmgmt.jar
Field Description	Enter the location of the jar file.
Example	`/opt/ibm/javapos/lib/jpos_sysmgmt.jar`

Details	Content
Field Title	xercesImpl.jar
Field Description	Enter the location of the jar file.
Example	`/opt/ibm/javapos/lib/xercesImpl.jar`

Details	Content
Field Title	xmlParserAPIs.jar
Field Description	Enter the location of the jar file.
Example	`/opt/ibm/javapos/lib/xmlParserAPIs.jar`

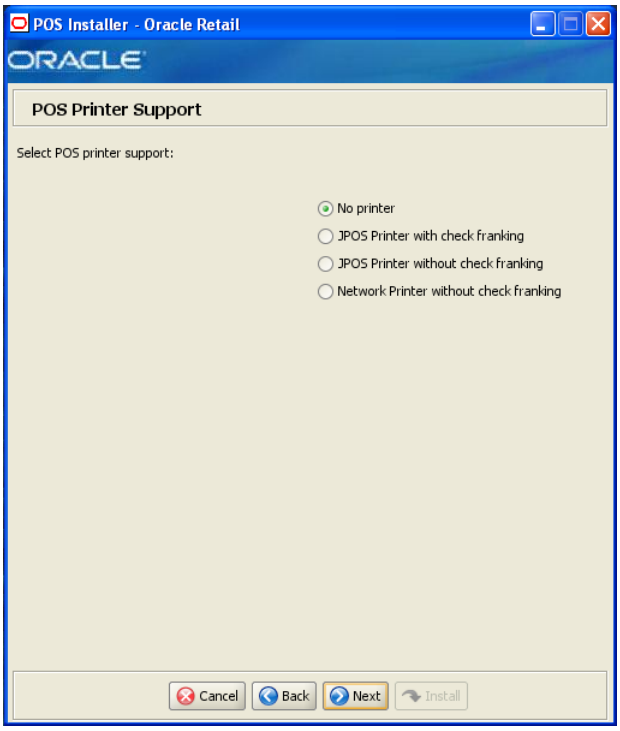
Figure B–34 JPOS Device Setup: jpos.xml directory



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

Details	Content
Field Title	dir for jpos.xml
Field Description	Enter the location of the directory.
Example	`/opt/`

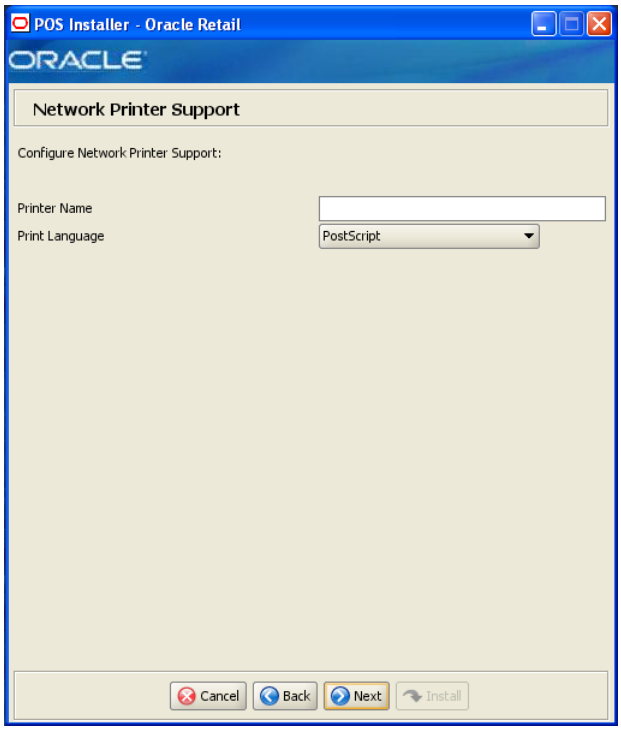
Figure B–35 POS Printer Support



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

Details	Content
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	No Printer

Figure B–36 Network Printer Support Configuration



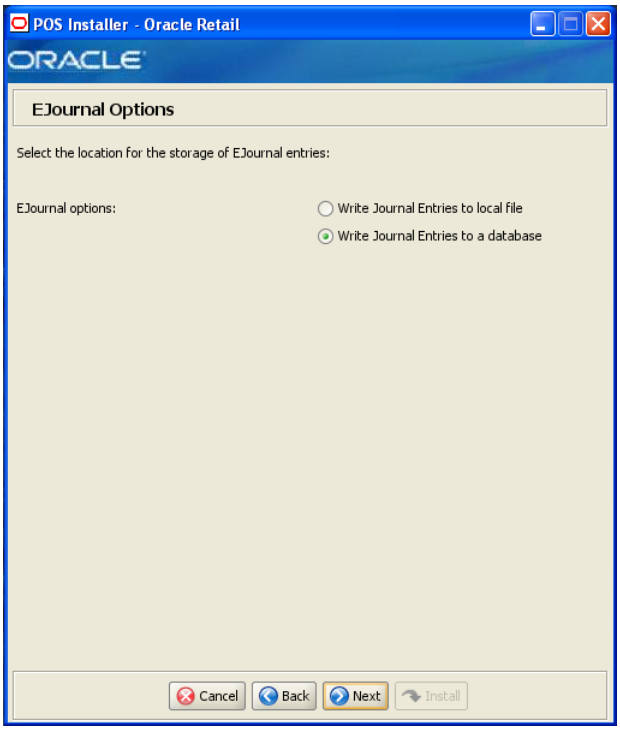
This screen is only displayed if **Network Printer without check franking** is selected on the POS Printer Support screen.

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

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

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

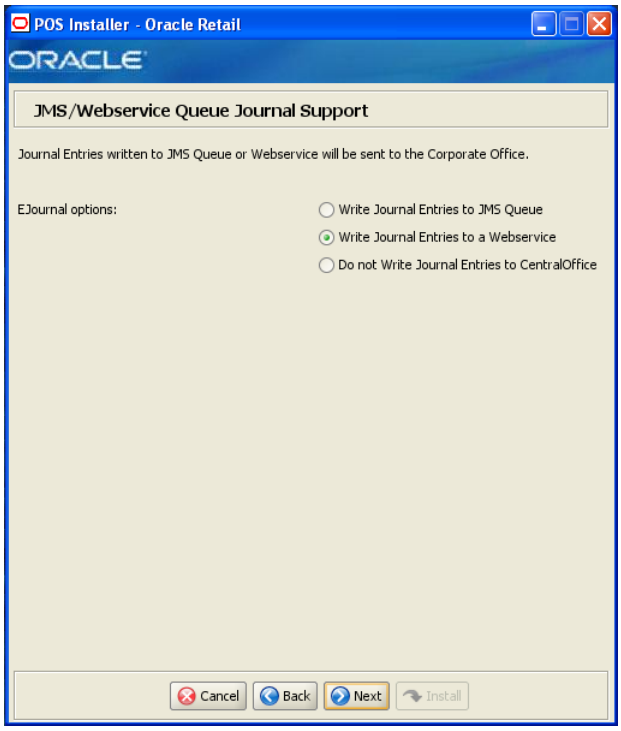
Figure B–37 EJournal Options



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

Details	Content
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–38 JMS/Webservice Queue Journal Support

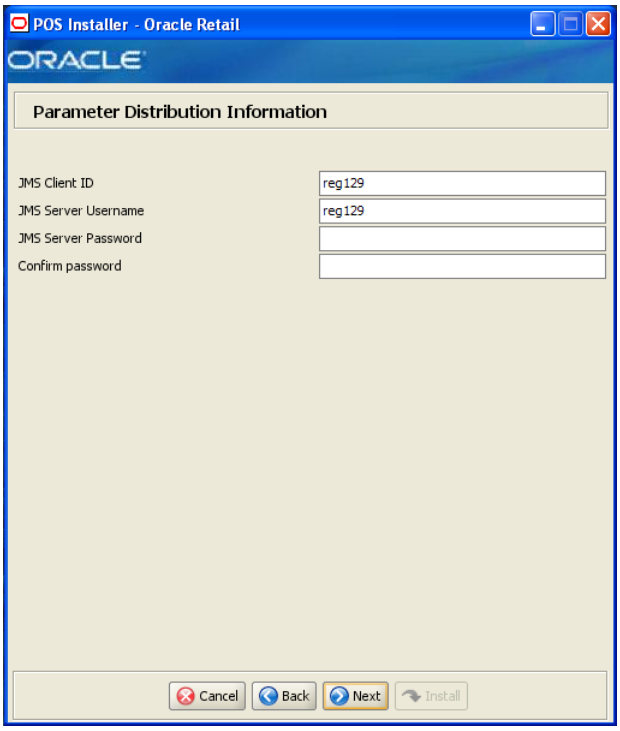


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

Details	Content
Field Title	EJournal Options
Field Description	Select an option for journaling. Journal entries written to a JMS queue or Web service are sent to the corporate office. ▪ Write Journal Entries to JMS Queue ▪ Write Journal Entries to a Webservice ▪ Do not Write Journal Entries to CentralOffice **Note:** The same selection must be made for the server and the client.
Example	Write Journal Entries to a Webservice

Figure B–39 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.

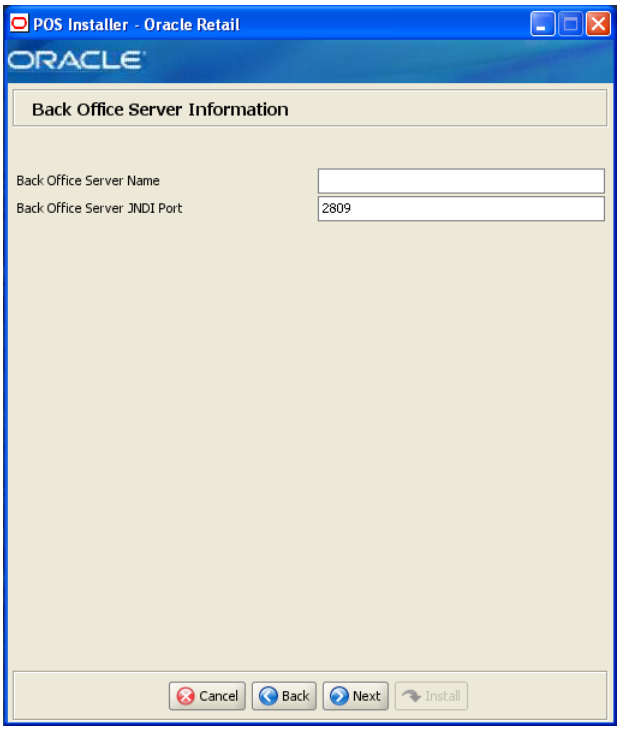
Details	Content
Field Title	JMS Client ID
Field Description	Identifier of the JMS client used for receiving parameter updates.
Example	reg129

Field Title	JMS Username
Field Title	JMS Username
Field Description	Identifier of the JMS user for receiving parameter updates.
Example	reg129 **Note:** You must create a UNIX user on the host where Oracle Retail Back Office is installed and on the Point-of-Service client. Add that user to the `mqm` group. The user must be a member of the `mqm` group and no other operating system group.

Details	Content
Field Title	JMS Password
Field Description	Password of the JMS user receiving parameter updates.

Field Title	Confirm Password
Field Description	Reentered JMS Password used to confirm the password. **Note:** The passwords in the JMS Password and Confirm Password fields must match.

Figure B–40 Back Office Server Information



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

To find the JNDI port number, the information is available in:

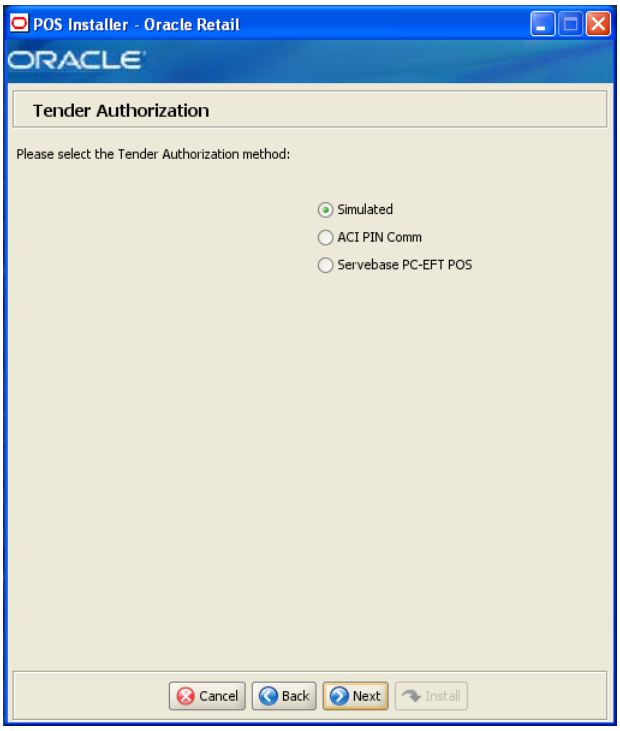
<WebSphere Application Server install>/profiles/*<profile name>*/logs/AboutThisProfile.txt.
BOOTSTRAP_ADDRESS is the port number.

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

Details	Content
Field Title	Back Office Server Name
Field Description	Enter the host name for the Back Office application.

Details	Content
Field Title	Back Office Server JNDI Secure 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	2809

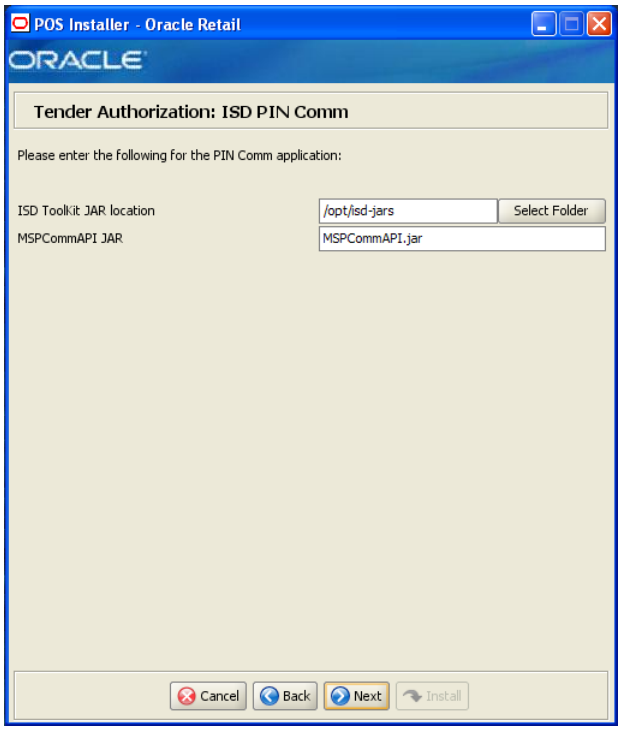
Figure B–41 Tender Authorization



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

Details	Content
Field Title	Please select the tender authorization method
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 **ACI PIN Comm** or **Servebase PC_EFT POS**. **Note:** Demo installations should use the Simulated option.
Example	Simulated

Figure B–42 Tender Authorization: ISD PIN Comm



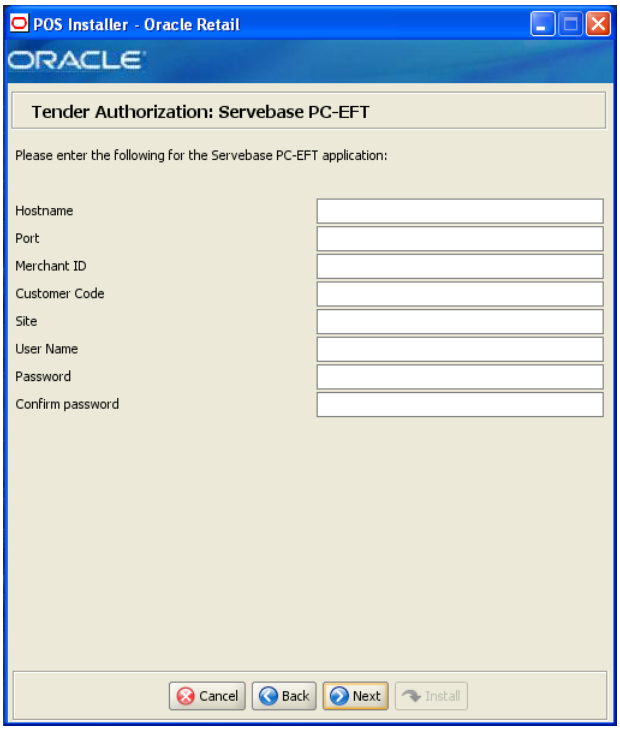
This screen is only displayed if **ACI PIN Comm** is selected for the Tender Authorization.

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

Details	Content
Field Title	ISD ToolKit JAR Location
Field Description	Enter the path to the ISD ToolKit JAR file.
Example	`/opt/isd-jars`

Details	Content
Field Title	MSPCommAPI JAR
Field Description	Enter the name of the MSPCommAPI JAR file.
Example	MSPCommAPI.jar

Figure B–43 Tender Authorization: Servebase PC-EFT



This screen is only displayed if **Servebase PC-EFT POS** is selected for the Tender Authorization.

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

Details	Content
Field Title	Hostname
Field Description	Enter the host name of the PXP Solutions server.

Details	Content
Field Title	Port
Field Description	Enter the port number for the PXP Solutions server.

Details	Content
Field Title	Merchant ID
Field Description	Enter the ID of the merchant used to access the PXP Solutions application.

Details	Content
Field Title	Customer Code
Field Description	Enter the customer code used to access the PXP Solutions application.

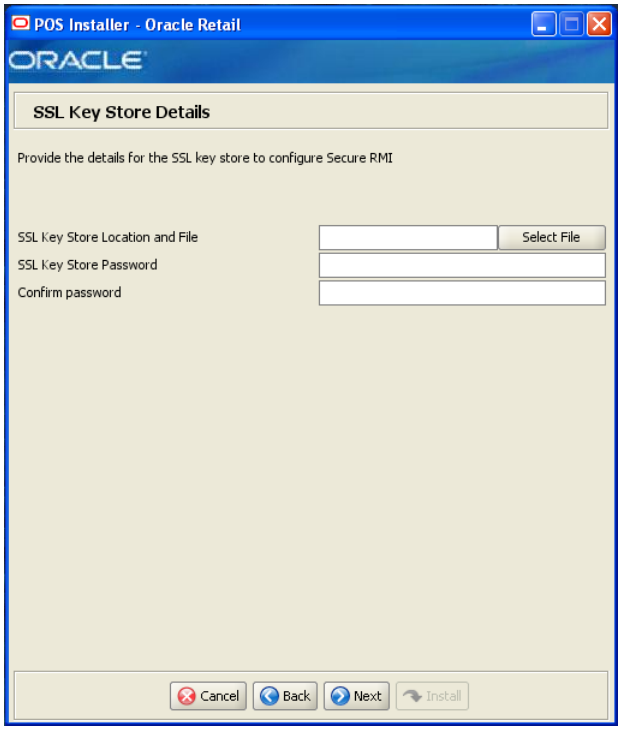
Details	Content
Field Title	Site
Field Description	Enter the site to access the PXP Solutions application.

Details	Content
Field Title	User Name
Field Description	Enter the user name to use to access the PXP Solutions application.

Details	Content
Field Title	Password
Field Description	Enter the password to use to access the PXP Solutions application.

Details	Content
Field Title	Confirm Password
Field Description	Reentered Password used to confirm the password. **Note:** The passwords in the Password and Confirm Password fields must match.

Figure B–44 SSL Key Store Details



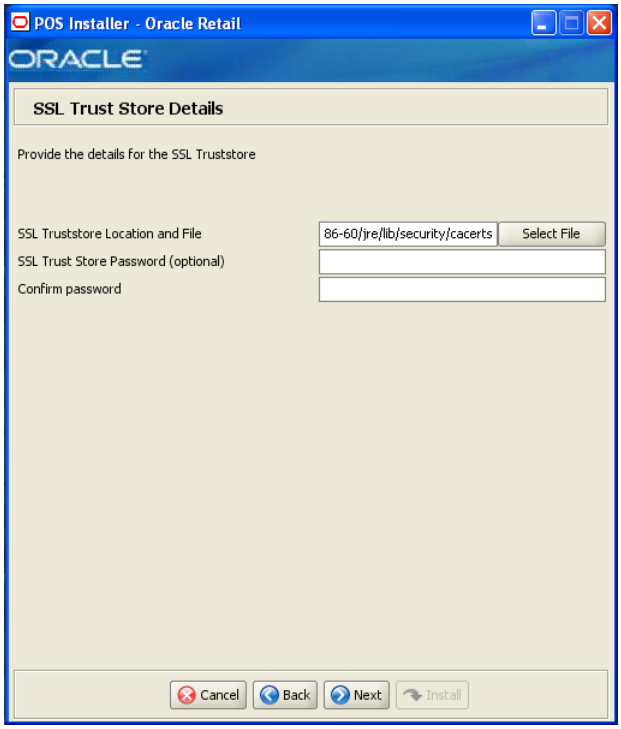
The fields on this screen are described in the following tables.

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

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

Details	Content
Field Title	Confirm Password
Field Description	Reentered SSL Key Store Password used to confirm the password. **Note:** The passwords in the SSL Key Store Password and Confirm Password fields must match.

Figure B–45 SSL Trust Store Details



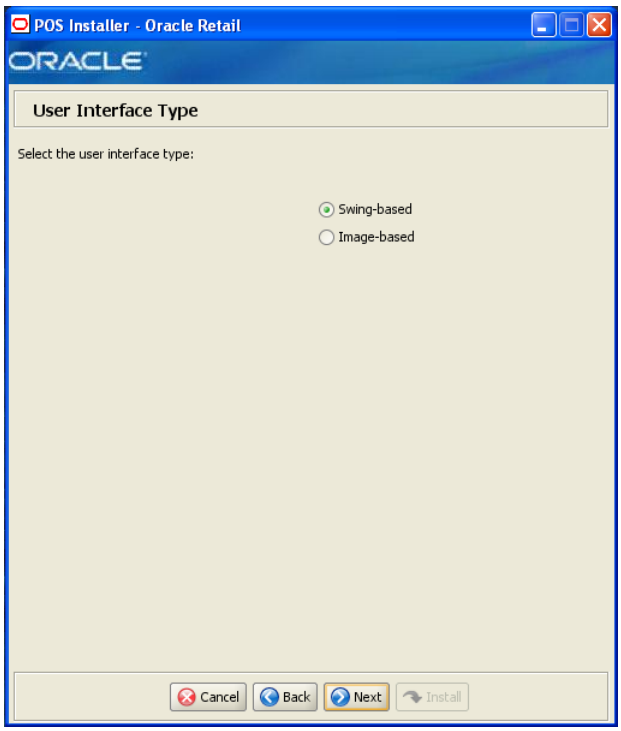
The field on this screen is described in the following table.

Details	Content
Field Title	SSL Truststore Location and File
Field Description	Enter the location and name of the truststore file.
Example	`/opt/ibm/java-i386-60/security/cacerts`

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

Details	Content
Field Title	Confirm Password
Field Description	Reentered SSL Trust Store Password used to confirm the password. **Note:** The passwords in the SSL Trust Store Password and Confirm Password fields must match.

Figure B–46 User Interface Type



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

Details	Content
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–47 Installation Progress

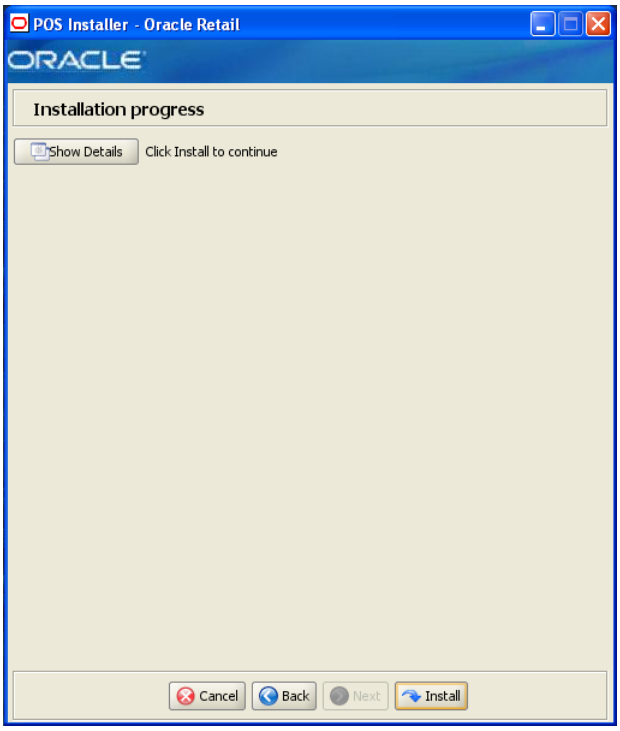
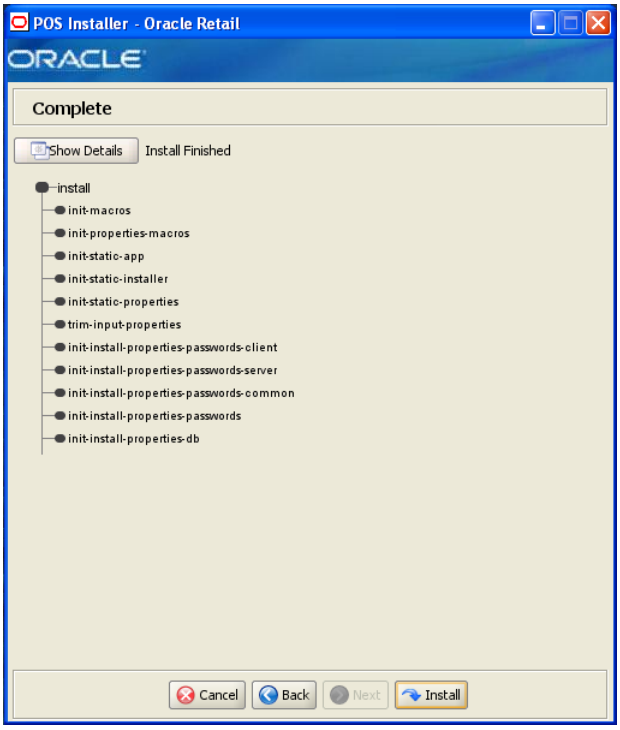


Figure B–48 Install Complete



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.sh silent` or `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 IBM DB2 Database

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

Syntax: `jdbc:db2://<dbhost>:<dbport>/<dbsid>`

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

For example, `jdbc:db2://myhost:50000/mydatabase`

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
oracle.retail.stores.foundation.tour.conduit.Dispatcher.<init>(Dispatcher.java:461
)
     [java]     at
oracle.retail.stores.foundation.tour.conduit.Dispatcher.getDispatcher(Dispatcher.j
ava:1301)
     [java]     at
oracle.retail.stores.foundation.tour.conduit.Dispatcher.main(Dispatcher.java:2439)
     [java]     at
oracle.retail.stores.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` file, for example, `jre/lib/security/java.security`.

"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:oracle.retail.stores.foundation.manager.data.JdbcDataConnection):

[oracle.retail.stores.foundation.manager.data.JdbcDataConnection.logSQLException(J
dbcDataConnection.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 IBM 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.

Performing a Manual Integration

The following steps need to be completed for Point-of-Service to communicate with Back Office and Central Office. These steps enable Point-of-Service to receive parameter updates and to send EJournal and POSLogs up to Central Office.

Client Configuration

To configure the client:

1. If the host names of the Back Office and Central Office servers are not available on a DNS server, update the /etc/hosts file with the IP address and host name where Point-of-Service is installed. This step is required for JMS messaging to work properly.
2. Remove the following class path entries from the *<POS_install_directory>*/pos/bin/posenv.sh file.

```
CP=$CP:$_360COMMON_PATH/common/build/oc4j-internal.jar
CP=$CP:$_360COMMON_PATH/common/build/javax77.jar
CP=$CP:$_360COMMON_PATH/common/build/jms.jar
CP=$CP:$_360COMMON_PATH/common/build/optic.jar
CP=$CP:$_360COMMON_PATH/common/build/jta.jar
```

```
CP=$CP:$_360COMMON_PATH/common/build/ejb.jar
```

3. Add the following class path entries to the *<POS_install_directory>*/pos/bin/posenv.sh file.

```
CP=$CP:<WAS_INSTALL_DIR>/AppServer/plugins/
com.ibm.websphere.v7_7.0.0.v20080817/wasJars/runtime.jar
CP=$CP:<WAS_INSTALL_DIR>/AppServer/runtimes/
com.ibm.ws.admin.client_7.0.0.jar
CP=$CP:<WAS_INSTALL_DIR>/AppServer/runtimes/
com.ibm.ws.ejb.thinclient_7.0.0.jar
CP=$CP:<WAS_INSTALL_DIR>/plugins/com.ibm.ws.runtime.jar
CP=$CP:<WAS_INSTALL_DIR>/AppServer/plugins/com.ibm.ws.sib.server.jar
```

4. Change the *<POS_install_directory>*/pos/bin/jndi.properties file to point to Back Office.

```
java.naming.provider.url=
corbaloc:iiop:<Back Office Server Name>:<Back Office Port Number>
```

5. Add the Back Office queue and topic connection factory entries to the *<POS_install_directory>*/pos/bin/comm.properties file.

```
comm.jms.topicConnectionFactory.name=jms/ApplicationTCF
comm.jms.queueConnectionFactory.name=jms/ApplicationQCF
```

6. Delete the comm.properties file from *<POS_install_directory>*/pos/config.

7. Edit ParameterTechnician in the *<POS_install_directory>* /pos/config/conduit/ClientConduit.xml file.

```
<TECHNICIAN name="ParameterTechnician" class = "ParameterTechnician"
               package = "oracle.retail.stores.foundation.manager.parameter"
               export = "Y" >
          <PROPERTY propname="paramScript"
 propvalue="classpath://config/manager/PosParameterTechnician.xml"/>
          <PROPERTY propname="JmsProviderTopicName"
 propvalue="jms/parameters"/>
   <PROPERTY propname="listenForUpdates" propvalue="Y"/>
          <PROPERTY propname="clientID" propvalue="reg129"/>
          <PROPERTY propname="jmsID" propvalue="<UNIX user>"/>
          <PROPERTY propname="jmsPassword" propvalue="!<password>"/>
   </TECHNICIAN>
```

Note: The value of clientID must match the WorkstationID specified in the application.properties file.

Note: You must create a UNIX user on the host where Back Office is installed and add that user to the mqm group. The values for jmsID and jmsPassword specified in the Password Technician definition must match the values for the UNIX user and password.

Store Server Configuration

To configure the store server:

1. Update the `/etc/hosts` file with the IP address and host name where Point-of-Service is installed. This step is required for JMS messaging to work properly.
2. Update the `/etc/group` file with the user ID that will be used to run the store server. Add that user ID to the `mqm` group. The user ID must be part of the `mqm` group in order to use JMS.
3. Remove the following class path entries from the *<POS_install_directory>*`/pos/bin/posenv.sh` file.

```
SET CLASSPATH=$CLASSPATH:$_360COMMON_PATH\common\build\oc4j-internal.jar
SET CLASSPATH=$CLASSPATH:$_360COMMON_PATH\common\build\javax77.jar
SET CLASSPATH=$CLASSPATH:$_360COMMON_PATH\common\build\jms.jar
SET CLASSPATH=$CLASSPATH:$_360COMMON_PATH\common\build\optic.jar
SET CLASSPATH=$CLASSPATH:jboss-4.0.2/lib/jboss-common.jar
SET CLASSPATH=$CLASSPATH:jboss-4.0.2/client/jboss-j2ee.jar
SET CLASSPATH=$CLASSPATH:jboss-4.0.2/client/jbossmq-client.jar
SET CLASSPATH=$CLASSPATH:jboss-4.0.2/client/jnp-client.jar
```

4. Add the following class path entries to the *<POS_install_directory>*`/pos/bin/posenv.sh` file.

```
CP=$CP:<WAS_INSTALL_DIR>/AppServer/plugins/
com.ibm.websphere.v7_7.0.0.v20080817/wasJars/runtime.jar
CP=$CP:<WAS_INSTALL_DIR>/AppServer/runtimes/
com.ibm.ws.admin.client_7.0.0.jar
CP=$CP:<WAS_INSTALL_DIR>/AppServer/runtimes/
com.ibm.ws.ejb.thinclient_7.0.0.jar
CP=$CP:<WAS_INSTALL_DIR>/plugins/com.ibm.ws.runtime.jar
CP=$CP:<WAS_INSTALL_DIR>/AppServer/plugins/com.ibm.ws.sib.server.jar
```

5. Change the *<POS_install_directory>*`/pos/config/backoffice.jndi.properties` and *<POS_install_directory>*`/pos/bin/jndi.properties` files to point to Back Office.

```
java.naming.provider.url=
corbaloc:iiop:<Back Office Server Name>:<Back Office Port Number>
```

6. To use Centralized Transaction Retrieval, there are jar files that must be copied into the Point-of-Service directory.

> **Note:** Oracle Retail Central Office must be installed and deployed on WebSphere before these jar files can be copied into the Point-of-Service directory. These files are created during the deployment.

Copy the following jar files to *<POS_install_directory>*`/common/lib`:

- *<WAS_PROFILE_DIR>*`/installedApps/`*<hostnameNodeNNCell>*`/CentralOffice.ear/transaction-retrieval-ejb.jar`
- *<WAS_PROFILE_DIR>*`/installedApps/`*<hostnameNodeNNCell>*`/CentralOffice.ear/customer-retrieval-ejb.jar`

7. Change the *<POS_install_directory>* /pos/config/centraloffice.jndi.properties file to point to Central Office. This creates access to the POSLog and EJournalImport queues and enables Centralized Transaction Retrieval to access the EJBs and POSLog and EJournalImport queues.

   ```
   java.naming.provider.url=
   corbaloc:iiop:<Central Office Server Name>:<Central Office Port Number>
   ```

8. Add the Back Office and Central Office queue and topic connection factory entries to the *<POS_install_directory>*/pos/bin/comm.properties file.

   ```
   comm.jms.topicConnectionFactory.name=jms/ApplicationTCF
   comm.jms.queueConnectionFactory.name=jms/ApplicationQCF
   comm.jms.topicConnectionFactory.name.<Central Office Server Name>=
   jms/ApplicationTCF
   comm.jms.queueConnectionFactory.name.<Central Office Server Name>=
   jms/ApplicationQCF
   ```

9. Delete the comm.properties file from *<POS_install_directory>*/pos/config.

10. Edit the log export configuration in the *<POS_install_directory>* /pos/config/conduit/StoreServerConduit.xml file by changing only one of the following sections.

    - To use data replication, edit the DataReplicationDaemonTechnician section.

      ```
      <TECHNICIAN name="DataReplicationDaemonTechnician
                    class="DataReplicationDaemonTechnician"
                  package="oracle.retail.stores.domain.manager.datareplication"
                    export="Y">
              <PROPERTY propname="daemonClassName"
      propvalue="oracle.retail.stores.domain.manager.datareplication.DataReplicat
      ionExportDaemonThread"/>
              <PROPERTY propname="sleepInterval"
                        propvalue="50"/>
              <PROPERTY propname="logWriterClass"
      propvalue="oracle.retail.stores.domain.manager.datareplication.JMSDataRepli
      cationWriter"/>
              <PROPERTY propname="extractorConfigurationFileName"
                        propvalue="config/ReplicationExportConfig.xml"/>
              <PROPERTY propname="queueHostName"
                        propvalue=""/>
              <PROPERTY propname="maximumTransactionsToExport"
                        propvalue="2"/>
              <PROPERTY propname="queueName"
                        propvalue="jms/POSLog"/>
      </TECHNICIAN>
      ```

    - To use the POSLog, edit the PosLogDaemonTechnician section. Edit the version that exports to a JMS queue.

      ```
      TECHNICIAN name="POSLogDaemonTechnician"
                    class="POSLogDaemonTechnician"
                    package="oracle.retail.stores.domain.manager.export"
                    export="Y">
              <PROPERTY propname="daemonClassName"

      propvalue="oracle.retail.stores.domain.manager.export.POSLogExportDaemonThr
      ead"/>
      ```

```
            <PROPERTY propname="sleepInterval"
                      propvalue="60"/>
            <PROPERTY propname="logWriterClass"
    propvalue="oracle.retail.stores.domain.ixretail.log.POSLogWriter"/>
            <PROPERTY propname="queueHostName"
                      propvalue="<Central Office Server Name>"/>
            <PROPERTY propname="queueName"
                      propvalue="jms/POSLog"/>
            <PROPERTY propname="logWriterClass"
    propvalue="oracle.retail.stores.domain.ixretail.log.JMSPOSLogWriter"/>
        </TECHNICIAN>
```

11. Edit `JMSJournalTechnician` in the *<POS_install_directory>* `/pos/config/conduit/StoreServerConduit.xml` file.

```
 <TECHNICIAN name="JMSJournalTechnician"
                class="JMSJournalTechnician"
                package="oracle.retail.stores.foundation.manager.journal"
                export="Y">
                <PROPERTY propname="journalFormatterClass"
propvalue="oracle.retail.stores.pos.manager.journal.POSJournalFormatter"/>
                <PROPERTY propname="journalHandlerClass"
propvalue="oracle.retail.stores.pos.manager.journal.POSJMSJournalHandler"/>
                <PROPERTY propname="queueName" propvalue="jms/EJournal"/>
                <PROPERTY propname="consolePrintable" propvalue="N"/>
    </TECHNICIAN>
```

12. Edit `MessageCenterDaemonTechnician` in the *<POS_install_directory>* `/pos/config/conduit/StoreServerConduit.xml` file.

```
 <TECHNICIAN name="MessageCenterDaemonTechnician"
               class="MessageCenterDaemonTechnician"
               package="oracle.retail.stores.domain.manager.messagecenter"
               export="Y">
        <PROPERTY propname="daemonClassName"
propvalue="oracle.retail.stores.domain.manager.messagecenter.MessageCenterDaemo
nThread"/>
        <PROPERTY propname="senderQueueName"
                  propvalue="jms/EJournalImport"/>
        <PROPERTY propname="senderBrokerName"
                  propvalue="<Central Office Server Name>"/>
        <PROPERTY propname="receiverQueueName"
                  propvalue="jms/EJournal"/>
        <PROPERTY propname="receiverBrokerName"
                  propvalue=""/>
  </TECHNICIAN>
```

> **Note:** The value set for the `queueName` property for the `JMSJournalTechnician` and the value set for the `receiverQueueName` property for the `MessageCenterDaemonTechnician` must be the same.

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.sh` file and restart the server:

  ```
  COMMAND "java ${JAVA_OPTIONS} -Djavax.net.debug=all
  oracle.retail.stores.foundation.config.TierLoader ${CONDUIT_CONFIG}"
  ```

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

  ```
  COMMAND "java ${JAVA_OPTIONS} -Djavax.net.debug=all
  oracle.retail.stores.foundation.config.TierLoader ${CONDUIT_CONFIG}"
  ```

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

http://docs.oracle.com/javase/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 the *Oracle Retail POS Suite Security Guide*.
- 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 `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 the *Oracle Retail POS Suite Security Guide* 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: 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 `opt/POS/IBMJPOS/jpos.xml`.

> **Note:** When configuring a register running SLEPOS, you must disable IBM Management for JPOS.

For the updates for the devices, see the applicable section:

- "Configuring Devices for an IBM SurePOS Register"
- "Configuring a Device for ACI PIN Comm"

Configuring Devices for an IBM SurePOS Register

To configure the devices for an IBM SurePOS register:

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

```
<JposEntry logicalName="defaultScanner">
    <creation
        factoryClass="com.ibm.jpos.services.IBMJposServiceInstanceFactory"
        serviceClass="com.ibm.jpos.services.ScannerUSBOEM"/>
    <vendor name="IBM" url="http://www.ibm.com"/>
    <jpos category="Scanner" version="1.12.1"/>
    <product description="IBM JavaPOS(TM) Scanner USB Service for OEM Hand Held
        Scanner" name="IBM JavaPOS for Linux/Windows Version 1.12.1"
        url="http://www.pc.ibm.com/store/"/>

    <prop name="setEnableCODE39" type="Boolean" value="true"/>
    <prop name="setEnableCode128" type="Boolean" value="true"/>
    <prop name="setEnableInterleaved2of5" type="Boolean" value="true"/>
    <prop name="com.ibm.posj.bus.hid.usagePage" type="String" value="0xFF45"/>
    <prop name="abstractionClass" type="String"
        value="com.ibm.jpos.services.ScannerUSBOEM"/>
    <prop name="setEnableUCC_EAN128" type="Boolean" value="true"/>
    <prop name="setEnableCodabar" type="Boolean" value="true"/>
    <prop name="impClass" type="String"
        value="com.ibm.jpos.services.sdi.ScannerServiceImp"/>
    <prop name="setEnableUPCD1D5" type="Boolean" value="true"/>
    <prop name="setEnableCode93" type="Boolean" value="true"/>
```

```
    <prop name="setEnableUPCAE_EANJAN813" type="Boolean" value="true"/>
    <prop name="deviceBus" type="String" value="HID"/>
    <prop name="com.ibm.posj.bus.hid.usageId" type="String" value="0x4B00"/>
    <prop name="setEnable_5_DigitSupplementals" type="Boolean" value="true"/>
    <prop name="setEnable_2_DigitSupplementals" type="Boolean" value="true"/>
    <prop name="setITFLengthSpecifiedTwo" type="Boolean" value="true"/>
    <prop name="setITFLength1" type="Byte" value="12"/>
    <prop name="setITFLength2" type="Byte" value="16"/>
    <prop name="com.ibm.posj.bus.deviceNumber" type="String" value="0"/>
    <prop name="setEnableUPC_A_CheckDigit" type="Boolean" value="true"/>
    <prop name="setEnableUPC_E_CheckDigit" type="Boolean" value="true"/>
</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.ibm.jpos.services.IBMJposServiceInstanceFactory"
        serviceClass="com.ibm.jpos.services.SdiIBM4610EPOSPrinter"/>
    <vendor name="IBM" url="http://www.ibm.com"/>
    <jpos category="POSPrinter" version="1.9.3"/>
    <product description="IBM JavaPOS(TM) POSPrinter RS485 Service for IBM
        4610 TI2/3/4/5/8/9 TM/F 6/7 Printer" name="IBM JavaPOS for
        Linux/Windows Version 1.9.3" url="http://www.pc.ibm.com/store/"/>
    <prop name="deviceBus" type="String" value="RS485"/>
    <prop name="com.ibm.posj.bus.rs485.sioDeviceNumber" type="String"
        value="0x35"/>
    <prop name="com.ibm.posj.bus.rs485.sioPortNumber" type="String"
        value="0x11"/>
    <prop name="com.ibm.posj.bus.rs485.sioSlotNumber" type="String"
        value="0x01"/>
    <prop name="abstractionClass" type="String"
        value="com.ibm.jpos.services.SdiIBM4610EPOSPrinter"/>
    <prop name="impClass" type="String"
        value="com.ibm.jpos.services.sdi.IBM4610PrinterServiceImp"/>
    <prop name="com.ibm.posj.bus.deviceNumber" type="String" value="0"/>
</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.ibm.jpos.services.IBMJposServiceInstanceFactory"
        serviceClass="com.ibm.jpos.services.IBM4610MICR"/>
    <vendor name="IBM" url="http://www.ibm.com"/>
    <jpos category="MICR" version="1.9.3"/>
    <product description="IBM JavaPOS(TM) MICR RS485 Service for IBM 4610
        TI2/4/8/9 Printer" name="IBM JavaPOS for Linux/Windows Version 1.9.3"
        url="http://www.pc.ibm.com/store/"/>
    <prop name="deviceBus" type="String" value="RS485"/>
    <prop name="abstractionClass" type="String"
        value="com.ibm.jpos.services.IBM4610MICR"/>
    <prop name="impClass" type="String"
        value="com.ibm.jpos.services.sdi.MICRServiceImp"/>
    <prop name="com.ibm.posj.bus.deviceNumber" type="String" value="0"/>
    <prop name="com.ibm.posj.bus.rs485.sioSlotNumber" type="String"
        value="0x01"/>
    <prop name="com.ibm.posj.bus.rs485.sioPortNumber" type="String"
        value="0x11"/>
```

```
    <prop name="com.ibm.posj.bus.rs485.sioDeviceNumber" type="String"
        value="0x35"/>
    <prop name="com.ibm.jpos.sdi.config.MICR.exceptionTableFile"
        type="String" value="[file-path-goes-here]"/>
    <prop name="com.ibm.jpos.sdi.config.MICR.exceptionTable4" type="String"
        value="B778899001D154R"/>
    <prop name="com.ibm.jpos.sdi.config.MICR.exceptionTable3" type="String"
        value="B667788990D153R"/>
    <prop name="com.ibm.jpos.sdi.config.MICR.exceptionTable2" type="String"
        value="P123456780AAAAAXXSSS"/>
    <prop name="com.ibm.jpos.sdi.config.MICR.exceptionTable1" type="String"
        value="B445566778D151R"/>
    <prop name="com.ibm.jpos.sdi.config.MICR.exceptionTable0" type="String"
        value="B334455667D150R"/>
    <prop name="com.ibm.jpos.sdi.config.MICR.stripAccountDashes"
        type="String" value="false"/>
    <prop name="com.ibm.jpos.sdi.config.MICR.stripTransitDashes"
        type="String" value="false"/>
    <prop name="com.ibm.jpos.sdi.config.MICR.switchTransitDashToSpace"
        type="String" value="false"/>
</JposEntry>
```

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

```
<JposEntry logicalName="defaultPOSKeyboard">
    <creation
        factoryClass="com.ibm.jpos.services.IBMJposServiceInstanceFactory"
        serviceClass="com.ibm.jpos.services.IBMPOSKeyboard"/>
    <vendor name="IBM" url="http://www.ibm.com"/>
    <jpos category="POSKeyboard" version="1.9.3"/>
    <product description="IBM JavaPOS(TM) POSKeyboard PS2 Service for IBM
        4820/ANKPOS/CANPOS/NANPOS/SureONE Keyboards" name="IBM JavaPOS for
        Linux/Windows Version 1.9.3" url="http://www.pc.ibm.com/store/"/>
    <prop name="com.ibm.jpos.sdi.config.POSKeyboard.Click" type="Byte"
        value="0"/>
    <prop name="com.ibm.posj.bus.poskbd.functionNumber" type="String"
        value="0"/>
    <prop name="com.ibm.jpos.sdi.config.POSKeyboard.Typematic"
        type="Boolean" value="true"/>
    <prop name="com.ibm.jpos.sdi.config.POSKeyboard.ExtendedKeyMapping"
        type="Boolean" value="true"/>
    <prop name="abstractionClass" type="String"
        value="com.ibm.jpos.services.IBMPOSKeyboard"/>
    <prop name="impClass" type="String"
        value="com.ibm.jpos.services.sdi.POSKeyboardServiceImp"/>
    <prop name="com.ibm.posj.bus.poskbd.keyboardNumber" type="String"
        value="0"/>
    <prop name="deviceBus" type="String" value="Proprietary"/>
    <prop name="com.ibm.posj.bus.ProprietaryBusSubType" type="String"
        value="PosKbd"/>
    <prop name="com.ibm.jpos.sdi.config.POSKeyboard.KbdScanning"
        type="Boolean" value="true"/>
</JposEntry>
```

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

```
<JposEntry logicalName="defaultMSR">
    <creation
        factoryClass="com.ibm.jpos.services.IBMJposServiceInstanceFactory"
```

```
        serviceClass="com.ibm.jpos.services.IBMMSR"/>
    <vendor name="IBM" url="http://www.ibm.com"/>
    <jpos category="MSR" version="1.12.1"/>
    <product description="IBM JavaPOS(TM) MSR USB Service for IBM
        ANKPOS/Keyboard V/Modular/NANPOS/133 key/4685/4820/50key Keyboard"
        name="IBM JavaPOS for Linux/Windows Version 1.12.1"
        url="http://www.pc.ibm.com/store/"/>

    <prop name="com.ibm.posj.bus.hid.usageId" type="String" value="0x1600"/>
    <prop name="deviceBus" type="String" value="HID"/>
    <prop name="abstractionClass" type="String"
        value="com.ibm.jpos.services.IBMMSR"/>
    <prop name="impClass" type="String"
        value="com.ibm.jpos.services.sdi.MSRServiceImp"/>
    <prop name="com.ibm.posj.bus.hid.usagePage" type="String" value="0xFF45"/>
    <prop name="com.ibm.posj.bus.deviceNumber" type="String" value="0"/>
</JposEntry>
```

6. 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.ibm.jpos.services.IBMJposServiceInstanceFactory"
        serviceClass="com.ibm.jpos.services.IBMCashDrawer"/>
    <vendor name="IBM" url="http://www.ibm.com"/>
    <jpos category="CashDrawer" version="1.9.3"/>
    <product description="IBM JavaPOS(TM) CashDrawer Service for IBM
        SurePOS 300/72x/74x/78x-A" name="IBM JavaPOS for Linux/Windows Version
        1.9.3 "url="http://www.pc.ibm.com/store/"/>
    <prop name="deviceBus" type="String" value="Proprietary"/>
    <prop name="com.ibm.posj.bus.ProprietaryBusSubType" type="String"
        value="Embedded"/>
    <prop name="abstractionClass" type="String"
        value="com.ibm.jpos.services.IBMCashDrawer"/>
    <prop name="impClass" type="String"
        value="com.ibm.jpos.services.sdi.CashDrawerServiceImp"/>
    <prop name="com.ibm.posj.bus.deviceNumber" type="String" value="0"/>
</JposEntry>
```

7. 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="com.ibm.jpos.services.IBMJposServiceInstanceFactory"
        serviceClass="com.ibm.jpos.services.LineDisplayLCVFD"/>
    <vendor name="IBM" url="http://www.ibm.com"/>
    <jpos category="LineDisplay" version="1.9.3"/>
    <product description="IBM JavaPOS(TM) LineDisplay USB Service for IBM
        Vaccum Fluorescent Display (VFD)-A" name="IBM JavaPOS for Linux/Windows
        Version 1.9.3" url="http://www.pc.ibm.com/store/"/>
    <prop name="com.ibm.posj.bus.hid.usageId" type="String"
        value="0x2400"/>
    <prop name="deviceBus" type="String" value="HID"/>
    <prop name="abstractionClass" type="String"
        value="com.ibm.jpos.services.LineDisplayLCVFD"/>
    <prop name="impClass" type="String"
        value="com.ibm.jpos.services.sdi.LineDisplayServiceImp"/>
    <prop name="com.ibm.posj.bus.hid.usagePage" type="String"
        value="0xFF45"/>
```

```
    <prop name="com.ibm.posj.bus.deviceNumber" type="String" value="0"/>
</JposEntry>
```

Configuring a Device for ACI PIN Comm

To configure an ACI PIN Comm device:

1. Make the following changes to the *<PinComm Install Root>*/conf/pinCommConfig.xml file:
   a. Add the following line to the <TenderTypes> section:

      ```
      <customerDefinedTender01>77</customerDefinedTender01>
      ```

   b. Add the following line to the <PromptSequences> section:

      ```
      <customerDefinedTender01Sequence>N</customerDefinedTender01Sequence>
      ```

2. When putting a refund credit on a card not used in the original transaction, the customer is prompted for the credit/debit card. To avoid prompting the customer, add the following custom parameter to the *<PinComm Install Root>*/conf/isd.custom.properties file:

   ```
   configurationManagerFactory.overridePoeSuppliedTenderType=false
   ```

3. It is recommended that static IP addresses are used for VeriFone devices. For information on how to configure the device for register mapping, see the *ISD PIN Comm Configuration User Manual*.

H

Appendix: Installation Order

This appendix 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 Invoice Matching (ReIM)
7. 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.

8. Oracle Retail Allocation
9. Oracle Retail Central Office (ORCO)
10. Oracle Retail Returns Management (ORRM)
11. Oracle Retail Back Office (ORBO)
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 Analytics
33. Oracle Retail Workspace (ORW)