Oracle® Retail Point-of-Service

Installation Guide, Volume 1 - Oracle Stack

Release 13.4.5

E38102-02

December 2012

Oracle Retail Point-of-Service Installation Guide, Volume 1 - Oracle Stack, Release 13.4.5

E38102-02

Primary Author: Bernadette Goodman

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

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

U.S. GOVERNMENT 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.

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

Value-Added Reseller (VAR) Language

Oracle Retail VAR Applications

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

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

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

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

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

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

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

Contents

2 Secure Configuration

3 Installation on the Oracle Stack using Windows

4 Installation of Mobile Point-of-Service

A Appendix: Installer Screens for Server Installation on Windows

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

C Appendix: Installer Screens for Mobile Point-of-Service Server

D Appendix: Installer Silent Mode

E Appendix: URL Reference

F Appendix: Common Installation Errors

G Appendix: Troubleshooting Problems on the Oracle Stack

H Appendix: Device Configuration

I Appendix: Installation Order

List of Figures

List of Tables

Send Us Your Comments

Oracle Retail Point-of-Service Installation Guide, Volume 1 - Oracle Stack, Release 13.4.5

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 the Oracle Retail Point-of-Service and Oracle Retail Mobile Point-of-Service releases.

Audience

This Installation Guide is written for the following audiences:

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

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/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 13.4.5 documentation set:

- *Oracle Retail Point-of-Service Installation Guide, Volume 2 - IBM Stack*
- *Oracle Retail Point-of-Service User Guide*
- *Oracle Retail POS Suite Configuration Guide*
- *Oracle Retail POS Suite Data Dictionary*
- *Oracle Retail POS Suite Implementation Guide, Volume 5 - Mobile Point-of-Service*
- *Oracle Retail POS Suite Licensing Information*
- *Oracle Retail POS Suite Security Guide*

Customer Support

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

`https://support.oracle.com`

When contacting Customer Support, please provide the following:

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

Review Patch Documentation

When you install the application for the first time, you install either a base release (for example, 13.4) or a later patch release (for example, 13.4.5). 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.

Oracle Retail Documentation on the Oracle Technology Network

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

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

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

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

Conventions

The following text conventions are used in this document:

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

1 Preinstallation Tasks

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

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

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

Check for the Current Version of the Installation Guide

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

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

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

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

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

Check Supported Store Server Software Requirements

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

Table 1–1 Store Server Requirements

Supported on	Versions Supported
Operating System	Microsoft Windows 2008 Server R2 Standard Edition (64-bit)
Database	Oracle Database 11gR2 Enterprise Edition 11.2.0.3 (64-bit) **Note:** Oracle Retail Point-of-Service is not certified with Real Application Clusters (RAC).
JDK/JRE	Oracle Java Standard Edition 6 or later within the Java 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	Register Versions Supported
Register	HP POS RP5700, RP3000
Operating System	■ Microsoft Windows Embedded POSReady 2009 **Note:** POSReady2009 must be installed with command-line utilities. See "Install Optional Components for Microsoft POSReady2009". ■ Microsoft Windows 7 Pro FP-1 (32-bit)
JVM	Oracle Java Standard Edition 6 or later within the Java 6 code line
Persistent Storage	Apache Derby 10.5.3
Cash drawer	HP Cash Drawer #EY024AA
Pole Display	VFD LD220
Keyboard	HP USB POS Keyboard Model SPOS
Scanner	HP USB Barcode Scanner LS2208
PIN Pad	■ VeriFone MX860 ■ VeriFone VX810 (EMV)
Receipt Printer	HP USB Hybrid Receipt Printer with MICR Model A776
Biometric Device	DigitalPersona U.are.U UPOS for JavaPOS for Windows Version 1.1.0

Install Optional Components for Microsoft POSReady2009

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

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

Install DigitalPersona Software

Registers that support a fingerprint device require the installation of the following software:

- DigitalPersona Windows SDK (`otwsdk1401.zip`)
- DigitalPersona JavaPOS drivers (`uareu-upos-javapos-win.zip`)

These installers should be included with your fingerprint readers or can be downloaded from the following Web site:

http://www.digitalpersona.com/oracle/biometrics/

After the installation is complete, use the Windows Device Manager to verify that you see the device.

Check Supported Mobile Point-of-Service Hardware and Software Requirements

Table 1–3 lists the general requirements for the Mobile Point-of-Service server capable of running Mobile Point-of-Service and the versions supported for this release.

Table 1–3 Mobile Point-of-Service Server Requirements

Supported on	Versions Supported
Operating System	Microsoft Windows 2008 Server R2 Standard Edition
J2EE Application Server	Oracle WebLogic Server 10.3.6.0 Standard Edition
J2EE Application Server JVM	Oracle Java Standard Edition 6 or later within the Java 6 code line
Messaging Provider	included in Oracle WebLogic Server

Table 1–4 lists the general requirements for a mobile device capable of running Mobile Point-of-Service and the versions supported for this release.

Table 1–4 Mobile Point-of-Service Device Requirements

Supported on	Mobile Device Versions Supported
Device	Apple iPod Touch (4th Generation)
Operating System	iOS 5.1.1
Sled	VeriFone VX600 ■ Hardware Version: 1.0.0 ■ Firmware Version: 1.0.0 **Note:** Mobile Point-of-Service can be run without a sled, but this is not suitable for a production environment.

Table 1–4 (Cont.) Mobile Point-of-Service Device Requirements

Supported on	Mobile Device Versions Supported
PIN Pad	▪ VeriFone MX860 ▪ VeriFone VX810 (EMV)

Install Required Patch for Oracle Retail Store Inventory Management

If Mobile Point-of-Service is integrated with Oracle Retail Store Inventory Management and you are selling items with serial numbers, you must download and apply patch number 13845833. Download the patch from My Oracle Support:

`https://support.oracle.com`

Check for SSL Certificate

The Mobile Point-of-Service server is accessed through a secure HTTP connection. The installation of an SSL Certificate is required on your WebLogic Server. If the certificate is not installed, Mobile Point-of-Service will not work.

For information on installing the SSL Certificate, refer to your Oracle WebLogic Server documentation.

Check Oracle Retail Software Dependencies

Table 1–5 lists the Oracle Retail products that Oracle Retail Point-of-Service is integrated with and the required versions.

Table 1–5 Supported Oracle Retail Products

Integrates with	Version
Oracle Retail Back Office	13.4.5
Oracle Retail Central Office	13.4.5
Oracle Retail Merchandising System	13.2.5
Oracle Retail Price Management	13.2.5
Oracle Retail Returns Management	2.4.5
Oracle Retail Sales Audit	13.2.5
Oracle Retail Store Inventory Management	13.2.5 (on Oracle WebLogic Server)

Check Additional Oracle Technologies

Table 1–6 lists the Oracle technologies used by Oracle Retail Point-of-Service and the required versions.

Table 1–6 Additional Oracle Technologies

Integrates with	Version
Siebel	8.1.1.3

Check Third-Party Software Dependencies

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

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–12. 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–13.
- When installing the Mobile Point-of-Service server, select the applications that the server is integrated with. See Figure C–39.

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–56.

See the following sections for more information.

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

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

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

Oracle Retail Returns Management

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

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

Bill Payment

The bill payment feature enables the retailer to 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 Servebase PC-EFT, the following details are required:

- Host name of the machine running PC-EFT
- Port number at which PC-EFT is listening
- Merchant ID provided by the bank
- Customer Code provided by the bank
- Store's site identification
- PC-EFT 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 for Point-of-Service" 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 Key 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 Key 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 for Point-of-Service

Tender authorization testing was done with ACI PIN Comm and Servebase PC-EFT POS. For each payment application, the version used for the testing and the transaction types and messages that were tested are listed below.

For testing done for Mobile Point-of-Service, see "Tender Authorization Testing for Mobile Point-of-Service".

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 1–7 shows the transaction types and messages that were tested.

Table 1–7 ACI PIN Comm Authorization Set Tested with Point-of-Service

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 1–7 (Cont.) ACI PIN Comm Authorization Set Tested with Point-of-Service

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

Servebase PC-EFT POS

The version used for testing was 2.0.0.52.

Table 1–8 shows the transaction types and messages that were tested.

Table 1–8 Servebase PC-EFT POS Authorization Set Tested with Point-of-Service

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

Table 1–8 (Cont.) Servebase PC-EFT POS Authorization Set Tested with Point-of-Service

Transaction Type	Transaction Type Message Sent from Servebase PC-EFT 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 Servebase is the payment application.
House Account Tender	■ House Account Sale Decline **Note:** Tendering with a house account is declined when Servebase is the payment application.

Tender Authorization Testing for Mobile Point-of-Service

Tender authorization testing was done with ACI PIN Comm and Servebase PC-EFT. For each payment application, the version used for the testing and the transaction types and messages that were tested are listed below.

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 1–9 shows the transaction types and messages that were tested.

Table 1–9 ACI PIN Comm Authorization Set Tested with Mobile Point-of-Service

Transaction Type	Transaction Type Message Sent from ACI PIN Comm to Mobile Point-of-Service
Credit Card Tender	■ 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 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
Gift Card Issue	■ Gift Card Issue Approval ■ Gift Card Issue Authorization Offline ■ Gift Card Issue Authorization Timeout ■ Gift Card Issue Decline
Gift Card Tender	■ Gift Card Sale Approval ■ Gift Card Sale Authorization Offline ■ Gift Card Sale Authorization Timeout ■ Gift Card Sale Decline ■ Gift Card Sale Referral

Servebase PC-EFT POS

The version used for testing was v2.0.0.52, Vx810 PEDs wired using TCP/IP.

Table 1–10 shows the transaction types and messages that were tested.

Table 1–10 Servebase PC-EFT POS Authorization Set Tested with Mobile Point-of-Service

Transaction Type	Transaction Type Message Sent from Servebase PC-EFT POS to Mobile Point-of-Service
Chip and Pin Credit Card Tender	■ Chip and Pin Credit Card Sale Approval ■ Chip and Pin Credit Card Sale Authorization Offline (Decline) ■ Chip and Pin Credit Card Sale Authorization Offline (Store and Forward) ■ Chip and Pin Credit Card Sale Authorization Timeout ■ Chip and Pin Credit Card Sale Decline ■ Chip and Pin Credit Card Sale Referral
Chip and Pin Debit Card Tender	■ Chip and Pin Debit Card Sale Approval ■ Chip and Pin Debit Card Sale Authorization Offline (Decline) ■ Chip and Pin Debit Card Sale Authorization Offline (Store and Forward) ■ Chip and Pin Debit Card Sale Authorization Timeout ■ Chip and Pin Debit Card Sale Decline
Credit Card Tender	■ Credit Card Sale Approval ■ Credit Card Sale Authorization Offline (Decline) ■ Credit Card Sale Authorization Offline (Store and Forward) ■ Credit Card Sale Authorization Timeout ■ Credit Card Sale Decline ■ 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.

When using Microsoft Windows XP, the system restore point must be disabled. This restore point may possibly contain sensitive data (test or real) in previous versions of the operating system. To disable the system restore point:

1. Open the Control Panel.
2. Select **System** and then the **System Restore** tab.
3. Check the **Turn off System Restore** box and click **OK**.

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

Additional Resources

The Center for Internet Security has published benchmarks for securing your systems at the operating system level. You can find the benchmark for Microsoft Windows 2008 at the following link:

http://benchmarks.cisecurity.org/en-us/?route=downloads.browse.category.benchmarks.os.windows.2008

You can find the benchmark for Apple iOS, which maps to iOS 5.0.x, at the following link:

https://benchmarks.cisecurity.org/tools2/iphone/CIS_Apple_iOS_Benchmark_v1.4.0.pdf

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 Oracle Database, see the *Oracle Database 2 Day + Security Guide*. The guide is available at the following link on the Oracle Technology Network Web site:

http://download.oracle.com/docs/cd/E11882_01/server.112/e10575.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

Except for Oracle Retail Mobile Point-of-Service, Oracle Retail POS Suite applications are not designed as wireless applications. Where 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 13.4.1 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 13.4.1 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 Oracle Stack using Windows

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

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

Create the Database Schema Owner and Data Source Users

The following recommendations should be considered for schema owners:

- Database administrators should create an individual schema owner for each application, unless the applications share the same data. In the case of Oracle Retail Back Office and Point-of-Service, the database schema owner 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 a role in the database to be used for the schema owner.

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

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

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

4. Create the schema owner user in the database.

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

5. Grant the schema owner role to the user.

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

To create the data source user:

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

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

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

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

4. Create the data source user.

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

5. Grant the data source role to the user.

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

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

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.

Table 3–1 (Cont.) Server Tier Logical Components

Machine	Description
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

The following settings must be made during database creation:

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

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

Installing Point-of-Service on Machines

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

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

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

- Installs Foundation, Retail Domain, and Oracle Retail Point-of-Service jar files.
- Installs database build scripts and start-up files.

- Defines Server Tier in the conduit script that starts Point-of-Service for the given machine.
- Defines hostnames or IP addresses and port numbers for the Store Server and database server.
- Defines device availability.
- Defines application properties for Store ID and Register Number.

Updating Device Configuration

Instructions for configuring peripheral devices are in Appendix H:

- "Configuring Devices for an HP 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 13.4.5 distribution zip file.
2. Create a new staging directory for the Point-of-Service application distribution `ORPOS-13.4.5.zip` file, for example, `c:\tmp\orpos\orpos-staging`.

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

3. Copy or upload `ORPOS-13.4.5.zip` to *<staging_directory>* and extract its contents. The following files and directories should be created under *<staging_directory>*`\ORPOS-13.4.5`:

```
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-13.4.5` is referred to as `<INSTALL_DIR>`.

Obtain the JRE Required for Client Install

This release requires Oracle Java Standard Edition 6 Update 24 for client installs on HP registers. The download is available at the following Web site:

http://www.oracle.com/technetwork/java/javasebusiness/downloads/java-archive-downloads-javase6-419409.html

Increase the Heap Size on the Client

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

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

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–20.
  - 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–16.
  - 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–18.

> **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–19. You can obtain the `sample-dataset-13.4.5.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 Key Manager

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

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

Obtain the RSA Key Manager Version 3.1 Jar Files

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

1. Obtain the following jar files from your RSA Key Manager provider:
   - `cryptoj.jar`
   - `kmsclient.jar`

- sslj.jar

2. Copy the jar files into <*INSTALL_DIR*>/rsa-jars.

Install the Java Cryptography Extension (JCE)

If a payment application or RSA Key Manager version 3.1 will be used, you must update the security for your JRE. You need to obtain version 6 of the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.

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

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

   - On the client:

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

2. Download version 6 of the JCE.
   a. Go to the following Web site:

      http://www.oracle.com/technetwork/java/javase/downloads/index.html

   b. Under Additional Resources, find **Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6**.

   c. Click **Download**.

   d. Follow the instructions to download the JCE.

3. Copy the jar files into the JRE security directory. The files are bundled as jce_policy-6.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, 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 Java 6 Update 24.

3. When installing the store server, set the account of the user running the installer to run as an administrator. Set the account using Microsoft Windows 2008 Server.

4. Run the `install.cmd` script. This will launch the installer. After installation is complete, a detailed installation log file is created at `<POS_install_directory>\pos-install-yyyyMMddHHmm.log`

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

   > **Note:** The typical usage for GUI mode does not use arguments.
   >
   > ```
   > install.cmd
   > ```

5. If this is a client install and you are using a fingerprint device, verify the following:

   - The fingerprint device properties are correct in the following file:

     ```
     <POS_install_
     directory>\<client>\pos\config\technician\PosDeviceTechnician.xml
     ```

     Verify the following properties:

     ```
     ## Properties from Page:fingerPrintDevice
     input.client.device.dpfingerprint = true
     ## Properties from Page:DPEnvironmentClasspath
     input.dpfingerprint.dpjavapos =
     C:\\DigitalPersona\\Bin\\JavaPOS\\dpjavapos.jar
     input.dpfingerprint.jpos = C:\\DigitalPersona\\Bin\\JavaPOS\\jpos111.jar
     input.dpfingerprint.dpenrollment =
     C:\\DigitalPersona\\Bin\\Java\\dpfpenrollment.jar
     input.dpfingerprint.dpverification =
     C:\\DigitalPersona\\Bin\\Java\\dpfpverification.jar
     input.dpfingerprint.dpotjni = C:\\DigitalPersona\\Bin\\Java\\dpotjni.jar
     ```

   - The fingerprint device is enabled in the `jpos.xml` file.

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 F.

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.

   ```
   SET JAVA_HOME=<JDK_INSTALL_DIR>\jre
   SET ANT_HOME=<INSTALL_DIR>\ant
   ```

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

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

4. Run 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-13.4.5.zip` file from the Oracle Software Delivery Cloud at the following Web site:

     https://edelivery.oracle.com/
   - 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.cmd 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.cmd 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.cmd 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 number 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 Misprinted Character Problems in eReceipts"
- "Resolve Misprinted Character Problems in Network Printed Receipts and Reports"

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. For example on Microsoft Windows, MS Gothic can be used to display Chinese characters and Courier New can be used to display Russian characters.

   > **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. 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 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 in the following file:

   ```
   <POS_install_directory>\<client>\pos\receipts\printing\templates\xsl\ipp_default.xsl
   ```

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 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. For example on Microsoft Windows, MS Gothic can be used to display Chinese characters and Courier New can be used to display Russian characters.

   > **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. 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 of receipt or report data into the type of output designated for the configured network printer. 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 in the following file:

   ```
   <POS_install_directory>\<client>\pos\receipts\printing\templates\xsl\ipp_
   default.xsl
   ```

Enable Browser Functionality in the Client Installation

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

To enable browser functionality:

1. Install JDIC on the client:

   JDIC version 0.9.5 is available at the following Web site:

   ```
   http://java.net/projects/jdic/sources/svn/show/tags/RELEASE_JDIC_0_
   9_5/src/jdic/ndist?rev=1736
   ```

   a. Download the `jdic.jar` file.

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

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

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

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

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

Accessing Web Sites Through a Secure HTTP Connection

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

1. Add the server or IP address, on which the secured application is deployed, to the list of Trusted sites.
2. Uncheck the option to require server verification (https:) for all sites in the zone.

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 OracleRetailStore applications on Windows for the store server is `C:\OracleRetailStore\Server`. For the client, the default directory is `C:\OracleRetailStore\Client`. In this guide, these directories are referred to as *<POS_install_directory>*. The subdirectories listed in Table 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 batch files and shell scripts
config	XML configuration files, `.properties` files, and `.dat` files
lib	Point-of-Service application and resource jar files
lib/locales	Text bundles for localization
logs	Log files (additional log files are in the `bin` directory)
receipts	Files for printing of receipts and blueprint jar file

Running Point-of-Service

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

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

To run Point-of-Service:

1. Start the store server:

   ```
   StoreServerConduit.bat
   ```

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

2. Start the registers.

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

   ```
   ClientConduit.bat
   ```

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

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

Creating a Custom Installation

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

- Install Point-of-Service using the installer on a reference machine, and copy the resulting installation to other machines.
  - With this method, you can change the configuration settings of the installation as described in the *Oracle Retail 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 that allows for various hardware options but specifies the software choices your company has chosen.

4

Installation of Mobile Point-of-Service

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

During installation, the Mobile Point-of-Service server application will be deployed to an Oracle WebLogic Server domain. When the domain was created, the JDK was selected. This is the JDK that is used to run the Mobile Point-of-Service server application. For the remainder of this chapter, the JDK installation directory is referred to as
<JDK_INSTALL_DIR>.

This chapter also includes information on setting up the Mobile POS application on the mobile device. See "Mobile POS Application".

Create a New WebLogic Server Domain for Mobile Point-of-Service Server

You can skip this section if you are redeploying to an existing domain.

The Mobile Point-of-Service server application must be deployed to its own dedicated domain. For information on how to perform the following steps, consult your Oracle WebLogic Server documentation.

> **Note:** Back Office, Central Office, Returns Management, and the Mobile Point-of-Service server must have all unique domain names and server names in order to integrate successfully.

To create a new domain:

1. Log on to the server, which is running your WebLogic Server installation, as the user who owns the WebLogic Server installation.
2. Choose a name for the new domain. In the remainder of this installation guide, *<ormpos-domain>* is used for the name.
3. Create this domain.
   - The Mobile Point-of-Service server is accessed through a secure HTTP connection. You need to enable SSL when creating the domain.
   - Set the listen port and SSL listen port numbers so that the numbers are unique for each domain in your configuration.

> **Note:** All domains running Oracle Retail applications must have the same domain credentials.

4. Verify that the administration domain is started and is in running mode.

Expand the Mobile Point-of-Service Distribution

To extract the Mobile Point-of-Service files:

1. Extract the Mobile Point-of-Service Release 13.4.5 distribution zip file.
2. Create a new staging directory for the Mobile Point-of-Service application distribution `ORMPOS-13.4.5.zip` file, for example, `c:\tmp\ormpos\ormpos-staging`.

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

3. Copy or upload `ORMPOS-13.4.5.zip` to *<staging_directory>* and extract its contents. The following files and directories should be created under *<staging_directory>*`\ORMPOS-13.4.5`:

```
ant\
ant-ext\
antinstall\
connectors\
external-lib\
installer-resources\
mobilepos\
.postinstall.cmd
.postinstall.sh
.preinstall.cmd
.preinstall.sh
.preinstall-oas.cmd
.preinstall-oas.sh
.preinstall-was.cmd
.preinstall-was.sh
.preinstall-wl.cmd
.preinstall-wl.sh
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-webapps.xml
build-common-wl.xml
checkdeps.cmd
checkdeps.sh
install.cmd
install.sh
prepare.xml
wallet.xml
```

For the remainder of this chapter, *<staging_directory>*\ORMPOS-13.4.5 is referred to as *<INSTALL_DIR>*.

Set Up for Integration with Central Office

On the Integrate Applications screen, you select the applications that the Mobile Point-of-Service server is integrated with. See Figure C–39. If Central Office is selected on the screen, that application must be running in order for the Mobile Point-of-Service files to be installed correctly.

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 with the store server.

- If **Yes** is selected on the Enable Secure JDBC screen, 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*. See Figure C–9.
- If **Yes** is selected on the Enable Secure RMI, 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*. See Figure C–45.

Obtain the Files Needed for RSA Key Manager

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

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

Obtain the RSA Key Manager Version 3.1 Jar Files

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

1. Obtain the following jar files from your RSA Key Manager provider:
   - cryptoj.jar
   - kmsclient.jar
   - sslj.jar
2. Copy the jar files into *<INSTALL_DIR>*/rsa-jars.

Install the Java Cryptography Extension (JCE)

You must update the security for your JRE. You need to obtain version 6.0 of the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.

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

```
cd <WEBLOGIC_INSTALL_DIR>/<jdk>/jre/lib/security
mv local_policy.jar local_policy.jar.bak
mv US_export_policy.jar US_export_policy.jar.bak
```

2. Download version 6 of the JCE.

   a. Go to the following Web site:

      http://www.oracle.com/technetwork/java/javase/downloads/index.html

   b. Under Additional Resources, find **Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6**.

   c. Click **Download**.

   d. Follow the instructions to download the JCE.

3. Copy the `local_policy.jar` and `US_export_policy.jar` files into the JRE security directory. The files are bundled as `jce_policy-6.zip`.

Run the Mobile Point-of-Service Server Installer

A WebLogic Server domain must be configured and started before you can run the Mobile Point-of-Service server installer. This installer will configure and deploy the Mobile Point-of-Service server.

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

> **Note:** To see details on every screen and field for the installation, see Appendix C.

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

2. Set the `JAVA_HOME` environment variable to the location of the Java JRE used by the WebLogic Server instance for the Mobile Point-of-Service server.

   > **Note:** The installer is not compatible with versions of Java earlier than Java 6 Update 24.

3. When installing the server, set the account of the user running the installer to run as an administrator. Set the account using Microsoft Windows 2008 Server.

4. Run the `install.cmd` script. This will launch the installer. After installation is complete, a detailed installation log file is created at `<ORMPOS_install_directory>\ormpos-install-yyyyMMddHHmm.log`

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

   > **Note:** The typical usage for GUI mode does not use arguments.
   >
   > ```
   > install.cmd
   > ```

Resolve Errors Encountered During Application Installation

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

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

Disabled Non-SSL Port

You can choose to disable the non-SSL port on the Turn Off the Application Server's Non-SSL Port screen. See Figure C–49. If you select **Yes** on the screen, you must delete the transaction log files.

To delete the files:

1. Stop the application server.
2. Delete the transaction log files:

   ```
   <ormpos-domain>/server/<serverName>/data/store/default/WLS*.dat
   ```

3. Start the application server.

For more information, see the following Web site. Refer to the *Moving a Server* section.

http://download.oracle.com/docs/cd/E12839_01/web.1111/e13731/trxman.htm#i1053371

Manual Deployment of the Mobile Point-of-Service Server Application

Skip this section if you chose the default option of allowing the installer to complete installation to the application server on the Manual Deployment Option screen. See Figure C–47.

The installer includes the option to configure the application locally and skip deployment to the application server. If this option is chosen, the installer will make the configured application files available under `<INSTALL_DIR>\mobilepos\configured-output\`.

If you chose this installer option, you complete the installation by following these steps:

- To deploy using the ant target:
  1. Update the following property in the `ant.install.properties` file.

     ```
     input.install.to.appserver = true
     ```

  2. Run the following ant target:

     ```
     install.cmd ant init app-ear-deploy -propertyfile ant.install.properties
     ```

- To deploy from the application server console:
  1. Run the following target:

     ```
     install.cmd ant init-app-ear-deploy
     ```

  2. Deploy the ear file from the following location:

     ```
     <INSTALL_DIR>\mobilepos\mobilepos.war
     ```

     Note: When deploying the war file, provide the same application name and context root you gave to the installer. These values were stored in the `<INSTALL_DIR>\ant.install.properties` file by the installer.

Mobile POS Application

This section contains information for setting up the Mobile POS application. The following information is included:

- "Setting Up the Mobile POS Application Xcode Project"
- "Configuring and Deploying the MPOS UI Certificate"
- "Configuring the Mobile Point-of-Service Application on a Mobile Device"

Setting Up the Mobile POS Application Xcode Project

This section describes how to set up the Mobile POS Xcode project included in the Mobile Point-of-Service Release 13.4.5 distribution zip file.

The `ORMPOS-13.4.5_client.zip` file in the distribution zip file contains the Xcode workspace. It contains project for use in distributing and customizing the Mobile POS iOS application that runs on iPod Touch (4th Generation) devices.

The following sections describe the steps needed to set up the project. The instructions are for an Apple computer, as code is only available for the Apple OS.

Extract the Xcode Project

To extract the Xcode project:

1. Create a directory to hold the extracted contents of the `ORMPOS-13.4.5_client.zip` file.
2. Copy the `ORMPOS-13.4.5_client.zip` file into the new directory.
3. Unzip the file into the new directory.
4. Open the `mobilepos` directory created in Step 3.

The `mobilepos` directory structure is a typical iOS application. This is a hybrid application in that most of the business logic and presentation are run in a Web view, with most programming done in Web technologies (HTML, CSS, and JavaScript) rather than native iOS Objective C. For best practices in extending, adding, and changing functionality and presentation in Mobile POS, see the *Oracle Retail POS Suite Implementation Guide, Volume 5 - Mobile Point-of-Service*.

Most application files are in the `mobilepos/www` directory, including the following:

- HTML files used by the Web view
- JavaScript in the `mobilepos/www/js` directory
- CSS files in the `mobilepos/www/css` directory
- Translation bundles in the `mobilepos/www/js/translations` directory

Adding new JavaScript and CSS files to the project requires referencing those files in the `mobilepos/www/index.html` file.

Ensure MobilePOS.framework is in Place

To ensure that `MobilePOS.framework` is in place:

1. In the `mobilepos` directory, verify that there is a `MobilePOS.framework` directory. This is a native iOS package that enables communication with the internal hardware of the iPod Touch.

2. In the `mobilepos/Classes` directory, verify that the following four files are present:

> **Note:** Do not edit these files.

- `AppDelegate.h`
- `AppDelegate.m`
- `MobilePOSPlugins.h`
- `MobilePOSPlugins.m`

Install the Sled Framework

Mobile POS requires that a sled framework be in place before the application can be built. A *null* sled framework is available from Oracle that enables compilation of the Mobile POS UI without a vendor sled framework. The application can also be built using a sled framework from VeriFone to enable Mobile POS to run with a VeriFone VX600 sled attached.

To configure the sled framework to enable compilation of the Mobile POS UI without a vendor sled framework:

1. Download the *null* sled framework from My Oracle Support. The patch number is 14792769. My Oracle Support is available at the following Web site:

   `https://support.oracle.com`

2. Unzip the package from Step 1. Inside, there is a directory named `VMF.framework`.
3. Copy the `VMF.framework` directory into the `/Developer/Library/Frameworks` directory.

To use Mobile POS with a VeriFone VX600 sled, install the VeriFone sled framework:

1. Obtain the supported version of the VeriFone framework, 1.0.2.109, directly from VeriFone.
2. Unzip the package from Step 1. Inside, there should a directory named `VMF.framework`.
3. Copy the `VMF.framework` directory into the `/Developer/Library/Frameworks` directory.

Install the PhoneGap Framework

Mobile POS also has an external dependency on the PhoneGap framework, specifically PhoneGap 1.4.1. It can be obtained in the Archives section at the following Web site:

`http://phonegap.com/download`

To install the PhoneGap framework:

1. Unzip the PhoneGap 1.4.1 package that was downloaded.
2. Navigate to the `lib/ios` subdirectory within the directory created in Step 1.
3. Double-click `PhoneGap-1.4.1.dmg`. This mounts the file and opens a new Finder window.

4. Run the `PhoneGap-1.4.1.pkg` in the window opened up in Step 3 by double-clicking the file. Follow all the steps to set up PhoneGap. This installs PhoneGap into the `Library/Frameworks` subdirectory in the current user's home directory. For example, `/Users/jdoe/Library/Frameworks`.
5. Create a directory named `PhoneGap` in the `/Developer/Library/Frameworks` directory.
6. Copy the `PhoneGap.framework` directory from Step 4 into the `/Developer/Library/Frameworks/PhoneGap` directory.

Verify the Build Settings

To verify the build settings:

1. Double-click the `mobilepos.xcodeproj` file in the `mobilepos` directory. This opens the project in Xcode. There should be no build errors after opening the project if the PhoneGap, VMF, and Mobile POS frameworks are in the locations specified in the previous steps.

   If there are build errors or warnings that Xcode cannot find any of those frameworks, verify their locations and update the Framework Search Path after any changes in framework location.
2. In the Xcode Navigator panel, click the `mobilepos` project. Then, in the Xcode main panel, click the `mobilepos` build target.
3. Click the **Build Settings** tab and scroll down to the Search Paths heading. Verify that `/Developer/Library/Frameworks/PhoneGap` and `/Developer/Library/Frameworks/VMF` are in the Framework Search Paths field. If any of the frameworks were put in a different location, that location must be added to the Framework Search Paths value.
4. Scroll to Architectures. Set the value of Valid Architectures to armv7. Depending on your version of Xcode, the value of Valid Architectures may default to `armv7 armv7s`. However, armv7s is not a valid architecture for Mobile POS 13.4.5.

Build the Project

By following the steps in the preceding sections, the `mobilepos` project is ready to be run in an iOS Simulator. For information on setting up and using the simulator, see the following Web site:

`https://developer.apple.com`

Before running the application on a device, install and configure two code signing identities. For instructions, see "Configuring and Deploying the MPOS UI Certificate".

Configuring and Deploying the MPOS UI Certificate

Before using the Mobile POS Xcode workspace to develop, test, or distribute a customized Mobile POS application, all developers need certificates and provisioning profiles in place to perform code signing.

In order to run the Mobile POS application on an iOS device, the tasks described in this section are performed in the iOS Provisioning Portal. An Apple ID and password is needed to access the iOS Provisioning Portal. The iOS Provisioning Portal is accessed at the following Web site:

`https://developer.apple.com/ios/my/overview/index.action`

The information in this section is based on the *iOS Team Administration Guide*. The guide describes how to use the iOS Provisioning Portal. It is available at the following Web site:

https://developer.apple.com/library/ios/#documentation/ToolsLanguages/Conceptual/DevPortalGuide/Introduction/Introduction.html#//apple_ref/doc/uid/TP40011159

The *iOS Team Administration Guide* uses the concepts of development team, team administrator, and team member. These concepts are also used in this section.

The team administrator needs to be involved in completing all steps in this section. Creating provisioning profiles is covered, but steps for administrating the team's settings are not included in this section. For specific information, see the *iOS Team Administration Guide*.

Create the Development Certificate

Running the Mobile POS application on a device requires a development certificate for each development team member. A developer creates a development certificate request in Xcode by following these steps:

1. Plug in an iOS device to the development computer.
2. Start Xcode.
3. Go to the Organizer. In the Xcode menu, go to Window/Organizer.
4. Select the device from the list on the left side of the Organizer.
5. Click **Use for Development**.
6. Copy the Unique Device Identifier (UDID) from the Organizer. This is a 40-digit hexadecimal number. Send this UDID to the team administrator and request that the device be added to the team's list of development devices in the iOS Provisioning Portal.

The team member must wait until the team administrator adds the device to the team provisioning portal. The team administrator should notify the team member when the device is added. For steps used by the team administrator to add a team member's device, see the *iOS Team Administration Guide*.

Once the team administrator notifies the team member that the device is added to the team’s provisioning portal, the team member should go back to the Organizer in Xcode:

1. In the Organizer's left column, click **Provisioning Profiles** under the Library heading.
2. Make sure the **Automatic Provisioning** check box is selected.
3. Click **Refresh**. If there is not a development certificate in the keychain, Xcode prompts to request one. Click **yes** on this request.

   The team administrator is notified of this development certificate request. The team administrator must approve this request before the team member can proceed.

If the team administrator has not already done so, the team administrator should use the iOS Provisioning Portal to create a development provisioning profile for the team. See the *iOS Team Administration Guide* for information on creating and configuring application IDs and creating and downloading development provisioning profiles.

After approving the developer certificate, the team administrator should notify the team member. The team member can then follow these steps:

1. Plug in the iOS device to the development computer and return to the Xcode Organizer.
2. Select **Provisioning Profiles** under the Library section. Click **Refresh** at the bottom of the Organizer. The developer certificate for Xcode and the provisioning profile are installed on the device.
3. Return to the Xcode project in the main window. Click the project in the Navigator view and then click the build target.
4. In the Build Settings tab, scroll down to the Code Signing section. Under Code Signing Identity, there should be Debug and Release options. Click the value next to Debug and choose the newly installed iOS developer identity from the list.
5. Make sure the project is built for debug and not release. In the Xcode scheme editor, click the build target and select **Edit Scheme**.
6. Click **Run <*project name*>**. In the Info tab, choose **Debug** for the Build Configuration setting.
7. Click **OK**. Development setup is complete.

Distribution

With the Enterprise Program, a team can sign iOS applications for distribution such that each device it runs on does not require a developer certificate and provisioning profile. This allows a company to use their own distribution procedure, whether it is through email, a customized Web store, simple URLs, or manually adding the application to a device through Apple iTunes.

Create the Distribution Certificate

The team administrator must create and manage the distribution certificate and provisioning profile. Only the team administrator can perform these tasks.

- If the team administrator has access to Xcode, the team administrator should follow the instructions in the *iOS Team Administration Guide* for using Xcode to create a distribution certificate.
- If the team administrator does not have access to Xcode, the team administrator should follow the instructions for manually managing a distribution certificate in the *iOS Team Administration Guide*.

> **Note:** When downloading and installing distribution certificates, be sure to keep the distribution certificate in a safe place.

Create the Distribution Provisioning Profile

After the team administrator creates a distribution certificate, the team administrator should create a distribution provisioning profile. Developer and distribution provisioning profiles are different. The team administrator should follow the instructions for creating and downloading a distribution provisioning profile in the *iOS Team Administration Guide*.

> **Note:** Keep the downloaded distribution provisioning profile in a safe place.

Install the Distribution Certificate and Provisioning Profile

If the team administrator is not going to sign and package the iOS application for distribution, the team administrator should send the distribution certificate and distribution provisioning profile to a team member to be responsible for these actions. The responsible team member should first install the distribution certificate by double clicking it. This installs the certificate into the keychain. The team member should then install the distribution provisioning profile by double clicking it. This installs the provisioning profile in the Organizer.

Create the Application for Distribution

To create the application for distribution:

1. Return to the Xcode project in the main window. Click the project in the Navigator view and then click the build target.
2. In the Build Settings tab, scroll down to the Code Signing section. Under Code Signing Identity are Debug and Release options. Click the value next to Release and choose the newly installed iOS distribution identity from the list.
3. Make sure the project is built for release and not debug. In the Xcode scheme editor, click the build target and select **Edit Scheme**.
4. Click **Run <*project name*>**. In the Info tab, choose Release for the Build Configuration setting.
5. In the Main Window, select **Product**, **Build For**, and then **Archiving**.
6. Click **Product** and then **Archive**. A list of archived builds appears. The distributable application is based on the build just created.
7. Select the build that was just created based on its timestamp. Click **Share**. A pop-up menu appears.
    a. For the Contents option, select **iOS App Store Package (.ipa)**.
    b. For the Identity option, make sure the iOS distribution identity is selected. Click **Next**.
    c. Choose a location where to save the application file and enter a name.
    d. Depending on the distribution method, select the appropriate option. Check the **Save for Enterprise Distribution** option and fill in the required fields. If the application is going to be installed through iTunes, do not check this option.
8. Click **Save**. There is now a fully functional and signed iOS application ready for distribution.

Additional Notes

Note the following:

- For all Mobile POS servers, only valid certificates from a trusted third-party signing authority will work. Self-signed certificates will not work. The trusted root certificates for iOS 5 are listed here:

  `http://support.apple.com/kb/HT5012`

- The application requires a valid UDID, even for the simulator. The UDID for the simulator is like any other Mobile POS UDID and needs to be registered with the server. The UDID of the simulator is the same as the UDID of the Mac. The UDID of the Mac can be obtained from System Profiler:

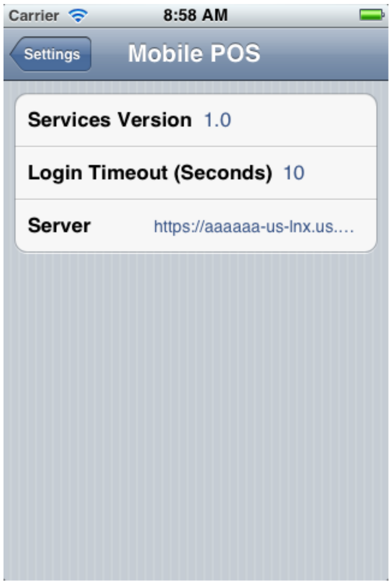
    1. To run System Profiler, select **Applications**, **Utilities**, and then **System Profiler**.
    2. Click **Hardware** in left column.
    3. Look for the UDID under Hardware UDID in the right column.

Configuring the Mobile Point-of-Service Application on a Mobile Device

The Mobile Point-of-Service application must be downloaded and installed on the mobile devices. To configure the mobile device after installation:

1. Open the Settings screen for the Mobile POS application.

Figure 4–1 Mobile POS Settings Screen



Services Version 1.0

Login Timeout (Seconds) 10

Server https://aaaaaa-us-lnx.us....

2. Set the address of the server that the device uses to communicate with the Mobile POS server.

A

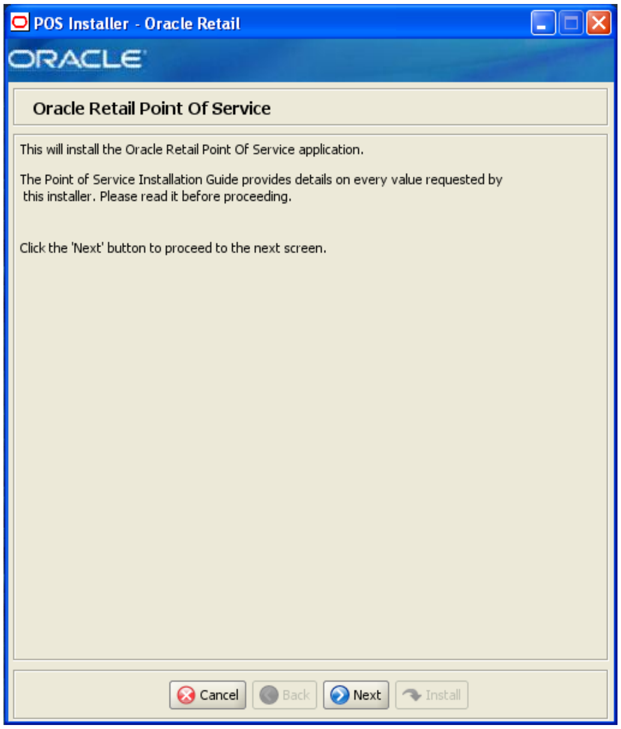
Appendix: Installer Screens for Server Installation on Windows

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

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

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

Figure A–1 Introduction



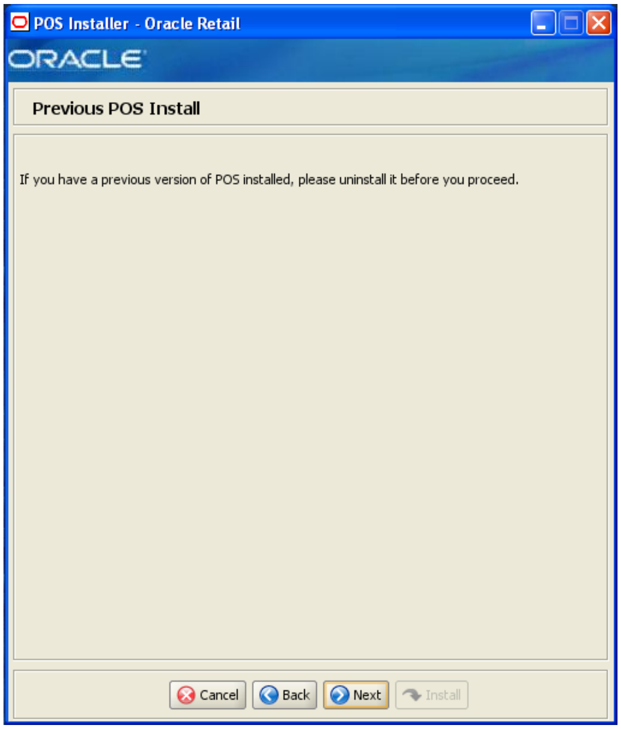
Oracle Retail Point Of Service

This will install the Oracle Retail Point Of Service application.

The Point of Service Installation Guide provides details on every value requested by this installer. Please read it before proceeding.

Click the 'Next' button to proceed to the next screen.

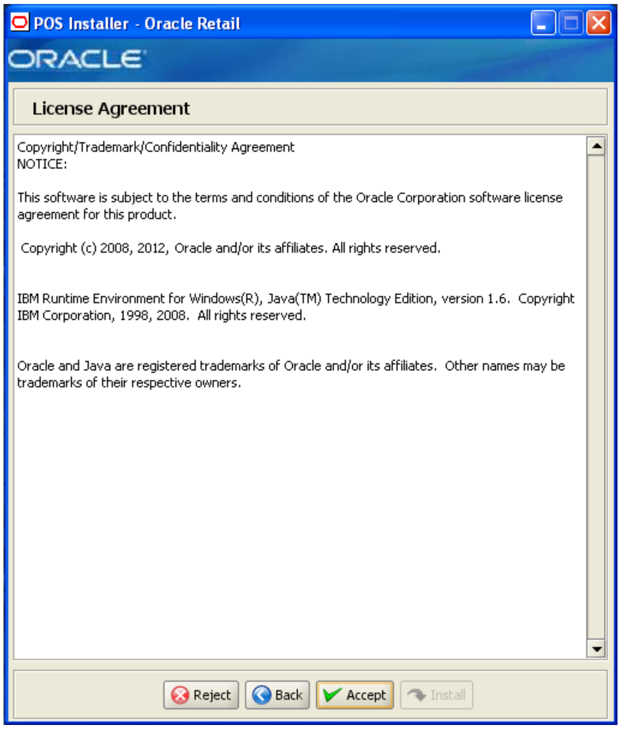
Figure A–2 Previous POS Install



Previous POS Install

If you have a previous version of POS installed, please uninstall it before you proceed.

Figure A–3 License Agreement



License Agreement

Copyright/Trademark/Confidentiality Agreement
NOTICE:

This software is subject to the terms and conditions of the Oracle Corporation software license agreement for this product.

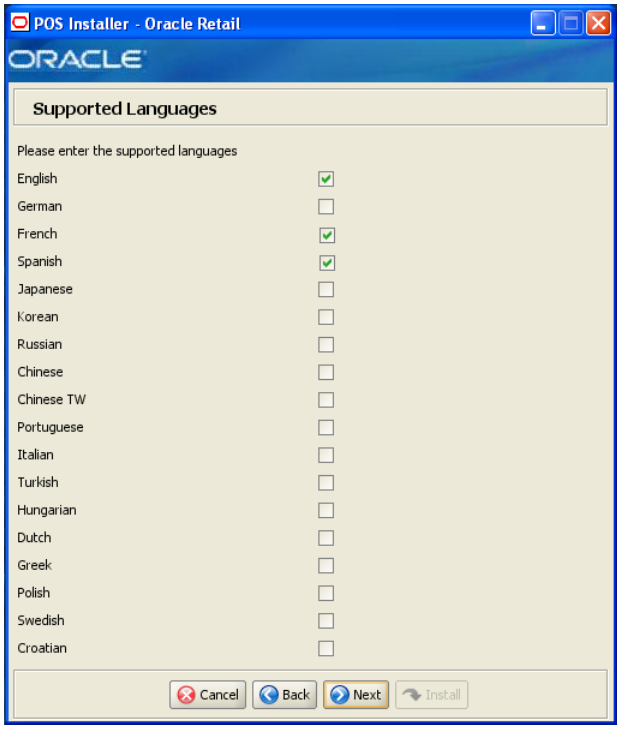
Copyright (c) 2008, 2012, Oracle and/or its affiliates. All rights reserved.

IBM Runtime Environment for Windows(R), Java(TM) Technology Edition, version 1.6. Copyright IBM Corporation, 1998, 2008. All rights reserved.

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

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

Figure A–4 Supported Languages



Supported Languages

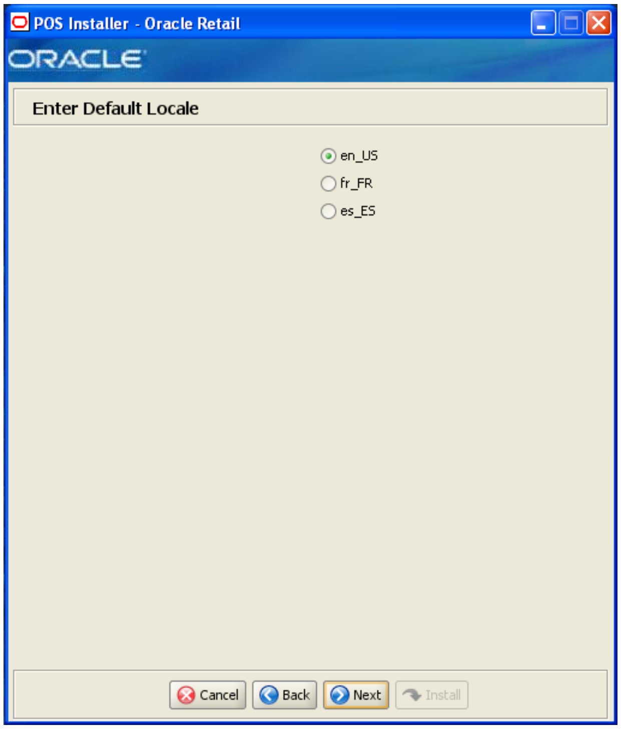
Please enter the supported languages

English ☑
German □
French ☑
Spanish ☑
Japanese □
Korean □
Russian □
Chinese □
Chinese TW □
Portuguese □
Italian □
Turkish □
Hungarian □
Dutch □
Greek □
Polish □
Swedish □
Croatian □

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, French, and Spanish

Figure A–5 Enter Default Locale



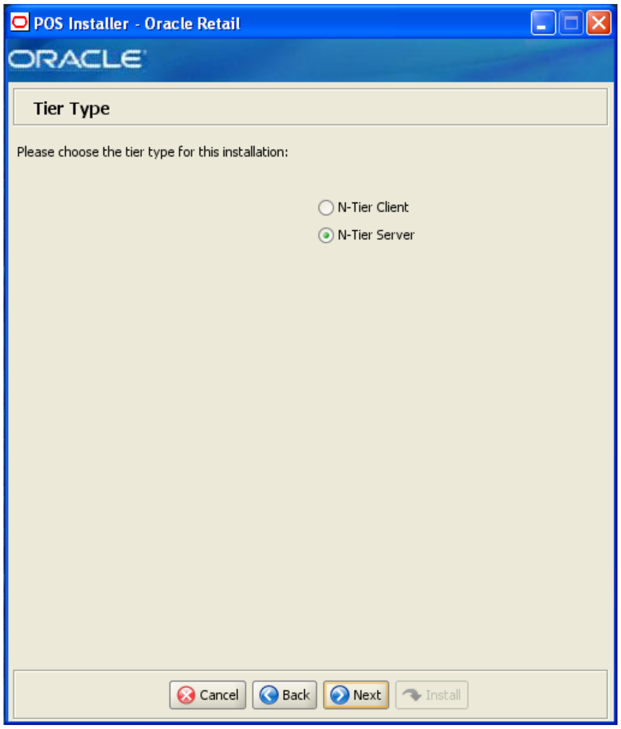
Enter Default Locale

● en_US
○ fr_FR
○ es_ES

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



POS Installer - Oracle Retail

Tier Type

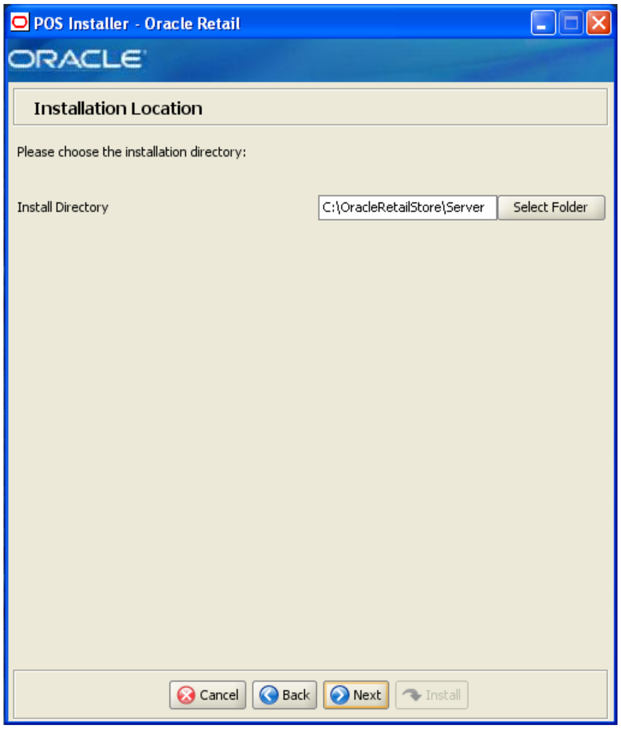
Please choose the tier type for this installation:

○ N-Tier Client
● N-Tier Server

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 Installation Location



POS Installer - Oracle Retail

Installation Location

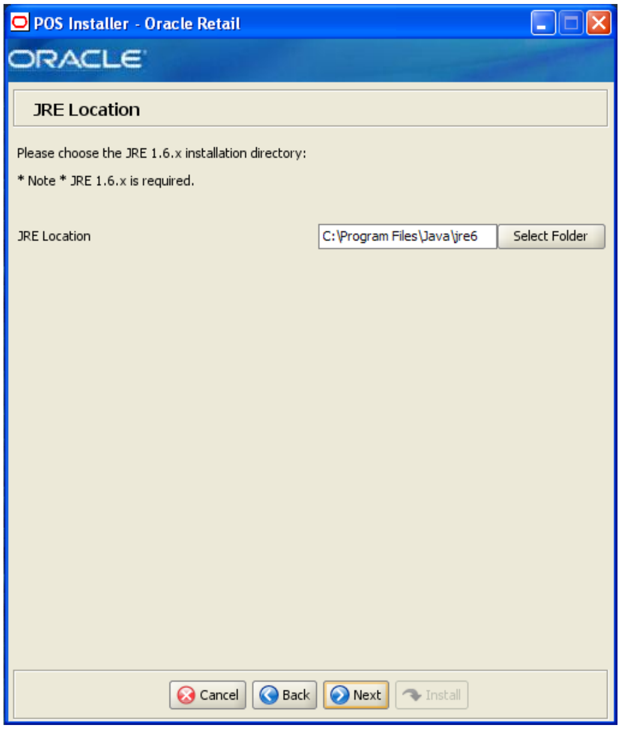
Please choose the installation directory:

Install Directory C:\OracleRetailStore\Server

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 installing for Windows and **N-Tier Server** is selected for the Tier Type, the default installation directory is `OracleRetailStore\Server`. **Note:** The server and the client must not be installed into the same directory. In this guide, *`<POS_install_directory>`* refers to the selected installation directory for the server or client. Files specific to Point-of-Service are copied to the `\pos` subdirectory of `<POS_install_directory>`.
Example	`C:\OracleRetailStore\Server`

Figure A–8 JRE Location



Please choose the JRE 1.6.x installation directory:

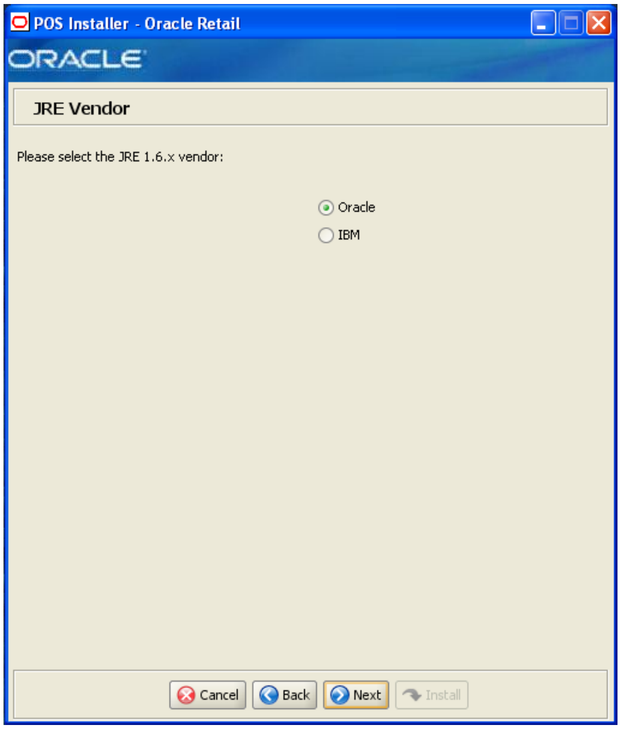
* Note * JRE 1.6.x is required.

JRE Location C:\Program Files\Java\jre6

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	`C:\Program Files\Java\jre6`

Figure A–9 JRE Vendor



POS Installer - Oracle Retail

JRE Vendor

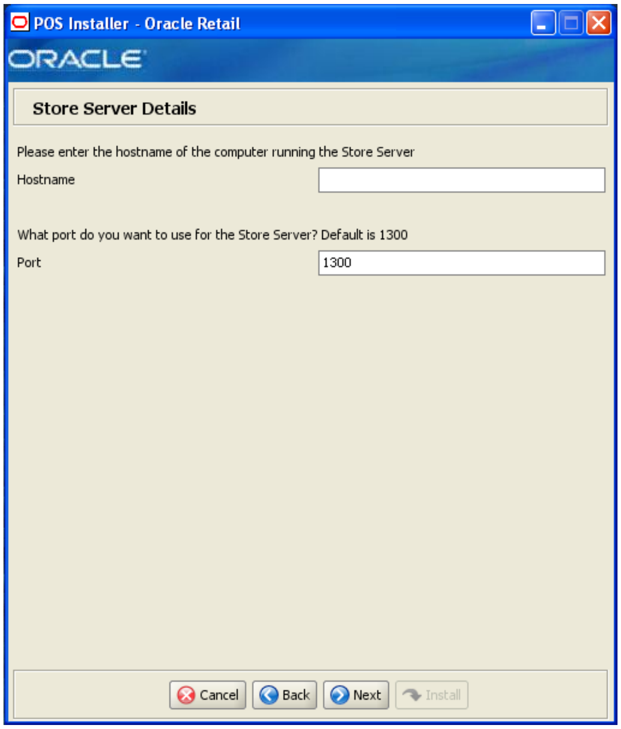
Please select the JRE 1.6.x vendor:

● Oracle
○ IBM

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 **Oracle**.

Figure A–10 Store Server Details



Store Server Details

Please enter the hostname of the computer running the Store Server

Hostname

What port do you want to use for the Store Server? Default is 1300

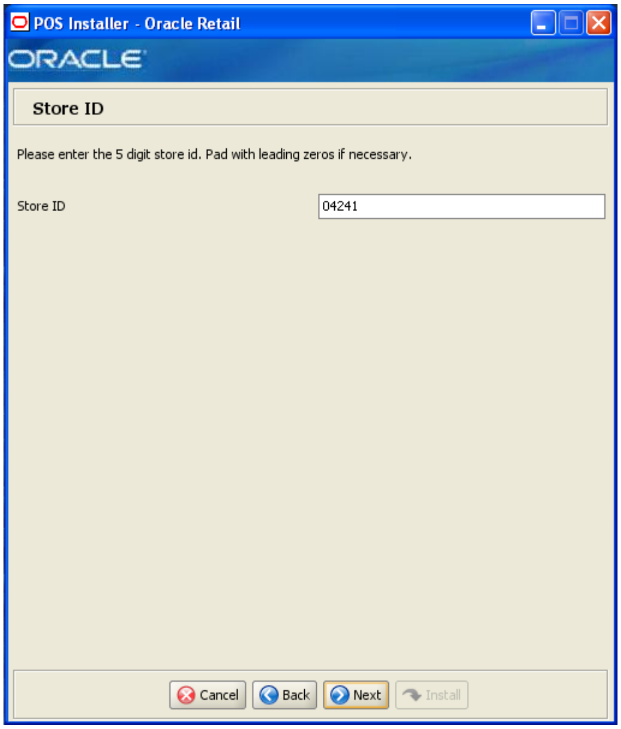
Port: 1300

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–11 Store ID



POS Installer - Oracle Retail

Store ID

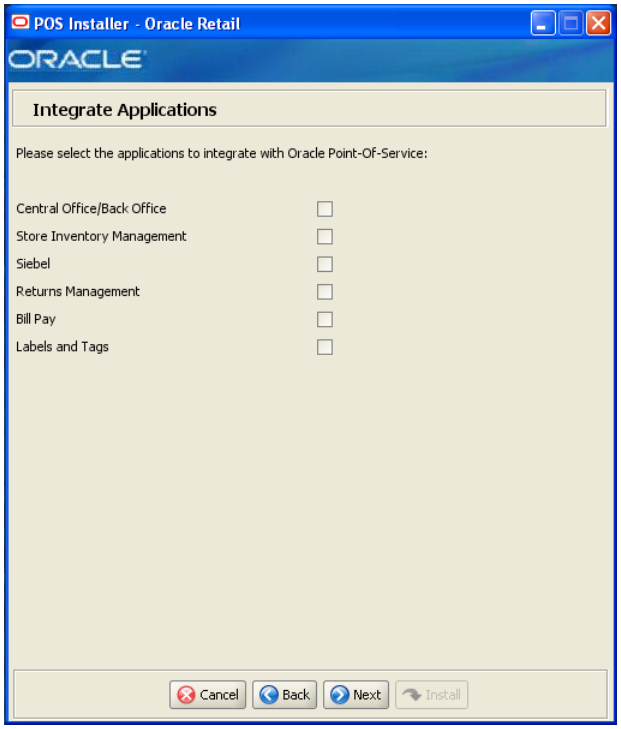
Please enter the 5 digit store id. Pad with leading zeros if necessary.

Store ID: 04241

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–12 Integrate Applications



Integrate Applications

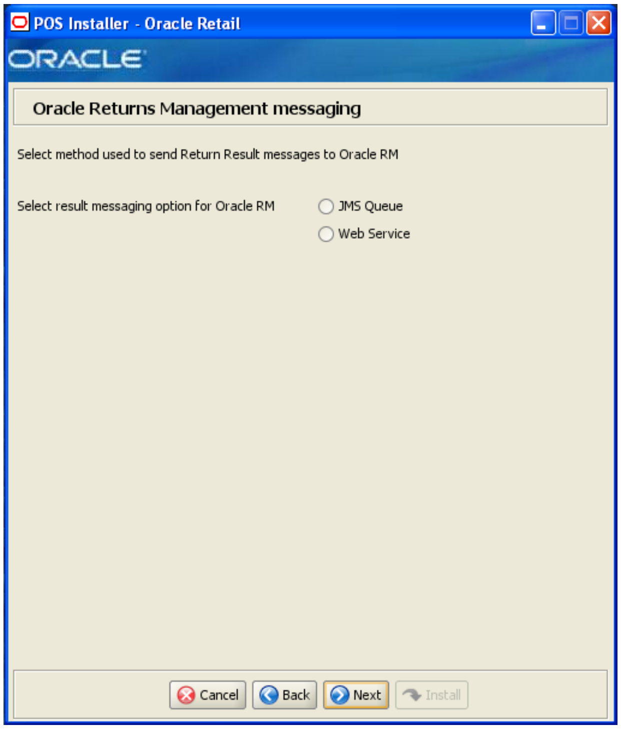
Please select the applications to integrate with Oracle Point-Of-Service:

Central Office/Back Office □
Store Inventory Management □
Siebel □
Returns Management □
Bill Pay □
Labels and Tags □

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–13 Oracle Returns Management Messaging



Oracle Returns Management messaging

Select method used to send Return Result messages to Oracle RM

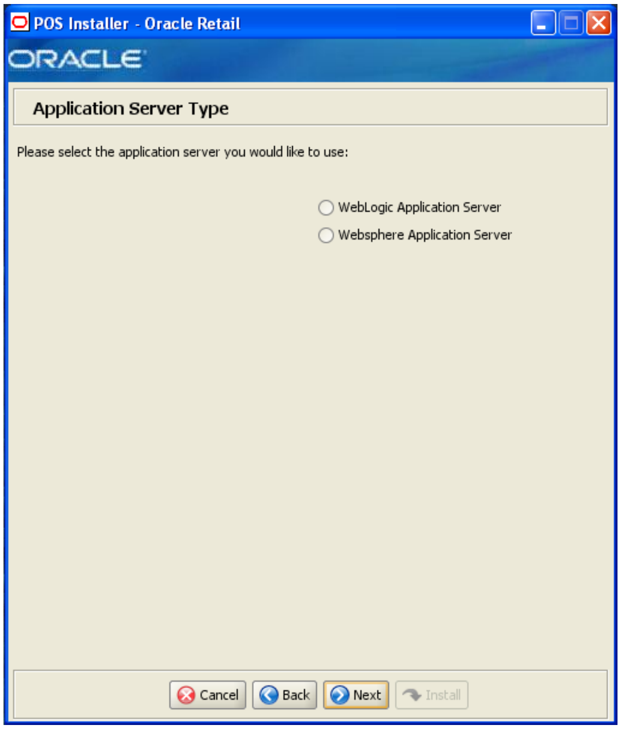
Select result messaging option for Oracle RM ○ JMS Queue ○ Web Service

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–14 Application Server Type



Application Server Type

Please select the application server you would like to use:

○ WebLogic Application Server

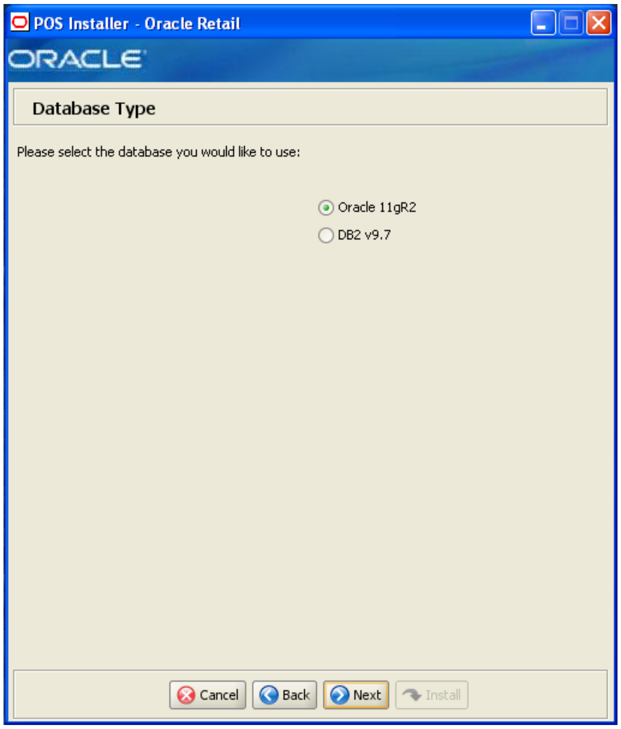
○ Websphere Application Server

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 **WebLogic Application Server**.

Figure A–15 Database Type



Database Type

Please select the database you would like to use:

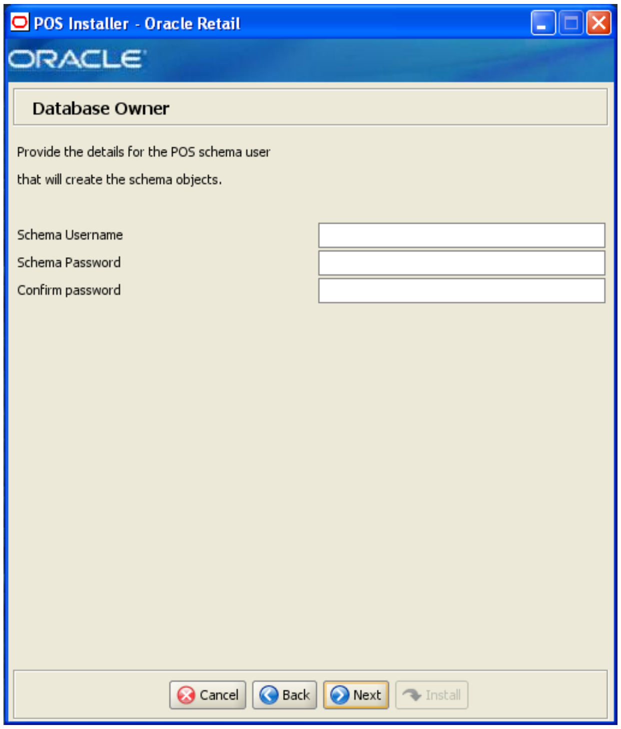
● Oracle 11gR2

○ DB2 v9.7

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 **Oracle 11gR2**.

Figure A–16 Database Owner



POS Installer - Oracle Retail

Database Owner

Provide the details for the POS schema user that will create the schema objects.

Schema Username

Schema Password

Confirm password

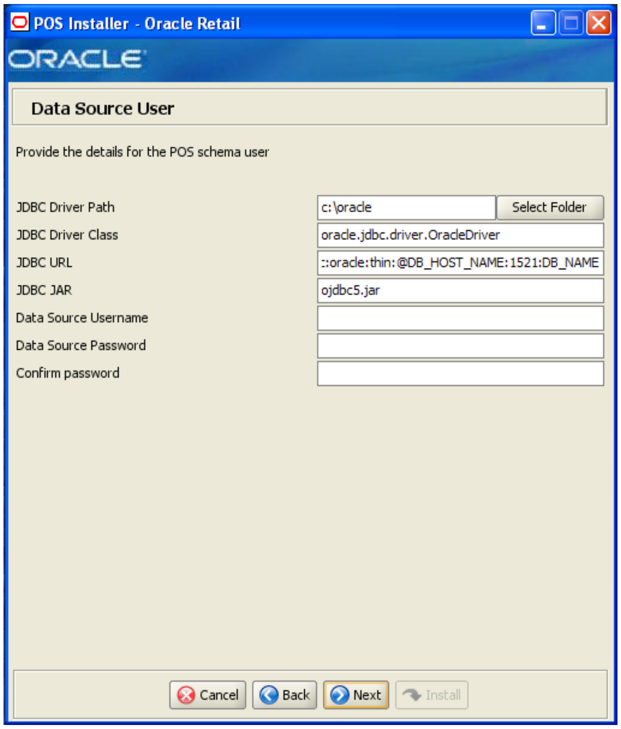
The fields on this screen are described in the following tables.

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–17 Database Source User



POS Installer - Oracle Retail

Data Source User

Provide the details for the POS schema user

JDBC Driver Path	c:\oracle
JDBC Driver Class	oracle.jdbc.driver.OracleDriver
JDBC URL	::oracle:thin:@DB_HOST_NAME:1521:DB_NAME
JDBC JAR	ojdbc5.jar
Data Source Username	
Data Source Password	
Confirm password	

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	`c:\oracle`

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

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 E.
Example	`jdbc:oracle:thin:@DB_HOST_NAME:1521:DB_NAME`

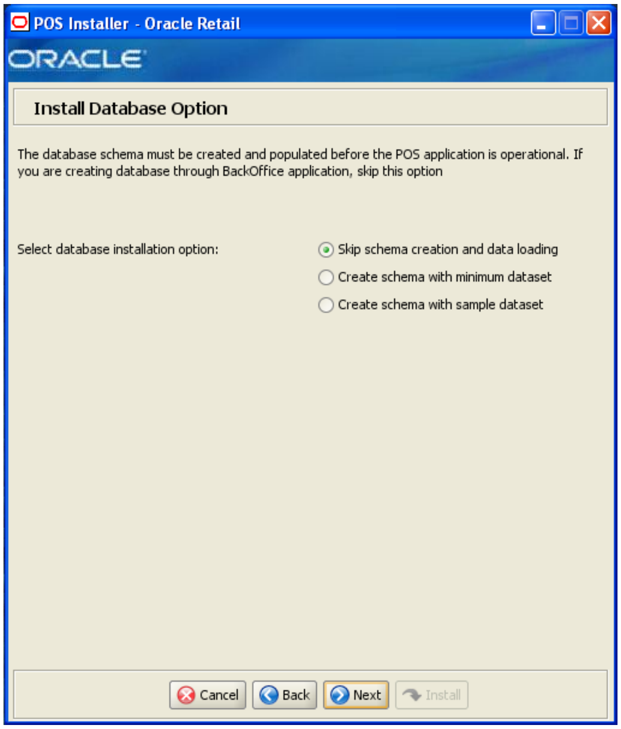
Details	Content
Field Title	JDBC JAR
Field Description	Enter the name of the jar containing the database driver.
Example	`ojdbc5.jar`

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–18 Install Database Option



Install Database Option

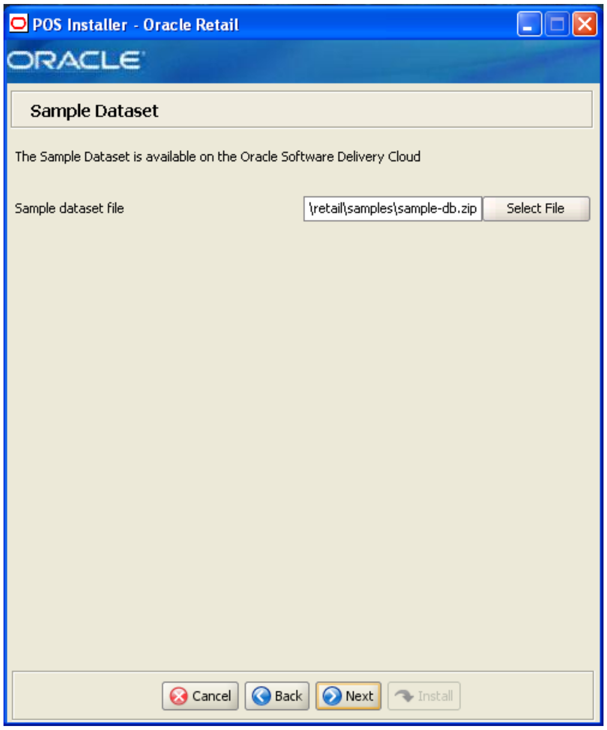
The database schema must be created and populated before the POS application is operational. If you are creating database through BackOffice application, skip this option

Select database installation option:
● Skip schema creation and data loading
○ Create schema with minimum dataset
○ Create schema with sample dataset

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–19 Sample Dataset



Sample Dataset

The Sample Dataset is available on the Oracle Software Delivery Cloud

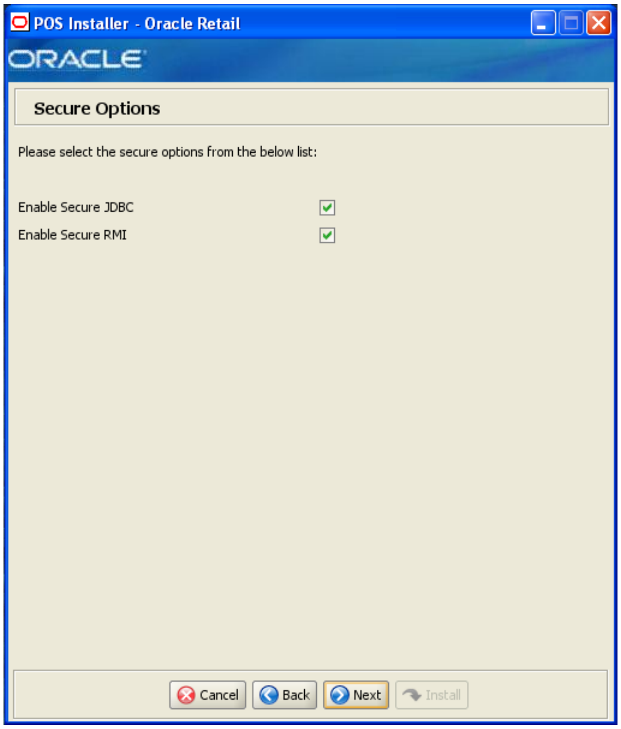
Sample dataset file \retail\samples\sample-db.zip

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-Release 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	`C:\oracle\retail\samples\sample-db.zip`

Figure A–20 Secure Options



Secure Options

Please select the secure options from the below list:

Enable Secure JDBC ☑

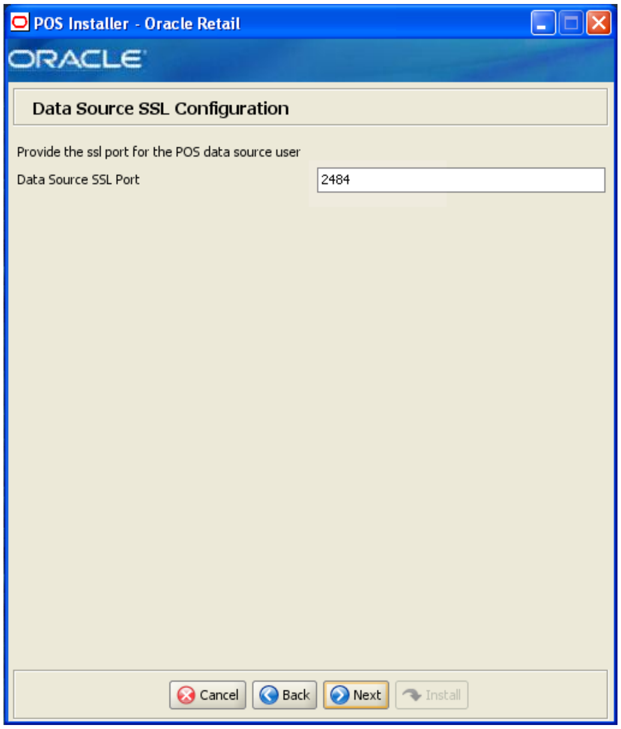
Enable Secure RMI ☑

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–21 Data Source SSL Configuration



Data Source SSL Configuration

Provide the ssl port for the POS data source user

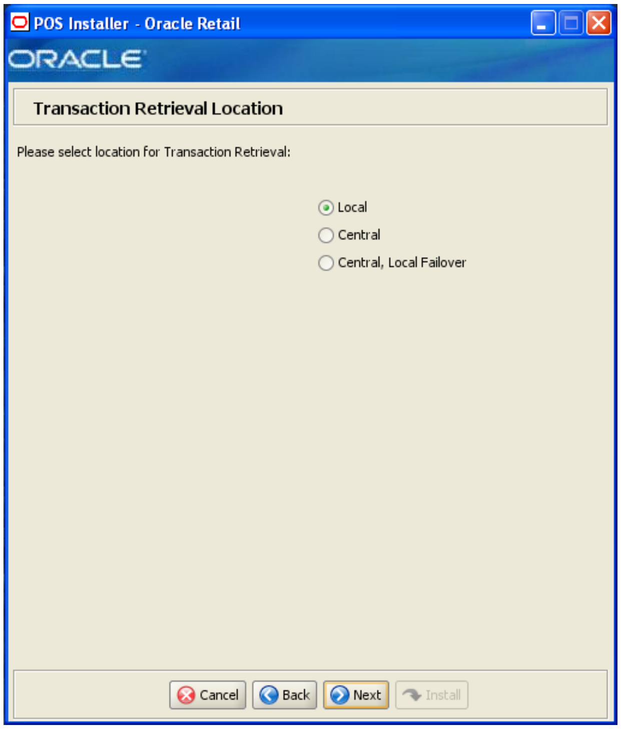
Data Source SSL Port: 2484

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	2484

Figure A–22 Transaction Retrieval Location



Transaction Retrieval Location

Please select location for Transaction Retrieval:

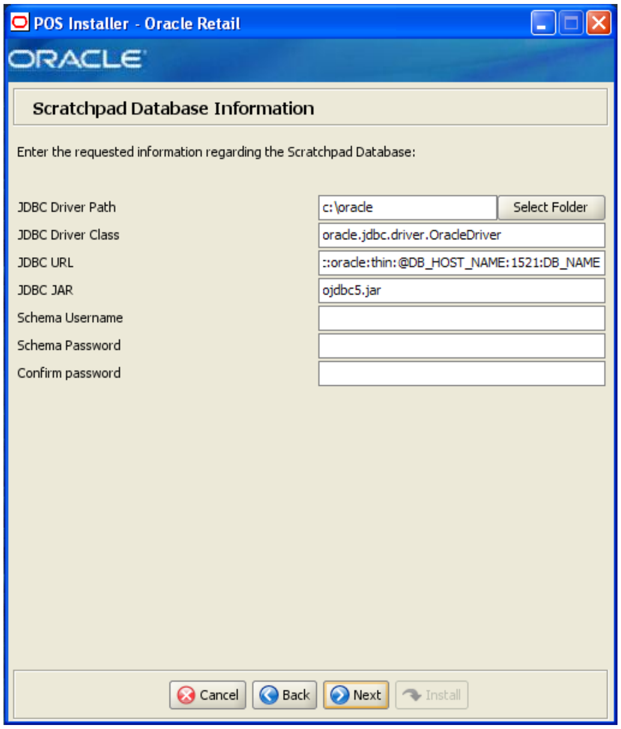
● Local
○ Central
○ Central, Local Failover

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–23 Scratchpad Database Information



Scratchpad Database Information

Enter the requested information regarding the Scratchpad Database:

JDBC Driver Path	c:\oracle
JDBC Driver Class	oracle.jdbc.driver.OracleDriver
JDBC URL	::oracle:thin:@DB_HOST_NAME:1521:DB_NAME
JDBC JAR	ojdbc5.jar
Schema Username	
Schema Password	
Confirm password	

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

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

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	`C:\oracle`

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

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 E.
Example	`jdbc:oracle:thin:@DB_HOST_NAME:1521:DB_NAME`

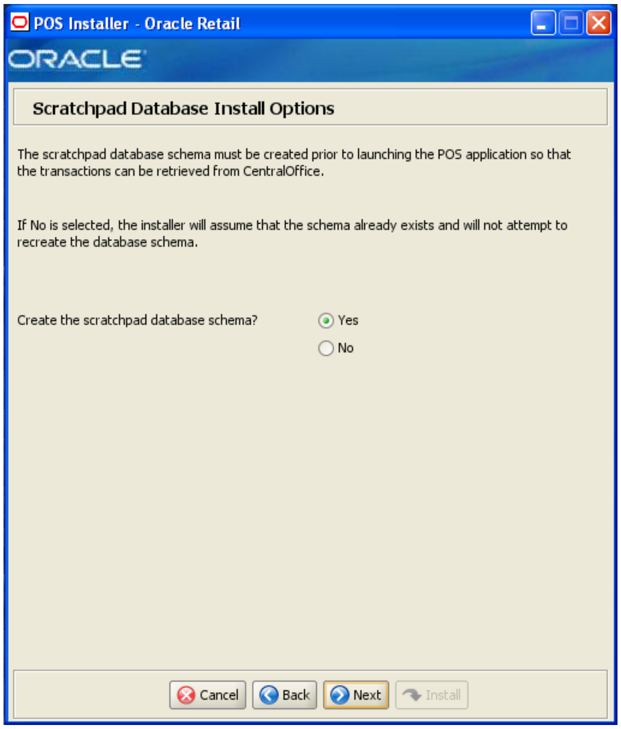
Details	Content
Field Title	JDBC JAR
Field Description	Enter the name of the jar containing the database driver.
Example	`ojdbc5.jar`

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–24 Scratchpad Database Install Options



Scratchpad Database Install Options

The scratchpad database schema must be created prior to launching the POS application so that the transactions can be retrieved from CentralOffice.

If No is selected, the installer will assume that the schema already exists and will not attempt to recreate the database schema.

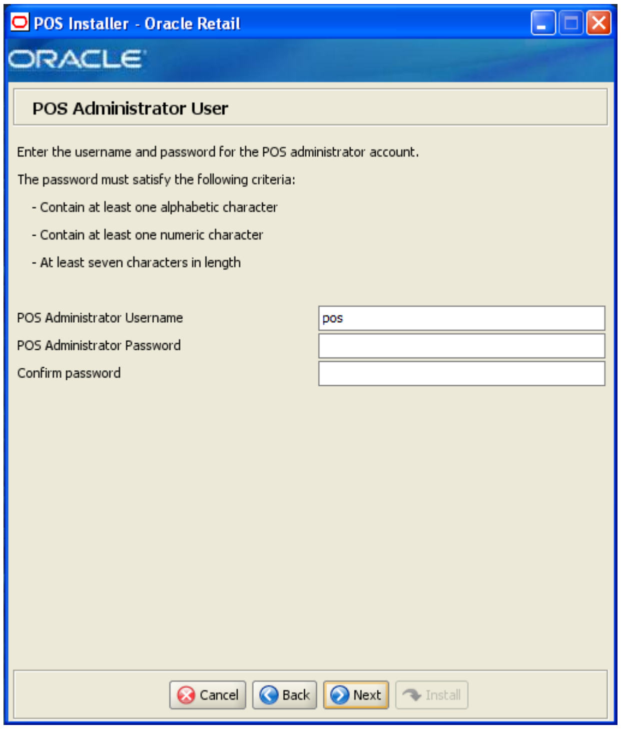
Create the scratchpad database schema? ● Yes ○ No

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–25 POS Administrator User



POS Administrator User

Enter the username and password for the POS administrator account.

The password must satisfy the following criteria:

- Contain at least one alphabetic character
- Contain at least one numeric character
- At least seven characters in length

POS Administrator Username: pos

POS Administrator Password:

Confirm password:

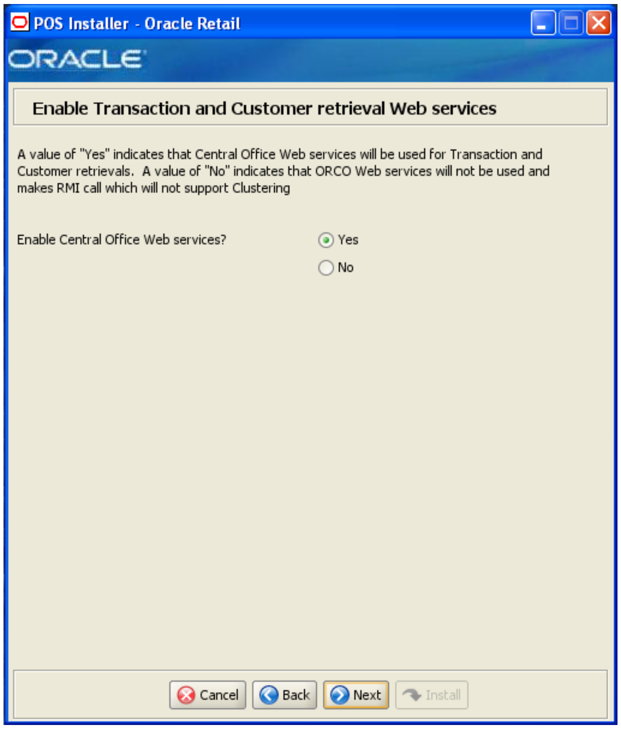
The fields on this screen are described in the following tables.

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–26 Enable Transaction and Customer Retrieval Web Services



Enable Transaction and Customer retrieval Web services

A value of "Yes" indicates that Central Office Web services will be used for Transaction and Customer retrievals. A value of "No" indicates that ORCO Web services will not be used and makes RMI call which will not support Clustering

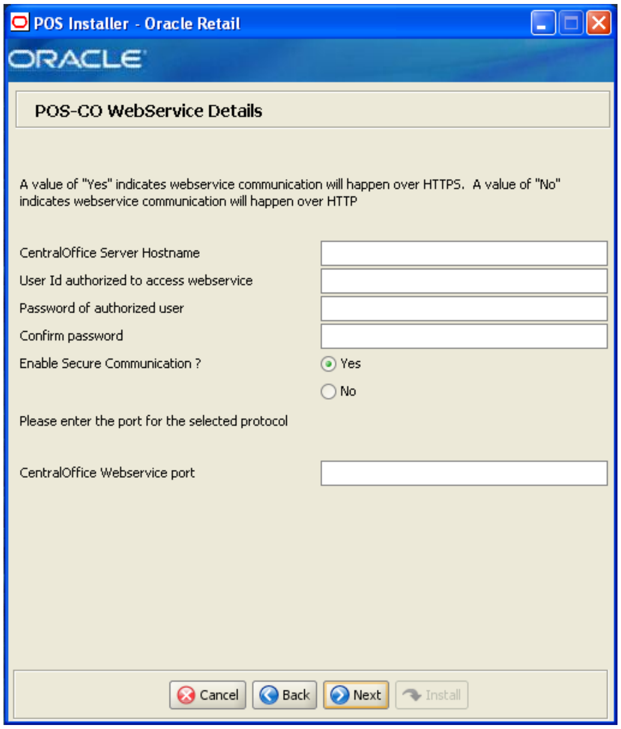
Enable Central Office Web services? ● Yes ○ No

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–27 POS-CO WebService Details



POS-CO WebService Details

A value of "Yes" indicates webservice communication will happen over HTTPS. A value of "No" indicates webservice communication will happen over HTTP

CentralOffice Server Hostname

User Id authorized to access webservice

Password of authorized user

Confirm password

Enable Secure Communication ? ● Yes ○ No

Please enter the port for the selected protocol

CentralOffice Webservice port

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 that is used to access the Web service.

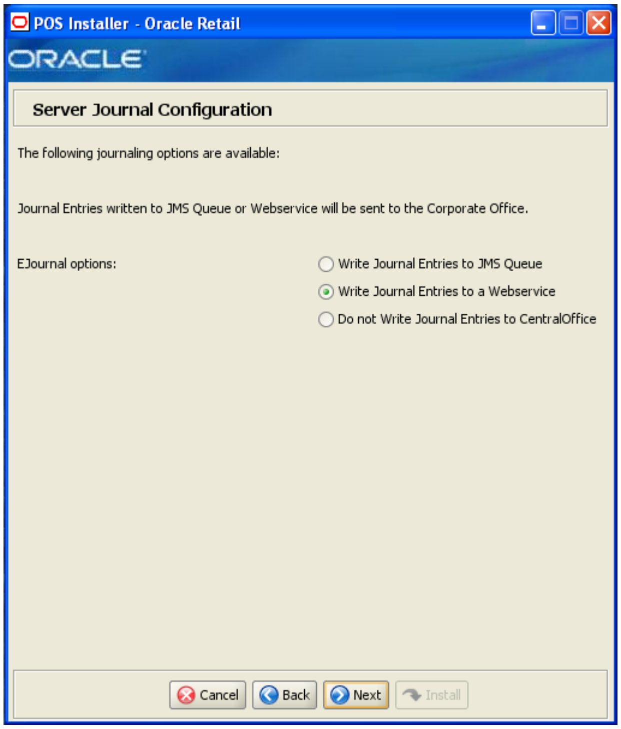
Details	**Content**
Field Title	Password of authorized user
Field Description	Enter the password of the authorized user.

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–28 Server Journal Configuration



POS Installer - Oracle Retail

ORACLE

Server Journal Configuration

The following journaling options are available:

Journal Entries written to JMS Queue or Webservice will be sent to the Corporate Office.

EJournal options:

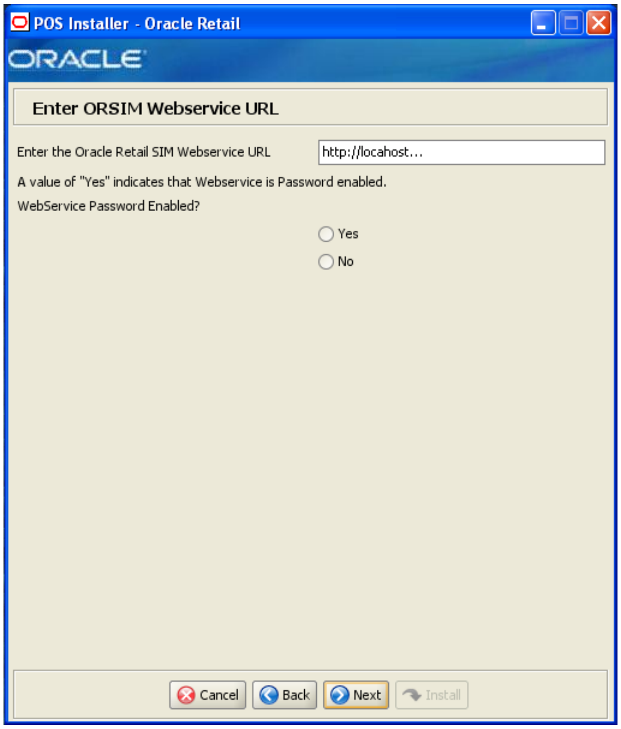
○ Write Journal Entries to JMS Queue
● Write Journal Entries to a Webservice
○ Do not Write Journal Entries to CentralOffice

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–29 Enter ORSIM Webservice URL



Enter ORSIM Webservice URL

Enter the Oracle Retail SIM Webservice URL: http://locahost...

A value of "Yes" indicates that Webservice is Password enabled.

WebService Password Enabled?

○ Yes

○ No

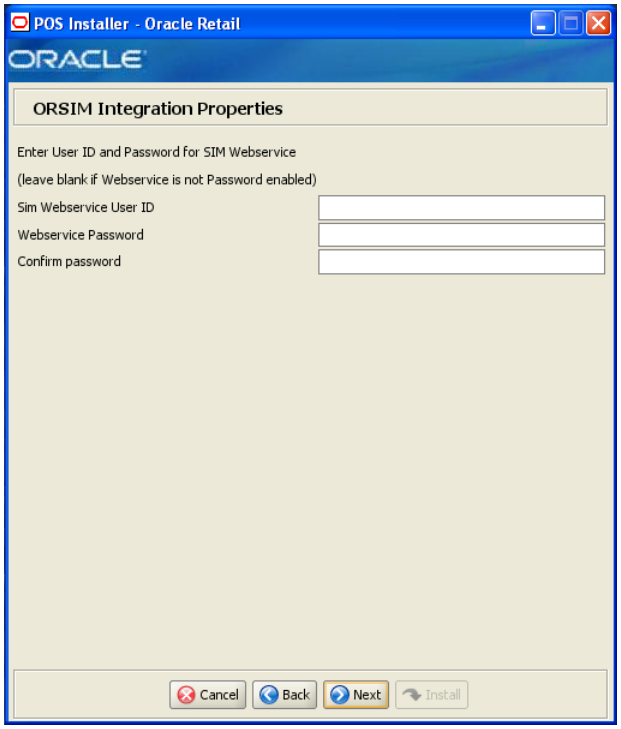
This screen is only displayed if **Store Inventory Management** is selected on the Integrate Applications screen.

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–30 ORSIM Integration Properties



POS Installer - Oracle Retail

ORACLE

ORSIM Integration Properties

Enter User ID and Password for SIM Webservice

(leave blank if Webservice is not Password enabled)

Sim Webservice User ID

Webservice Password

Confirm password

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

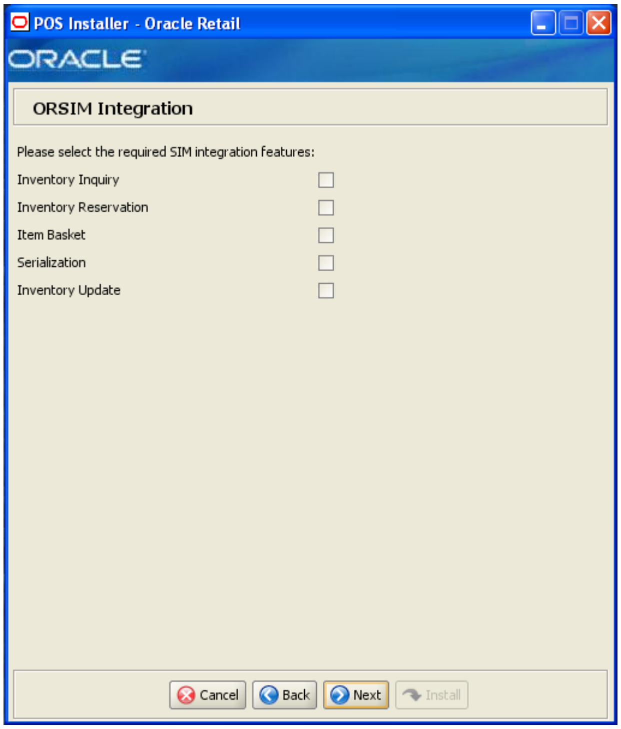
The fields on this screen are described in the following tables.

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–31 ORSIM Integration



Please select the required SIM integration features:

Inventory Inquiry □

Inventory Reservation □

Item Basket □

Serialization □

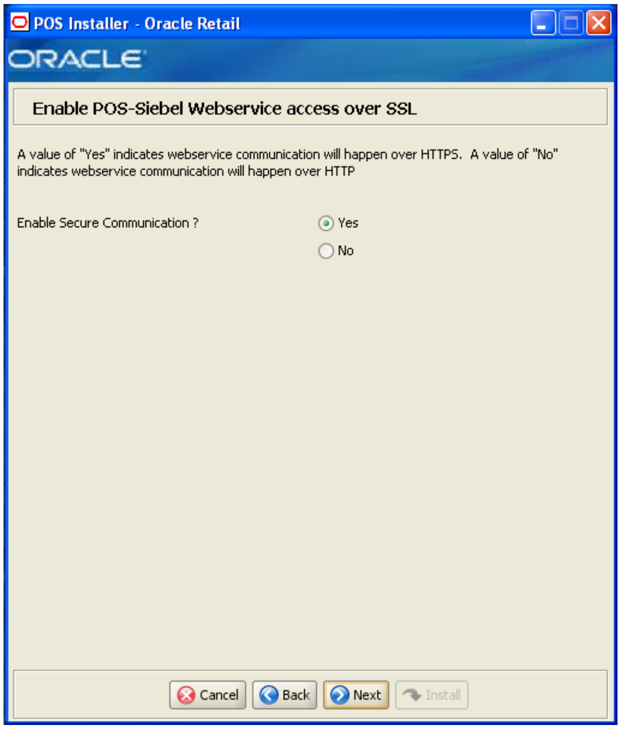
Inventory Update □

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–32 Enable POS-Siebel Webservice Access Over SSL



Enable POS-Siebel Webservice access over SSL

A value of "Yes" indicates webservice communication will happen over HTTPS. A value of "No" indicates webservice communication will happen over HTTP

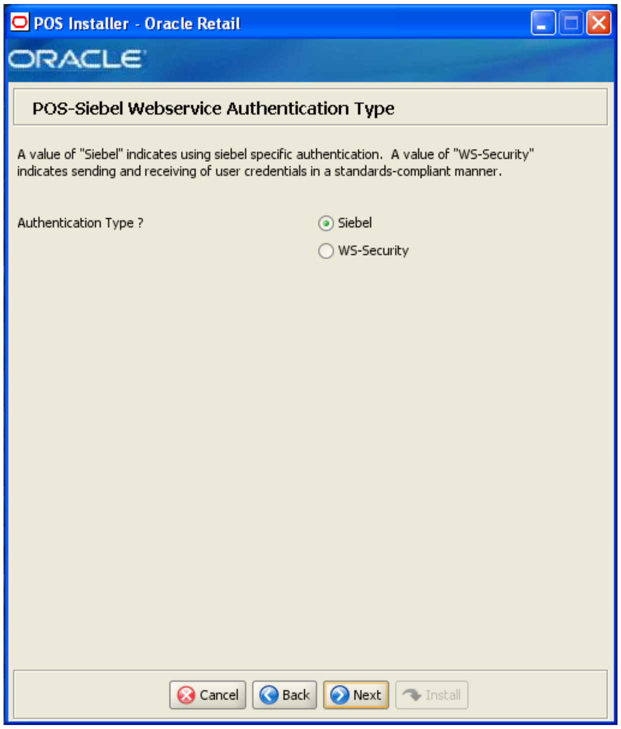
Enable Secure Communication ? ● Yes ○ No

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–33 POS-Siebel Webservice Authentication Type



POS-Siebel Webservice Authentication Type

A value of "Siebel" indicates using siebel specific authentication. A value of "WS-Security" indicates sending and receiving of user credentials in a standards-compliant manner.

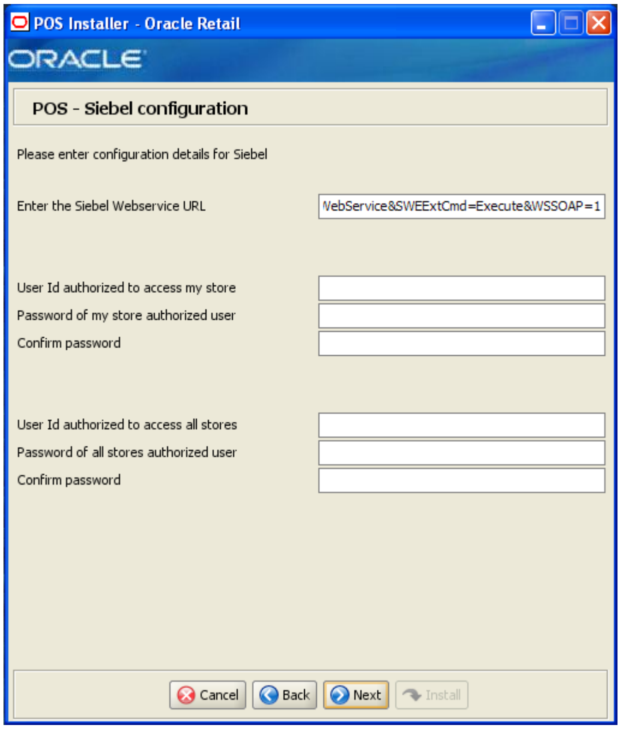
Authentication Type ? ● Siebel ○ WS-Security

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–34 POS-Siebel Configuration



POS Installer - Oracle Retail

POS - Siebel configuration

Please enter configuration details for Siebel

Enter the Siebel Webservice URL: VebService&SWEExtCmd=Execute&WSSOAP=1

User Id authorized to access my store:

Password of my store authorized user:

Confirm password:

User Id authorized to access all stores:

Password of all stores authorized user:

Confirm password:

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.

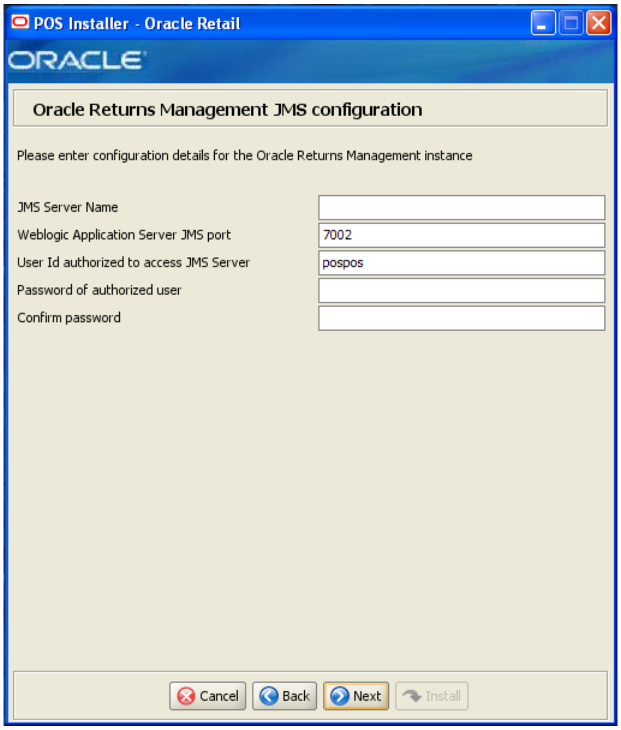
Details	Content
Field Title	Confirm Password
Field Description	Reentered password of my store authorized user used to confirm the password. **Note:** The passwords in the Password of my store authorized user and Confirm Password fields must match.

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–35 Oracle Returns Management JMS Configuration



Oracle Returns Management JMS configuration

Please enter configuration details for the Oracle Returns Management instance

JMS Server Name	
Weblogic Application Server JMS port	7002
User Id authorized to access JMS Server	pospos
Password of authorized user	
Confirm password	

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

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

Details	Content
Field Title	JMS Server Name
Field Description	Enter the name for the JMS server.

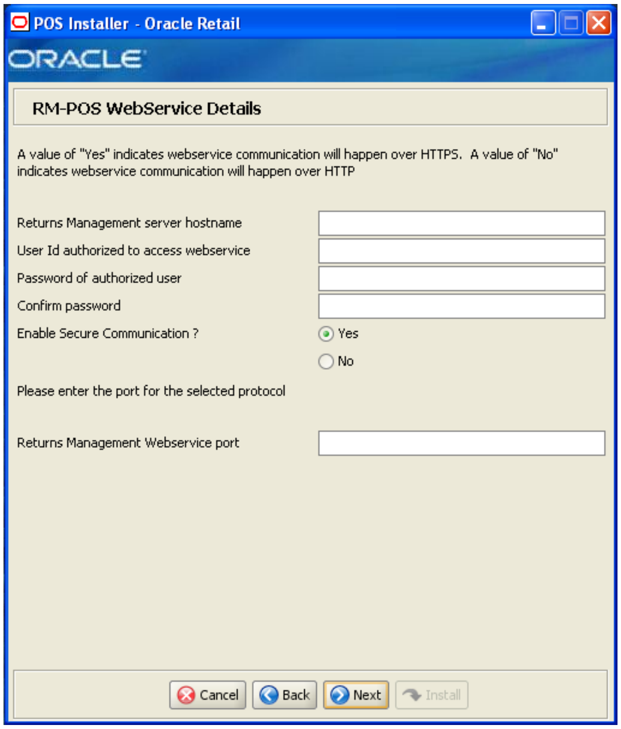
Details	Content
Field Title	Weblogic Application Server JMS port
Field Description	Enter the port number of the JMS server to use to send return result messages to Oracle Retail Returns Management.
Example	7002

Details	Content
Field Title	User Id authorized to access JMS Server
Field Description	Enter the user ID that is used to access the JMS Server.

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–36   RM-POS WebService Details



RM-POS WebService Details

A value of "Yes" indicates webservice communication will happen over HTTPS. A value of "No" indicates webservice communication will happen over HTTP

Returns Management server hostname

User Id authorized to access webservice

Password of authorized user

Confirm password

Enable Secure Communication ? ● Yes ○ No

Please enter the port for the selected protocol

Returns Management Webservice port

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 that is used to access the Web service.

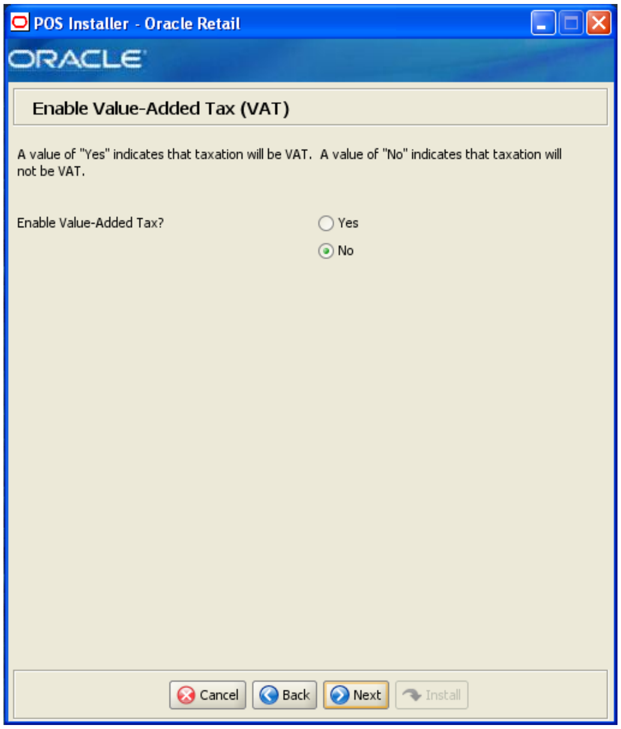
Details	Content
Field Title	Password of authorized user
Field Description	Enter the password of the authorized user.

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	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–37 Enable Value-Added Tax (VAT)



Enable Value-Added Tax (VAT)

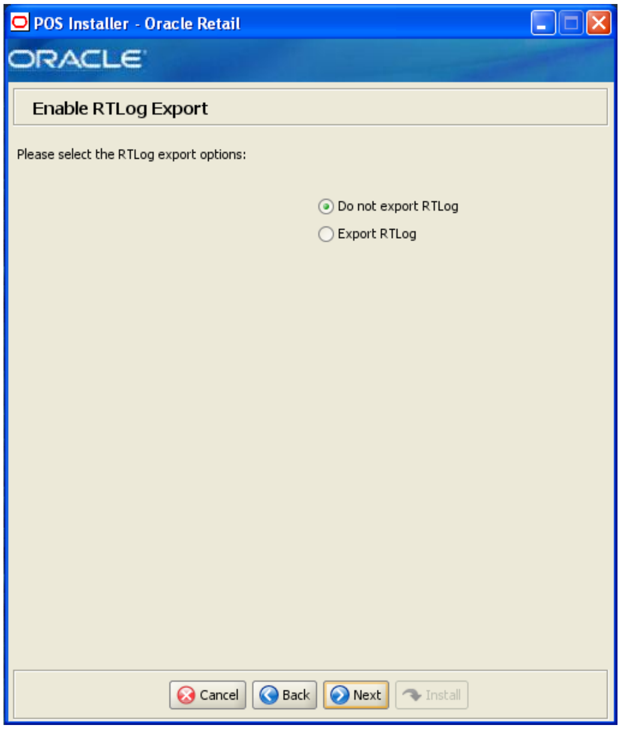
A value of "Yes" indicates that taxation will be VAT. A value of "No" indicates that taxation will not be VAT.

Enable Value-Added Tax? ○ Yes ● No

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–38 Enable RTLog Export



POS Installer - Oracle Retail

Enable RTLog Export

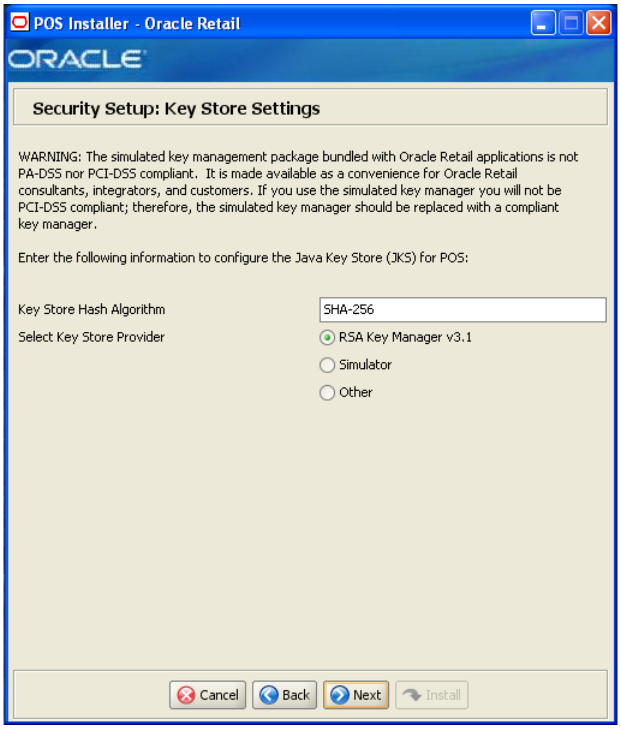
Please select the RTLog export options:

● Do not export RTLog
○ Export RTLog

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–39 Security Setup: Key Store Settings



Security Setup: Key Store Settings

WARNING: The simulated key management package bundled with Oracle Retail applications is not PA-DSS nor PCI-DSS compliant. It is made available as a convenience for Oracle Retail consultants, integrators, and customers. 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.

Enter the following information to configure the Java Key Store (JKS) for POS:

Key Store Hash Algorithm: SHA-256

Select Key Store Provider:
● RSA Key Manager v3.1
○ Simulator
○ Other

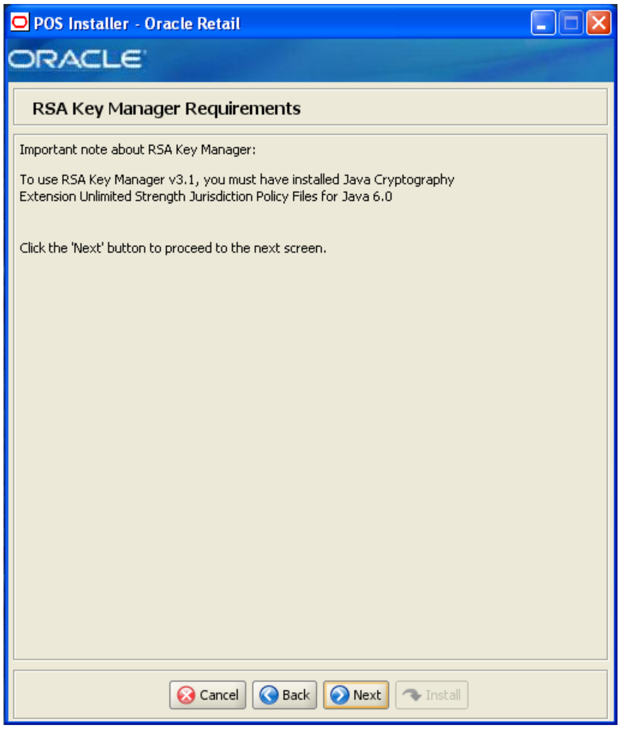
This screen is used to configure the Encryption Key Store provider.

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

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

Details	Content
Field Title	Select Key Store Provider
Field Description	Provider for Key Store management. ■ To use the RSA key management package, select **RSA Key Manager v3.1**. The next screen displayed is Figure A–40. ■ To use the simulated key management package, select **Simulator**. The next screen displayed is Figure A–44. ■ To use a different key management provider, select **Other**. The next screen displayed is Figure A–45.
Example	RSA Key Manager v3.1

Figure A–40 RSA Key Manager Requirements for RSA Key Manager 3.1



RSA Key Manager Requirements

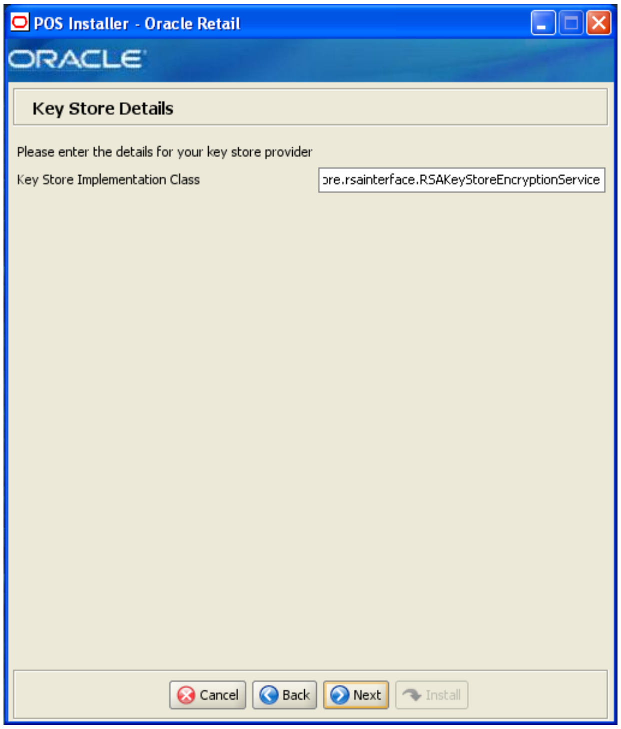
Important note about RSA Key Manager:

To use RSA Key Manager v3.1, you must have installed Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files for Java 6.0

Click the 'Next' button to proceed to the next screen.

This screen is only displayed if **RSA Key Manager v3.1** is selected for the Key Store provider on the Security Setup: Key Store screen. This informational screen explains the requirements to use the RSA Key Manager. Verify that you meet the requirements and then click **Next**.

Figure A–41 Key Store Details for RSA Key Manager 3.1



Key Store Details

Please enter the details for your key store provider

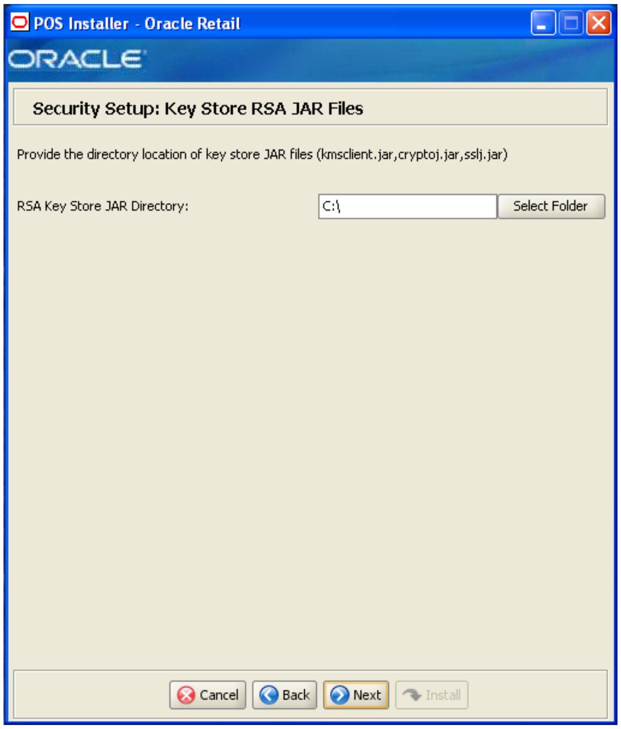
Key Store Implementation Class: ore.rsainterface.RSAKeyStoreEncryptionService

This screen is only displayed if **RSA Key Manager v3.1** is selected for the Key Store provider on the Security Setup: Key Store screen.

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

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

Figure A–42 Security Setup: Key Store JAR Files for RSA Key Manager 3.1



Security Setup: Key Store RSA JAR Files

Provide the directory location of key store JAR files (kmsclient.jar,cryptoj.jar,sslj.jar)

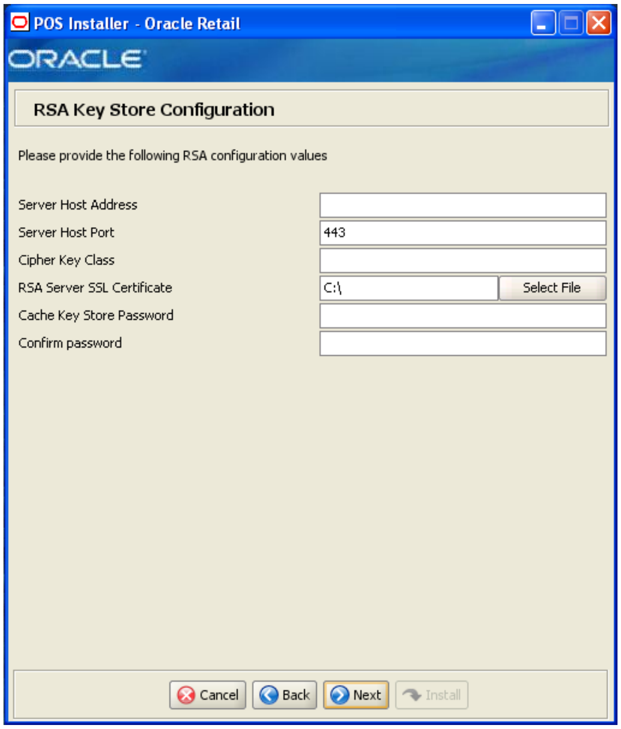
RSA Key Store JAR Directory: C:\ Select Folder

This screen is only displayed if **RSA Key Manager v3.1** is selected for the Key Store provider on the Security Setup: Key Store screen.

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

Details	**Content**
Field Title	Key Store JAR Directory
Field Description	Choose the directory where the following Key Store jar files are located: ■ `kmsclient.jar` ■ `cryptoj.jar` ■ `sslj.jar`
Example	`C:\`

Figure A–43 RSA Key Store Configuration for RSA Key Manager 3.1



POS Installer - Oracle Retail

RSA Key Store Configuration

Please provide the following RSA configuration values

Server Host Address	
Server Host Port	443
Cipher Key Class	
RSA Server SSL Certificate	C:\
Cache Key Store Password	
Confirm password	

This screen is only displayed if **RSA Key Manager v3.1** is selected for the Key Store provider on the Security Setup: Key Store screen.

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

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

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

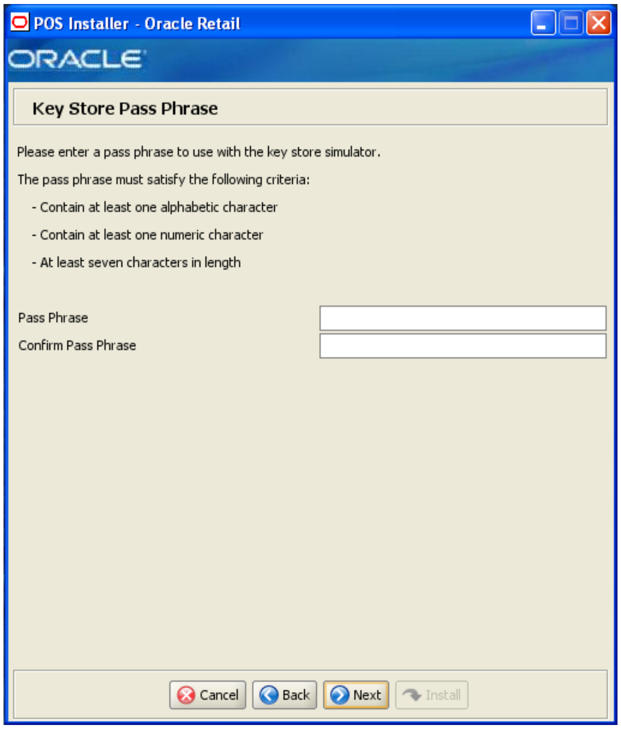
Details	Content
Field Title	Cipher Key Class
Field Description	Enter the RSA Key Manager cipher key class.

Details	Content
Field Title	RSA Server SSL Certificate
Field Description	Select the location of the RSA Key Manager server SSL certificate. **Note:** You should verify that the SSL certificate at this location is valid.

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

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

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



Please enter a pass phrase to use with the key store simulator.

The pass phrase must satisfy the following criteria:

- Contain at least one alphabetic character
- Contain at least one numeric character
- At least seven characters in length

Pass Phrase

Confirm Pass Phrase

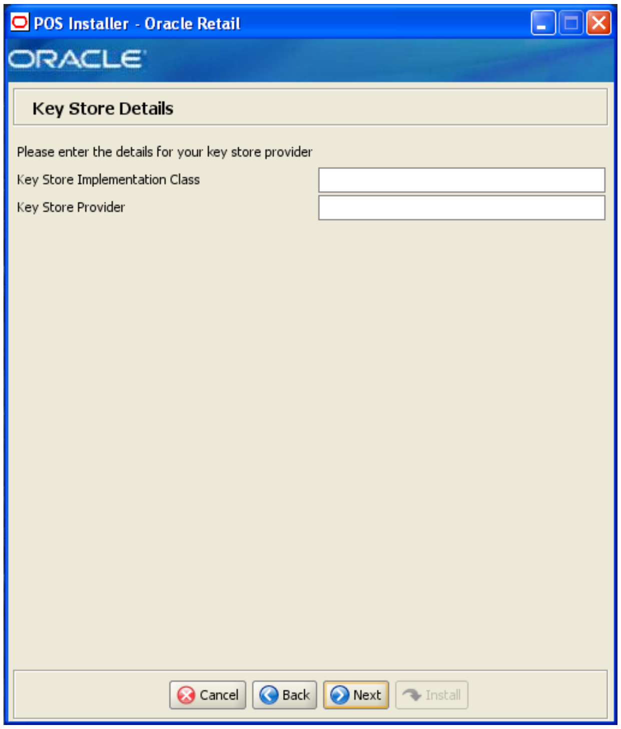
This screen is only displayed if **Simulator** is selected for the Key Store provider on the Security Setup: Key Store screen.

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

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–45 Key Store Details for Other Key Manager



Key Store Details

Please enter the details for your key store provider

Key Store Implementation Class

Key Store Provider

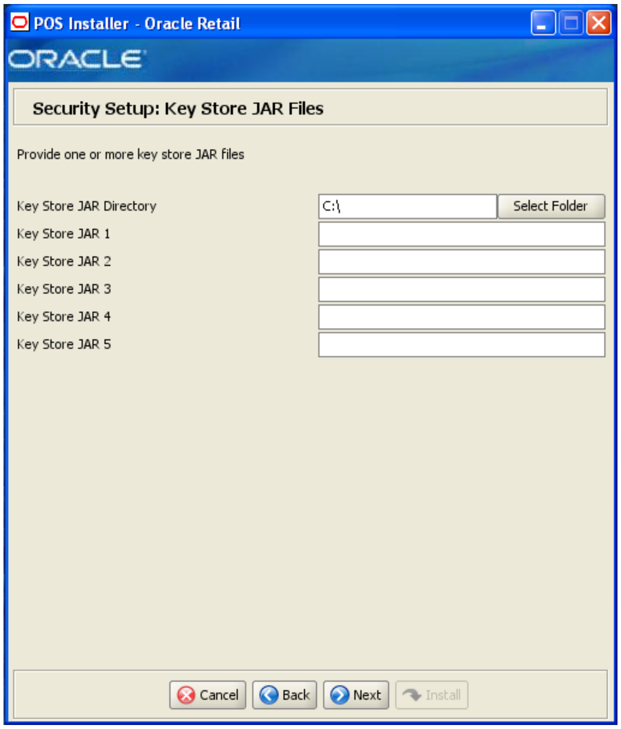
This screen is only displayed if **Other** is selected for the Key Store provider on the Security Setup: Key Store screen.

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

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

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

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



Security Setup: Key Store JAR Files

Provide one or more key store JAR files

Key Store JAR Directory: C:\

Key Store JAR 1

Key Store JAR 2

Key Store JAR 3

Key Store JAR 4

Key Store JAR 5

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

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

Details	Content
Field Title	Key Store JAR Directory
Field Description	Choose the directory where the Key Store jar files are located.
Example	C:\

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

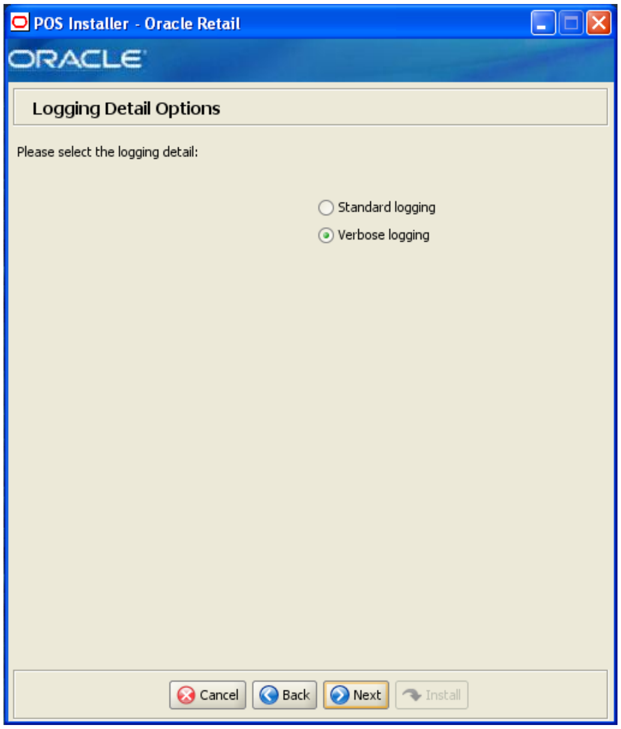
Details	Content
Field Title	Key Store JAR 2
Field Description	Enter the name of a Key Store jar file.

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

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

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

Figure A–47 Logging Detail Options



Logging Detail Options

Please select the logging detail:

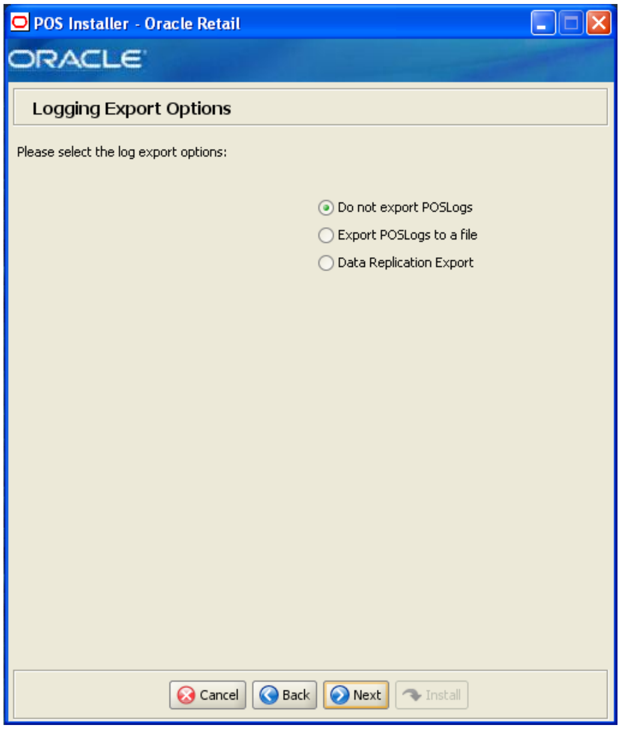
○ Standard logging

● Verbose logging

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



Logging Export Options

Please select the log export options:

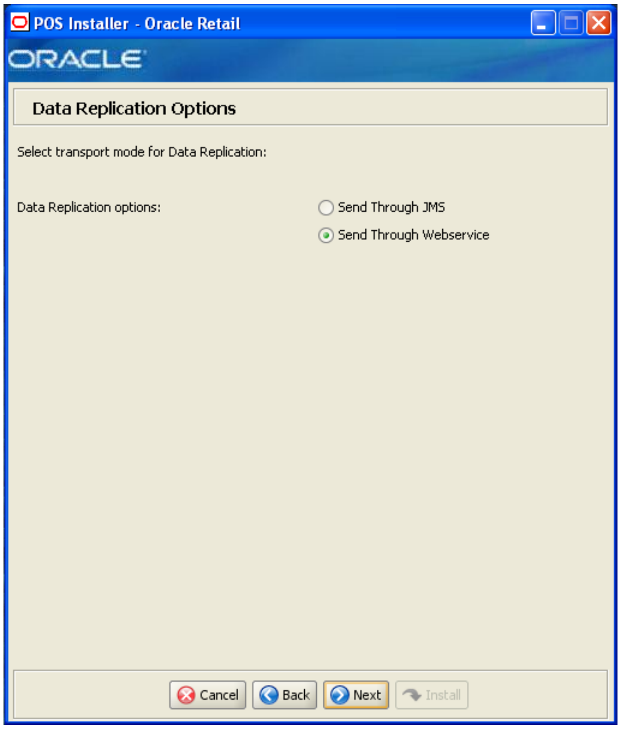
● Do not export POSLogs
○ Export POSLogs to a file
○ Data Replication Export

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



Data Replication Options

Select transport mode for Data Replication:

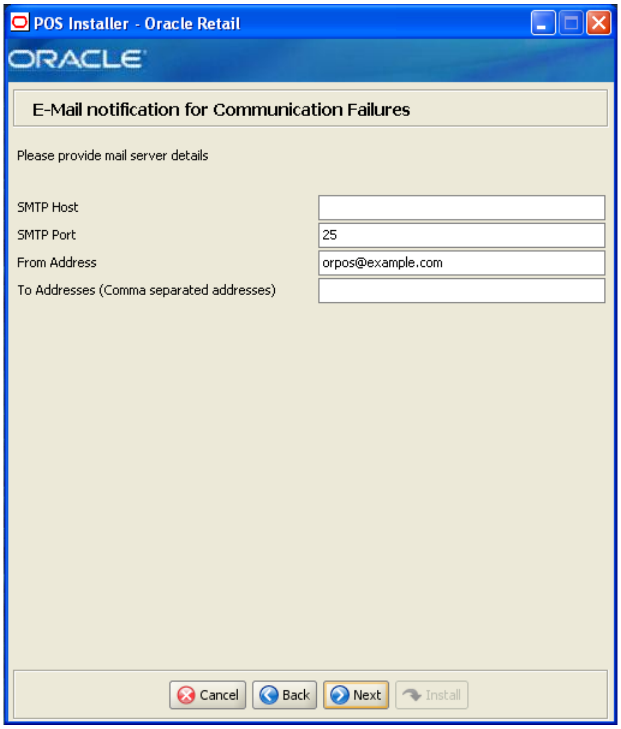
Data Replication options: ○ Send Through JMS ● Send Through Webservice

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



E-Mail notification for Communication Failures

Please provide mail server details

SMTP Host

SMTP Port: 25

From Address: orpos@example.com

To Addresses (Comma separated addresses)

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.

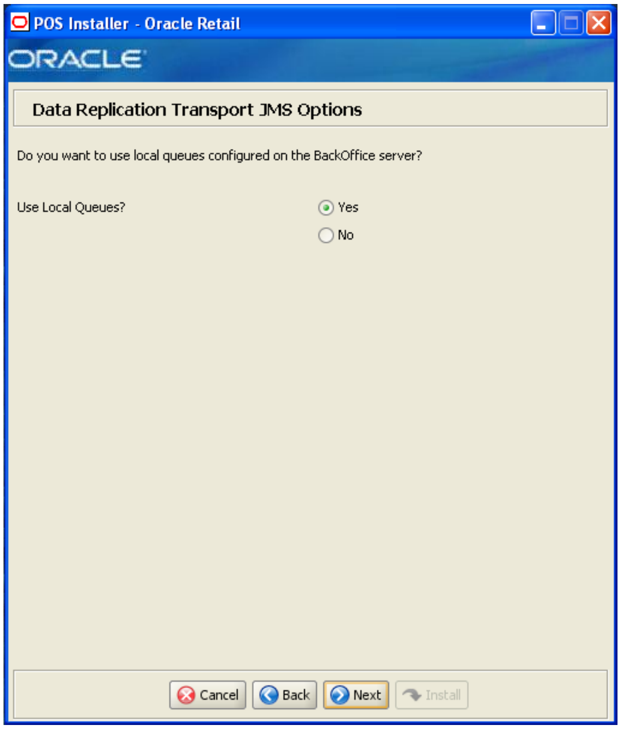
Details	Content
Field Title	SMTP host
Field Description	Host where the SMTP server is running.

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



Data Replication Transport JMS Options

Do you want to use local queues configured on the BackOffice server?

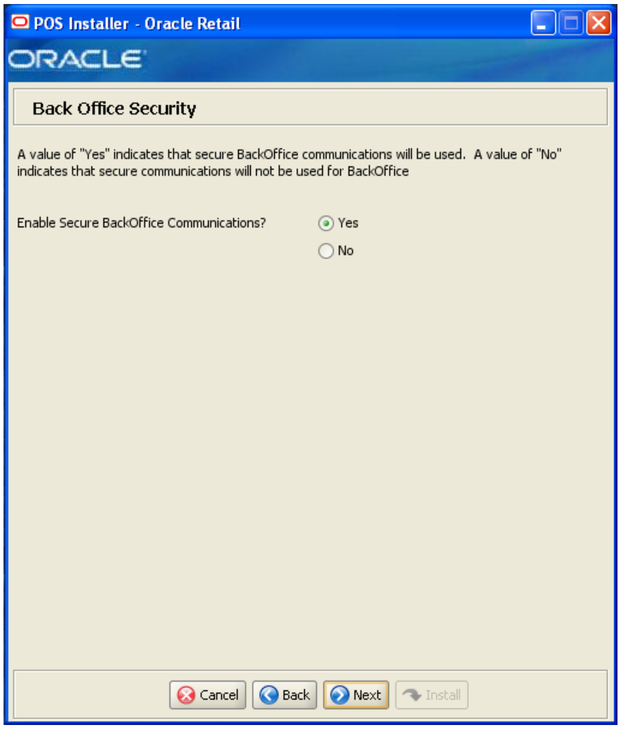
Use Local Queues? ● Yes ○ No

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 Back Office Security



Back Office Security

A value of "Yes" indicates that secure BackOffice communications will be used. A value of "No" indicates that secure communications will not be used for BackOffice

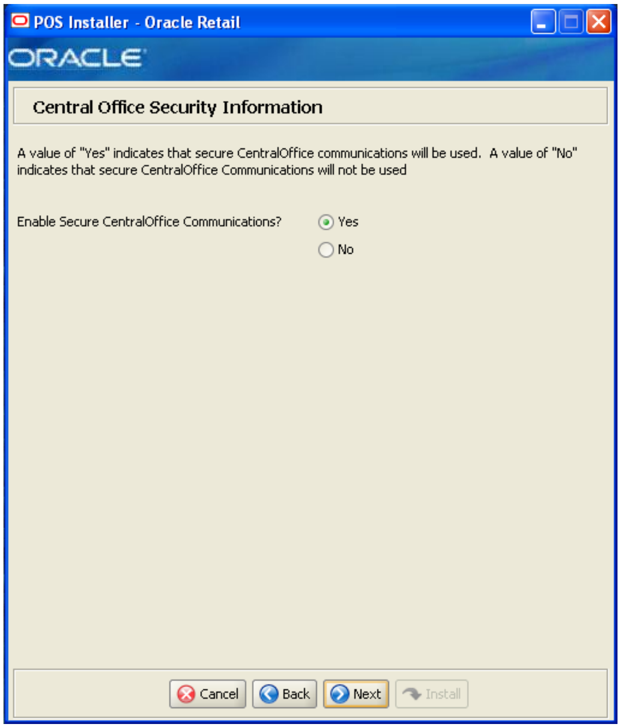
Enable Secure BackOffice Communications? ● Yes ○ No

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

Figure A–53 Central Office Security Information



Central Office Security Information

A value of "Yes" indicates that secure CentralOffice communications will be used. A value of "No" indicates that secure CentralOffice Communications will not be used

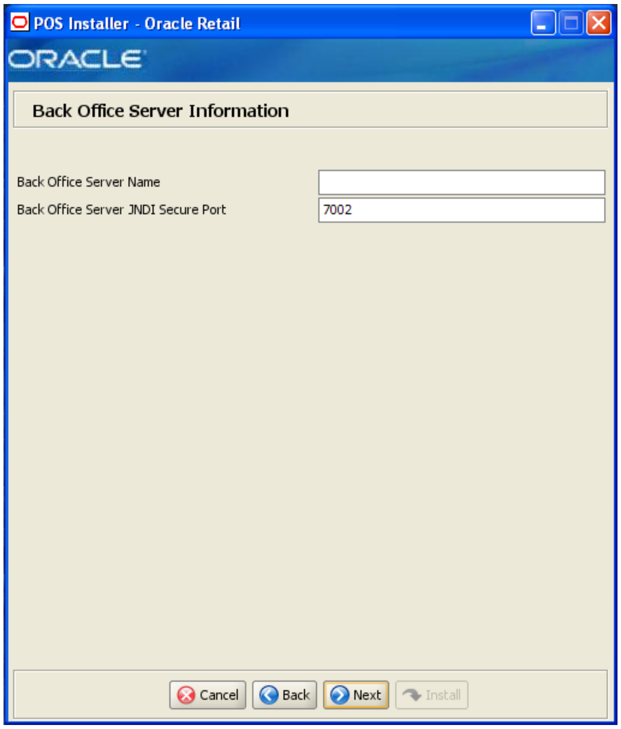
Enable Secure CentralOffice Communications? ● Yes ○ No

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

Figure A–54 Back Office Server Information



POS Installer - Oracle Retail

Back Office Server Information

Back Office Server Name:

Back Office Server JNDI Secure Port: 7002

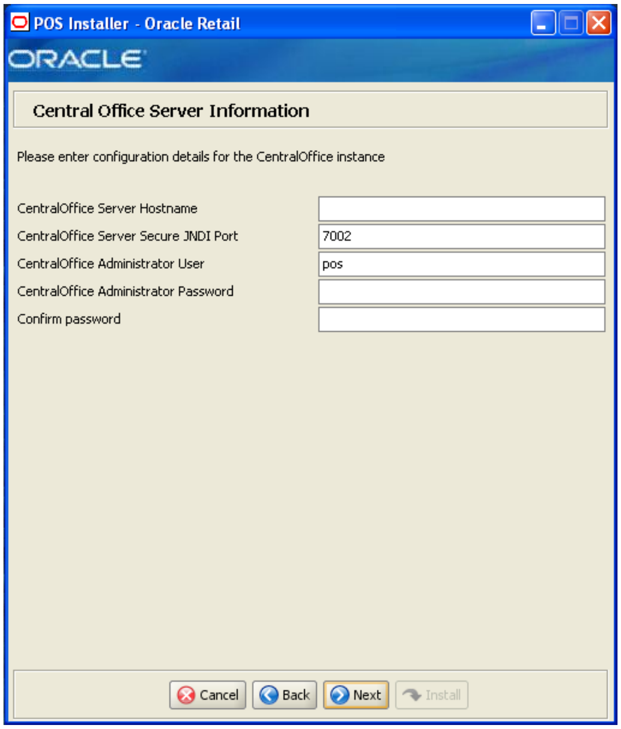
This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

Details	Content
Field Title	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	7002

Figure A–55 Central Office Server Information



Central Office Server Information

Please enter configuration details for the CentralOffice instance

CentralOffice Server Hostname	
CentralOffice Server Secure JNDI Port	7002
CentralOffice Administrator User	pos
CentralOffice Administrator Password	
Confirm password	

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

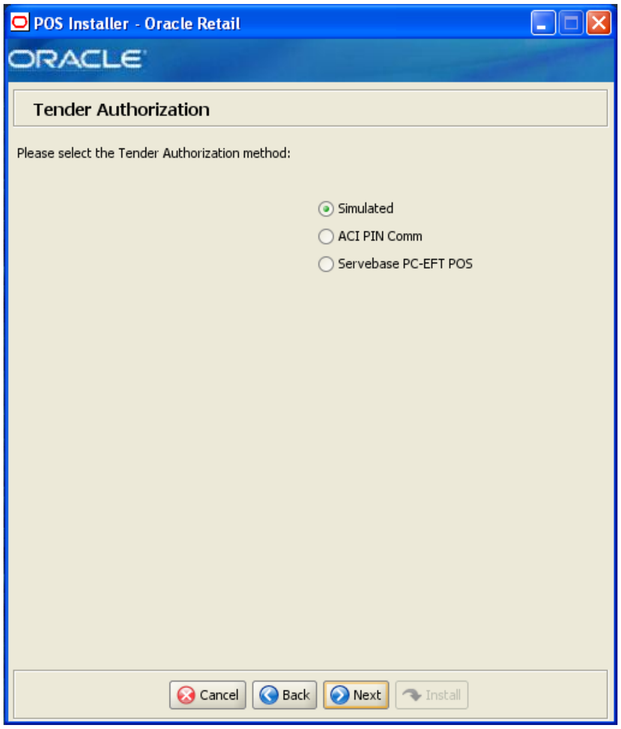
Details	Content
Field Title	Central Office Server Secure JNDI Port
Field Description	Enter the port number for the Central Office application. This is the port number that was selected when the Central Office domain was created.
Example	7002

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

Details	Content
Field Title	Central Office Administrator Password
Field Description	Enter the password for the Central Office administrator 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–56 Tender Authorization



Tender Authorization

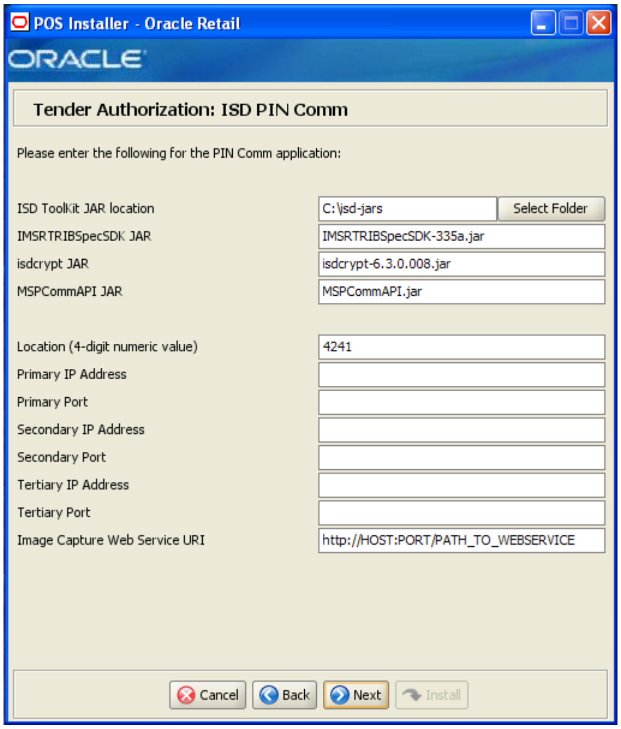
Please select the Tender Authorization method:

● Simulated
○ ACI PIN Comm
○ Servebase PC-EFT POS

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 A–57 Tender Authorization: ISD PIN Comm



Tender Authorization: ISD PIN Comm

Please enter the following for the PIN Comm application:

ISD Toolkit JAR location	C:\isd-jars
IMSRTRIBSpecSDK JAR	IMSRTRIBSpecSDK-335a.jar
isdcrypt JAR	isdcrypt-6.3.0.008.jar
MSPCommAPI JAR	MSPCommAPI.jar
Location (4-digit numeric value)	4241
Primary IP Address	
Primary Port	
Secondary IP Address	
Secondary Port	
Tertiary IP Address	
Tertiary Port	
Image Capture Web Service URI	http://HOST:PORT/PATH_TO_WEBSERVICE

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	`C:\isd-jars`

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

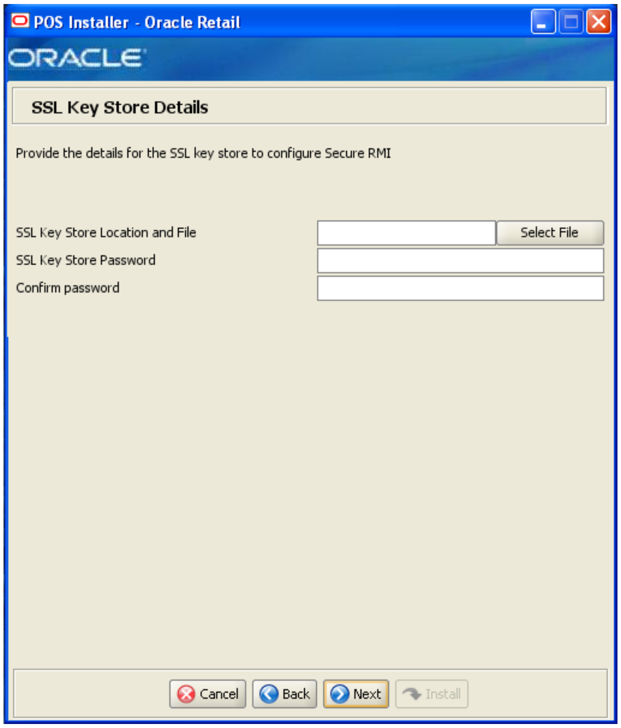
Details	Content
Field Title	Secondary Port
Field Description	Enter the secondary port number used for the communication between the store server and the tender authorizer.

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–58 SSL Key Store Details



POS Installer - Oracle Retail

SSL Key Store Details

Provide the details for the SSL key store to configure Secure RMI

SSL Key Store Location and File

SSL Key Store Password

Confirm password

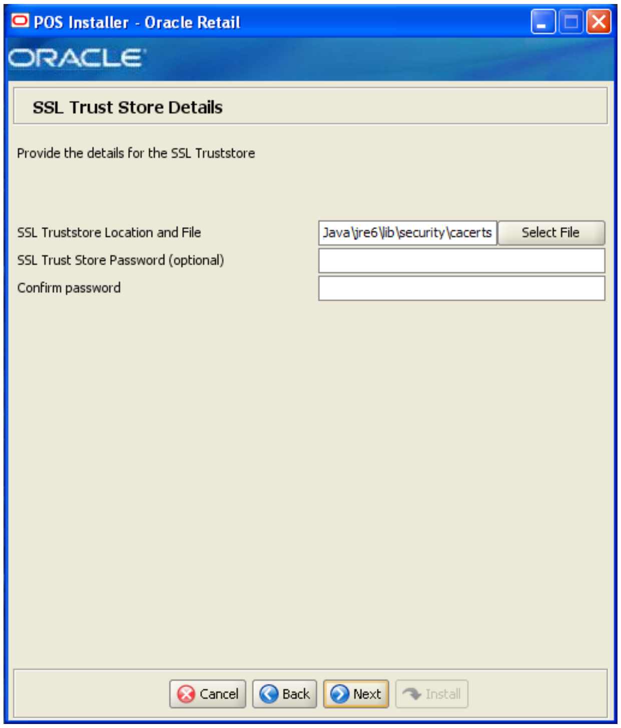
The fields on this screen are described in the following tables.

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–59 SSL Trust Store Details



SSL Trust Store Details

Provide the details for the SSL Truststore

SSL Truststore Location and File: Java\jre6\lib\security\cacerts

SSL Trust Store Password (optional):

Confirm password:

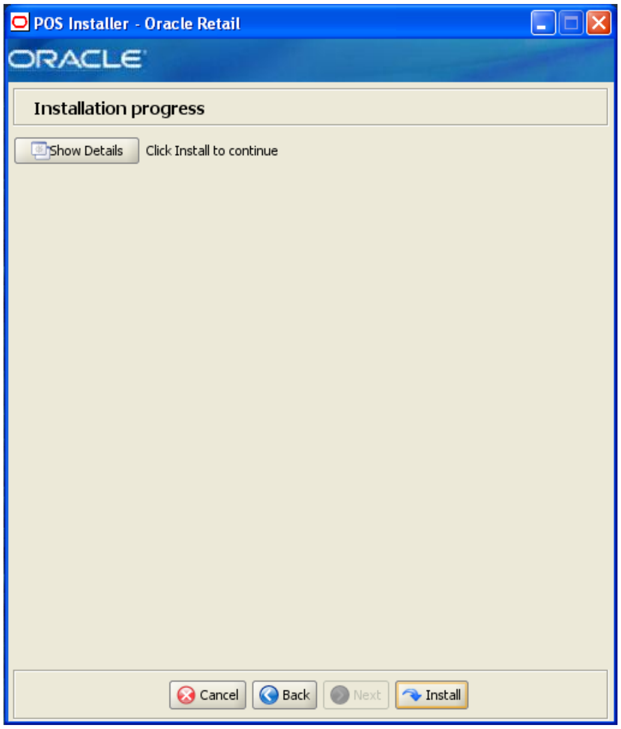
The fields on this screen are described in the following tables.

Details	Content
Field Title	SSL Truststore Location and File
Field Description	Enter the location and name of the truststore file.
Example	`C:\Program Files\Java\jre6\lib\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.

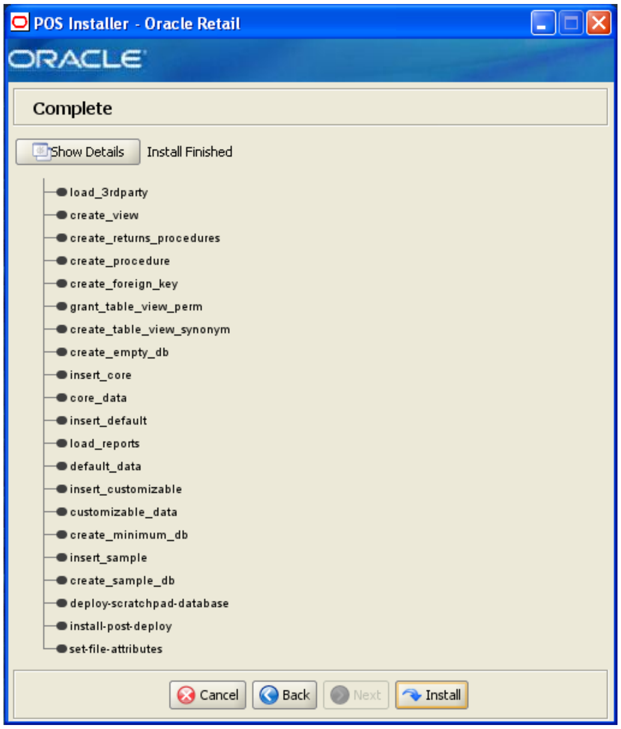
Figure A–60 Installation Progress



Installation progress

Click Install to continue

Figure A–61 Install Complete



Complete

Install Finished

```
├─● load_3rdparty
├─● create_view
├─● create_returns_procedures
├─● create_procedure
├─● create_foreign_key
├─● grant_table_view_perm
├─● create_table_view_synonym
├─● create_empty_db
├─● insert_core
├─● core_data
├─● insert_default
├─● load_reports
├─● default_data
├─● insert_customizable
├─● customizable_data
├─● create_minimum_db
├─● insert_sample
├─● create_sample_db
├─● deploy-scratchpad-database
├─● install-post-deploy
└─● set-file-attributes
```

B

Appendix: Installer Screens for Client Installation on the Oracle Stack

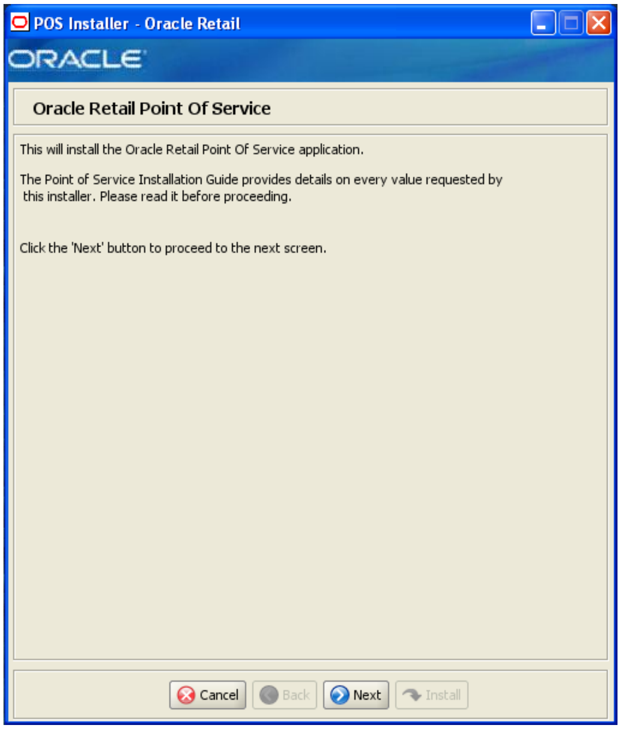
You need the following details about your environment for the installer to successfully install the Point-of-Service application. This appendix shows the screens that are displayed during the installation of the Point-of-Service client on the Oracle stack. Depending on the options you select, you may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

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

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

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

Figure B–1 Introduction



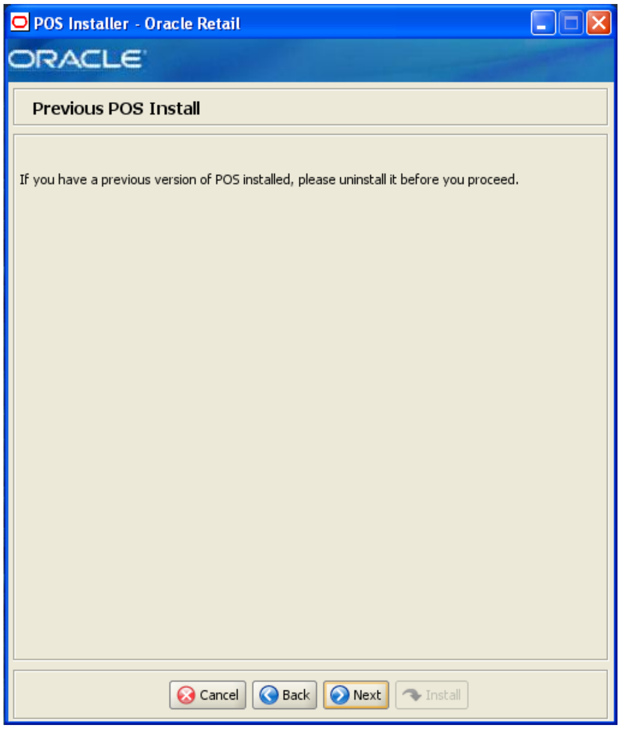
Oracle Retail Point Of Service

This will install the Oracle Retail Point Of Service application.

The Point of Service Installation Guide provides details on every value requested by this installer. Please read it before proceeding.

Click the 'Next' button to proceed to the next screen.

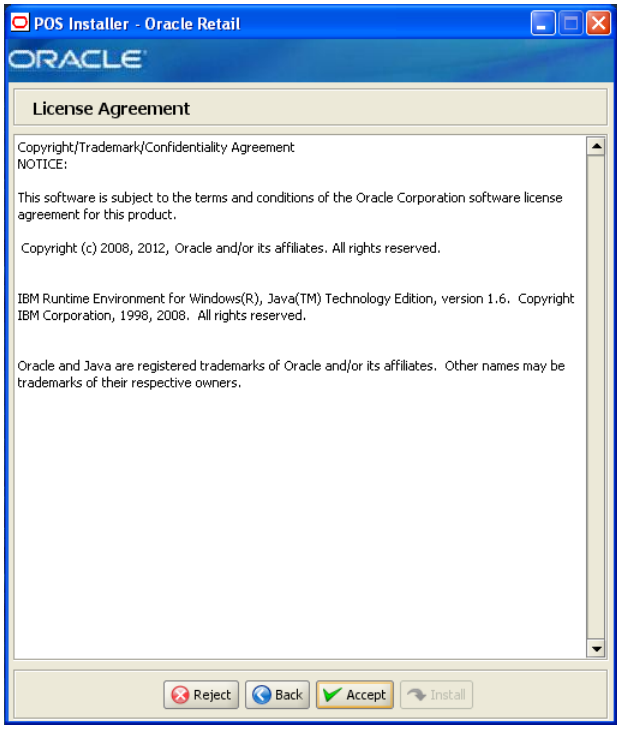
Figure B–2 Previous POS Install



Previous POS Install

If you have a previous version of POS installed, please uninstall it before you proceed.

Figure B–3 License Agreement



License Agreement

Copyright/Trademark/Confidentiality Agreement
NOTICE:

This software is subject to the terms and conditions of the Oracle Corporation software license agreement for this product.

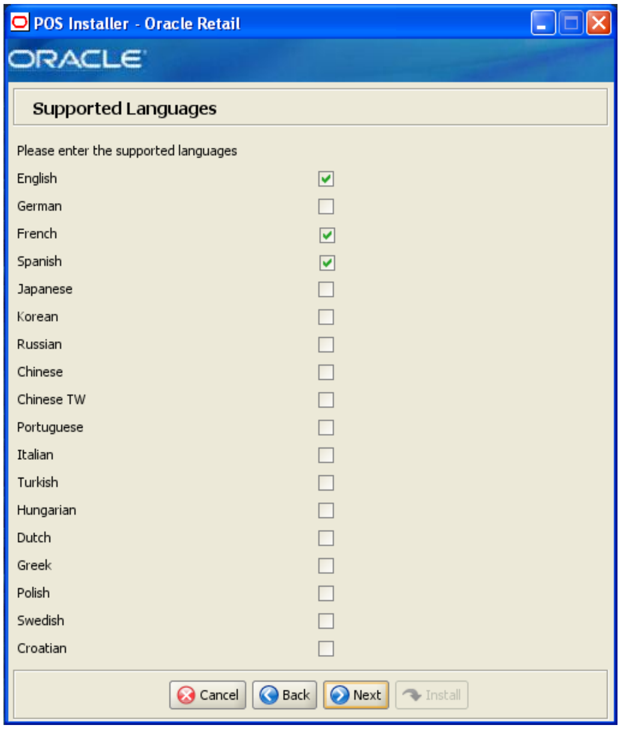
Copyright (c) 2008, 2012, Oracle and/or its affiliates. All rights reserved.

IBM Runtime Environment for Windows(R), Java(TM) Technology Edition, version 1.6. Copyright IBM Corporation, 1998, 2008. All rights reserved.

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

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

Figure B–4 Supported Languages



POS Installer - Oracle Retail

ORACLE

Supported Languages

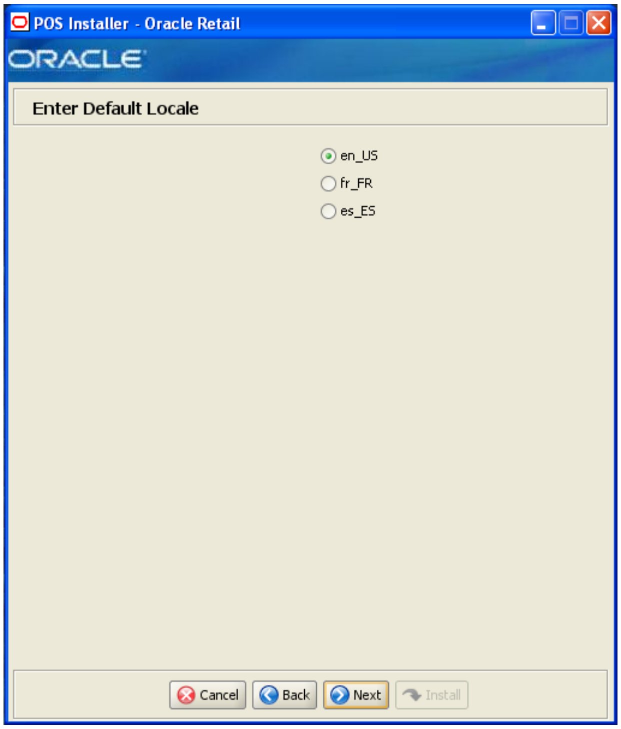
Please enter the supported languages

English	☑
German	□
French	☑
Spanish	☑
Japanese	□
Korean	□
Russian	□
Chinese	□
Chinese TW	□
Portuguese	□
Italian	□
Turkish	□
Hungarian	□
Dutch	□
Greek	□
Polish	□
Swedish	□
Croatian	□

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, French, and Spanish

Figure B–5 Enter Default Locale



POS Installer - Oracle Retail

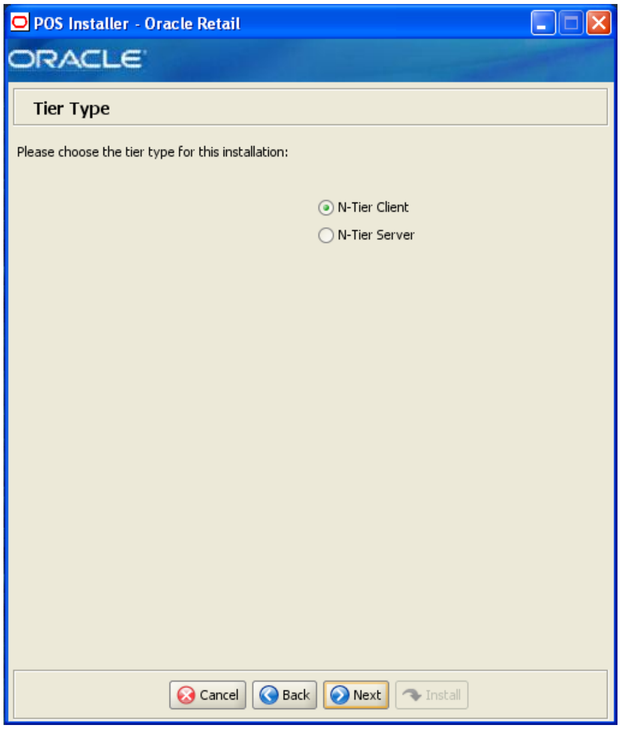
Enter Default Locale

● en_US
○ fr_FR
○ es_ES

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


POS Installer - Oracle Retail

Tier Type

Please choose the tier type for this installation:

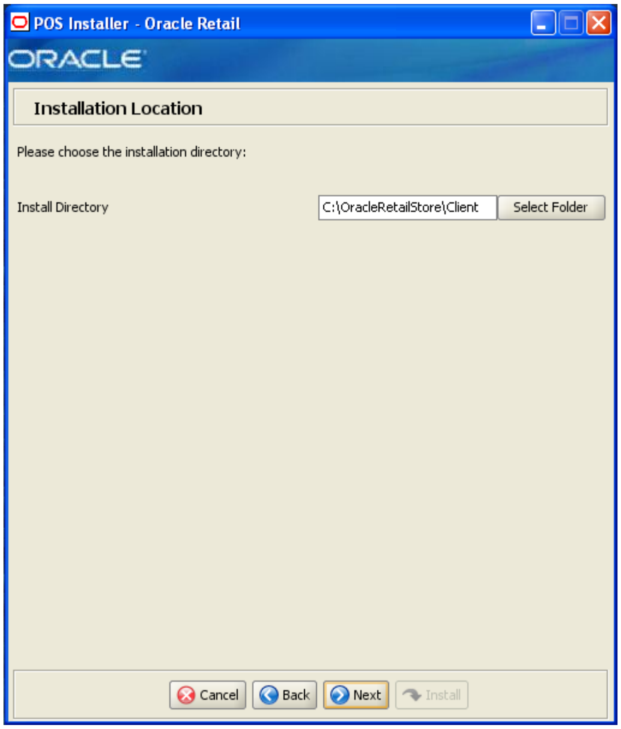
● N-Tier Client

○ N-Tier Server

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 Installation Location



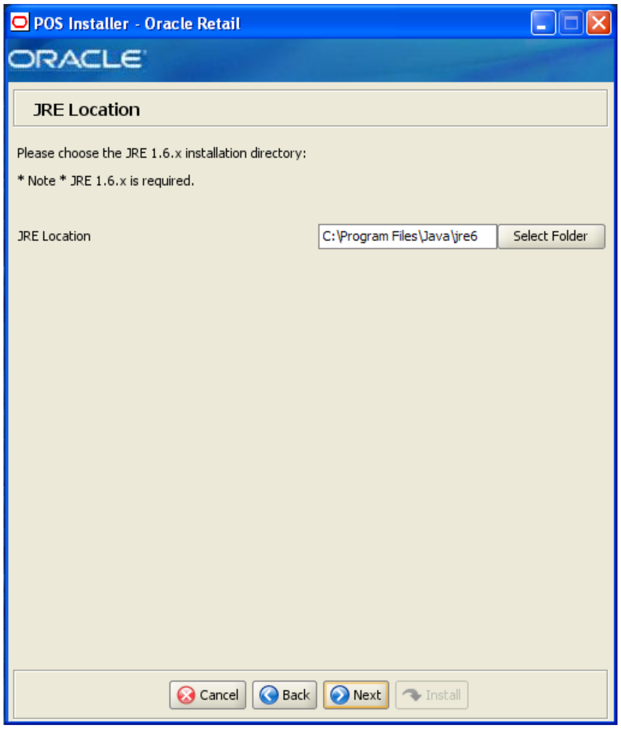
Please choose the installation directory:

Install Directory: C:\OracleRetailStore\Client

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	`C:\OracleRetailStore\Client`

Figure B–8 JRE Location



POS Installer - Oracle Retail

ORACLE

JRE Location

Please choose the JRE 1.6.x installation directory:

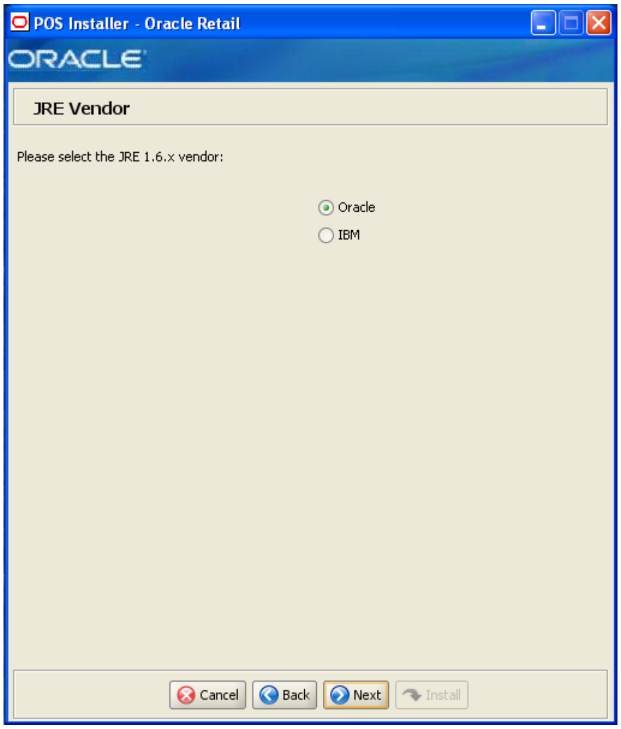
* Note * JRE 1.6.x is required.

JRE Location C:\Program Files\Java\jre6

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	`C:\Program Files\Java\jre6`

Figure B–9 JRE Vendor



JRE Vendor

Please select the JRE 1.6.x vendor:

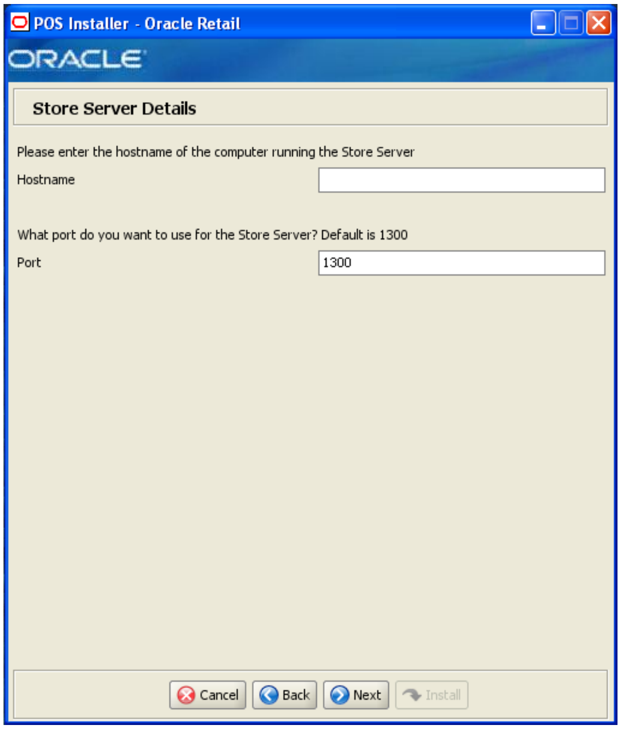
● Oracle

○ IBM

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 **Oracle**.

Figure B–10 Store Server Details



Store Server Details

Please enter the hostname of the computer running the Store Server

Hostname

What port do you want to use for the Store Server? Default is 1300

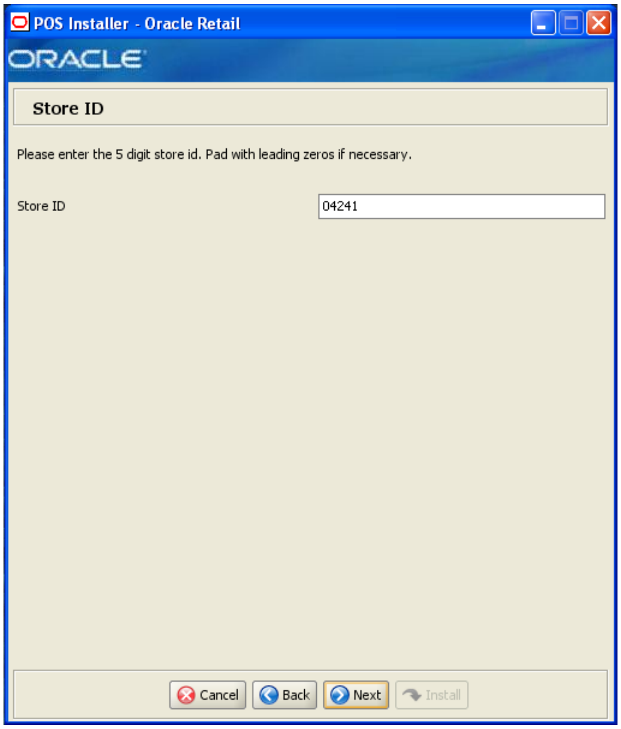
Port: 1300

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–11 Store ID



Store ID

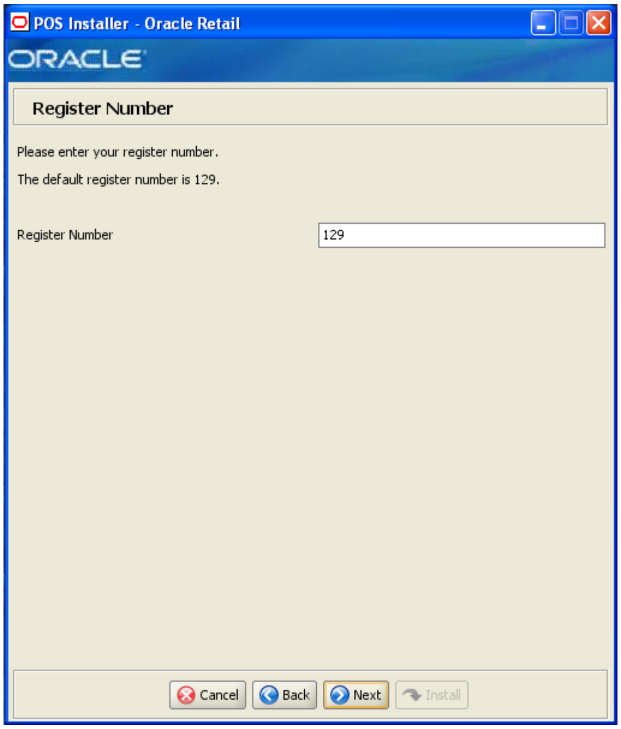
Please enter the 5 digit store id. Pad with leading zeros if necessary.

Store ID: 04241

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–12 Register Number



Register Number

Please enter your register number.

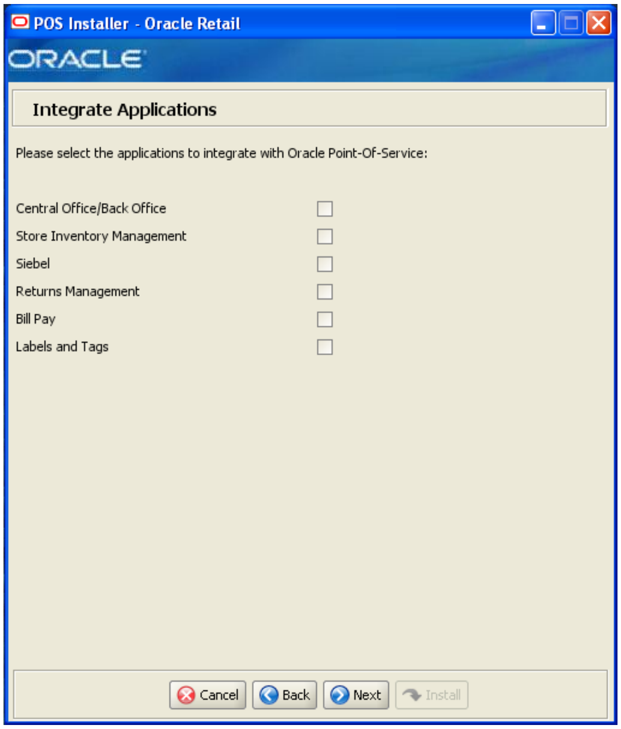
The default register number is 129.

Register Number: 129

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–13 Integrate Applications



Integrate Applications

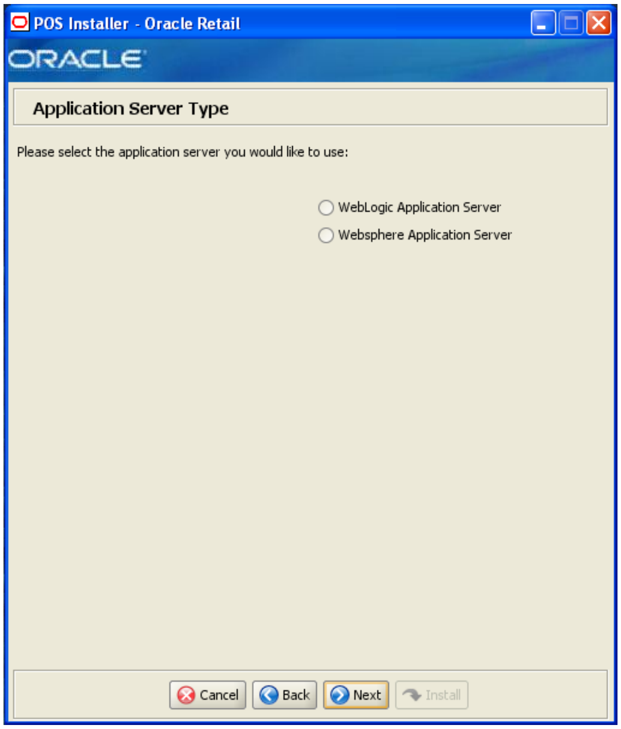
Please select the applications to integrate with Oracle Point-Of-Service:

Central Office/Back Office □
Store Inventory Management □
Siebel □
Returns Management □
Bill Pay □
Labels and Tags □

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–14 Application Server Type



POS Installer - Oracle Retail

ORACLE

Application Server Type

Please select the application server you would like to use:

○ WebLogic Application Server

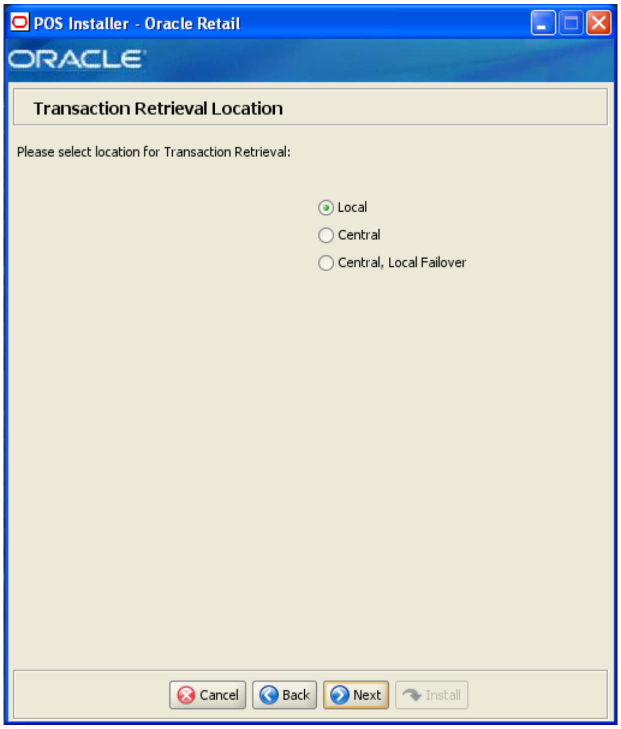
○ Websphere Application Server

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 **WebLogic Application Server**.

Figure B–15 Transaction Retrieval Location



POS Installer - Oracle Retail

Transaction Retrieval Location

Please select location for Transaction Retrieval:

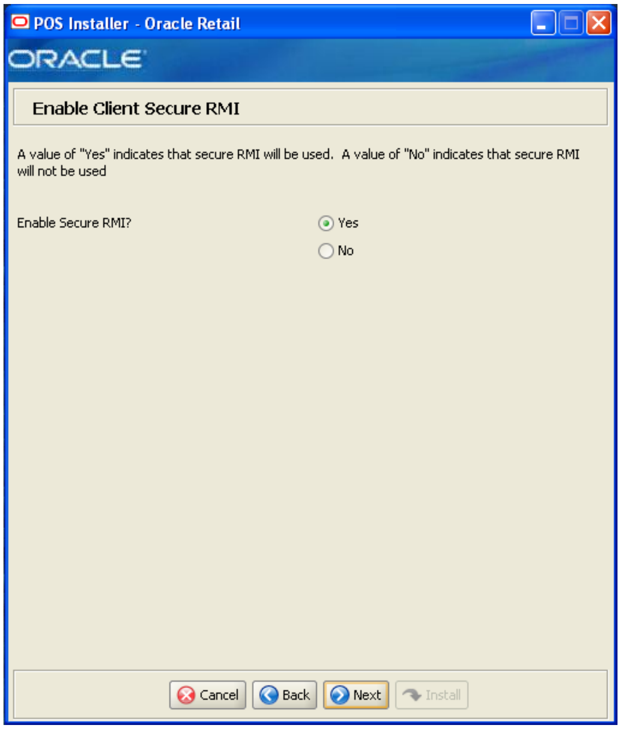
● Local
○ Central
○ Central, Local Failover

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–16 Enable Client Secure RMI



Enable Client Secure RMI

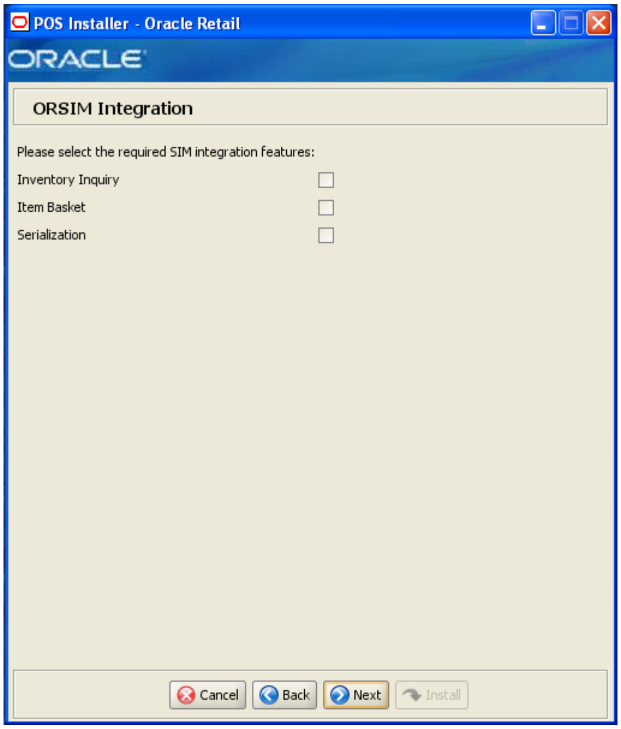
A value of "Yes" indicates that secure RMI will be used. A value of "No" indicates that secure RMI will not be used

Enable Secure RMI? ● Yes ○ No

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–17 ORSIM Integration



ORSIM Integration

Please select the required SIM integration features:

Inventory Inquiry □

Item Basket □

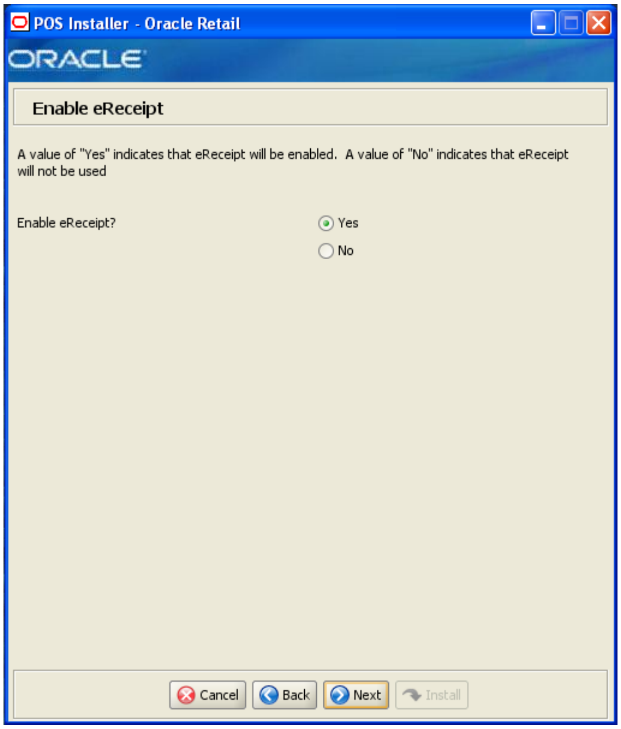
Serialization □

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–18 Enable eReceipt



Enable eReceipt

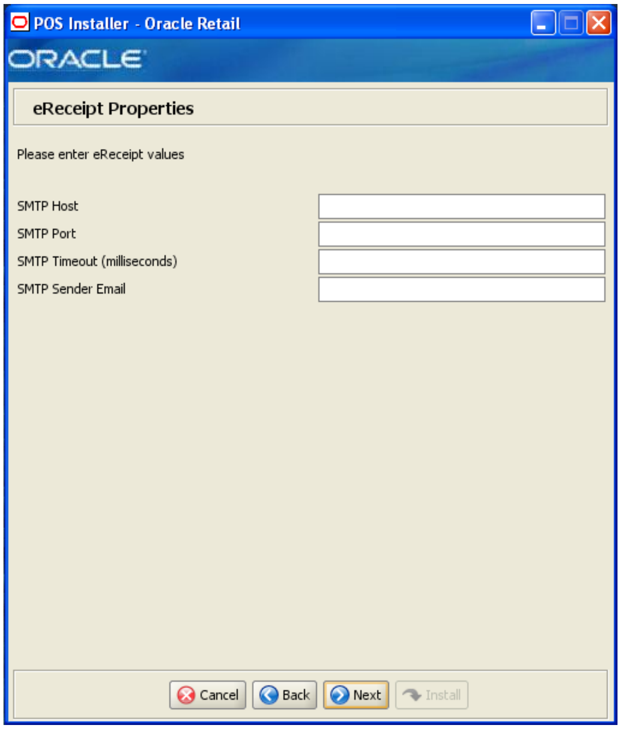
A value of "Yes" indicates that eReceipt will be enabled. A value of "No" indicates that eReceipt will not be used

Enable eReceipt? ● Yes ○ No

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–19 eReceipt Properties



eReceipt Properties

Please enter eReceipt values

SMTP Host

SMTP Port

SMTP Timeout (milliseconds)

SMTP Sender Email

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.

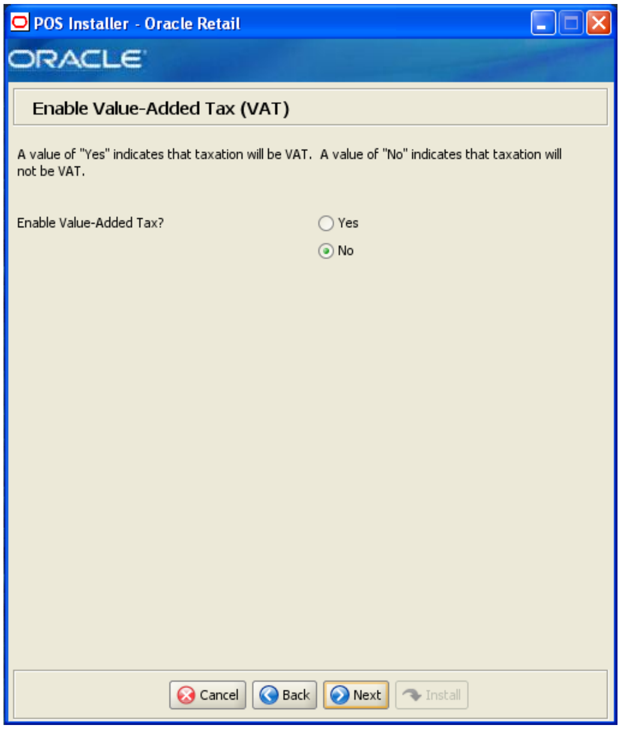
Details	Content
Field Title	SMTP Host
Field Description	Enter the host name for the SMTP server.

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–20 Value-Added Tax (VAT)



Enable Value-Added Tax (VAT)

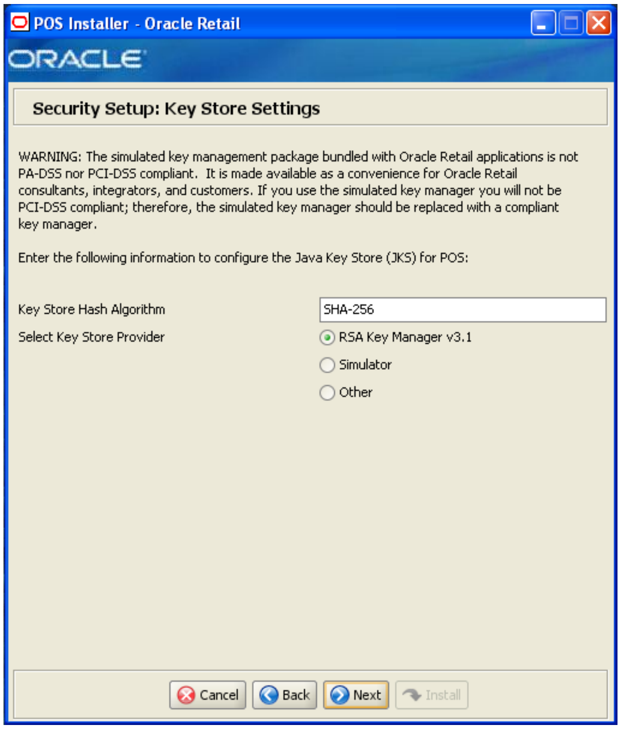
A value of "Yes" indicates that taxation will be VAT. A value of "No" indicates that taxation will not be VAT.

Enable Value-Added Tax? ○ Yes ● No

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–21 Security Setup: Key Store Settings



Security Setup: Key Store Settings

WARNING: The simulated key management package bundled with Oracle Retail applications is not PA-DSS nor PCI-DSS compliant. It is made available as a convenience for Oracle Retail consultants, integrators, and customers. 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.

Enter the following information to configure the Java Key Store (JKS) for POS:

Key Store Hash Algorithm: SHA-256

Select Key Store Provider:
- ● RSA Key Manager v3.1
- ○ Simulator
- ○ Other

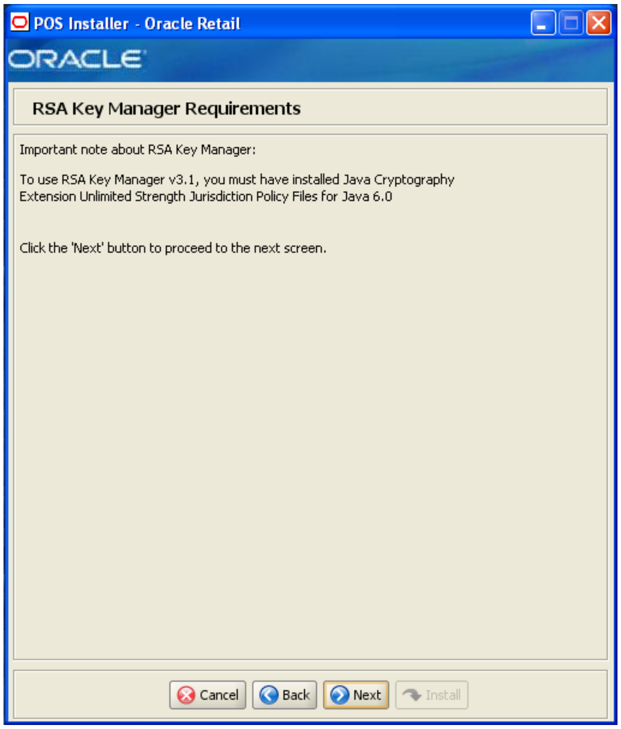
This screen is used to configure the Encryption Key Store provider.

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

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

Details	Content
Field Title	Select Key Store Provider
Field Description	Provider for Key Store management. ■ To use the RSA key management package, select **RSA Key Manager v3.1**. The next screen displayed is Figure B–22. ■ To use the simulated key management package, select **Simulator**. The next screen displayed is Figure B–26. ■ To use a different key management provider, select **Other**. The next screen displayed is Figure B–27.
Example	RSA Key Manager v3.1

Figure B–22 RSA Key Manager Requirements for RSA Key Manager 3.1



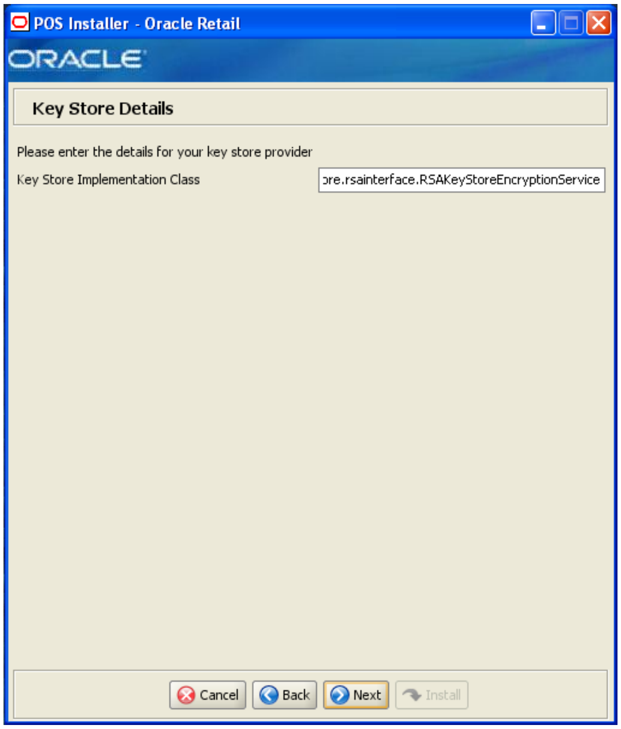
Important note about RSA Key Manager:

To use RSA Key Manager v3.1, you must have installed Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files for Java 6.0

Click the 'Next' button to proceed to the next screen.

This screen is only displayed if **RSA Key Manager v3.1** is selected for the Key Store provider on the Security Setup: Key Store screen. This informational screen explains the requirements to use the RSA Key Manager. Verify that you meet the requirements and then click **Next**.

Figure B–23 Key Store Details for RSA Key Manager 3.1



POS Installer - Oracle Retail

ORACLE

Key Store Details

Please enter the details for your key store provider

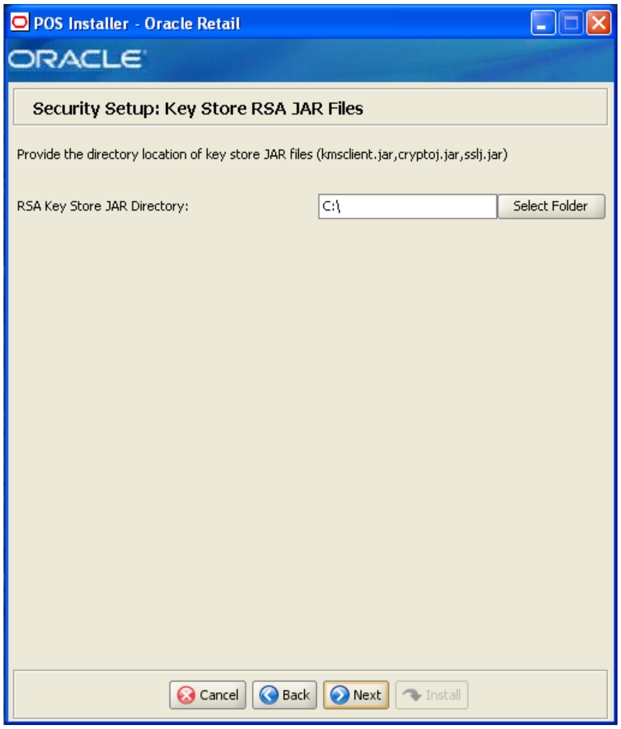
Key Store Implementation Class: ore.rsainterface.RSAKeyStoreEncryptionService

This screen is only displayed if **RSA Key Manager v3.1** is selected for the Key Store provider on the Security Setup: Key Store screen.

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

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

Figure B–24 Security Setup: Key Store JAR Files for RSA Key Manager 3.1



Security Setup: Key Store RSA JAR Files

Provide the directory location of key store JAR files (kmsclient.jar,cryptoj.jar,sslj.jar)

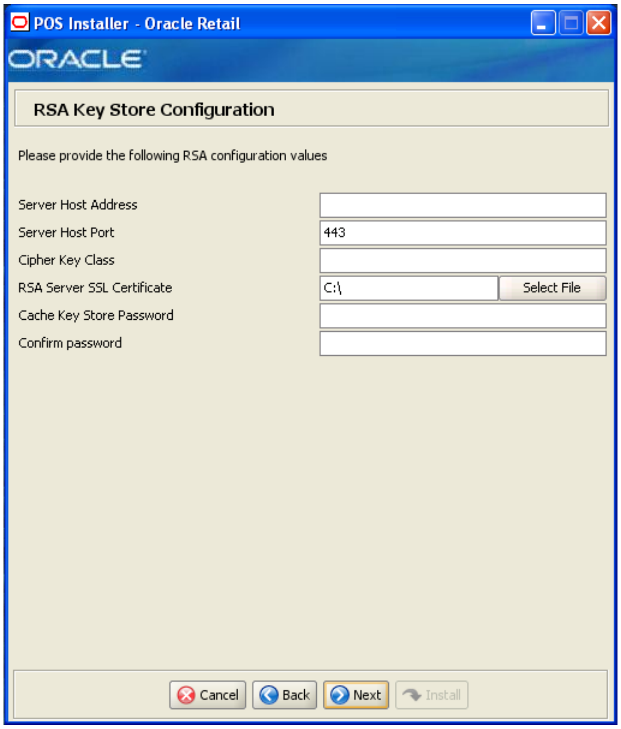
RSA Key Store JAR Directory: C:\

This screen is only displayed if **RSA Key Manager v3.1** is selected for the Key Store provider on the Security Setup: Key Store screen.

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

Details	**Content**
Field Title	Key Store JAR Directory
Field Description	Choose the directory where the following Key Store jar files are located: ■ `kmsclient.jar` ■ `cryptoj.jar` ■ `sslj.jar`
Example	`C:\`

Figure B–25 RSA Key Store Configuration for RSA Key Manager 3.1



RSA Key Store Configuration

Please provide the following RSA configuration values

Server Host Address	
Server Host Port	443
Cipher Key Class	
RSA Server SSL Certificate	C:\
Cache Key Store Password	
Confirm password	

This screen is only displayed if **RSA Key Manager v3.1** is selected for the Key Store provider on the Security Setup: Key Store screen.

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

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

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

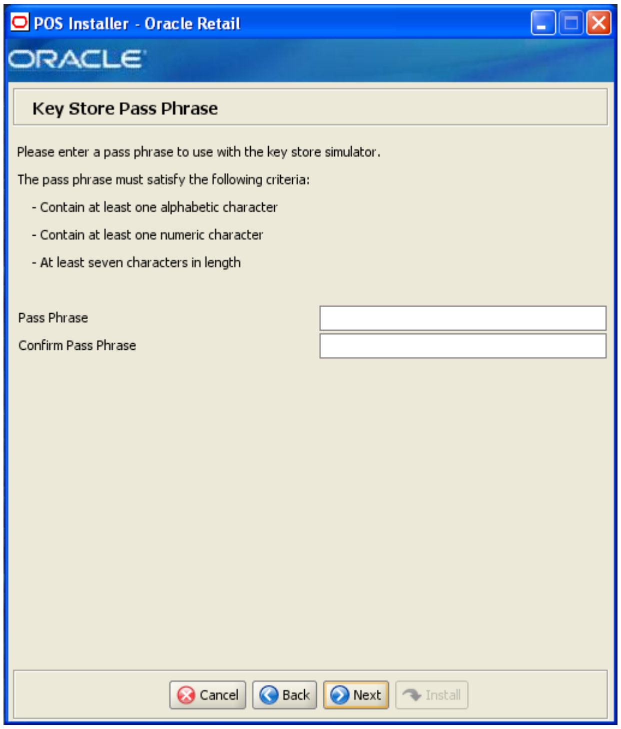
Details	Content
Field Title	Cipher Key Class
Field Description	Enter the RSA Key Manager cipher key class.

Details	Content
Field Title	RSA Server SSL Certificate
Field Description	Select the location of the RSA Key Manager server SSL certificate.

Details	Content
Field Title	Cache Key Store Password
Field Description	Enter the password used to access the RSA Key Manager cache. **Note:** You should verify that the SSL certificate at this location is valid.

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

Figure B–26 Key Store Pass Phrase for Simulator Key Manager



Please enter a pass phrase to use with the key store simulator.

The pass phrase must satisfy the following criteria:

- Contain at least one alphabetic character
- Contain at least one numeric character
- At least seven characters in length

Pass Phrase

Confirm Pass Phrase

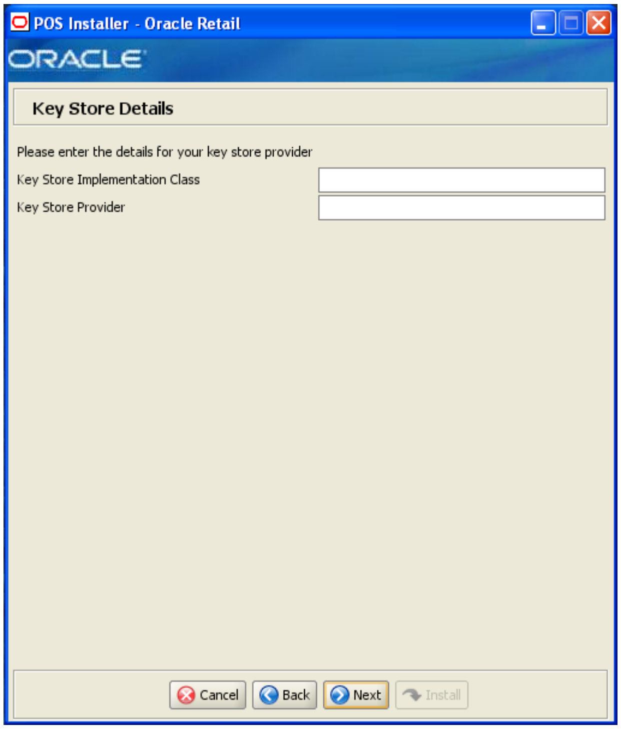
This screen is only displayed if **Simulator** is selected for the Key Store provider on the Security Setup: Key Store screen.

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

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–27 Key Store Details for Other Key Manager



Please enter the details for your key store provider

Key Store Implementation Class

Key Store Provider

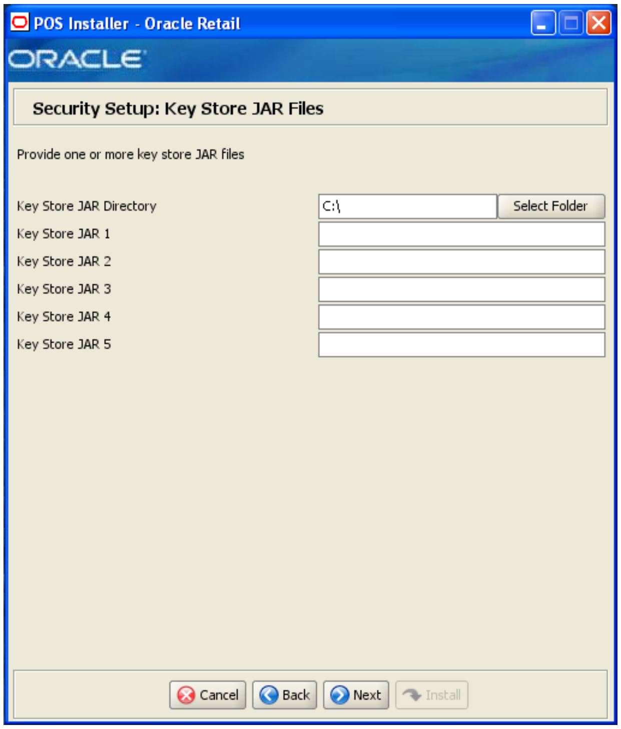
This screen is only displayed if **Other** is selected for the Key Store provider on the Security Setup: Key Store screen.

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

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

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

Figure B–28 Security Setup: Key Store JAR Files for Other Key Manager



Security Setup: Key Store JAR Files

Provide one or more key store JAR files

Key Store JAR Directory: C:\
Key Store JAR 1:
Key Store JAR 2:
Key Store JAR 3:
Key Store JAR 4:
Key Store JAR 5:

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

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

Details	Content
Field Title	Key Store JAR Directory
Field Description	Choose the directory where the Key Store jar files are located.
Example	`C:\`

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

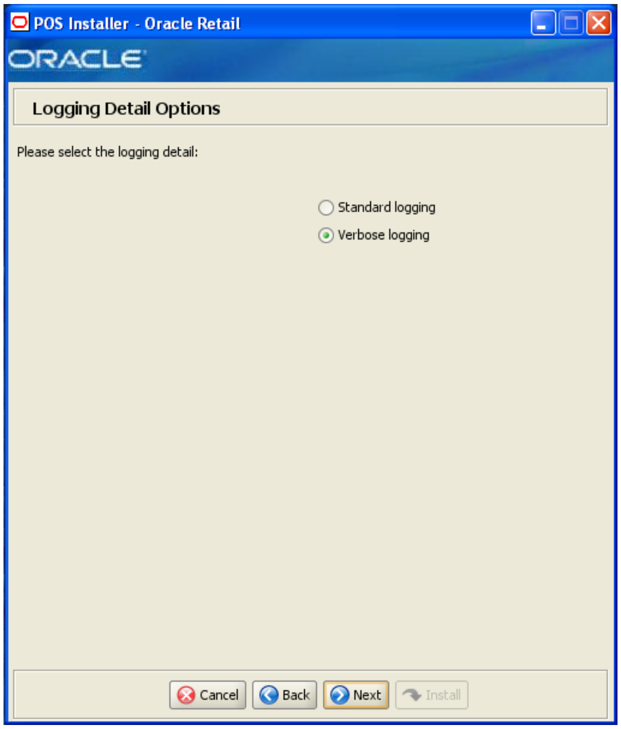
Details	Content
Field Title	Key Store JAR 2
Field Description	Enter the name of a Key Store jar file.

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

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

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

Figure B–29 Logging Detail Options



POS Installer - Oracle Retail

Logging Detail Options

Please select the logging detail:

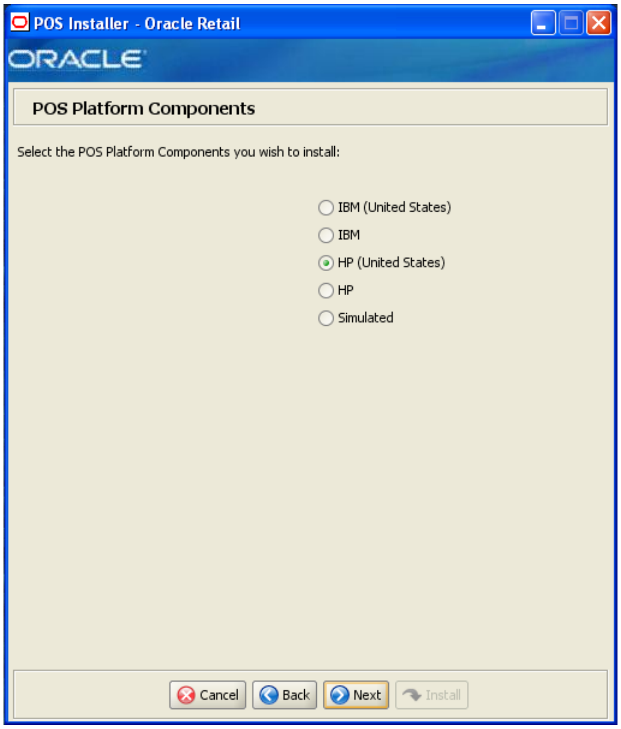
○ Standard logging

● Verbose logging

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



POS Installer - Oracle Retail

ORACLE

POS Platform Components

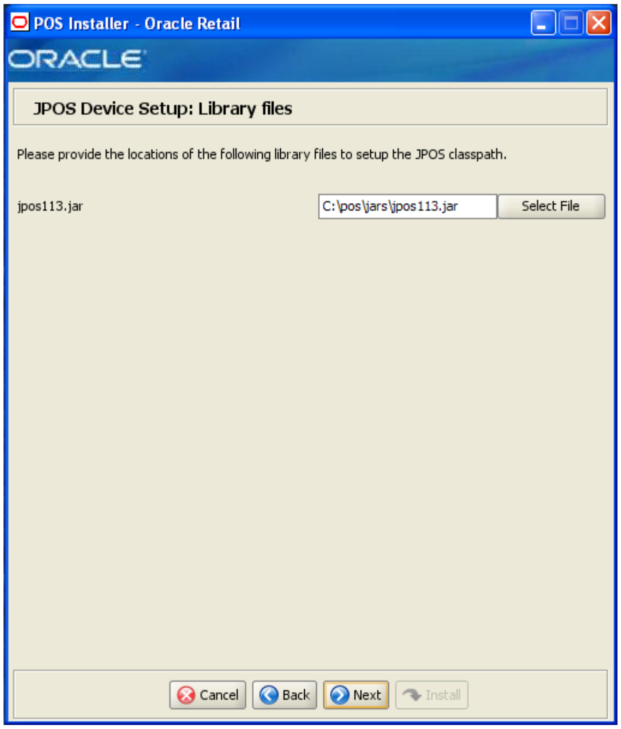
Select the POS Platform Components you wish to install:

○ IBM (United States)
○ IBM
● HP (United States)
○ HP
○ Simulated

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 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 HP (United States), HP, and Simulated are supported on the Oracle stack.
Example	HP (United States)

Figure B–31 JPOS Device Setup: Library Files



JPOS Device Setup: Library files

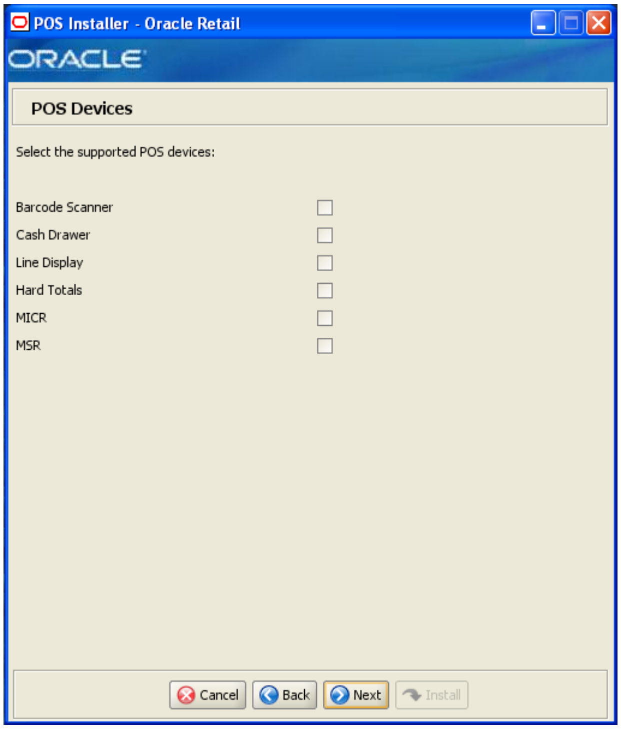
Please provide the locations of the following library files to setup the JPOS classpath.

jpos113.jar C:\pos\jars\jpos113.jar

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

Details	Content
Field Title	jpos113.jar
Field Description	Enter the location of the jar file.
Example	`C:\pos\jars\pos113.jar`

Figure B–32 POS Devices



POS Devices

Select the supported POS devices:

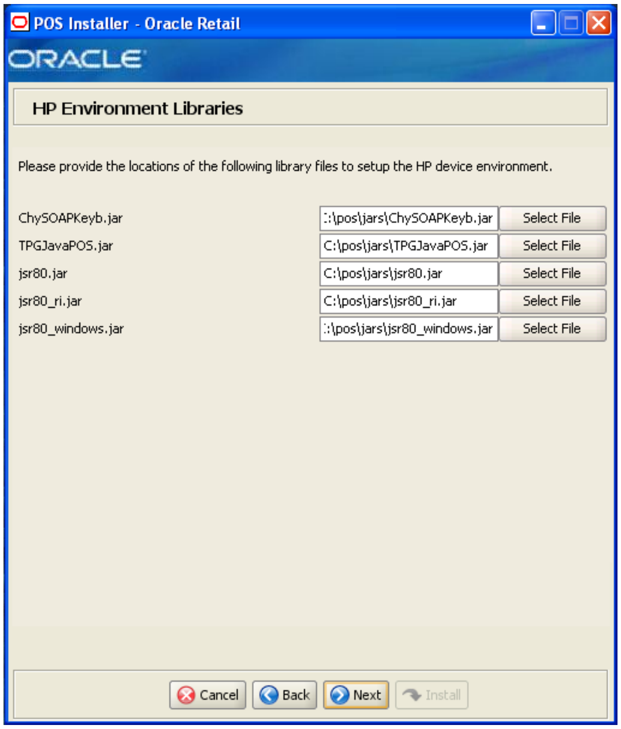
Barcode Scanner □
Cash Drawer □
Line Display □
Hard Totals □
MICR □
MSR □

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

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

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

Figure B–33 HP Environment Libraries



HP Environment Libraries

Please provide the locations of the following library files to setup the HP device environment.

ChySOAPKeyb.jar	:\pos\jars\ChySOAPKeyb.jar
TPGJavaPOS.jar	C:\pos\jars\TPGJavaPOS.jar
jsr80.jar	C:\pos\jars\jsr80.jar
jsr80_ri.jar	C:\pos\jars\jsr80_ri.jar
jsr80_windows.jar	:\pos\jars\jsr80_windows.jar

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

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

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

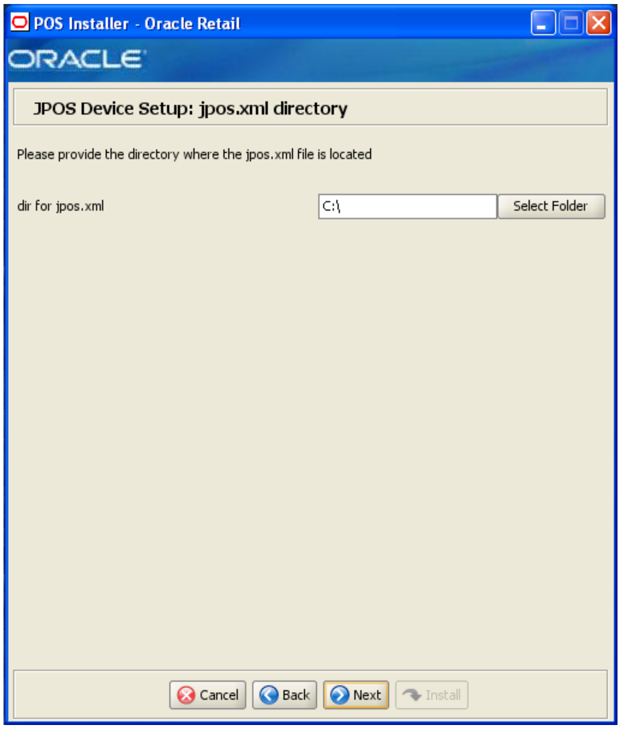
Details	**Content**
Field Title	TPGJavaPOS.jar
Field Description	Enter the location of the jar file.
Example	`C:\pos\jars\TPGHJavaPOS.jar`

Details	**Content**
Field Title	jsr80.jar
Field Description	Enter the location of the jar file.
Example	`C:\pos\jars\jsr80.jar`

Details	Content
Field Title	jsr80_ri.jar
Field Description	Enter the location of the jar file.
Example	`C:\pos\jars\jsr80_ri.jar`

Details	Content
Field Title	jsr80_windows.jar
Field Description	Enter the location of the jar file.
Example	`C:\pos\jars\jsr80_windows.jar`

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



JPOS Device Setup: jpos.xml directory

Please provide the directory where the jpos.xml file is located

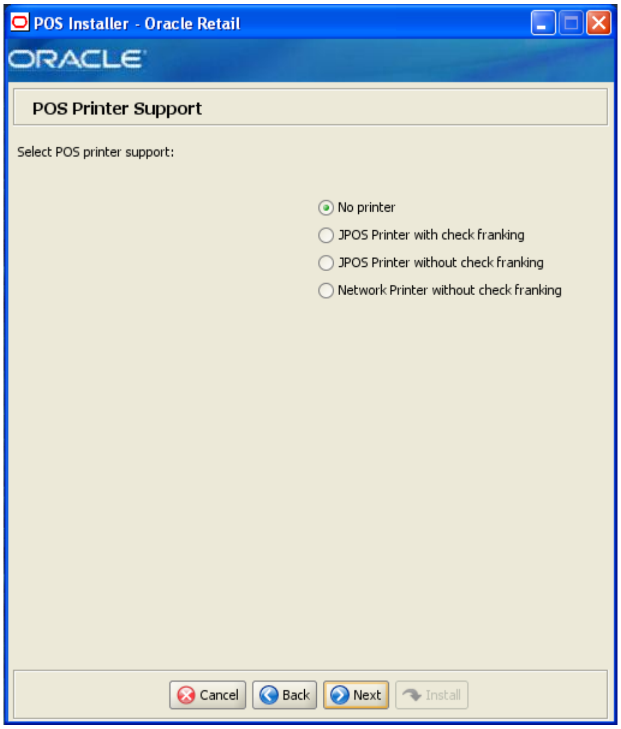
dir for jpos.xml: C:\

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

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

Details	Content
Field Title	dir for jpos.xml
Field Description	Enter the location of the directory.
Example	`C:\`

Figure B–35 POS Printer Support



POS Printer Support

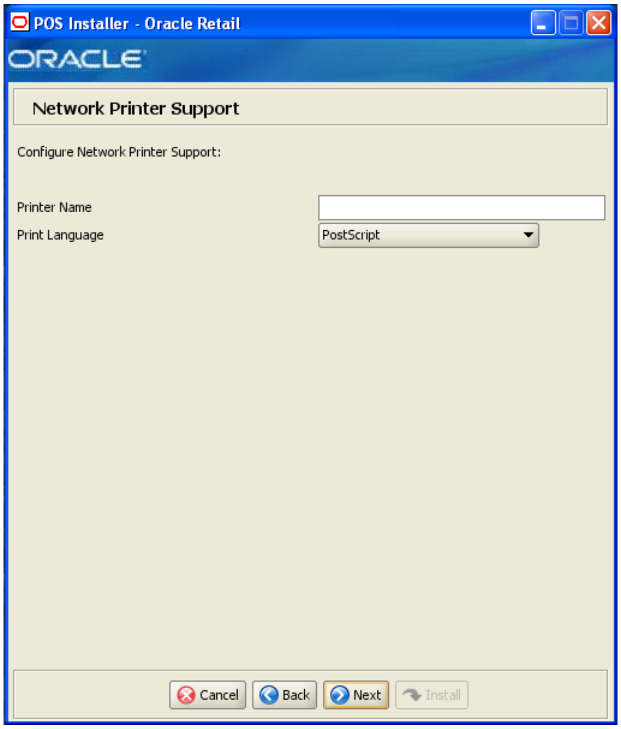
Select POS printer support:

● No printer
○ JPOS Printer with check franking
○ JPOS Printer without check franking
○ Network Printer without check franking

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



Configure Network Printer Support:

Printer Name

Print Language: PostScript

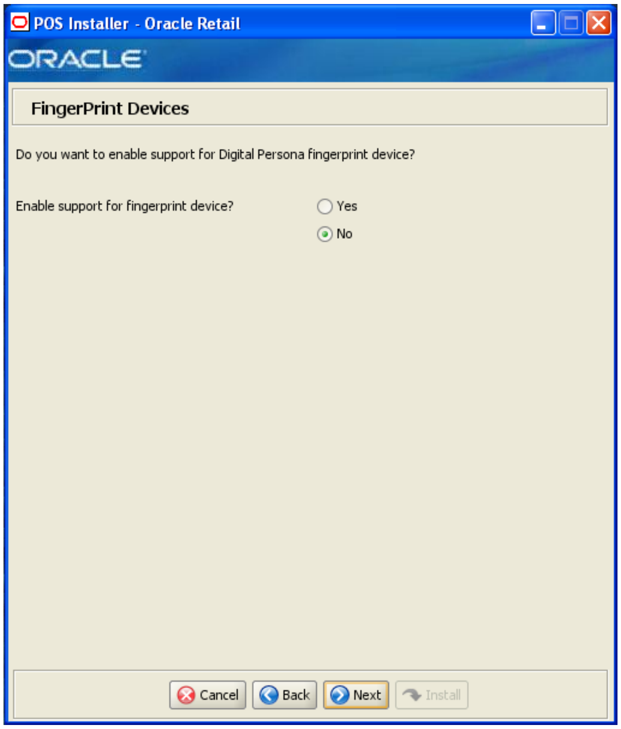
This screen is only displayed if **Network Printer without check franking** is selected on the POS Printer Support screen.

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 Fingerprint Devices



POS Installer - Oracle Retail

FingerPrint Devices

Do you want to enable support for Digital Persona fingerprint device?

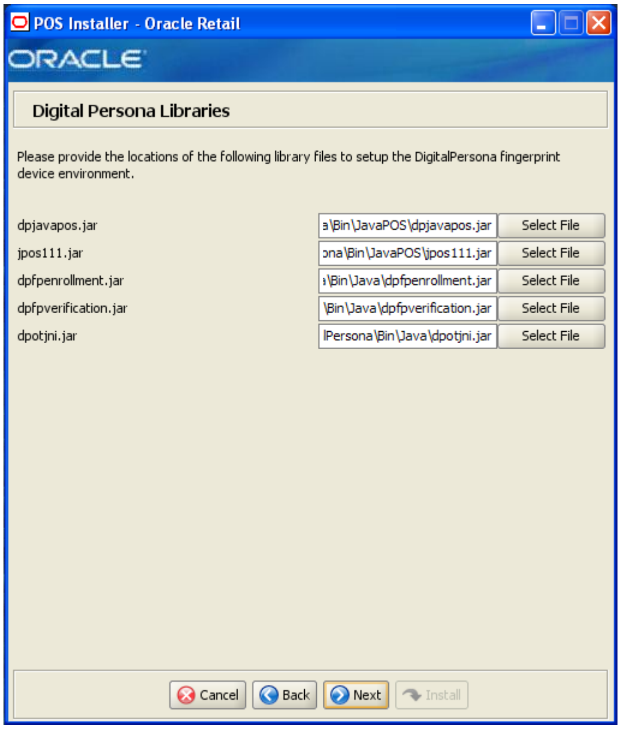
Enable support for fingerprint device? ○ Yes ● No

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

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

Details	Content
Field Title	Enable support for fingerprint device?
Field Description	Choose whether the use of a fingerprint device is enabled.
Example	Yes

Figure B–38 Digital Persona Libraries



Digital Persona Libraries

Please provide the locations of the following library files to setup the DigitalPersona fingerprint device environment.

dpjavapos.jar	a\Bin\JavaPOS\dpjavapos.jar
jpos111.jar	ona\Bin\JavaPOS\jpos111.jar
dpfpenrollment.jar	\Bin\Java\dpfpenrollment.jar
dpfpverification.jar	\Bin\Java\dpfpverification.jar
dpotjni.jar	lPersona\Bin\Java\dpotjni.jar

This screen is only displayed if **Yes** is selected on the Fingerprint Devices screen.

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

Details	Content
Field Title	dpjavapos.jar
Field Description	Enter the location of the jar file.
Example	`C:\DigitalPersona\Bin\JavaPOS\dpjavapos.jar`

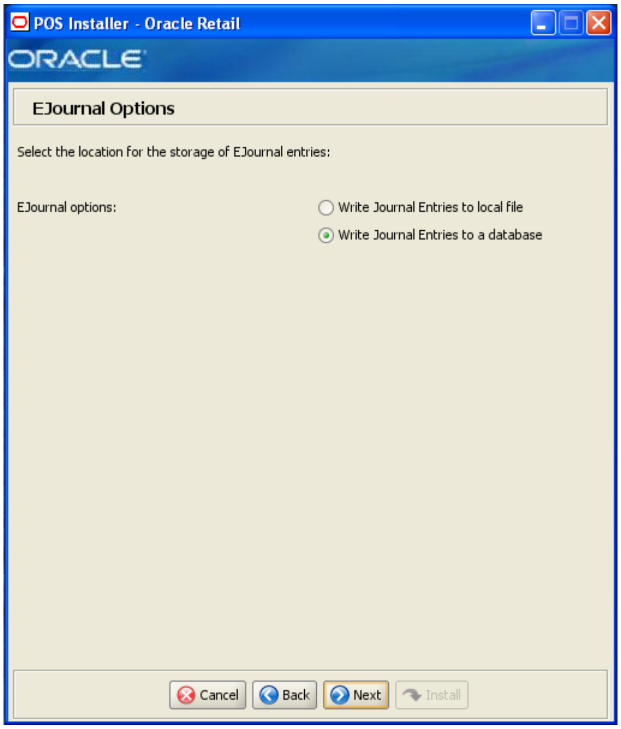
Details	Content
Field Title	jpos111.jar
Field Description	Enter the location of the jar file.
Example	`C:\DigitalPersona\Bin\JavaPOS\jpos111.jar`

Details	Content
Field Title	dpfpenrollment.jar
Field Description	Enter the location of the jar file.
Example	`C:\DigitalPersona\Bin\JavaPOS\dpfpenrollment.jar`

Details	Content
Field Title	dpfpverification.jar
Field Description	Enter the location of the jar file.
Example	`C:\DigitalPersona\Bin\JavaPOS\dpfpverification.jar`

Details	Content
Field Title	dpotjni.jar
Field Description	Enter the location of the jar file.
Example	`C:\DigitalPersona\Bin\JavaPOS\dpotjni.jar`

Figure B–39 EJournal Options



Select the location for the storage of EJournal entries:

EJournal options:

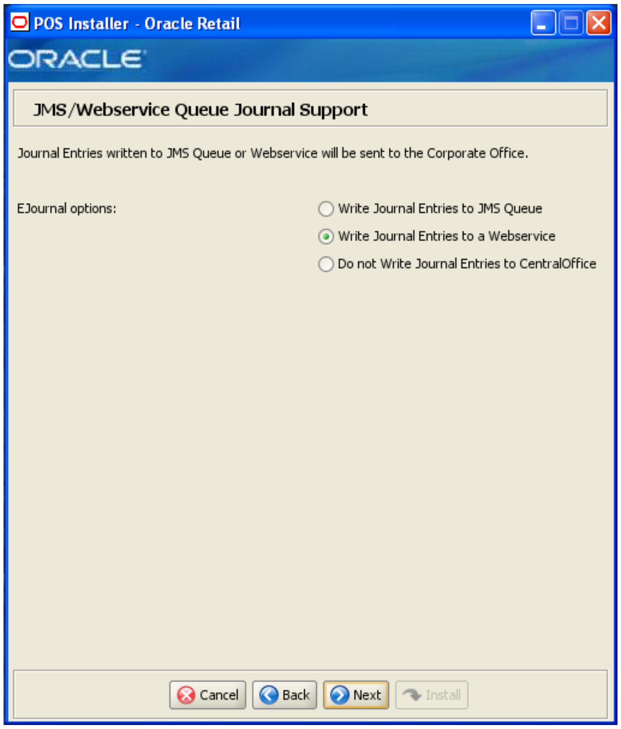
○ Write Journal Entries to local file

● Write Journal Entries to a database

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–40 JMS /Webservice Queue Journal Support



JMS/Webservice Queue Journal Support

Journal Entries written to JMS Queue or Webservice will be sent to the Corporate Office.

EJournal options:

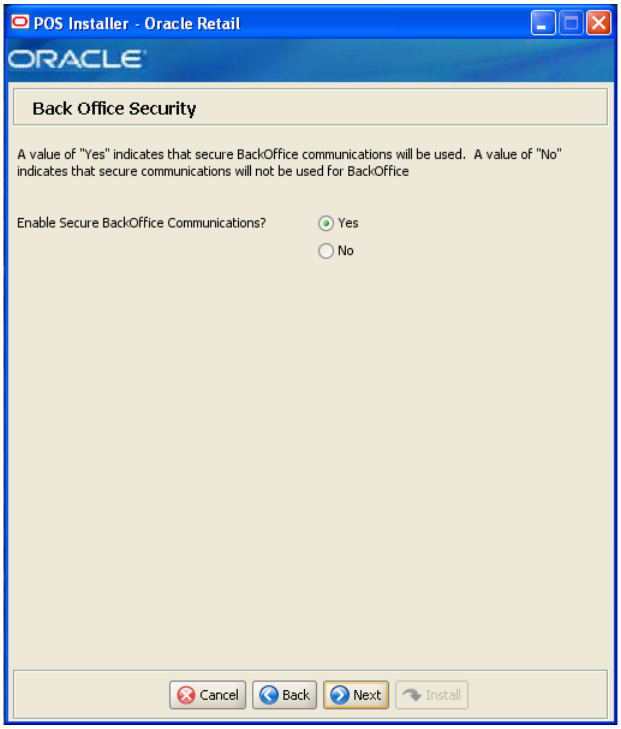
○ Write Journal Entries to JMS Queue
● Write Journal Entries to a Webservice
○ Do not Write Journal Entries to CentralOffice

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–41 Back Office Security



Back Office Security

A value of "Yes" indicates that secure BackOffice communications will be used. A value of "No" indicates that secure communications will not be used for BackOffice

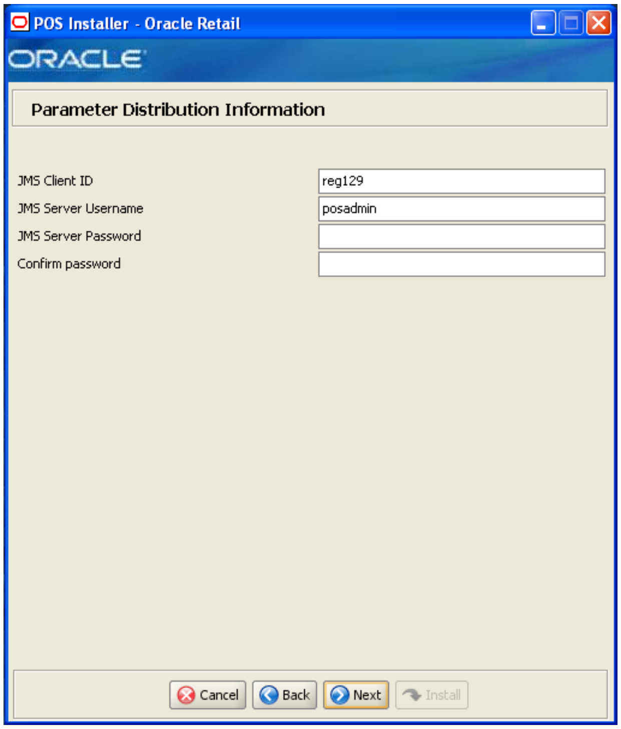
Enable Secure BackOffice Communications? ● Yes ○ No

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

Figure B–42 Parameter Distribution Information



Parameter Distribution Information

JMS Client ID	reg129
JMS Server Username	posadmin
JMS Server Password	
Confirm password	

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.

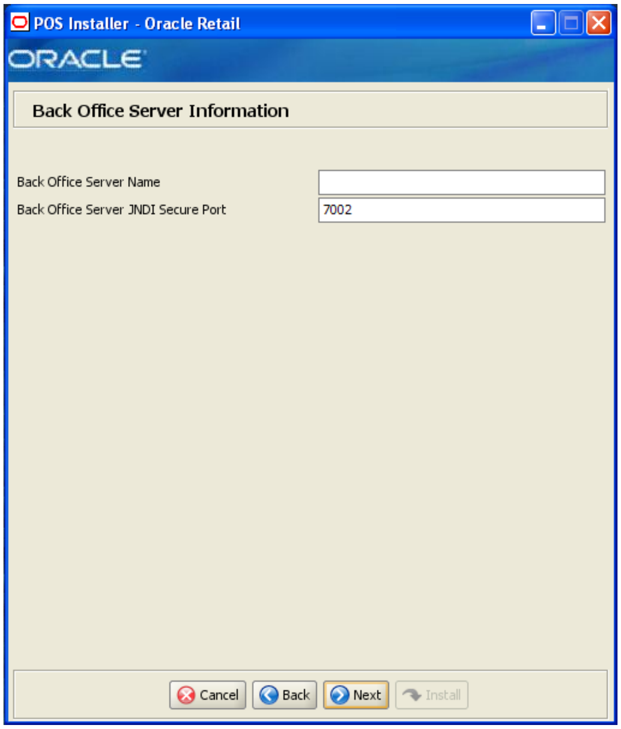
Details	Content
Field Title	JMS Client ID
Field Description	Identifier of the JMS client used for receiving parameter updates.
Example	reg129

Details	Content
Field Title	JMS Username
Field Description	Identifier of the JMS user for receiving parameter updates.
Example	posadmin

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

Details	Content
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–43 Back Office Server Information



Back Office Server Name

Back Office Server JNDI Secure Port 7002

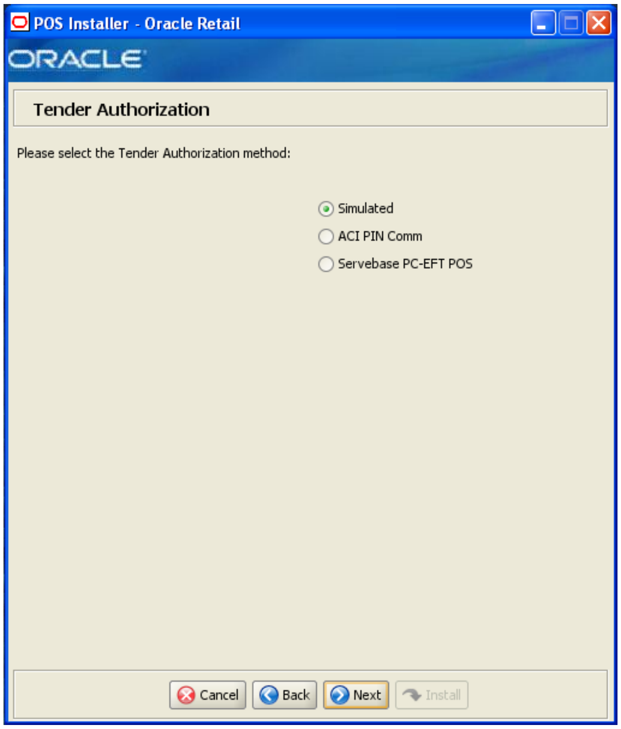
This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

Details	Content
Field Title	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	7002

Figure B–44 Tender Authorization



Tender Authorization

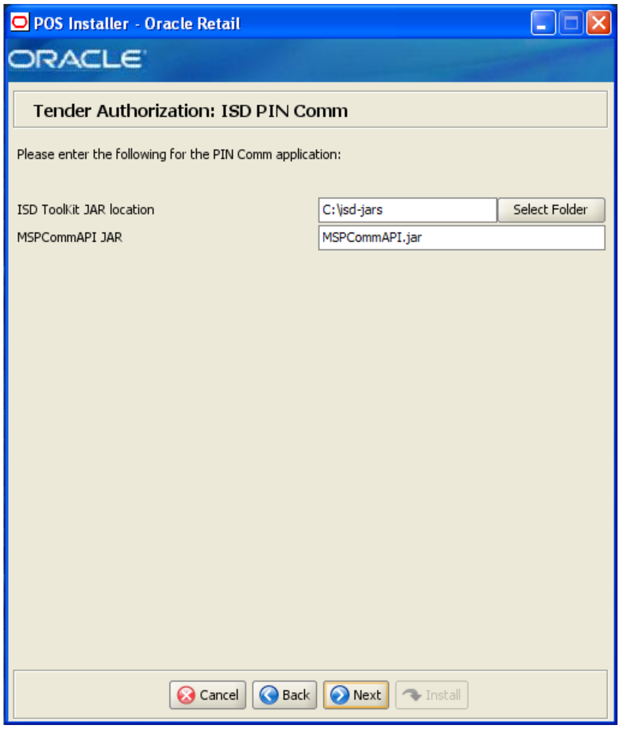
Please select the Tender Authorization method:

● Simulated
○ ACI PIN Comm
○ Servebase PC-EFT POS

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–45 Tender Authorization: ISD PIN Comm


POS Installer - Oracle Retail
ORACLE
Tender Authorization: ISD PIN Comm

Please enter the following for the PIN Comm application:

ISD ToolKit JAR location: C:\isd-jars

MSPCommAPI JAR: MSPCommAPI.jar

Select Folder
Cancel
Back
Next
Install

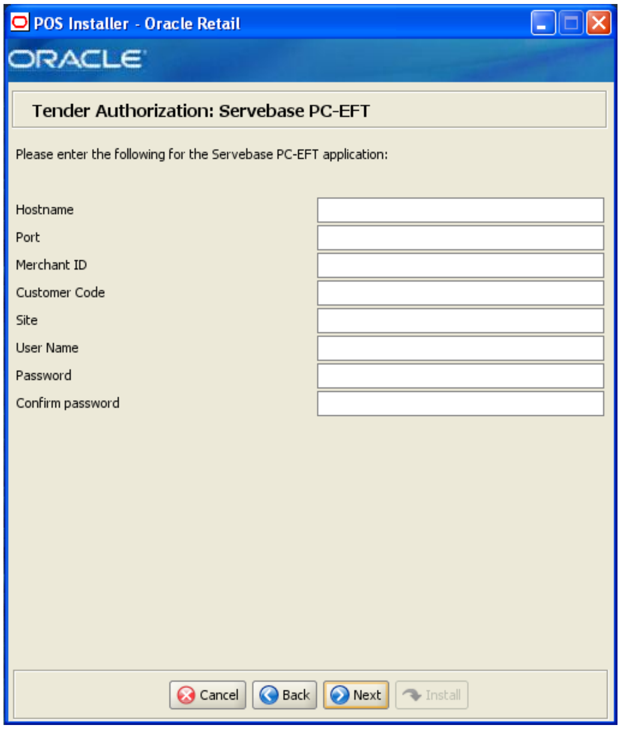
This screen is only displayed if **ACI PIN Comm** is selected for the Tender Authorization.

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	`C:\isd-jars`

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

Figure B–46 Tender Authorization: Servebase PC-EFT



Tender Authorization: Servebase PC-EFT

Please enter the following for the Servebase PC-EFT application:

Hostname

Port

Merchant ID

Customer Code

Site

User Name

Password

Confirm password

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 Servebase server.

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

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

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

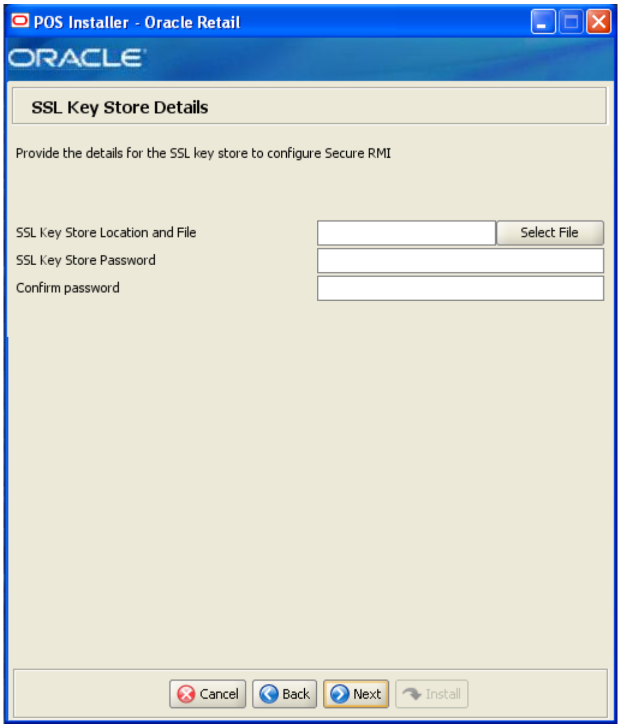
Details	Content
Field Title	Site
Field Description	Enter the site to access the Servebase application.

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

Details	Content
Field Title	Password
Field Description	Enter the password to use to access the Servebase 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–47 SSL Key Store Details



SSL Key Store Details

Provide the details for the SSL key store to configure Secure RMI

SSL Key Store Location and File

SSL Key Store Password

Confirm password

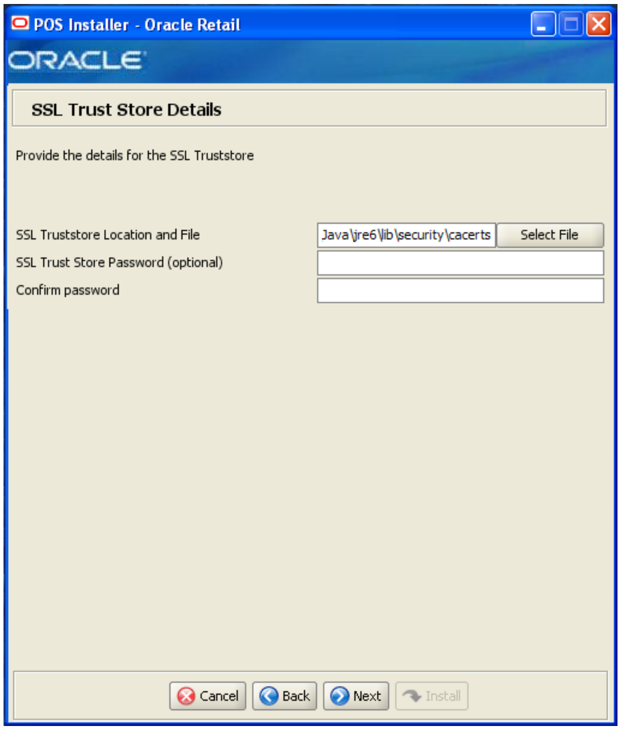
The fields on this screen are described in the following tables.

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–48 SSL Trust Store Details



SSL Trust Store Details

Provide the details for the SSL Truststore

SSL Truststore Location and File	Java\jre6\lib\security\cacerts
SSL Trust Store Password (optional)	
Confirm password	

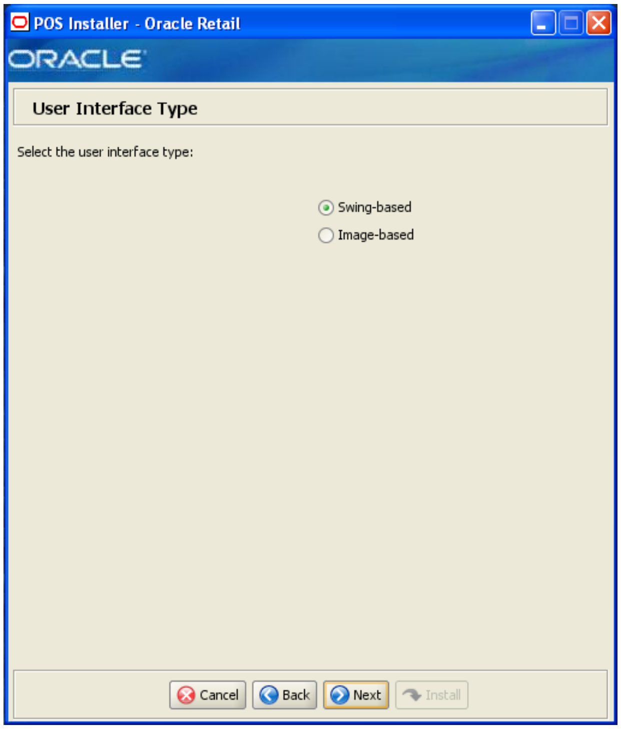
The fields on this screen are described in the following tables.

Details	Content
Field Title	SSL Truststore Location and File
Field Description	Enter the location and name of the truststore file.
Example	`C:\Program Files\Java\jre6\lib\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–49 User Interface Type



POS Installer - Oracle Retail

User Interface Type

Select the user interface type:

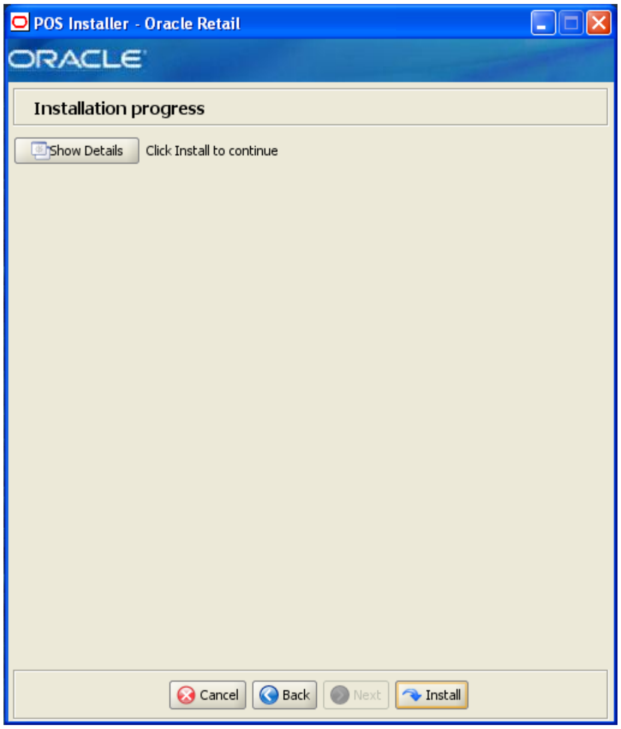
● Swing-based

○ Image-based

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

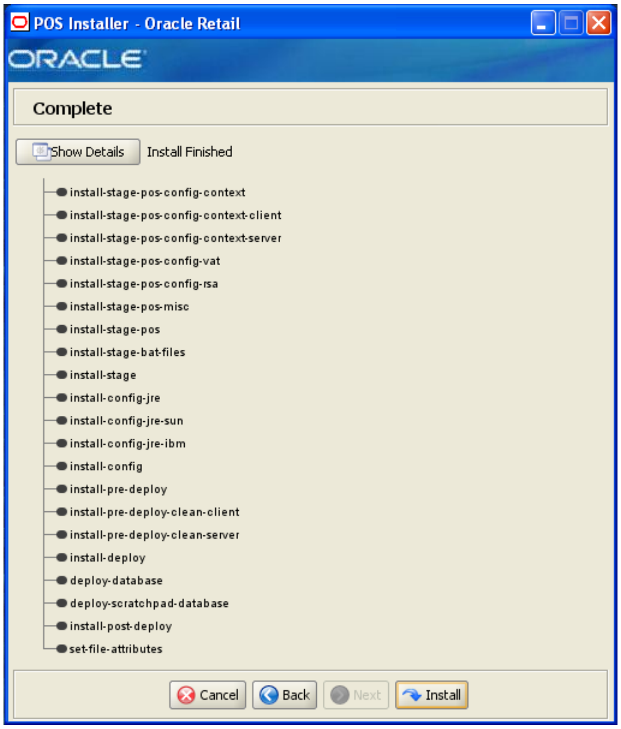
Figure B–50 Installation Progress



Installation progress

Click Install to continue

Figure B–51 Install Complete



Complete

Install Finished

```
├─● install-stage-pos-config-context
├─● install-stage-pos-config-context-client
├─● install-stage-pos-config-context-server
├─● install-stage-pos-config-vat
├─● install-stage-pos-config-rsa
├─● install-stage-pos-misc
├─● install-stage-pos
├─● install-stage-bat-files
├─● install-stage
├─● install-config-jre
├─● install-config-jre-sun
├─● install-config-jre-ibm
├─● install-config
├─● install-pre-deploy
├─● install-pre-deploy-clean-client
├─● install-pre-deploy-clean-server
├─● install-deploy
├─● deploy-database
├─● deploy-scratchpad-database
├─● install-post-deploy
└─● set-file-attributes
```

C

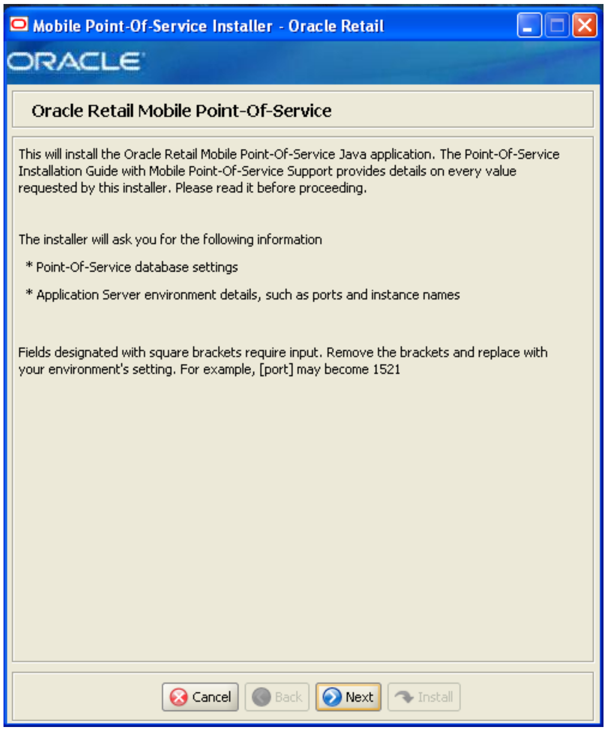
Appendix: Installer Screens for Mobile Point-of-Service Server

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

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

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

Figure C–1 Introduction



Oracle Retail Mobile Point-Of-Service

This will install the Oracle Retail Mobile Point-Of-Service Java application. The Point-Of-Service Installation Guide with Mobile Point-Of-Service Support provides details on every value requested by this installer. Please read it before proceeding.

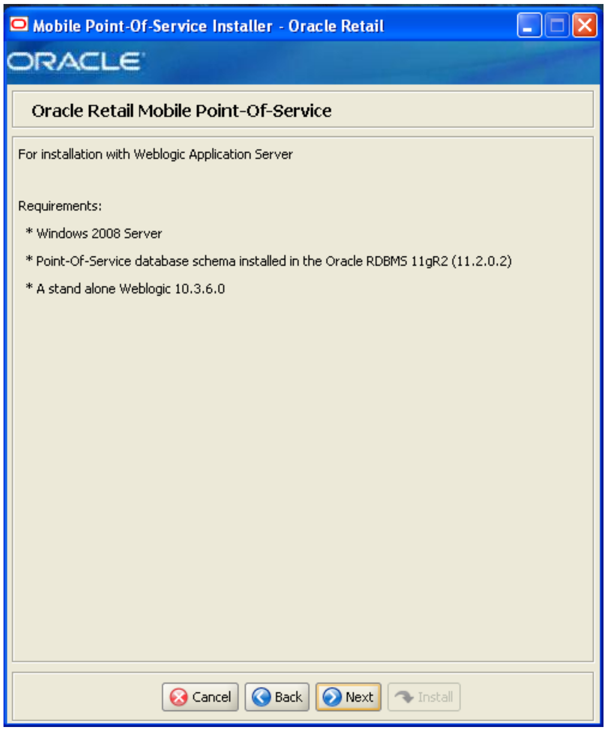
The installer will ask you for the following information

* Point-Of-Service database settings

* Application Server environment details, such as ports and instance names

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

Figure C–2 Requirements



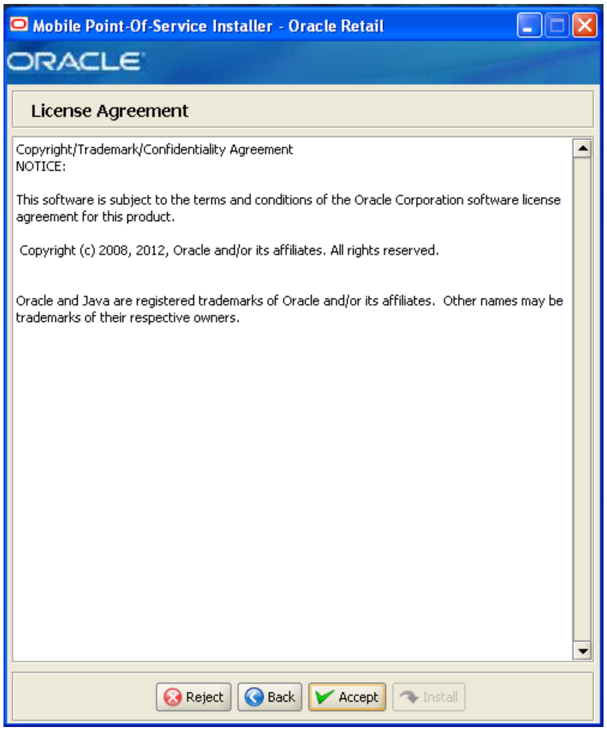
Oracle Retail Mobile Point-Of-Service

For installation with Weblogic Application Server

Requirements:

* Windows 2008 Server
* Point-Of-Service database schema installed in the Oracle RDBMS 11gR2 (11.2.0.2)
* A stand alone Weblogic 10.3.6.0

Figure C–3 License Agreement



License Agreement

Copyright/Trademark/Confidentiality Agreement
NOTICE:

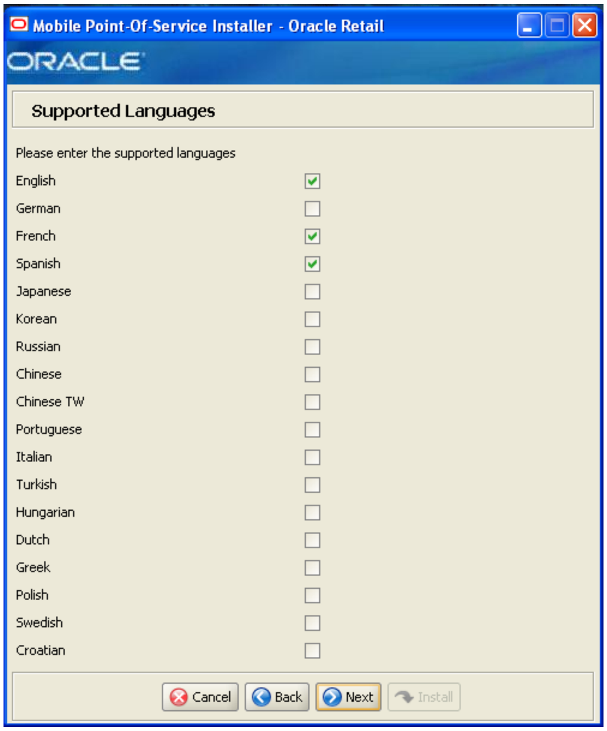
This software is subject to the terms and conditions of the Oracle Corporation software license agreement for this product.

Copyright (c) 2008, 2012, Oracle and/or its affiliates. All rights reserved.

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

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

Figure C–4 Supported Languages



Supported Languages

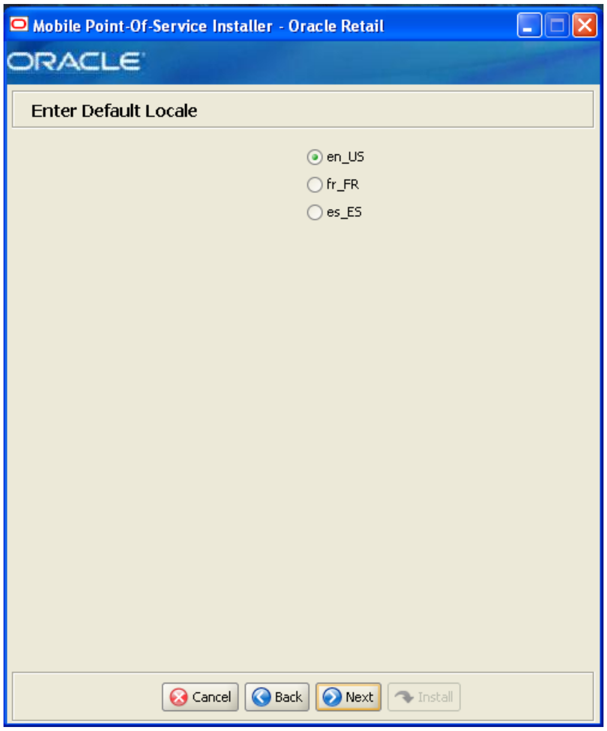
Please enter the supported languages

English	☑
German	□
French	☑
Spanish	☑
Japanese	□
Korean	□
Russian	□
Chinese	□
Chinese TW	□
Portuguese	□
Italian	□
Turkish	□
Hungarian	□
Dutch	□
Greek	□
Polish	□
Swedish	□
Croatian	□

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 Mobile Point-of-Service application. The languages selected on this screen determine the available choices on the Enter Default Locale screen.
Example	English, French, and English

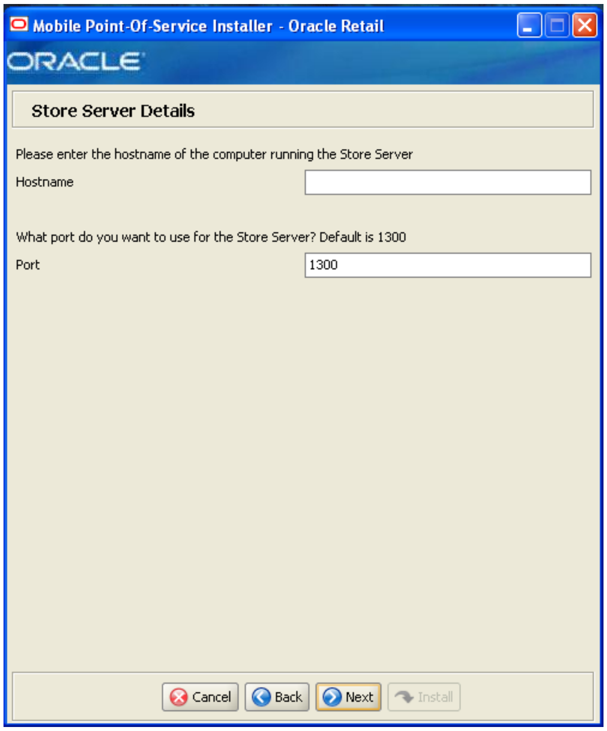
Figure C–5 Enter Default Locale



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

Details	Content
Field Title	Enter Default Locale
Field Description	Locale support in Mobile 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 C–6 Store Server Details



Store Server Details

Please enter the hostname of the computer running the Store Server

Hostname

What port do you want to use for the Store Server? Default is 1300

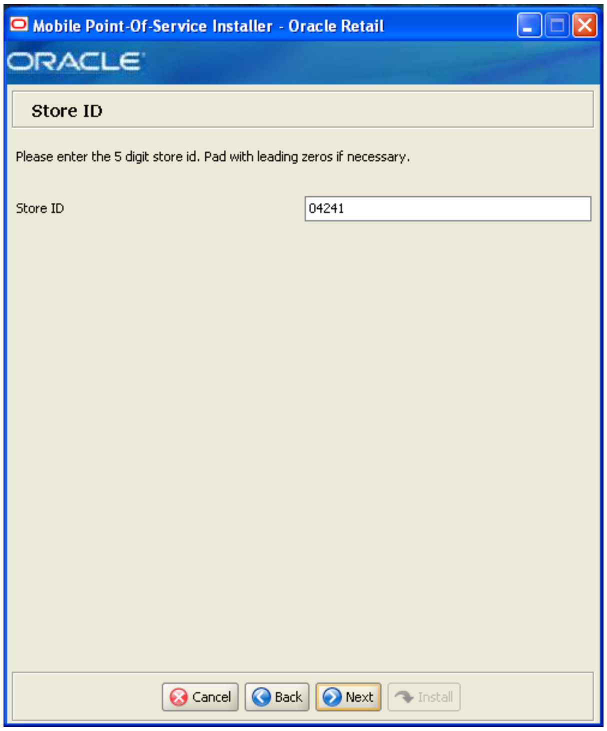
Port 1300

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 C–7 Store ID



Mobile Point-Of-Service Installer - Oracle Retail

Store ID

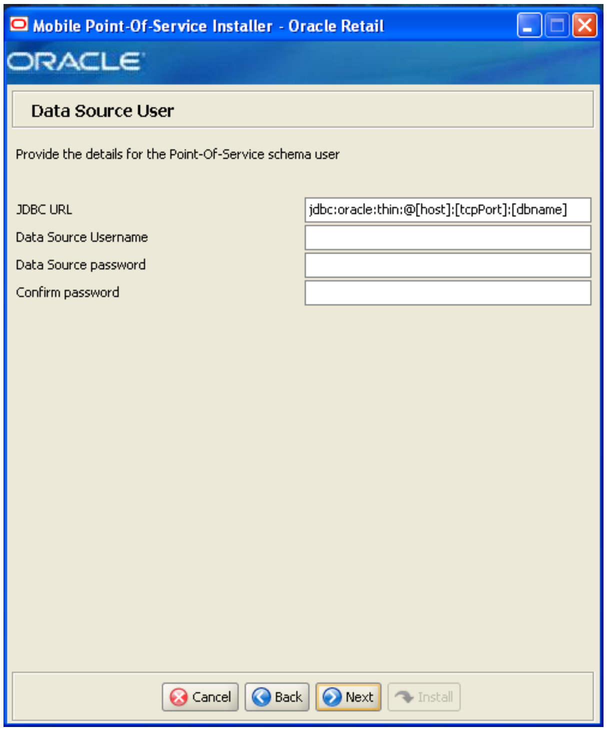
Please enter the 5 digit store id. Pad with leading zeros if necessary.

Store ID 04241

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 C–8 Database Source User



Mobile Point-Of-Service Installer - Oracle Retail

Data Source User

Provide the details for the Point-Of-Service schema user

JDBC URL: jdbc:oracle:thin:@[host]:[tcpPort]:[dbname]

Data Source Username:

Data Source password:

Confirm password:

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

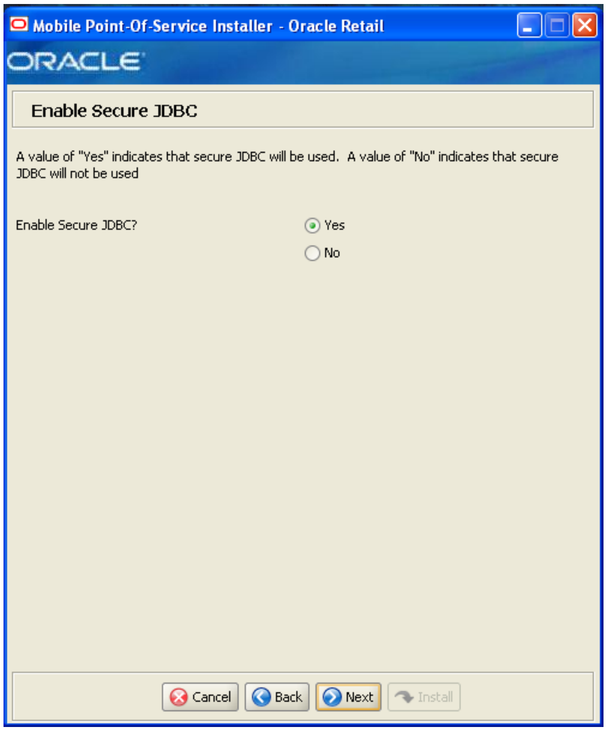
Details	Content
Field Title	JDBC URL
Field Description	Enter the URL used by the Mobile Point-of-Service application to access the database schema. For the expected syntax, see Appendix E.
Example	`jdbc:oracle:thin:@DB_HOST_NAME:1521:DB_NAME`

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 Mobile 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 C–9 Enable Secure JDBC



Enable Secure JDBC

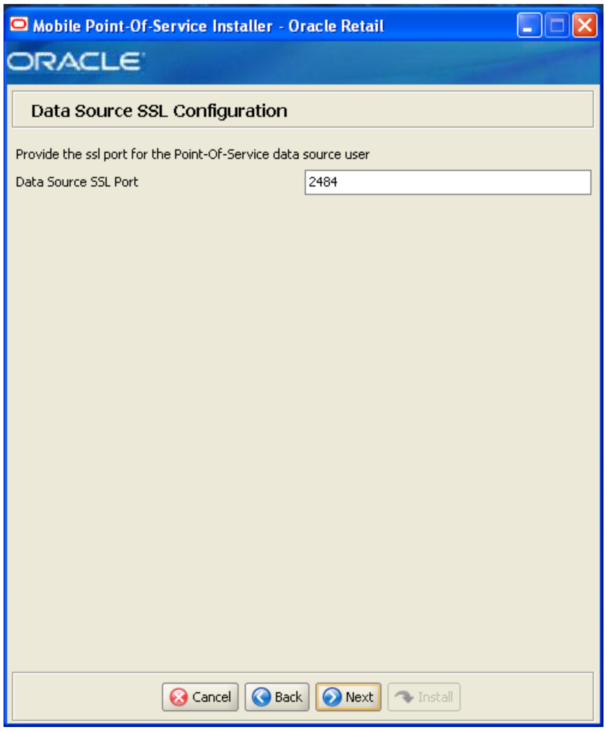
A value of "Yes" indicates that secure JDBC will be used. A value of "No" indicates that secure JDBC will not be used

Enable Secure JDBC? ● Yes ○ No

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

Details	Content
Field Title	Enable Secure JDBC?
Field Description	Select whether secure JDBC is to be used for communication between the mobile server and mobile devices.
Example	Yes

Figure C–10 Data Source SSL Configuration



Mobile Point-Of-Service Installer - Oracle Retail

Data Source SSL Configuration

Provide the ssl port for the Point-Of-Service data source user

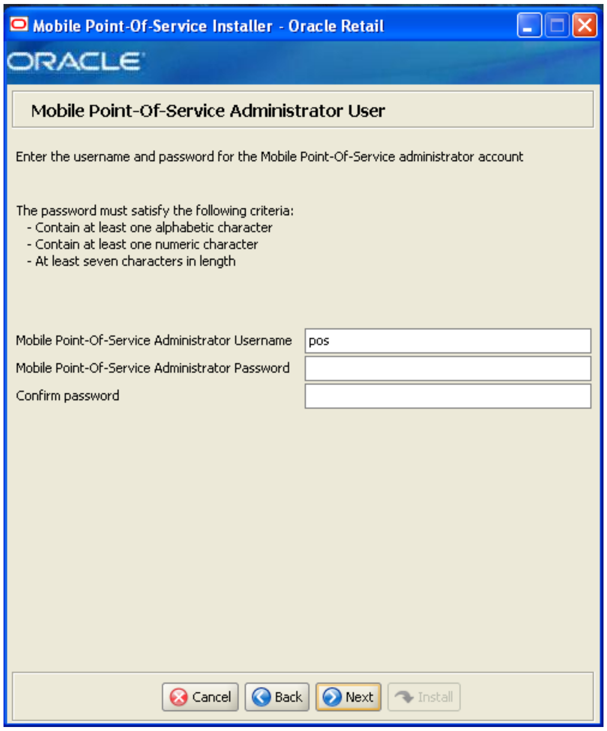
Data Source SSL Port: 2484

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

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

Details	Content
Field Title	Data Source SSL Port
Field Description	SSL port used to access the database.
Example	2484

Figure C–11 Mobile Point-of-Service Administrator User



Mobile Point-Of-Service Installer - Oracle Retail

Mobile Point-Of-Service Administrator User

Enter the username and password for the Mobile Point-Of-Service administrator account

The password must satisfy the following criteria:
- Contain at least one alphabetic character
- Contain at least one numeric character
- At least seven characters in length

Mobile Point-Of-Service Administrator Username: pos
Mobile Point-Of-Service Administrator Password:
Confirm password:

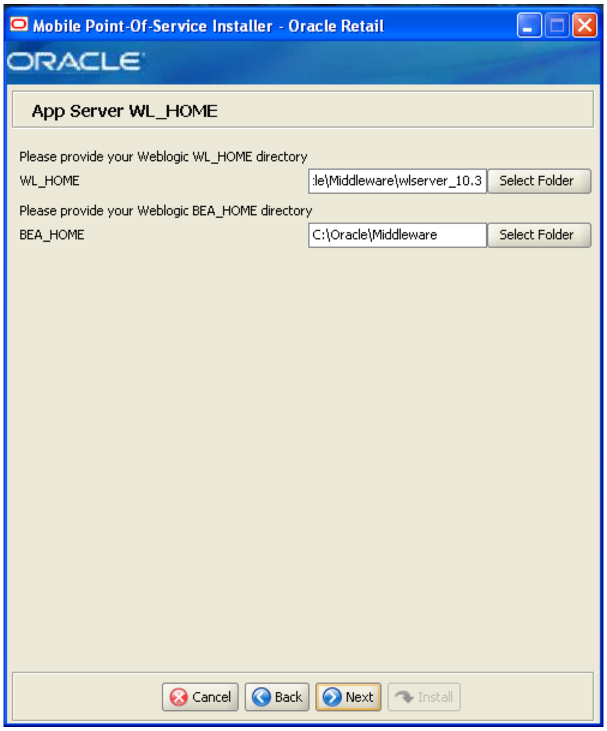
The fields on this screen are described in the following tables.

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

Details	**Content**
Field Title	Mobile Point-of-Service Administrator Password
Field Description	Enter the password for the administrator user.

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

Figure C–12 App Server WL_HOME



Mobile Point-Of-Service Installer - Oracle Retail

App Server WL_HOME

Please provide your Weblogic WL_HOME directory

WL_HOME :le\Middleware\wlserver_10.3

Please provide your Weblogic BEA_HOME directory

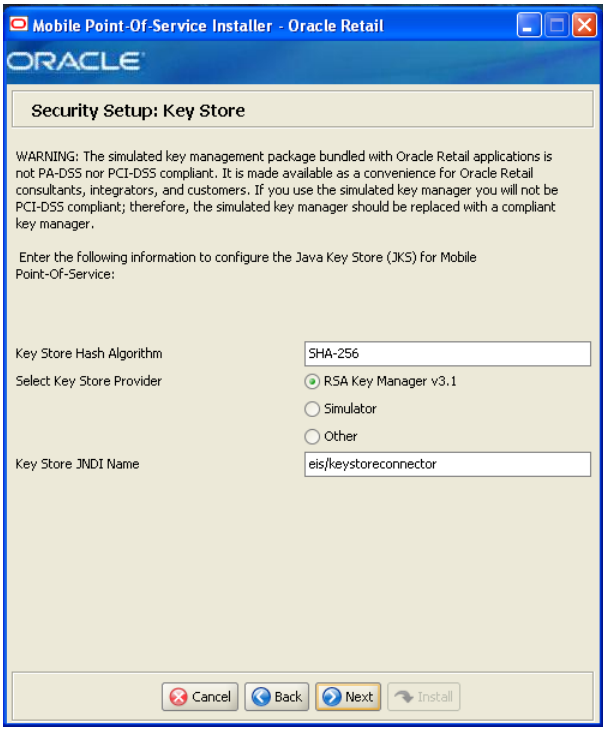
BEA_HOME C:\Oracle\Middleware

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

Details	Content
Field Title	WL_HOME
Field Description	Home directory for the Oracle WebLogic Server installation.
Example	`C:\Oracle\Middleware\wlserver_10.3`

Details	Content
Field Title	BEA_HOME
Field Description	Home directory for the Oracle BEA installation.
Example	`C:\Oracle\Middleware`

Figure C–13 Security Setup: Key Store Settings



Security Setup: Key Store

WARNING: The simulated key management package bundled with Oracle Retail applications is not PA-DSS nor PCI-DSS compliant. It is made available as a convenience for Oracle Retail consultants, integrators, and customers. 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.

Enter the following information to configure the Java Key Store (JKS) for Mobile Point-Of-Service:

Key Store Hash Algorithm: SHA-256

Select Key Store Provider: ● RSA Key Manager v3.1 ○ Simulator ○ Other

Key Store JNDI Name: eis/keystoreconnector

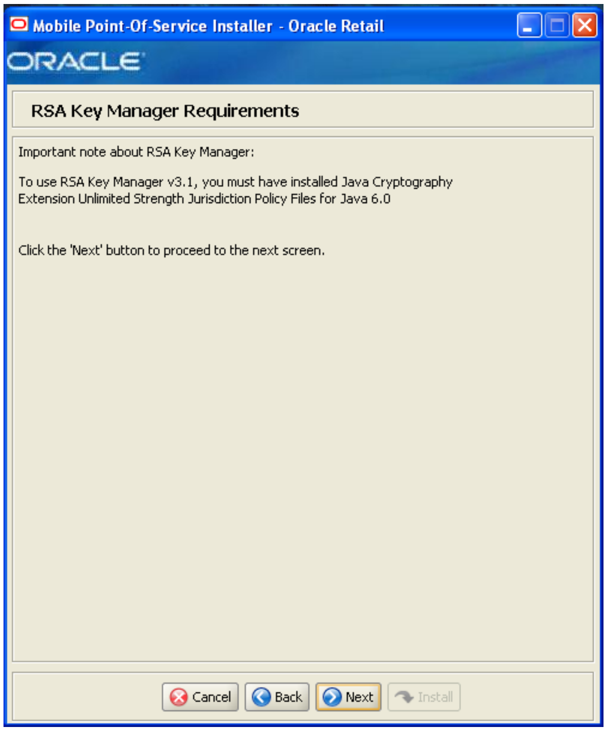
This screen is used to configure the Encryption Key Store provider.

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

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

Details	Content
Field Title	Select Key Store Provider
Field Description	Provider for Key Store management. ▪ To use the RSA key management package, select **RSA Key Manager v3.1**. The next screen displayed is Figure C–14. ▪ To use the simulated key management package, select **Simulator**. The next screen displayed is Figure C–18. ▪ To use a different key management provider, select **Other**. The next screen displayed is Figure C–19.
Example	RSA Key Manager v3.1

Figure C–14 RSA Key Manager Requirements for RSA Key Manager 3.1



RSA Key Manager Requirements

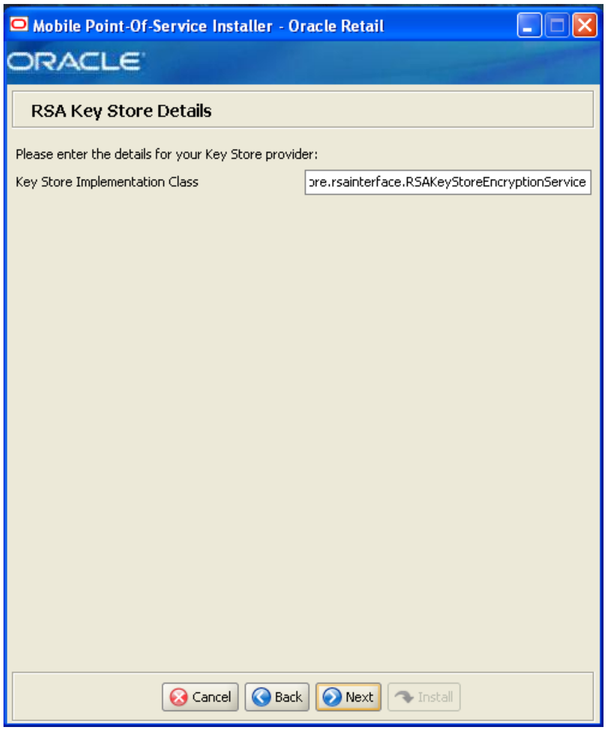
Important note about RSA Key Manager:

To use RSA Key Manager v3.1, you must have installed Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files for Java 6.0

Click the 'Next' button to proceed to the next screen.

This screen is only displayed if **RSA Key Manager v3.1** is selected for the Key Store provider on the Security Setup: Key Store screen. This informational screen explains the requirements to use the RSA Key Manager. Verify that you meet the requirements and then click **Next**.

Figure C–15 Key Store Details for RSA Key Manager 3.1



RSA Key Store Details

Please enter the details for your Key Store provider:

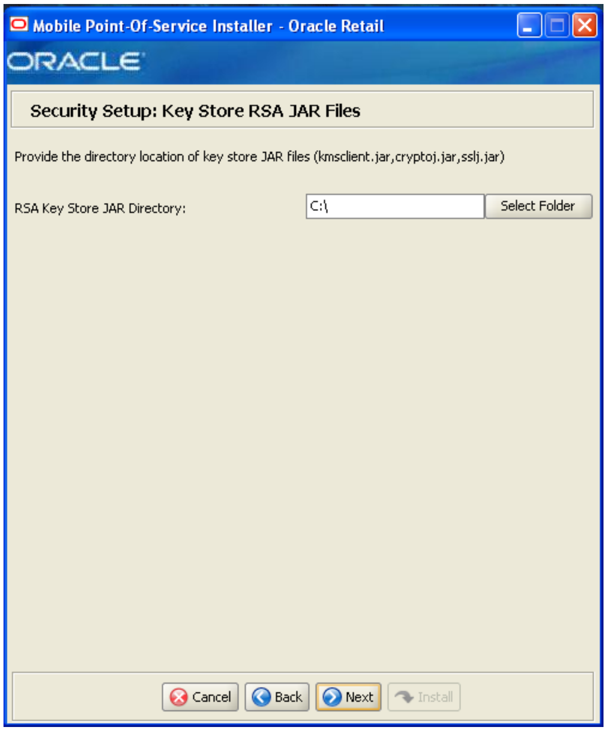
Key Store Implementation Class: ɔre.rsainterface.RSAKeyStoreEncryptionService

This screen is only displayed if **RSA Key Manager v3.1** is selected for the Key Store provider on the Security Setup: Key Store screen.

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

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

Figure C–16 Security Setup: Key Store RSA JAR Files for RSA Key Manager 3.1



Security Setup: Key Store RSA JAR Files

Provide the directory location of key store JAR files (kmsclient.jar,cryptoj.jar,sslj.jar)

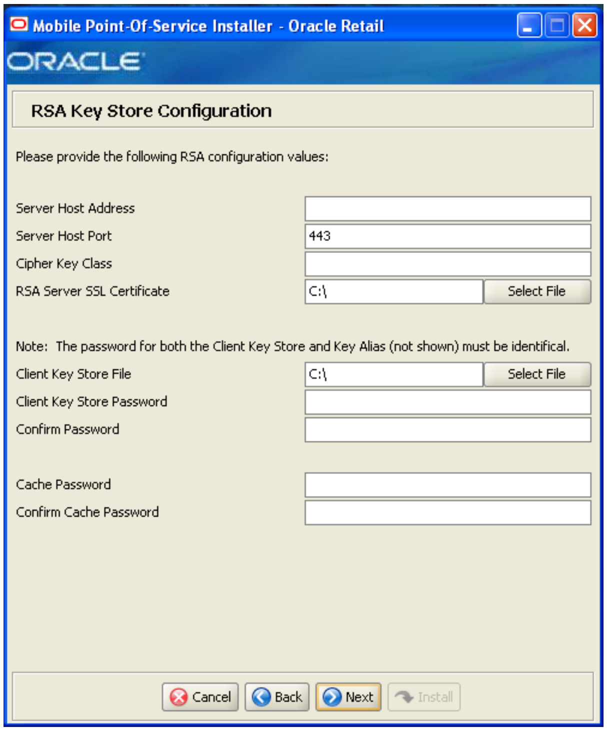
RSA Key Store JAR Directory: C:\

This screen is only displayed if **RSA Key Manager v3.1** is selected for the Key Store provider on the Security Setup: Key Store screen.

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

Details	Content
Field Title	RSA Key Store JAR Directory
Field Description	Choose the directory where the following Key Store jar files are located: ■ `kmsclient.jar` ■ `cryptoj.jar` ■ `sslj.jar`

Figure C–17   RSA Key Store Configuration for RSA Key Manager 3.1



Mobile Point-Of-Service Installer - Oracle Retail

RSA Key Store Configuration

Please provide the following RSA configuration values:

Server Host Address	
Server Host Port	443
Cipher Key Class	
RSA Server SSL Certificate	C:\

Note: The password for both the Client Key Store and Key Alias (not shown) must be identifical.

Client Key Store File	C:\
Client Key Store Password	
Confirm Password	
Cache Password	
Confirm Cache Password	

This screen is only displayed if **RSA Key Manager v3.1** is selected for the Key Store provider on the Security Setup: Key Store screen.

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

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

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

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

Details	Content
Field Title	RSA Server SSL Certificate
Field Description	Select the location of the RSA Key Manager server SSL certificate.

Details	Content
Field Title	RSA Server SSL Certificate
Field Description	Select the location of the RSA Key Manager server SSL certificate. **Note:** You should verify that the SSL certificate at this location is valid.

Details	Content
Field Title	Client Key Store File
Field Description	Enter the path to the client key store file.

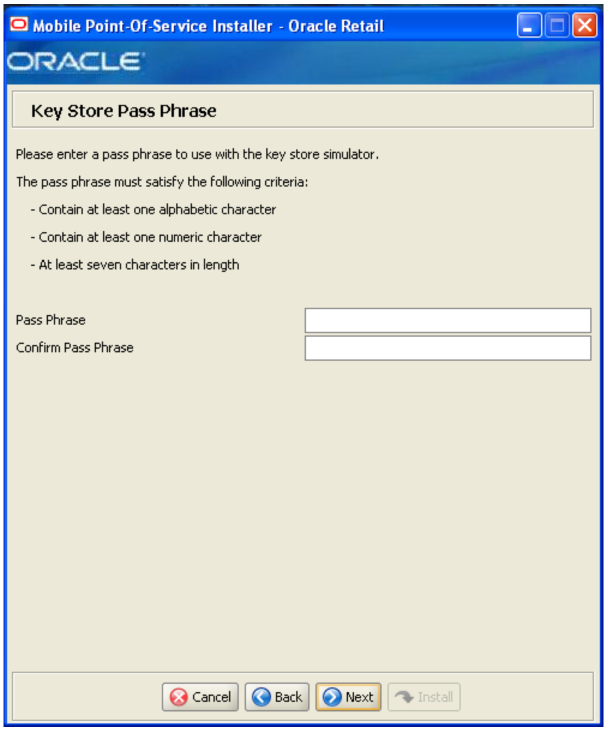
Details	Content
Field Title	Client Key Store Password
Field Description	Enter the password used to access the client key store file.

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

Details	Content
Field Title	Cache Password
Field Description	Enter the password used to access the RSA Key Manager cache. **Note:** You should verify that the SSL certificate at this location is valid.

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

Figure C–18 Key Store Pass Phrase for Simulator Key Manager



Key Store Pass Phrase

Please enter a pass phrase to use with the key store simulator.

The pass phrase must satisfy the following criteria:

- Contain at least one alphabetic character
- Contain at least one numeric character
- At least seven characters in length

Pass Phrase

Confirm Pass Phrase

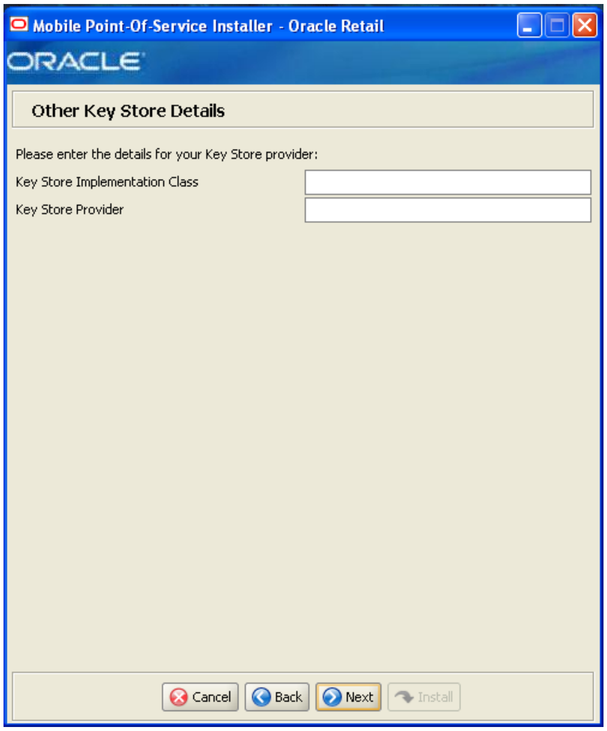
This screen is only displayed if **Simulator** is selected for the Key Store provider on the Security Setup: Key Store screen.

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

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 C–19 Key Store Details for Other Key Manager



Please enter the details for your Key Store provider:

Key Store Implementation Class

Key Store Provider

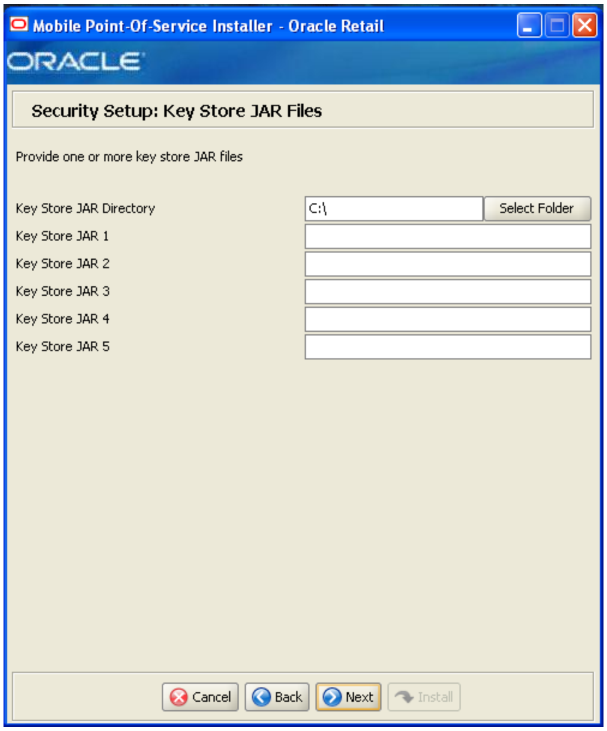
This screen is only displayed if **Other** is selected for the Key Store provider on the Security Setup: Key Store screen.

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

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

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

Figure C–20 Security Setup: Key Store JAR Files for Other Key Manager



Mobile Point-Of-Service Installer - Oracle Retail

Security Setup: Key Store JAR Files

Provide one or more key store JAR files

Key Store JAR Directory: C:\

Key Store JAR 1:

Key Store JAR 2:

Key Store JAR 3:

Key Store JAR 4:

Key Store JAR 5:

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

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

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

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

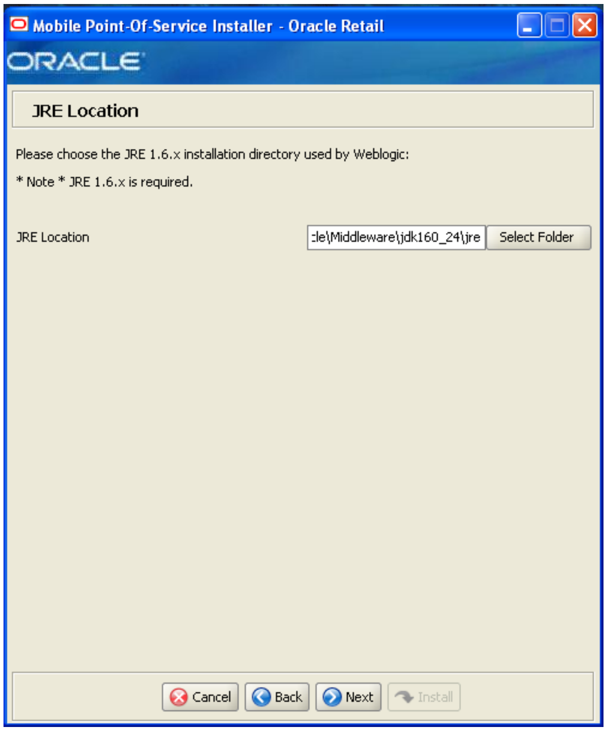
Details	Content
Field Title	Key Store JAR 2
Field Description	Enter the name of a Key Store jar file.

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

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

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

Figure C–21 JRE Location



JRE Location

Please choose the JRE 1.6.x installation directory used by Weblogic:

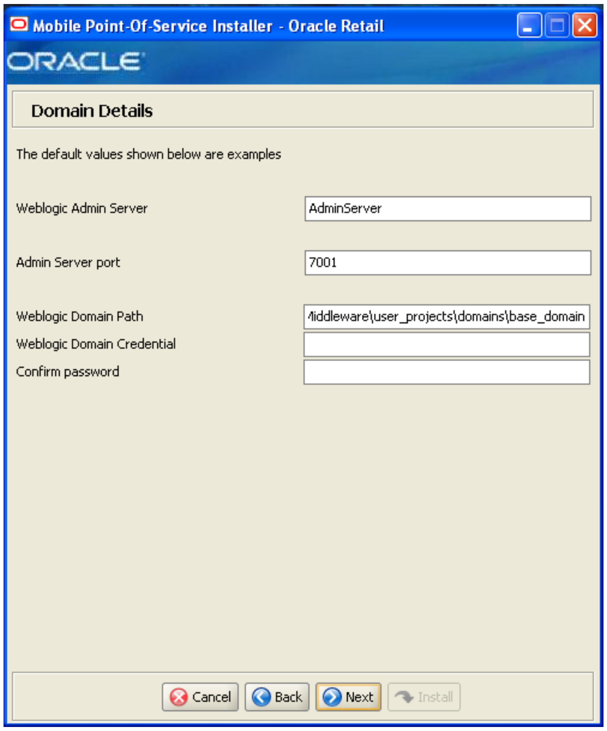
* Note * JRE 1.6.x is required.

JRE Location :le\Middleware\jdk160_24\jre

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	`C:\Oracle\Middleware\`jdk160_24\jre

Figure C–22 Domain Details



Mobile Point-Of-Service Installer - Oracle Retail

Domain Details

The default values shown below are examples

Weblogic Admin Server: AdminServer

Admin Server port: 7001

Weblogic Domain Path: /iddleware\user_projects\domains\base_domain

Weblogic Domain Credential:

Confirm password:

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

Details	Content
Field Title	Weblogic Admin Server
Field Description	Name of the admin server to which the Mobile Point-of-Service application is being deployed.
Example	AdminServer

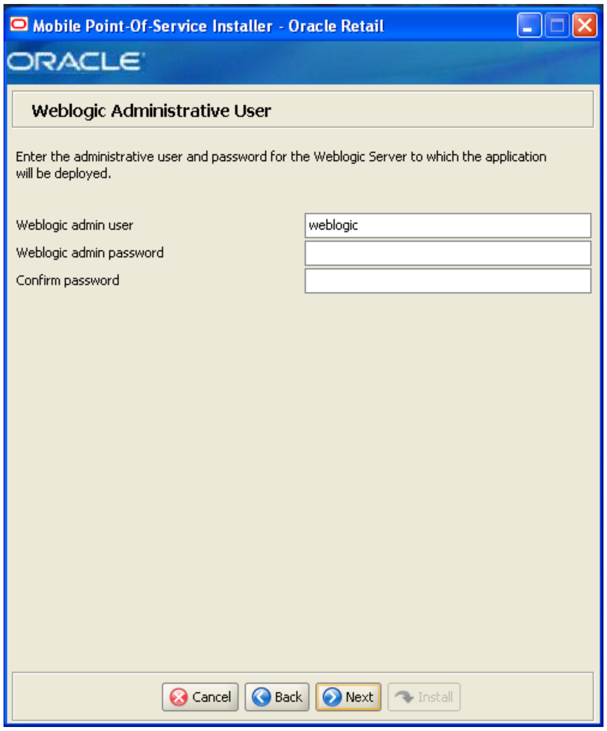
Details	Content
Field Title	Admin Server port
Field Description	Port used by the administration server. This port was selected when the administration domain was created.
Example	7001

Details	Content
Field Title	Weblogic Domain Path
Field Description	Path to the domain to which the Mobile Point-of-Service application is being deployed.
Example	`C:\Oracle\Middleware\user_projects\domains\base_domain`

Details	Content
Field Title	Weblogic Domain Credential
Field Description	Password shared between domains in order to establish a trust relationship. **Note:** Use the same password for all Oracle Retail applications in the trust relationship in your configuration.

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

Figure C–23 Weblogic Administrative User



Weblogic Administrative User

Enter the administrative user and password for the Weblogic Server to which the application will be deployed.

Weblogic admin user: weblogic

Weblogic admin password:

Confirm password:

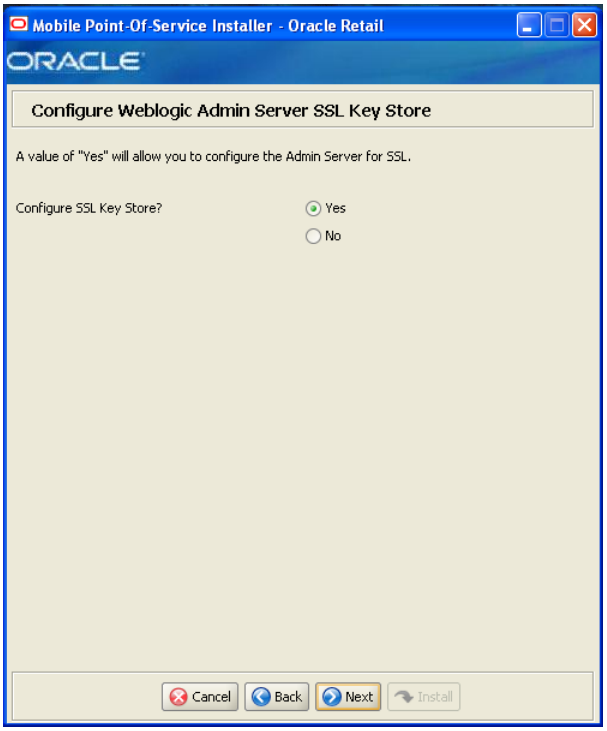
The fields on this screen are described in the following tables.

Details	Content
Field Title	Weblogic admin user
Field Description	User name of the administrative user for the WebLogic Server to which the Mobile Point-of-Service application is being deployed.
Example	weblogic

Details	Content
Field Title	Weblogic admin password
Field Description	Password for the WebLogic Server administrative user. You chose this password when you installed the WebLogic Server.

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

Figure C–24 Configure Weblogic Admin Server SSL Key Store



Configure Weblogic Admin Server SSL Key Store

A value of "Yes" will allow you to configure the Admin Server for SSL.

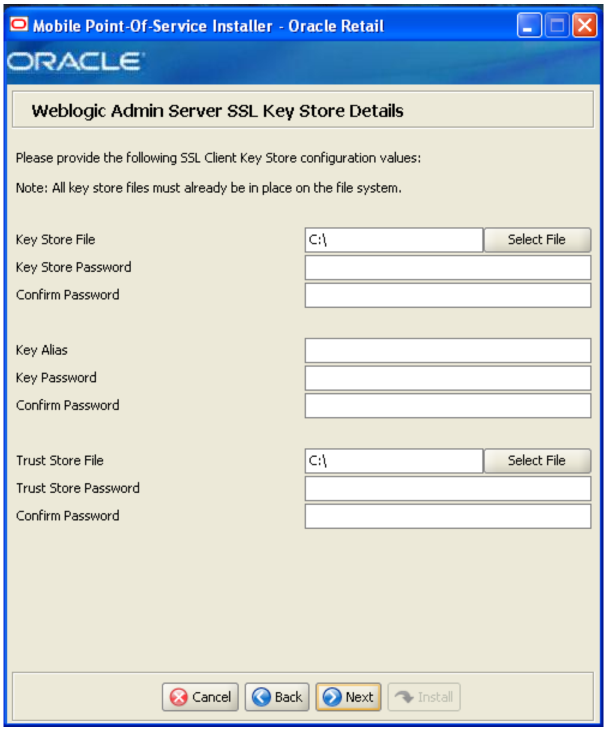
Configure SSL Key Store? ● Yes ○ No

This screen is only displayed if **Deploy to Admin Server** is selected on the Weblogic Deploy Server Type screen.

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

Details	Content
Field Title	Configure SSL Key Store?
Field Description	Select whether the Admin Server will be configured for SSL: ■ To configure the Admin Server for SSL, select **Yes**. ■ To not configure the Admin Server for SSL, select **No**.

Figure C–25 Weblogic Admin Server SSL Key Store Details



Mobile Point-Of-Service Installer - Oracle Retail

Weblogic Admin Server SSL Key Store Details

Please provide the following SSL Client Key Store configuration values:

Note: All key store files must already be in place on the file system.

Key Store File	C:\
Key Store Password	
Confirm Password	
Key Alias	
Key Password	
Confirm Password	
Trust Store File	C:\
Trust Store Password	
Confirm Password	

This screen is only displayed if **Yes** is selected on the Configure Weblogic Admin Server SSL Key Store screen.

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

Details	Content
Field Title	Key Store File
Field Description	Path to the Key Store file.

Details	Content
Field Title	Key Store Password
Field Description	Enter the password used to access the client Key Store.

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

Details	Content
Field Title	Key Alias
Field Description	Alias used to access the Key Store file.

Details	Content
Field Title	Key Password
Field Description	Enter the password used to access the client Key Store.

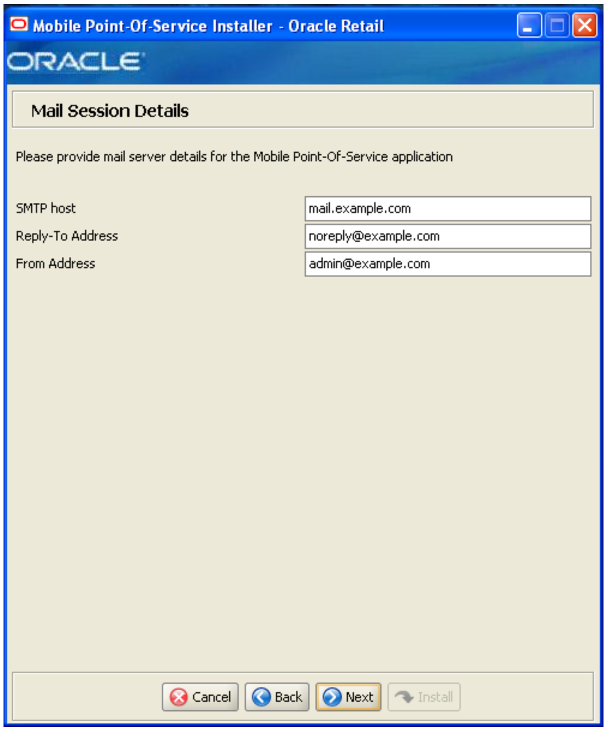
Details	Content
Field Title	Confirm Password
Field Description	Reentered Key Password used to confirm the password. **Note:** The passwords in the Key Password and Confirm Password fields must match.

Details	Content
Field Title	Trust Store File
Field Description	Path to the Trust Store file.

Details	Content
Field Title	Trust Store Password
Field Description	Enter the password used to access the Trust Store.

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

Figure C–26 Mail Session Details



Mail Session Details

Please provide mail server details for the Mobile Point-Of-Service application

SMTP host: mail.example.com

Reply-To Address: noreply@example.com

From Address: admin@example.com

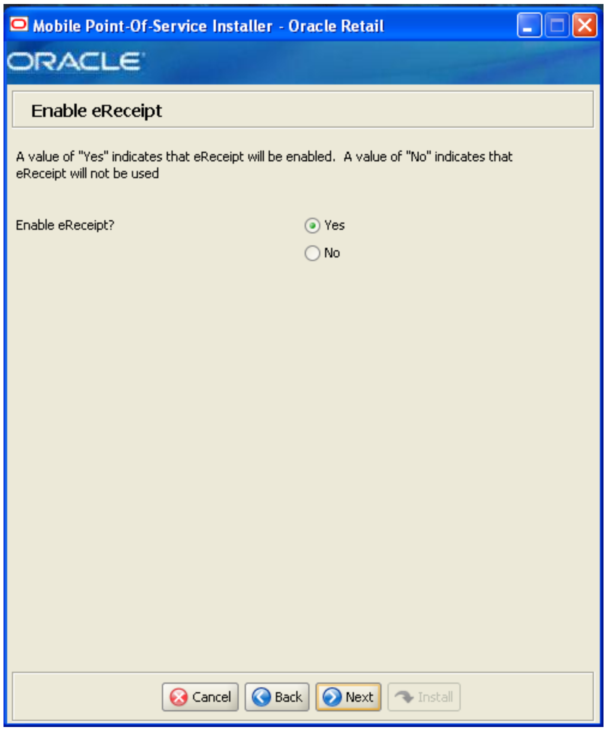
The fields on this screen are described in the following tables.

Details	Content
Field Title	SMTP host
Field Description	Host where the SMTP server is running.
Example	mail.example.com

Details	Content
Field Title	Reply-To Address
Field Description	Reply-to address in e-mails generated by Mobile Point-of-Service.
Example	noreply@example.com

Details	Content
Field Title	From Address
Field Description	From address in e-mails generated by Mobile Point-of-Service.
Example	admin@example.com

Figure C–27 Enable eReceipt



Enable eReceipt

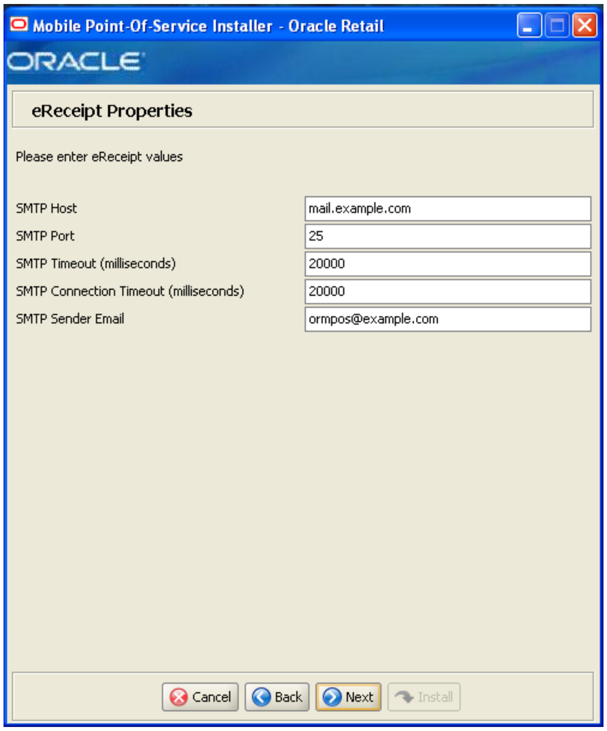
A value of "Yes" indicates that eReceipt will be enabled. A value of "No" indicates that eReceipt will not be used

Enable eReceipt? ● Yes ○ No

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 C–28 eReceipt Properties



eReceipt Properties

Please enter eReceipt values

SMTP Host: mail.example.com
SMTP Port: 25
SMTP Timeout (milliseconds): 20000
SMTP Connection Timeout (milliseconds): 20000
SMTP Sender Email: ormpos@example.com

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.
Example	mail.example.com

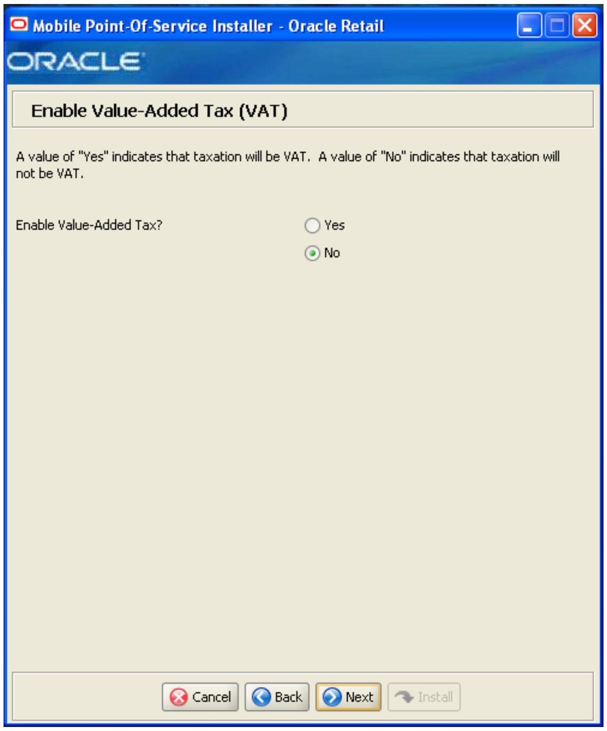
Details	Content
Field Title	SMTP Port
Field Description	Enter the port number for the SMTP server.
Example	25

Details	Content
Field Title	SMTP Timeout (milliseconds)
Field Description	Enter the amount of time to wait for the SMTP server.
Example	20000

Details	Content
Field Title	SMTP Connection Timeout (milliseconds)
Field Description	Enter the amount of time to wait for the connection to the SMTP server.
Example	20000

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 Mobile Point-of-Service.
Example	ormpos@example.com

Figure C–29 Value-Added Tax (VAT)



Enable Value-Added Tax (VAT)

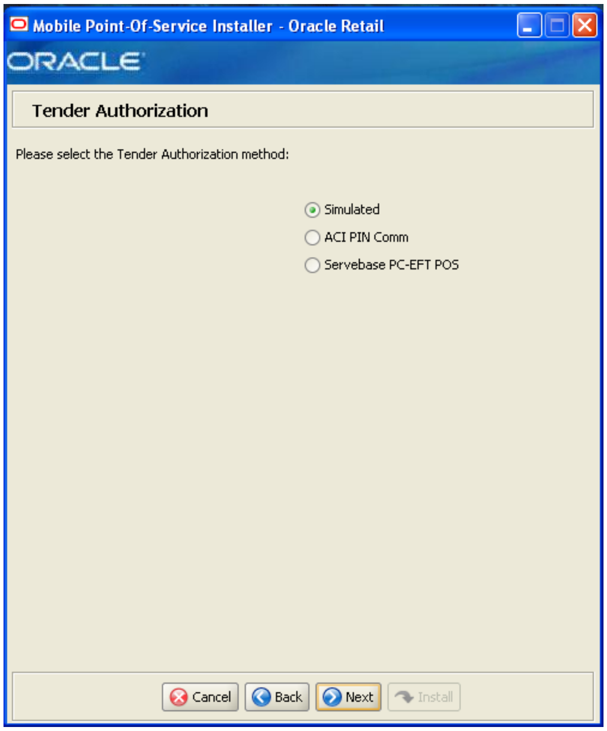
A value of "Yes" indicates that taxation will be VAT. A value of "No" indicates that taxation will not be VAT.

Enable Value-Added Tax? ○ Yes ● No

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 C–30 Tender Authorization



Tender Authorization

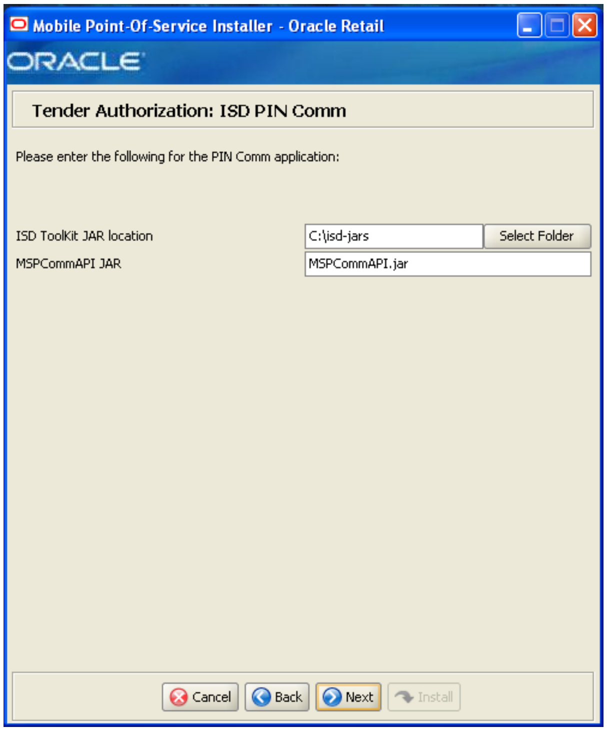
Please select the Tender Authorization method:

● Simulated
○ ACI PIN Comm
○ Servebase PC-EFT POS

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 C–31 Tender Authorization: ISD PIN Comm



Mobile Point-Of-Service Installer - Oracle Retail

Tender Authorization: ISD PIN Comm

Please enter the following for the PIN Comm application:

ISD ToolKit JAR location: C:\isd-jars

MSPCommAPI JAR: MSPCommAPI.jar

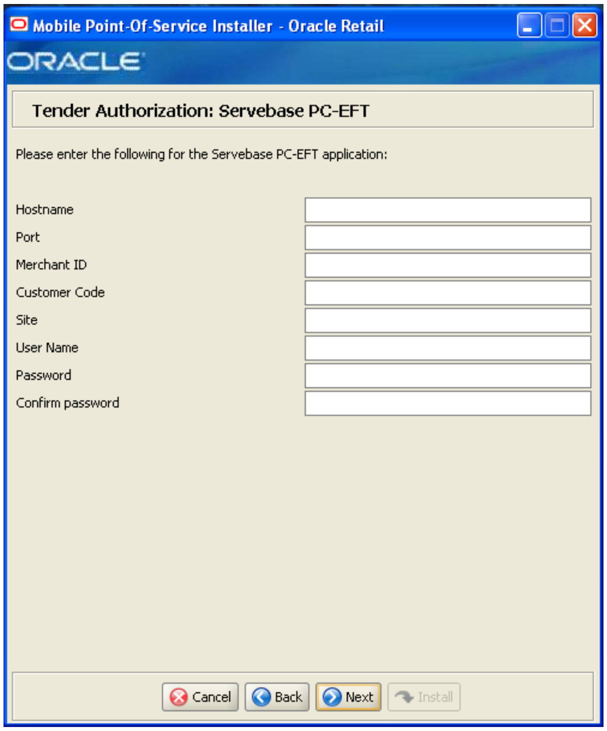
This screen is only displayed if **ACI PIN Comm** is selected for the Tender Authorization.

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	`C:\isd-jars`

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

Figure C–32 Tender Authorization: Servebase PC-EFT



Tender Authorization: Servebase PC-EFT

Please enter the following for the Servebase PC-EFT application:

Hostname
Port
Merchant ID
Customer Code
Site
User Name
Password
Confirm password

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 Servebase server.

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

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

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

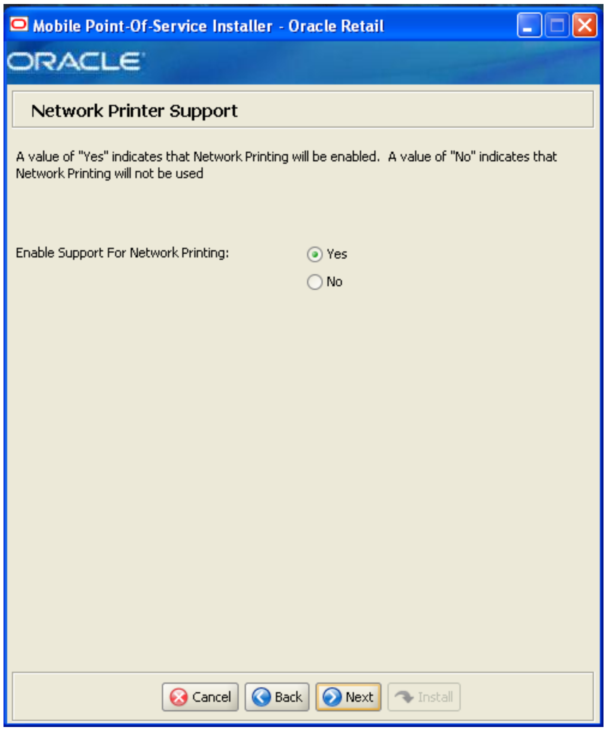
Details	Content
Field Title	Site
Field Description	Enter the site to access the Servebase application.

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

Details	Content
Field Title	Password
Field Description	Enter the password to use to access the Servebase 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 C–33 Network Printer Support



Network Printer Support

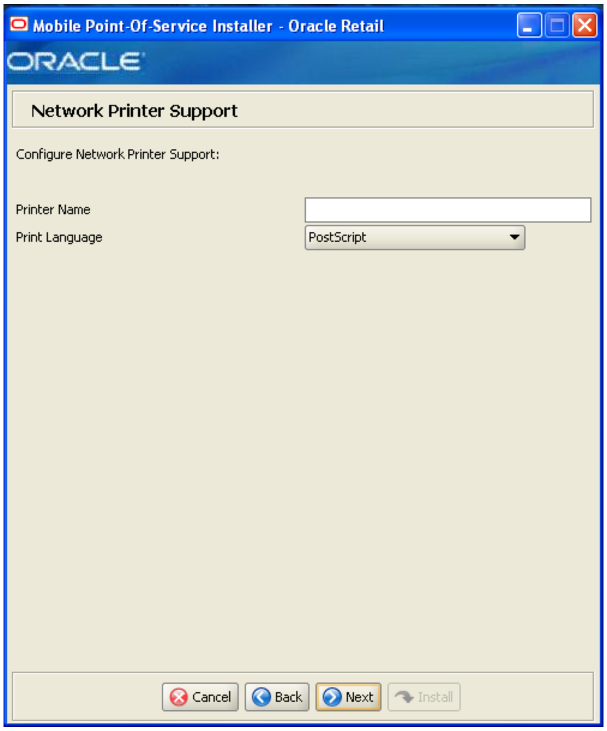
A value of "Yes" indicates that Network Printing will be enabled. A value of "No" indicates that Network Printing will not be used

Enable Support For Network Printing: ● Yes ○ No

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

Details	Content
Field Title	Enable Support for Network Printing?
Field Description	Choose whether the use of network printing is enabled.
Example	Yes

Figure C–34 Network Printer Support Configuration



Network Printer Support

Configure Network Printer Support:

Printer Name

Print Language: PostScript

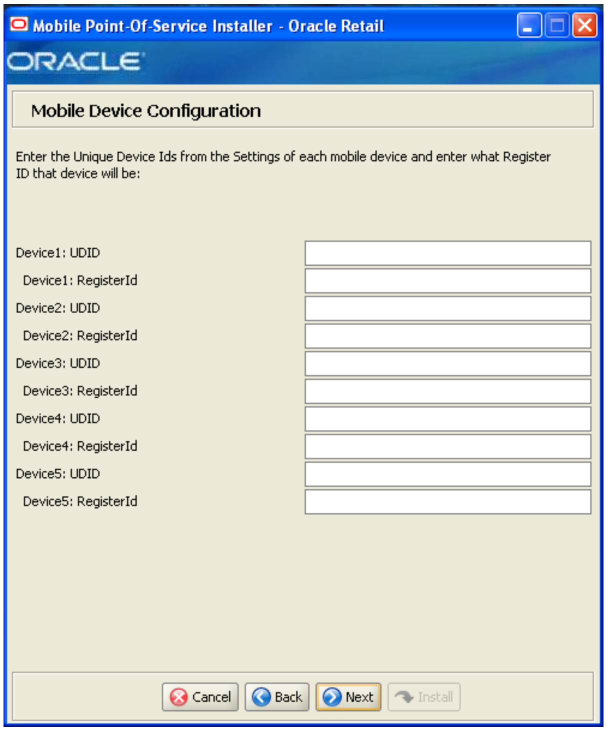
This screen is only displayed if **Yes** is selected on the Network Printer Support screen.

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

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.

Figure C–35 Mobile Device Configuration



Mobile Device Configuration

Enter the Unique Device Ids from the Settings of each mobile device and enter what Register ID that device will be:

Device1: UDID

Device1: RegisterId

Device2: UDID

Device2: RegisterId

Device3: UDID

Device3: RegisterId

Device4: UDID

Device4: RegisterId

Device5: UDID

Device5: RegisterId

If you need to find the UDID for a mobile device:

1. Attach the mobile device to a computer that has Apple iTunes installed.
2. Select the mobile device in the leftmost column.
3. Select the **Summary** tab at the top of the main screen.
4. Click the serial number label or text.
5. Once the serial number has switched to show the UDID, copy and paste the number to the right. The field does not need to be selected for copying; clicking the serial number enables the use of the copy keyboard shortcut.

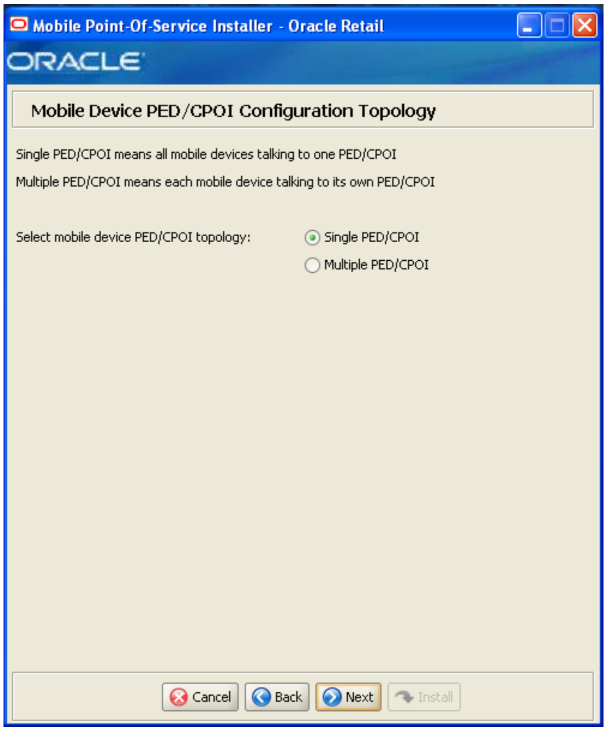
For information on adding more mobile devices, see the *Oracle Retail POS Suite Implementation Guide, Volume 5 - Mobile Point-of-Service*.

The fields on this screen are described in the following tables. Enter the following information for each mobile device.

Details	Content
Field Title	UDID
Field Description	Enter the unique hardware ID associated with a mobile device configured to work with the Mobile Point-of-Service server.

Details	Content
Field Title	RegisterId
Field Description	Enter the register ID to associate with the given hardware ID. **Note:** 1 to 255 is supported for the register number. Do not install more than one device with the same register number at a store.

Figure C–36 Mobile Device PED/CPOI Configuration Topology



Mobile Device PED/CPOI Configuration Topology

Single PED/CPOI means all mobile devices talking to one PED/CPOI

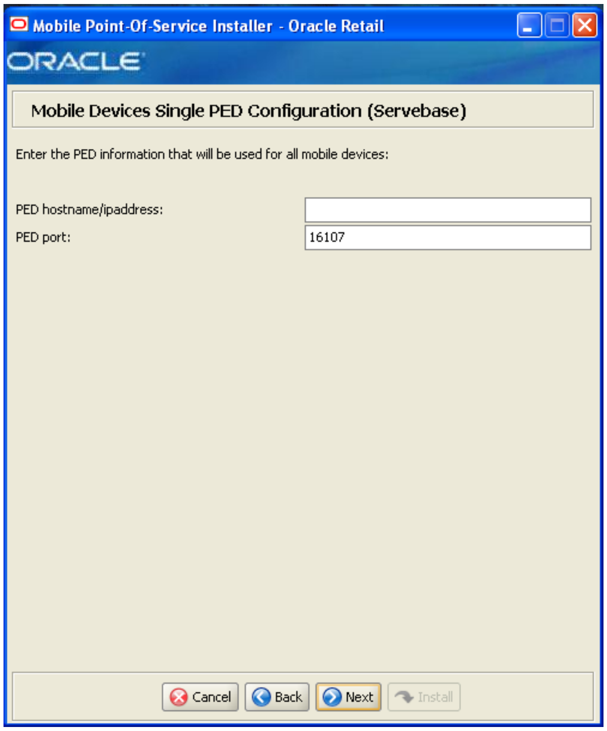
Multiple PED/CPOI means each mobile device talking to its own PED/CPOI

Select mobile device PED/CPOI topology: ● Single PED/CPOI ○ Multiple PED/CPOI

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

Details	Content
Field Title	Select mobile device PED/CPOI topology
Field Description	Select how the mobile devices will talk to a PED/CPOI: ■ To have a single PED/CPOI configured for all mobile devices, select **Single PED/CPOI**. ■ To have each mobile device configured for a separate PED/CPOI, select **Multiple PED/CPOI**.
Example	Single PED/CPOI

Figure C–37 Mobile Devices Single PED Configuration (Servebase)



Mobile Devices Single PED Configuration (Servebase)

Enter the PED information that will be used for all mobile devices:

PED hostname/ipaddress:

PED port: 16107

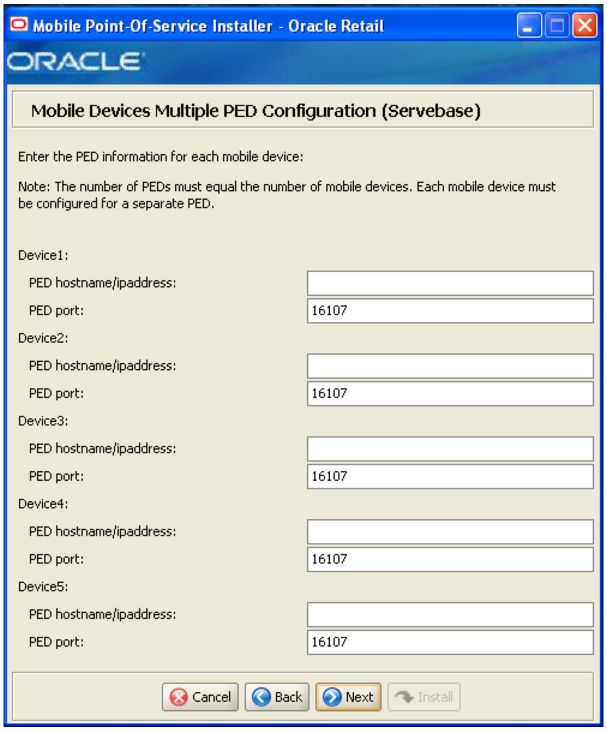
This screen is only displayed if **Servebase PC-EFT POS** is selected on the Tender Authorization screen and **Single PED/CPOI** is selected on the Mobile Device PED/CPOI Configuration Topology screen.

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

Details	Content
Field Title	PED hostname/ipaddress
Field Description	Enter the host name or IP address of the PED.

Details	Content
Field Title	PED port
Field Description	Enter the port number that the PED is listening on.
Example	16107

Figure C–38 Mobile Devices Multiple PED Configuration (Servebase)



Mobile Devices Multiple PED Configuration (Servebase)

Enter the PED information for each mobile device:

Note: The number of PEDs must equal the number of mobile devices. Each mobile device must be configured for a separate PED.

Device1:
PED hostname/ipaddress:
PED port: 16107

Device2:
PED hostname/ipaddress:
PED port: 16107

Device3:
PED hostname/ipaddress:
PED port: 16107

Device4:
PED hostname/ipaddress:
PED port: 16107

Device5:
PED hostname/ipaddress:
PED port: 16107

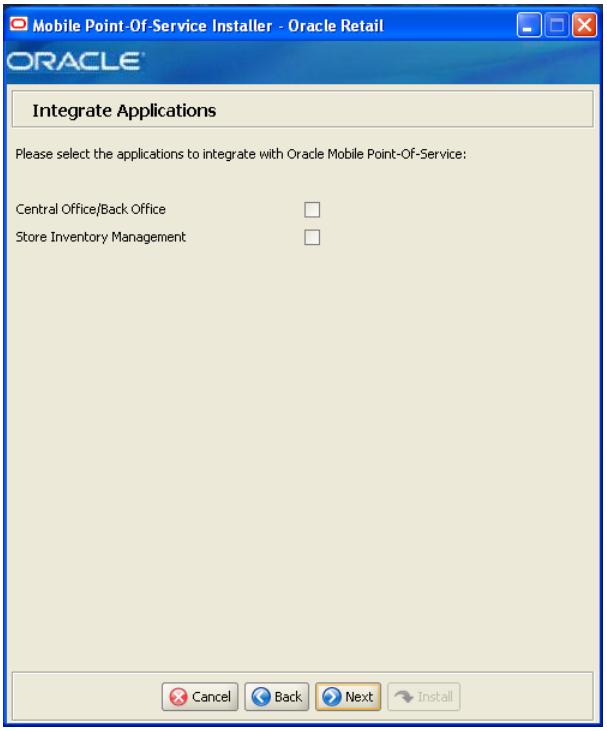
This screen is only displayed if **Servebase PC-EFT POS** is selected on the Tender Authorization screen and **Multiple PED/CPOI** is selected on the Mobile Device PED/CPOI Configuration Topology screen.

The fields on this screen are described in the following tables. Enter the following information for each mobile device.

Details	Content
Field Title	PED hostname/ipaddress
Field Description	Enter the host name or IP address of the PED.

Details	Content
Field Title	PED port
Field Description	Enter the port number that the PED is listening on.
Example	16107

Figure C–39 Integrate Applications



Integrate Applications

Please select the applications to integrate with Oracle Mobile Point-Of-Service:

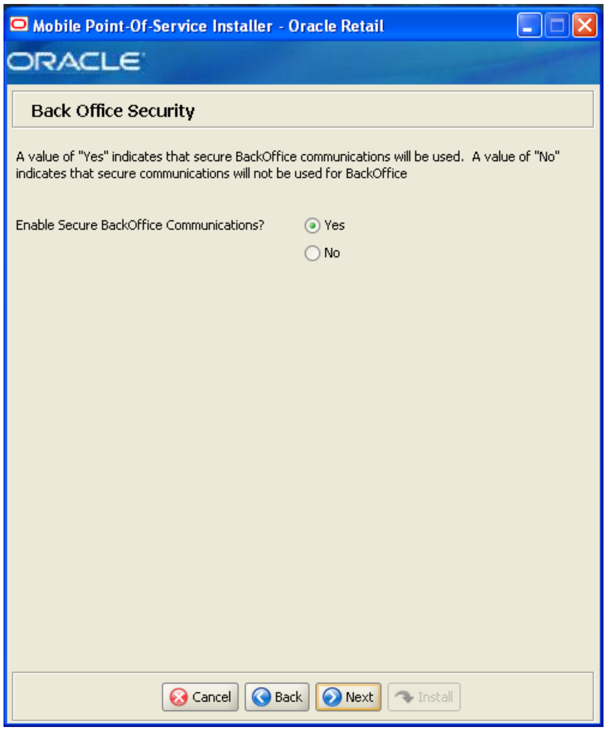
Central Office/Back Office □

Store Inventory Management □

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

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

Figure C–40 Back Office Security



Back Office Security

A value of "Yes" indicates that secure BackOffice communications will be used. A value of "No" indicates that secure communications will not be used for BackOffice

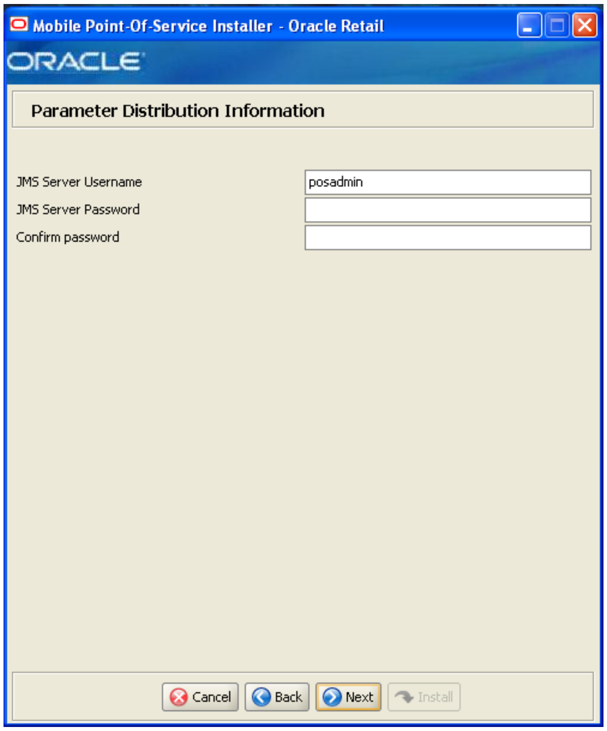
Enable Secure BackOffice Communications? ● Yes ○ No

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

Figure C–41 Parameter Distribution Information



Parameter Distribution Information

JMS Server Username: posadmin

JMS Server Password:

Confirm password:

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

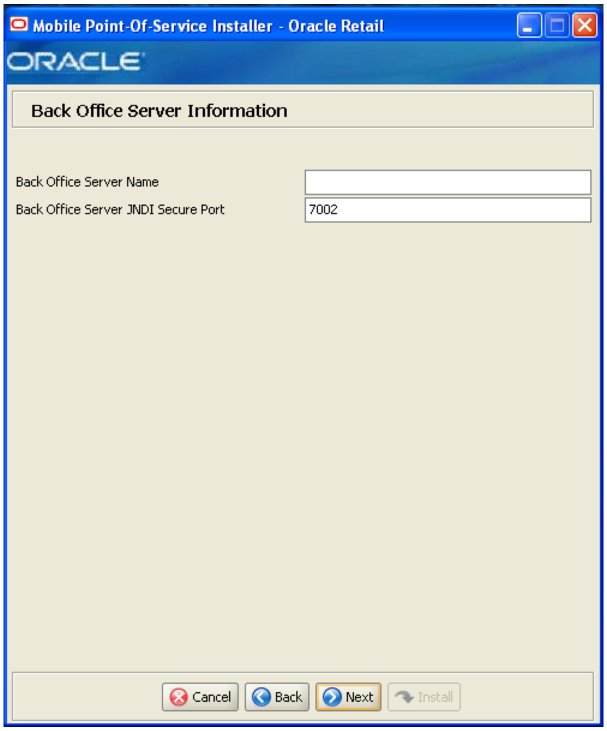
The fields on this screen are described in the following tables.

Details	Content
Field Title	JMS Server Username
Field Description	Identifier of the JMS server user for receiving parameter updates.
Example	posadmin

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

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

Figure C–42 Back Office Server Information



Mobile Point-Of-Service Installer - Oracle Retail

Back Office Server Information

Back Office Server Name:

Back Office Server JNDI Secure Port: 7002

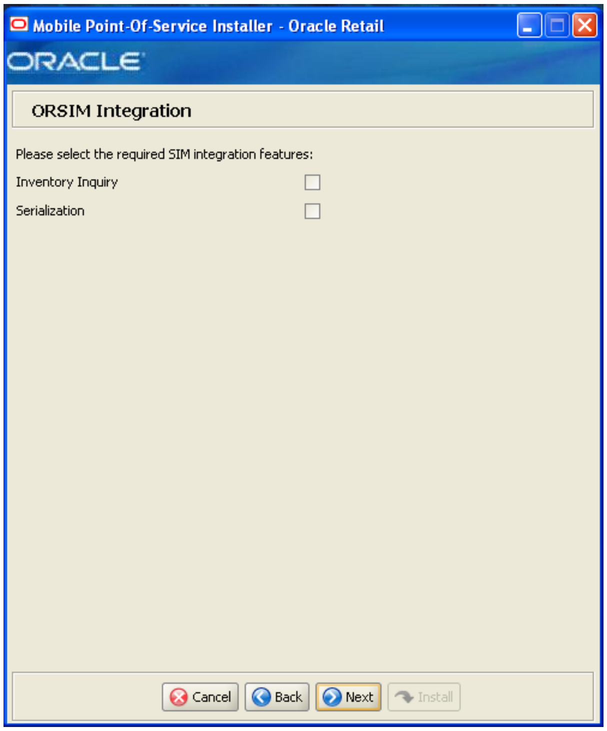
This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

Details	Content
Field Title	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	7002

Figure C–43 ORSIM Integration



Mobile Point-Of-Service Installer - Oracle Retail

ORSIM Integration

Please select the required SIM integration features:

Inventory Inquiry □

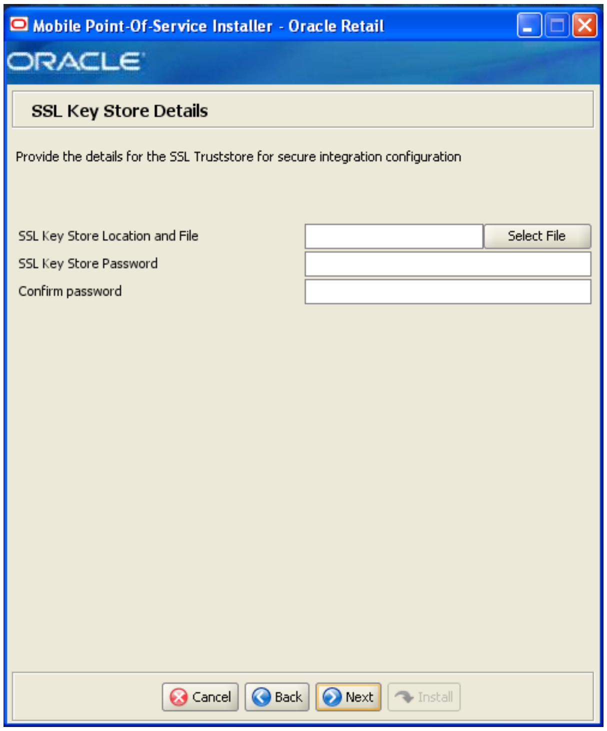
Serialization □

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 Mobile Point-of-Service: ■ To inquire about inventory using SIM, select **Inventory Inquiry**. ■ To enable serialization using SIM, select **Serialization**.

Figure C–44 SSL Key Store Details



SSL Key Store Details

Provide the details for the SSL Truststore for secure integration configuration

SSL Key Store Location and File

SSL Key Store Password

Confirm password

This screen is only displayed if **RSA Key Manager v3.1** is selected for the Key Store provider on the Security Setup: Key Store screen.

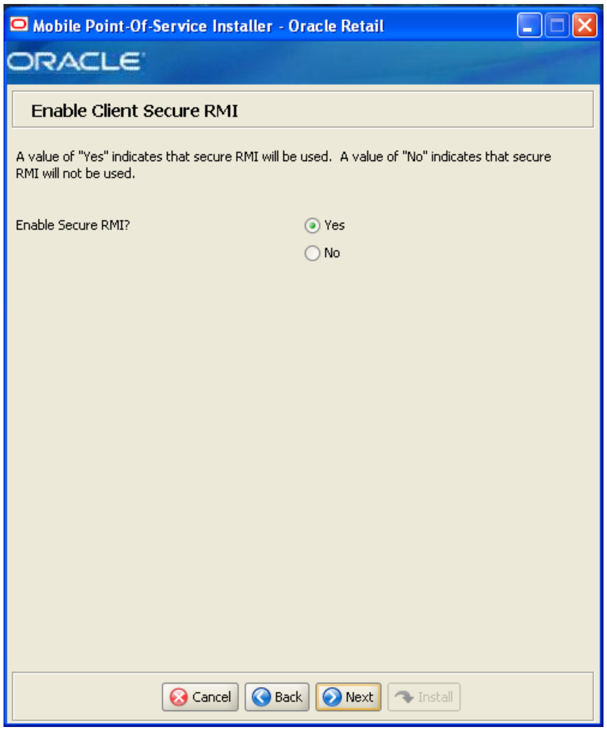
The fields on this screen are described in the following tables.

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

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 C–45 Enable Client Secure RMI



Enable Client Secure RMI

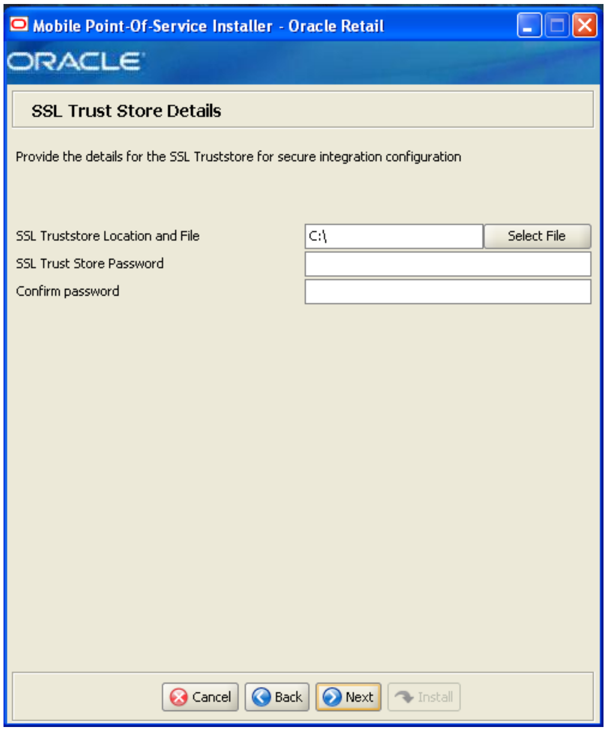
A value of "Yes" indicates that secure RMI will be used. A value of "No" indicates that secure RMI will not be used.

Enable Secure RMI? ● Yes ○ No

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

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

Figure C–46 SSL Trust Store Details



SSL Trust Store Details

Provide the details for the SSL Truststore for secure integration configuration

SSL Truststore Location and File: C:\

SSL Trust Store Password:

Confirm password:

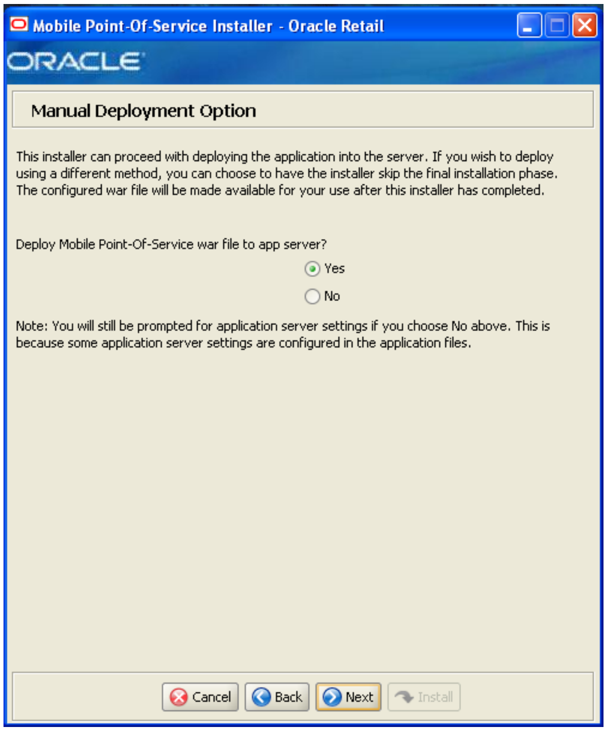
The fields on this screen are described in the following tables.

Details	Content
Field Title	SSL Truststore Location and File
Field Description	Enter the location and name of the truststore file.

Details	Content
Field Title	SSL Trust Store Password
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 C–47 Manual Deployment Option



Manual Deployment Option

This installer can proceed with deploying the application into the server. If you wish to deploy using a different method, you can choose to have the installer skip the final installation phase. The configured war file will be made available for your use after this installer has completed.

Deploy Mobile Point-Of-Service war file to app server?

● Yes

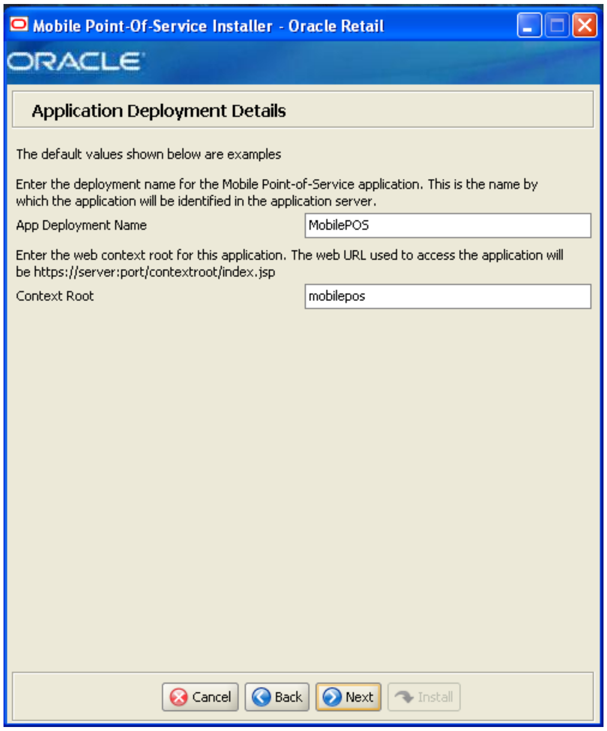
○ No

Note: You will still be prompted for application server settings if you choose No above. This is because some application server settings are configured in the application files.

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

Details	Content
Field Title	Deploy Mobile Point-of-Service war file to app server?
Field Description	By default, the installer will deploy the war file and copy files under the application server home directory. This screen gives you the option to leave the home directory unmodified and configure the application in the staging area for use in a manual installation at a later time. This option can be used in situations where modifications to files under the home directory must be reviewed by another party before being applied. If you choose No, see "Manual Deployment of the Mobile Point-of-Service Server Application" in Chapter 4 for the manual steps you need to perform after the installer completes.
Example	Yes

Figure C–48 Application Deployment Details



Application Deployment Details

The default values shown below are examples

Enter the deployment name for the Mobile Point-of-Service application. This is the name by which the application will be identified in the application server.

App Deployment Name: MobilePOS

Enter the web context root for this application. The web URL used to access the application will be https://server:port/contextroot/index.jsp

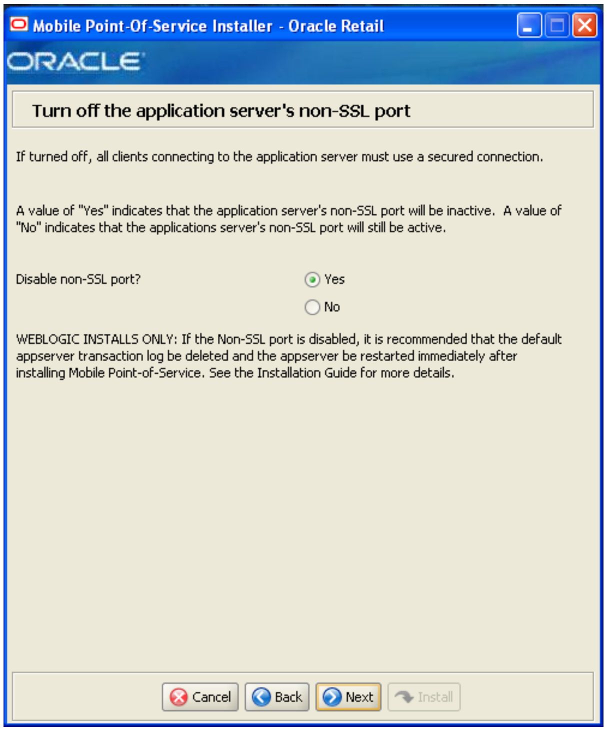
Context Root: mobilepos

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

Details	Content
Field Title	App Deployment Name
Field Description	Name by which the Mobile Point-of-Service application will be identified in the application server.
Example	MobilePOS

Details	Content
Field Title	Context Root
Field Description	Path under the HTTPS URL that will be used to access the Mobile Point-of-Service application. For example, a context root of mobilepos will result in the application being accessed at `https://host:port/mobilepos/index.jsp`.
Example	mobilepos

Figure C–49 Turn Off the Application Server's Non-SSL Port



Turn off the application server's non-SSL port

If turned off, all clients connecting to the application server must use a secured connection.

A value of "Yes" indicates that the application server's non-SSL port will be inactive. A value of "No" indicates that the applications server's non-SSL port will still be active.

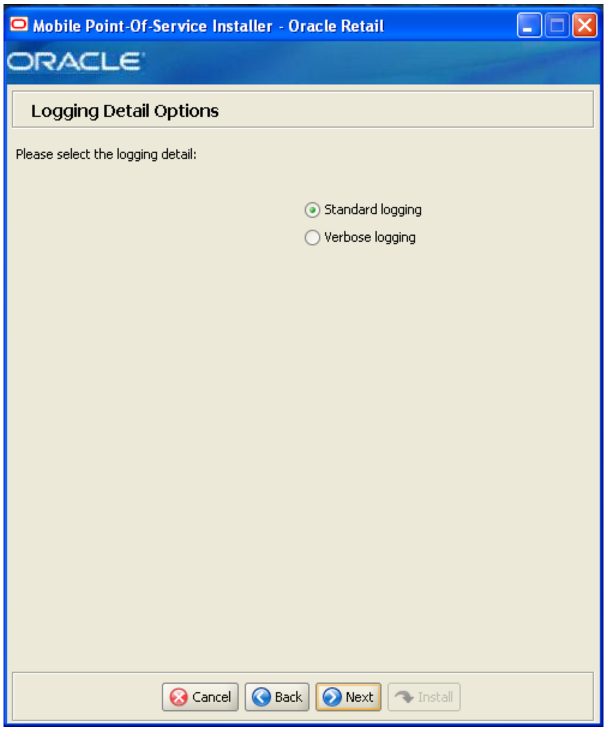
Disable non-SSL port? ● Yes ○ No

WEBLOGIC INSTALLS ONLY: If the Non-SSL port is disabled, it is recommended that the default appserver transaction log be deleted and the appserver be restarted immediately after installing Mobile Point-of-Service. See the Installation Guide for more details.

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

Details	Content
Field Title	Disable non-SSL port?
Field Description	Sets whether connecting to the application server requires a secured connection. **Note:** It is recommended that you disable the non-SSL port in order to increase the security of your environment. ■ To disable the use of a non-SSL port, choose **Yes**. ■ To enable using a non-SSL port, choose **No**. If you select **Yes**, see "Disabled Non-SSL Port" in Chapter 4.
Example	Yes

Figure C–50 Logging Detail Options



Logging Detail Options

Please select the logging detail:

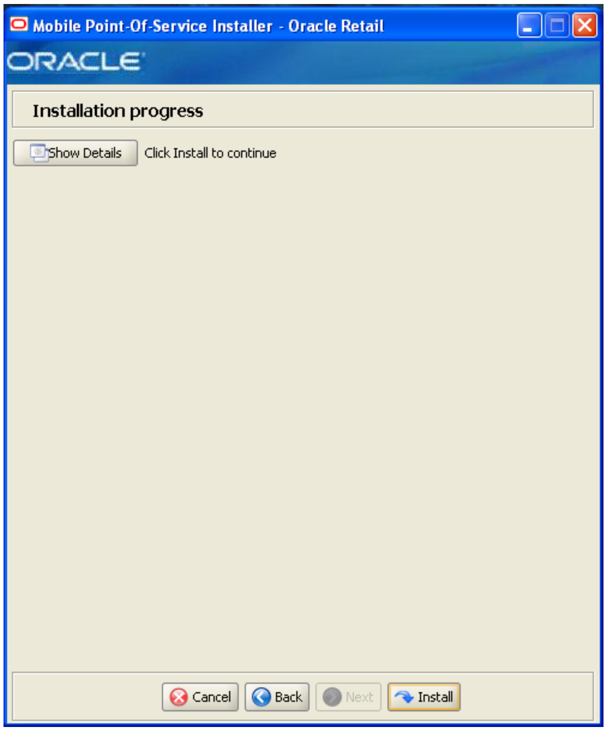
● Standard logging

○ Verbose logging

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 logging. ■ To only log some of the messages, choose **Standard Logging**. ■ To log all of the messages, choose **Verbose Logging**.
Example	Standard logging

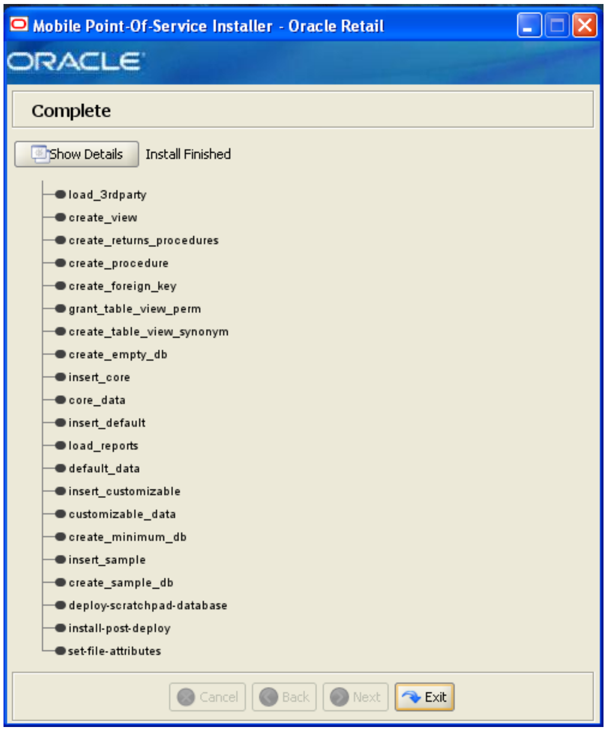
Figure C–51 Installation Progress



Installation progress

Click Install to continue

Figure C–52 Install Complete



Complete

Install Finished

```
load_3rdparty
create_view
create_returns_procedures
create_procedure
create_foreign_key
grant_table_view_perm
create_table_view_synonym
create_empty_db
insert_core
core_data
insert_default
load_reports
default_data
insert_customizable
customizable_data
create_minimum_db
insert_sample
create_sample_db
deploy-scratchpad-database
install-post-deploy
set-file-attributes
```

D

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>*.
   - For the silent install of the Mobile Point-of-Service server, the `cwallet.sso` file is found in the installation directory for the previous install. Copy the `cwallet.sso` file to *<INSTALL_DIR>* for this silent install.
3. If this is a client install and you are using a fingerprint device, make sure the following properties in the `ant.install.properties` file are correct:

```
## Properties from Page:fingerPrintDevice
input.client.device.dpfingerprint = true
## Properties from Page:DPEnvironmentClasspath
input.dpfingerprint.dpjavapos = C:\\DigitalPersona\\Bin\\JavaPOS\\dpjavapos.jar
input.dpfingerprint.jpos = C:\\DigitalPersona\\Bin\\JavaPOS\\jpos111.jar
input.dpfingerprint.dpenrollment =
C:\\DigitalPersona\\Bin\\Java\\dpfpenrollment.jar
input.dpfingerprint.dpverification =
C:\\DigitalPersona\\Bin\\Java\\dpfpverification.jar
input.dpfingerprint.dpotjni = C:\\DigitalPersona\\Bin\\Java\\dpotjni.jar
```

4. Run the installer again with the silent argument:

   ```
   install.cmd silent
   ```

5. If this is a client install and you are using a fingerprint device, verify the following:

   - The fingerprint device properties from Step 3 are correct in the following file:

     ```
     <POS_install_
     directory>\<client>\pos\config\technician\PosDeviceTechnician.xml
     ```

   - The fingerprint device is enabled in the `jpos.xml` file.

E

Appendix: URL Reference

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

JDBC URL for an Oracle 11g Database

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

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

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

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

URL for the Siebel Web Service

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

Syntax:

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

- Using a transport method of HTTP and Siebel authentication:

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

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

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

- Using a transport method of HTTPS and Siebel authentication:

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

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

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

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

JNDI Provider URL for an Application

Used for server-to-server calls between applications.

Syntax: `t3://`*`<host>:<port>`*

- *`<host>`*: host name selected when the WebLogic Server domain was created
- *`<port>`*: port number selected when the WebLogic Server domain was created

For example, `t3://adminserver:7001`

Deployer URI

Used by the Oracle Ant tasks to deploy an application to a WebLogic Server. The application installer does not ask the user for this value. It is constructed based on other inputs and written to the `ant.install.properties` file for input to the installation script. For repeat installations using silent mode, you may need to correct mistakes in the deployer URI.

Syntax: `input.deployer.uri = t3://`*`<host>:<port>`*

- *`<host>`*: host name selected when the WebLogic Server domain was created
- *`<port>`*: port number selected when the WebLogic Server domain was created

For example, `input.deployer.uri = t3://localhost:7003`

F

Appendix: Common Installation Errors

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

"Pos installer finished with errors"

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

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

Symptom:

The application fails when starting up:

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

Solution:

This error usually occurs because the JRE that you are pointing to does not contain the updated java.security 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:com.extendyourstore.foundation.manager.data.JdbcDataConnection):

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

Solution:

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

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

WebLogic Domain Does Not Exist

Symptom:

The application installer quits with the following error message:

```
BUILD FAILED
C:\tmp\j2ee\ormpos\staging\ORMPOS-trunk\build.xml:941: The following error
occurred while executing this line:
C:\tmp\j2ee\ormpos\staging\ORMPOS-trunk\build-common-wl.xml:83: startWebLogic.sh
 under C:/Oracle/Middleware/user_projects/domains/base_domain is missing.
 Installation cannot continue.
```

Solution:

This error occurs because the WebLogic Server domain provided does not exist.

Make sure that the domain exists, and then check the ant.install.properties file for entry mistakes. Pay close attention to the input.deployer.uri (see Appendix E), input.admin.user, and input.admin.password properties. If you need to make a correction, you can run the installer again with this file as input by running silent mode (see Appendix D).

WebLogic Domain Server is Not Started

Symptom:

The application installer quits with the following error message:

```
BUILD FAILED
C:\tmp\j2ee\ormpos\staging\ORMPOS-trunk\build.xml:1022: The following error
occurred while executing this line:
C:\tmp\j2ee\ormpos\staging\ORMPOS-trunk\build-common-wl.xml:152: url
http://localhost:
```

```
7001/console is not available. Installation cannot continue.
```

Solution:

This error occurs because the WebLogic domain server provided is not running.

Make sure that the WebLogic domain server is running, and then check the `ant.install.properties` file for entry mistakes. Pay close attention to the input.deployer.uri (see Appendix E), input.wl.domain.path, input.admin.user, and input.admin.password properties. If you need to make a correction, you can run the installer again with this file as input by running silent mode (see Appendix D).

G

Appendix: Troubleshooting Problems on the Oracle Stack

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

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

jndi.properties File Name

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

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

Secure RMI and Secure JDBC

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

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

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

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

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

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

http://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.

H

Appendix: Device Configuration

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

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

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

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

Configuring Devices for an HP Register

To configure the devices for an HP register:

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

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

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

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

```
<JposEntry logicalName="defaultPrinter">
    <creation
        factoryClass="com.tpg.javapos.jpos.TPGJposServiceInstanceFactory"
  serviceClass="com.tpg.javapos.jpos.services.posprinter.POSPrinterService"/>
    <vendor name="HP" url="http://www.hp.com"/>
    <jpos category="POSPrinter" version="1.8"/>
    <product description="HP POS Printer Service" name="HP Services for
        JavaPOS(TM) Standard" url="http://www.hp.com"/>
    <!--Other non JavaPOS required property (mostly vendor properties and bus
        specific properties i.e. RS232 )-->
    <prop name="sModelClassName" value="com.tpg.javapos.models.hydra.ptr_cd_
micr.tpg7xx.TPG7xxPtrCDMICRModelLoader"/>
    <!--prop name="commChannel" value="ethernet"/-->
    <prop name="Img_PortNumber" value="9001"/>
    <!--prop name="Ret_PortNumber" value="9000"/-->
    <prop name="dualClientImager" value ="false"/>
    <prop name="Img_IPAddress" value="10.1.2.33"/>
    <prop name="CloseOnTransmit" value="true"/>
    <!--prop name="commChannel" value="serial"/-->
    <!--prop name="portName" value="ethernet"/-->
    <prop name="commChannel" value="nativeusb"/>
    <!--prop name="portName" value="COM2"/-->
    <prop name="portName" value="nativeusb"/>
    <prop name="baudRate" value="115200"/>
    <prop name="dataBits" value="8"/>
    <prop name="stopBits" value="1"/>
    <prop name="parity" value="N"/>
    <prop name="flowControl" value="RTS"/>
    <!--prop name="ImagerCommChannel" value="ethernetserver"/-->
    <!--prop name="ImagerCommChannel" value="serial"/-->
    <prop name="ImagerCommChannel" value="nativeusb"/>
    <prop name="AutoLineFeed" value="true"/>
    <prop name="sModel" value="7176"/>
    <prop name="asciiBarCode" value="true"/>
</JposEntry>
```

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

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

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

4. To configure the default MSR:

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

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

   b. Install the drivers.

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

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

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

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

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

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

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

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

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

```
<JposEntry logicalName="defaultLineDisplay">
    <creation
        factoryClass="VFD.DeviceServiceInstanceFactory"
        serviceClass="VFD.HP_POLE_DISPLAY"/>
    <vendor name="Hewlett-Packard" url="http://www.HP.com"/>
    <jpos category="LineDisplay" version="1.5"/>
    <product description="Example LineDisplay " name="LineDisplay Service for
        JavaPOS(TM) Standard" url="http://www.HP.com"/>
    <prop name="portName3" type="String" value="COM3"/>
    <prop name="baudRate" type="String" value="9600"/>
    <!--Other non JavaPOS required property (mostly vendor properties and bus
        specific properties i.e. RS232 )-->
</JposEntry>
```

Configuring a 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*.

I

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)