Oracle® Retail Point-of-Service

Installation Guide, Volume 1 - Oracle Stack

Release 13.4.9

E71410-02

April 2016

ORACLE®

Oracle Retail Point-of-Service Installation Guide, Volume 1 - Oracle Stack, Release 13.4.9

E71410-02

Copyright © 2016, Oracle and/or its affiliates. All rights reserved.

Primary Author: Bernadette Goodman

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

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

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

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

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

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

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

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

Value-Added Reseller (VAR) Language

Oracle Retail VAR Applications

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

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

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

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

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

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

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

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

Contents

Send Us Your Comments xiii

Preface xv

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

1 Preinstallation Tasks

Requesting Infrastructure Software 1-1
Check Supported Store Server Software Requirements 1-1
Check Supported Client Hardware and Software Requirements 1-1
Install Optional Components for Microsoft POSReady2009 1-2
Install DigitalPersona Software 1-2
Check Supported Mobile Point-of-Service Hardware and Software Requirements 1-3
Install Required Patch for Oracle Retail Store Inventory Management 1-3
Check for SSL Certificate 1-4
Check Oracle Retail Software Dependencies 1-4
Check Additional Oracle Technologies 1-4
Check Third-Party Software Dependencies 1-4
Integration with Other Applications 1-4
Oracle Retail Central Office and Back Office 1-5
Oracle Retail Store Inventory Management 1-5
Siebel 1-5
Oracle Retail Returns Management 1-5
Bill Payment 1-6
Tender Authorization 1-6
Hardware Requirements 1-7
Store Server 1-7
Client 1-7

Peripheral Devices for Clients ... 1-7
Check Java Key Manager Requirement ... 1-7
Check Secure JDBC and Secure RMI ... 1-8
Tender Authorization Testing for Point-of-Service ... 1-8
ACI PIN Comm ... 1-8
PXP Solutions ANYpay POS ... 1-10
Tender Authorization Testing for Mobile Point-of-Service ... 1-11
ACI PIN Comm ... 1-11
PXP Solutions ANYpay POS ... 1-12
Implementation Guidelines for Security ... 1-13

2 Secure Configuration

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

3 Installation on the Oracle Stack using Windows

Create the Database Schema Owner and Data Source Users ... 3-1
Installing Point-of-Service ... 3-2
Determining Tier Type ... 3-2
Installing the Database ... 3-3
Required Settings for the Database ... 3-3
Installing Point-of-Service on Machines ... 3-3
Updating Device Configuration ... 3-4
Expand the Point-of-Service Distribution ... 3-4
Obtain the JRE Required for Client Install ... 3-5
Increase the Heap Size on the Client ... 3-5
Secure Communication ... 3-5
Database Install Options ... 3-5

Create the Database Schema with Oracle Retail Back Office ... 3-6
Obtain the Files Needed for RSA Data Protection Manager ... 3-6
Obtain the RSA Data Protection Manager Jar Files ... 3-6
Install the Java Cryptography Extension (JCE) ... 3-7
Run the Point-of-Service Application Installer ... 3-7
Resolve Errors Encountered During Application Installation ... 3-8
Create the Database Schema ... 3-8
Create without Oracle Retail Back Office ... 3-8
Resolve Issues with Misprinted Characters in eReceipts and Network Printed Reports and Receipts ... 3-9
Resolve Misprinted Character Problems in eReceipts ... 3-10
Resolve Misprinted Character Problems in Network Printed Receipts and Reports ... 3-11
Enable Browser Functionality in the Client Installation ... 3-12
Accessing Web Sites Through a Secure HTTP Connection ... 3-12
Set up the Store Server for Tender Authorization ... 3-12
Results of a Point-of-Service Installation ... 3-13
Running Point-of-Service ... 3-13
Creating a Custom Installation ... 3-14

4 Installation of Mobile Point-of-Service

Create a New WebLogic Server Domain for Mobile Point-of-Service Server ... 4-1
Expand the Mobile Point-of-Service Distribution ... 4-2
Set Up for Integration with Central Office ... 4-3
Secure Communication ... 4-3
Obtain the Files Needed for RSA Data Protection Manager ... 4-3
Obtain the RSA Data Protection Manager Jar Files ... 4-3
Install the Java Cryptography Extension (JCE) ... 4-3
Run the Mobile Point-of-Service Server Installer ... 4-4
Resolve Errors Encountered During Application Installation ... 4-4
Disabled Non-SSL Port ... 4-5
Manual Deployment of the Mobile Point-of-Service Server Application ... 4-5
Mobile POS Application ... 4-6
Setting Up the Mobile POS Application Xcode Project ... 4-6
Extract the Xcode Project ... 4-6
Ensure MobilePOS.framework is in Place ... 4-6
Install the Sled Framework ... 4-7
Install the PhoneGap Library ... 4-7
Install the PhoneGap Library for an iOS Device ... 4-7
Install the PhoneGap Library for an iOS Simulator ... 4-8
Verify the Build Settings ... 4-9
Build the Project ... 4-9
Configuring and Deploying the MPOS UI Certificate ... 4-9
Create the Development Certificate ... 4-10
Distribution ... 4-11
Create the Distribution Certificate ... 4-11
Create the Distribution Provisioning Profile ... 4-11
Install the Distribution Certificate and Provisioning Profile ... 4-11

Create the Application for Distribution 4-12
Additional Notes 4-12
Configuring the Mobile Point-of-Service Application on a Mobile Device 4-13
Obtaining the UVID after Installation 4-13

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

JDBC URL for an Oracle 12c Database E-1
JDBC URL for an Oracle 11g Database E-1
URL for the Siebel Web Service E-1
JNDI Provider URL for an Application E-2
Deployer URI E-2

F Appendix: Common Installation Errors

"Pos installer finished with errors" F-1
"Dispatcher.main, Exception: java.security.AccessControlException: access denied (java.util.PropertyPermission * read,write)" F-1
"java.lang.NullPointerException" F-2
WebLogic Domain Does Not Exist F-2
WebLogic Domain Server is Not Started F-2

G Appendix: Troubleshooting Problems on the Oracle Stack

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

H Appendix: Device Configuration

Configuring Devices for an HP Register H-1
Configuring a Device for ACI PIN Comm H-4

I Appendix: Installation Order

Enterprise Installation Order I-1

List of Figures

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

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

C–3 License Agreement C-2
C–4 Supported Languages C-3
C–5 Enter Default Locale C-4
C–6 Store Server Details C-5
C–7 Store ID C-6
C–8 Database Source User C-7
C–9 Enable Secure JDBC C-8
C–10 Data Source SSL Configuration C-9
C–11 Mobile Point-of-Service Administrator User C-10
C–12 App Server WL_HOME C-11
C–13 Security Setup: Key Manager C-12
C–14 RSA Data Protection Manager Requirements C-13
C–15 Security Setup: RSA Client JAR Files C-14
C–16 RSA Client Configuration C-15
C–17 Key Store Pass Phrase for Simulator Key Manager C-16
C–18 JRE Location C-17
C–19 Domain Details C-18
C–20 Weblogic Administrative User C-19
C–21 Configure Weblogic Admin Server SSL Key Store C-20
C–22 Weblogic Admin Server SSL Key Store Details C-21
C–23 Mail Session Details C-23
C–24 Enable eReceipt C-24
C–25 eReceipt Properties C-25
C–26 Value-Added Tax (VAT) C-26
C–27 Tender Authorization C-27
C–28 Tender Authorization: ISD PIN Comm C-28
C–29 Tender Authorization: Servebase PC-EFT C-29
C–30 Network Printer Support C-30
C–31 Network Printer Support Configuration for Page Printer C-31
C–32 Network Printer Support Configuration for Roll Receipt Printer C-32
C–33 Mobile Device Configuration C-33
C–34 Mobile Device PED/CPOI Configuration Topology C-34
C–35 Mobile Devices Single PED Configuration (PXP Solutions) C-35
C–36 Mobile Devices Multiple PED Configuration (PXP Solutions) C-36
C–37 Integrate Applications C-37
C–38 Back Office Security C-38
C–39 Parameter Distribution Information C-39
C–40 Back Office Server Information C-40
C–41 ORSIM Integration C-41
C–42 Enable Client Secure RMI C-42
C–43 SSL Trust Store Details C-43
C–44 Manual Deployment Option C-44
C–45 Application Deployment Details C-45
C–46 Turn Off the Application Server's Non-SSL Port C-46
C–47 Logging Detail Options C-47
C–48 Installation Progress C-48
C–49 Install Complete C-48

List of Tables

1–1 Store Server Requirements 1-1
1–2 Client Requirements 1-2
1–3 Mobile Point-of-Service Server Requirements 1-3
1–4 Mobile Point-of-Service Device Requirements 1-3
1–5 Supported Oracle Retail Products 1-4
1–6 Additional Oracle Technologies 1-4
1–7 ACI PIN Comm Authorization Set Tested with Point-of-Service 1-8
1–8 PXP Solutions ANYpay POS Authorization Set Tested with Point-of-Service 1-10
1–9 ACI PIN Comm Authorization Set Tested with Mobile Point-of-Service 1-12
1–10 PXP Solutions ANYpay POS Authorization Set Tested with Mobile Point-of-Service 1-12
3–1 Server Tier Logical Components 3-2
3–2 <POS_install_directory> Subdirectories 3-13
3–3 <POS_install_directory>\pos Subdirectories 3-13

Send Us Your Comments

Oracle Retail Point-of-Service Installation Guide, Volume 1 - Oracle Stack, Release 13.4.9

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

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

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

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

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

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

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

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

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

Preface

This Installation Guide describes the requirements and procedures to install 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

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

Access to Oracle Support

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

Related Documents

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

- *Oracle Retail Point-of-Service Installation Guide, Volume 2 - IBM Stack*
- *Oracle Retail Point-of-Service Release Notes*
- *Oracle Retail POS Suite Data Model Data Dictionary*

Customer Support

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

https://support.oracle.com

When contacting Customer Support, please provide the following:

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

Review Patch Documentation

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

Improved Process for Oracle Retail Documentation Corrections

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

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

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

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

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

Oracle Retail Documentation on the Oracle Technology Network

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

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

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

Conventions

The following text conventions are used in this document:

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

1

Preinstallation Tasks

This chapter describes the requirements for the 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.

Requesting Infrastructure Software

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

Check Supported Store Server Software Requirements

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

Table 1–1 Store Server Requirements

Supported on	Versions Supported
Operating System	Microsoft Windows 2012 Server R2 Standard Edition (64-bit)
Database	▪ Oracle Database 12c Standard Edition 12.1.0.2 (64-bit) ▪ Oracle Database 11gR2 Standard Edition 11.2.0.4 (64-bit) **Note:** Oracle Retail Point-of-Service is not certified with Real Application Clusters (RAC).
JDK/JRE	Oracle Java Standard Edition 7 or later within the Java 7 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 (32-bit) **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 7 or later within the Java 7 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.

You must update the PATH environment variable to include the pointers to the dynamic link library (dll) files. Following is an example of how to set the PATH variable:

```
SET FP_PATH=C:\DigitalPersona\Bin;C:\DigitalPersona\Bin\Java
SET PATH=%FP_PATH%;%PATH%
```

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 2012 Server R2 Standard Edition (64-bit)
J2EE Application Server	Oracle WebLogic Server 10.3.6.0 Standard Edition (32-bit)
J2EE Application Server JVM	Oracle Java Standard Edition 7 or later within the Java 7 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 (5th Generation)
Operating System	iOS 8.4
Sled	Verifone PAYware Mobile E315 VMF Framework 10.4.240 **Note:** Mobile Point-of-Service can be run without a sled, but this is not suitable for a production environment.
PIN Pad	▪ VeriFone MX860 ▪ VeriFone VX810 (EMV)
Network Printer	Programmable Logical Control System (PLCS) and Postscript

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	13.4.9
Oracle Retail Central Office	13.4.9
Oracle Retail Merchandising System	13.2.9
Oracle Retail Price Management	13.2.9
Oracle Retail Returns Management	2.4.9
Oracle Retail Sales Audit	13.2.9
Oracle Retail Store Inventory Management	13.2.9 (on Oracle WebLogic 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–37.

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–53.

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

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

For additional information:

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

If you are using the RSA Data Protection Manager, you must use version 3.5. You must obtain specific jar files for version 3.5 and install the Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files 7.0. See "Obtain the Files Needed for RSA Data Protection Manager" in Chapter 3.

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

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

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

Check Secure JDBC and Secure RMI

For information on enabling secure JDBC and RMI, see "Secure Communication" in Chapter 3.

Tender Authorization Testing for Point-of-Service

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

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
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
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

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 Tender	■ Gift Card Sale Approval ■ Gift Card Sale Authorization Offline ■ Gift Card Sale Authorization Timeout ■ Gift Card Sale Decline ■ Gift Card Post Void ■ Gift Card Sale Referral
House Account Tender	■ House Account Return Approval ■ House Account Return Authorization Offline ■ House Account Return Authorization Timeout ■ House Account Return Decline ■ House Account Sale Approval ■ House Account Sale Authorization Offline ■ House Account Sale Authorization Timeout ■ House Account Sale Decline ■ House Account Sale Post Void ■ House Account Sale Referral

PXP Solutions ANYpay POS

The version used for testing was 2.0.0.52.

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

Table 1–8 PXP Solutions ANYpay POS Authorization Set Tested with Point-of-Service

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

Table 1–8 (Cont.) PXP Solutions ANYpay POS Authorization Set Tested with

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

Tender Authorization Testing for Mobile Point-of-Service

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

PXP Solutions ANYpay 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 PXP Solutions ANYpay POS Authorization Set Tested with Mobile Point-of-Service

Transaction Type	Transaction Type Message Sent from PXP Solutions ANYpay 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

Table 1–10 (Cont.) PXP Solutions ANYpay POS Authorization Set Tested with Mobile Point-of-Service

Transaction Type	Transaction Type Message Sent from PXP Solutions ANYpay POS to Mobile Point-of-Service
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 links on the Oracle Technology Network Web site:

- 12.1.0.2:

  http://docs.oracle.com/database/121/TDPSG/toc.htm

- 11.2.0.4:

  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 3.5. 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 13.4.9 Oracle Retail POS Suite applications enable out-of-the-box audit logging by default. These logs should not be disabled.

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

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

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

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

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

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

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

File Name: audit.log

Location (in each register):

*<POS_install_directory>**<client>*\pos\logs

The following events should be captured at the system level:

- Login or logoff
- Start or stop a process
- Use of user rights
- Account administration
- Change the security policy
- Restart and shut down the system
- USB events and Mount andUnmount events
- Access a file or directory (create a file, remove a file, read a file, or change file descriptors)

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

Application Runtime Settings

After installation, these settings should be used.

Application Parameters

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

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

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

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

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

Integration with Other Applications

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

Scripts and Command Line Utilities

This section covers scripts and utilities used after installation.

Wallet Management Tool

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

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

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

Purge Scripts

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

3

Installation on the 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.
Point-of-Service Clients	The machines that execute the Point-of-Service transactions; they are typically cash registers.

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

Machine	Description
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 13.4.9 distribution zip file.
2. Create a new staging directory for the Point-of-Service application distribution `ORPOS-13.4.9.zip` file, for example, `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-13.4.9.zip` to *<staging_directory>* and extract its contents. The following files and directories should be created under *<staging_directory>*`\ORPOS-13.4.9`:

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

For the remainder of this chapter, *<staging_directory>*`\ORPOS-13.4.9` is referred to as *<INSTALL_DIR>*.

Obtain the JRE Required for Client Install

This release requires Oracle Java Standard Edition 7 for client installs on HP registers. The download is available at the following Web site:

http://www.oracle.com/technetwork/java/javase/downloads/index.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-13.4.1.zip` file from the Oracle Software Delivery Cloud at the following Web site:

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

- If you choose **Create schema with minimum dataset**, the installer creates and populates the database schema with the minimum amount of data needed to launch and run Point-of-Service. If you want to load your own data after installation, you can select this option.
- If you choose **Skip schema creation and data loading**, the installer does not create and populate the database schema. This is the default selection on the screen. You choose this option if you want to create and populate the database schema manually or the database schema was created using Back Office. For information on manually creating and populating the database schema, see "Create the Database Schema".

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

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

Create the Database Schema with Oracle Retail Back Office

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

Obtain the Files Needed for RSA Data Protection Manager

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

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

Obtain the RSA Data Protection Manager Jar Files

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

1. Obtain the following jar files from your RSA Data Protection Manager provider:
   - certj.jar
   - cryptojce.jar
   - cryptojcommon.jar

- jcm.jar
- kmsclient.jar
- sslj.jar

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

Install the Java Cryptography Extension (JCE)

You must update the security for your JRE. You need to obtain version 7.0 of the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.

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

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

   - On the client:

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

2. Download version 7 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 7**.
   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 UnlimitedJCEPolicyJDK7.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 7.

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.dpotjni = C:\\DigitalPersona\\Bin\\Java\\dpotjni.jar
     ```

   - The fingerprint device is enabled in the `jpos.xml` file.
   - The following is correct in the *<POS_install_directory>*`\`*<client>*`\pos\bin\posenv.bat` file:

     ```
     SET FP_PATH=C:\DigitalPersona\Bin;C:\DigitalPersona\Bin\Java
     SET PATH=%FP_PATH%;%PATH%
     ```

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-13.4.1.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. If the client is running, shut down the client.
3. In the style-sheet used by the Point-of-Service client for eReceipts, specify the best font available for the language on the operating system. Point-of-Service uses Extensible Style-sheet Language Formatting Objects (XSL-FO) to transform each line of receipt data into PDF output. The following file contains the style-sheet:

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

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

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

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

   ```
   <POS_install_directory>\<client>\config\context\DeviceContext.xml
   ```

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

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

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

   ```
   <POS_install_directory>\<client>\pos\config\technician\PosDeviceTechnician.xml
   ```

   Set the value of the alwaysPrintLineFeeds property to true:

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

Point-of-Service is configured to automatically search for fonts in the default paths for your operating system. Point-of-Service uses the Apache Formatting Objects Processor (FOP) to generate eReceipt PDF files. If the font identified in the style-sheet 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. If the client is running, shut down the client.

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

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

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

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

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

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

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

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

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

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

   Set the value of the alwaysPrintLineFeeds property to true:

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

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 13.4.9 distribution zip file.
2. Create a new staging directory for the Mobile Point-of-Service application distribution `ORMPOS-13.4.9.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-13.4.9.zip` to *<staging_directory>* and extract its contents. The following files and directories should be created under *<staging_directory>*`\ORMPOS-13.4.9`:

```
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-13.4.9 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–37. 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–42.

Obtain the Files Needed for RSA Data Protection Manager

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

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

Obtain the RSA Data Protection Manager Jar Files

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

1. Obtain the following jar files from your RSA Data Protection Manager provider:
   - certj.jar
   - cryptojce.jar
   - cryptojcommon.jar
   - jcm.jar
   - kmsclient.jar
   - sslj.jar
2. Copy the jar files into <*INSTALL_DIR*>/rsa-jars.

Install the Java Cryptography Extension (JCE)

You must update the security for your JRE. You need to obtain version 7.0 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 7 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 7**.
   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 `UnlimitedJCEPolicyJDK7.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 7.

   ---

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–46. 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–44.

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 13.4.7 distribution zip file.

The `ORMPOS-13.4.9_client.zip` file in the distribution zip file contains the Xcode project used for building the Mobile POS iOS application that runs on the Apple iPod Touch (5th Generation) devices.

The following sections describe the steps needed to set up the project. The instructions are for an Apple computer, since Xcode runs only on Apple OS.

Extract the Xcode Project

To extract the Xcode project:

1. Create a directory to hold the extracted contents of the `ORMPOS-13.4.9_client.zip` file.
2. Copy the `ORMPOS-13.4.9_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 provided 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. Open the `vmf` directory that was created when the `ORMPOS-13.4.9_client.zip` file was unzipped.
2. Inside the `vmf` directory, there is a subdirectory named `VMF.framework`. 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, 1.0.4.240, 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 Library

Mobile POS also has an external dependency on the PhoneGap library, specifically PhoneGap 2.1. To install the PhoneGap library, see the appropriate section:

- "Install the PhoneGap Library for an iOS Device"
- "Install the PhoneGap Library for an iOS Simulator"

Install the PhoneGap Library for an iOS Device To install the PhoneGap library:

1. Download the PhoneGap 2.1 package from the following web site:

   `http://phonegap.com/download`

2. Unzip the PhoneGap 2.1 package that was downloaded in Step 1. This creates a directory named `phonegap-phonegap-26d211b`.
3. In Finder, navigate to `phonegap-phonegap-26d211b/lib/ios/Cordovalib`.

4. Double-click `CordovaLib.xcodeproj` to open the `CordovaLib` project in Xcode.
5. Within Xcode, click the `CordovaLib` project in the Project Navigator.
6. Click the `CordovaLib` target in the main panel.
7. Click the Build Settings tab.
8. Change the Architectures setting to armv7 and armv7s.
9. Change the Valid Architectures to armv7 and armv7s.
10. Select Product and then Build from the Xcode menu by setting the target to ios Device. This creates the PhoneGap 2.1 library, `libCordova.a`.
11. In the Project Navigator, expand the Products folder. Right click `libCordova.a` and select **Show in Finder**.
12. A new Finder window opens showing a directory with `libCordova.a` and a directory named `include`. Copy `include` and `libCordova.a` to the `mobilepos/cordova` directory created in the "Extract the Xcode Project" section.
13. Double-click the `mobilepos-13.4.9.xcodeproj` file in the `mobilepos` directory. This opens the project in Xcode.
14. In the Project Navigator, click the `mobilepos` project. From the menu, select **File** and then **Add Files** to mobilepos.
15. In the Finder window, navigate to the same `cordova` folder as in Step 12. Select `libcordova.a` and click **Add**.

Install the PhoneGap Library for an iOS Simulator To install the PhoneGap library:

1. Download the PhoneGap 2.1 package from the following web site:

   `http://phonegap.com/download`

2. Unzip the PhoneGap 2.1 package that was downloaded in Step 1. This creates a directory named `phonegap-phonegap-26d211b`.
3. In Finder, navigate to `phonegap-phonegap-26d211b/lib/ios/Cordovalib`.
4. Double-click `CordovaLib.xcodeproj` to open the `CordovaLib` project in Xcode.
5. Within Xcode, click the `CordovaLib` project in the Project Navigator.
6. Click the `CordovaLib` target in the main panel.
7. Click the Build Settings tab.
8. Change the Architectures setting to armv7, armv7s, and i386.
9. Change the Valid Architectures to armv7 and armv7s, and i386.
10. Select Product and then Build from the Xcode menu by setting the target to the iPhone Simulator. This creates the PhoneGap 2.1 library, `libCordova.a`.
11. In the Project Navigator, expand the Products folder. Right click `libCordova.a` and select **Show in Finder**.
12. A new Finder window opens showing a directory with `libCordova.a` and a directory named `include`. Copy `include` and `libCordova.a`, created in the Debug-iphonesimulator, to the `mobilepos/cordova` directory created in the "Extract the Xcode Project" section.

13. Double-click the `mobilepos-13.4.9.xcodeproj` file in the `mobilepos` directory. This opens the project in Xcode.
14. In the Project Navigator, click the `mobilepos` project. From the menu, select **File** and then **Add Files** to mobilepos.
15. In the Finder window, navigate to the same `cordova` folder as in Step 12. Select `libcordova.a` and click **Add**.

Verify the Build Settings

To verify the build settings:

1. Double-click the `mobilepos-13.4.9.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 library and 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/VMF` is 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 13.4.9.

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/IDEs/Conceptual/AppDistributionGuide/ManagingYourTeam/ManagingYourTeam.html#//apple_ref/doc/uid/TP40012582-CH16-SW1

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 7.1 are listed here:

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

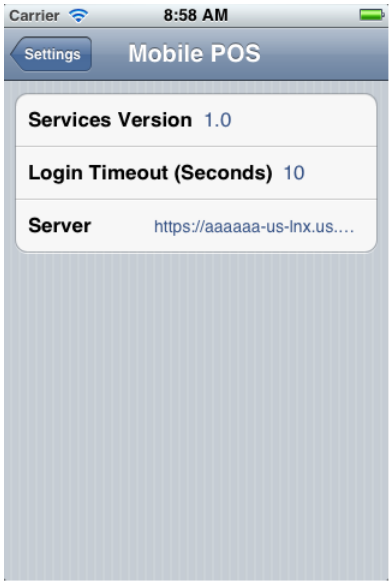
- The application requires a valid UVID, even for the simulator. The UVID for the simulator is like any other Mobile POS UVID and needs to be registered with the server. Unlike the previous versions of XCODE, the UVID of the simulator is not the same as the UVID of the Mac. For more information, see "Obtaining the UVID after Installation".

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



2. Set the address of the server that the device uses to communicate with the Mobile POS server as shown in the following example:

   `https://<host>:<port>/mobilepos`

Obtaining the UVID after Installation

UVID is the Unique Vendor ID; in Apple terms, Identifier for Vendor (IDFV). If the UVID for a device was not added to the server, an error occurs when trying to log on the device. You can add the UVID after installation. To add the UVID to the MPOS Server:

1. Log on to the device using a valid user name and password. An invalid user ID or password error occurs.
2. Find the error in the log of the <*ormpos-domain*> domain. The log file is found in the following location:

   `<WEBLOGIC_INSTALL_DIR>/user_projects/domains/<ormpos-domain>/registers/logs/orpos.log`

   Look for the line shown in the following example:

   ```
   No configuration profile found for hardware ID:
   51B4C782-12A5-49C3-9391-A19F71C10F05
   ```

3. Add the UVID, obtained from the orpos.log file, to the `DeviceContext.xml` found in the following location:

   `<WEBLOGIC_INSTALL_DIR>/user_projects/domains/<ormpos-domain>/servers/<mpos_AdminServer>/tmp/_WL_user/mobilepos/g9eznq/war/WEB-INF/lib`

Following is an example of an entry in the `DeviceContext.xml` file:

```
<!-- BEGIN devicemapping for UVID -->
<entry key="51B4C782-12A5-49C3-9391-A19F71C10F05">
<bean
class="oracle.retail.stores.mobilepos.status.register.RegisterProfileConfigurat
ion.StoreRegisterPair">
<property name="storeID" value="04241" />
<property name="registerID" value="101" />
<property name="printerID" value="device_IppReceiptPrinter" />
</bean>
</entry>
<!-- END devicemapping for UVID1 -->
```

4. Once the UVID is added, log on to the device using a valid user name and password.

Note: The UVID changes all the time when an application is removed and deployed. The Vendor ID is unique for an application per device and vendor. So, the tablet and handheld on a specific iOS device will have different UVIDs.

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

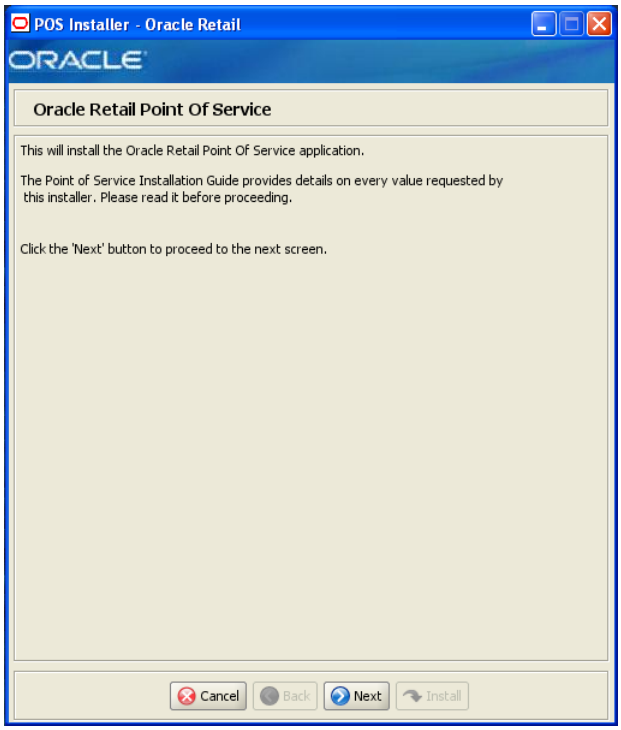


Figure A–2 Previous POS Install

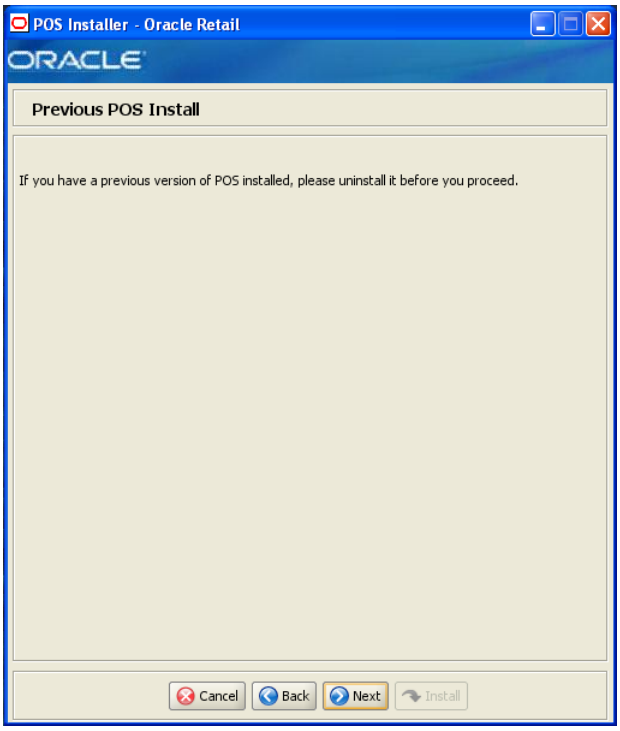
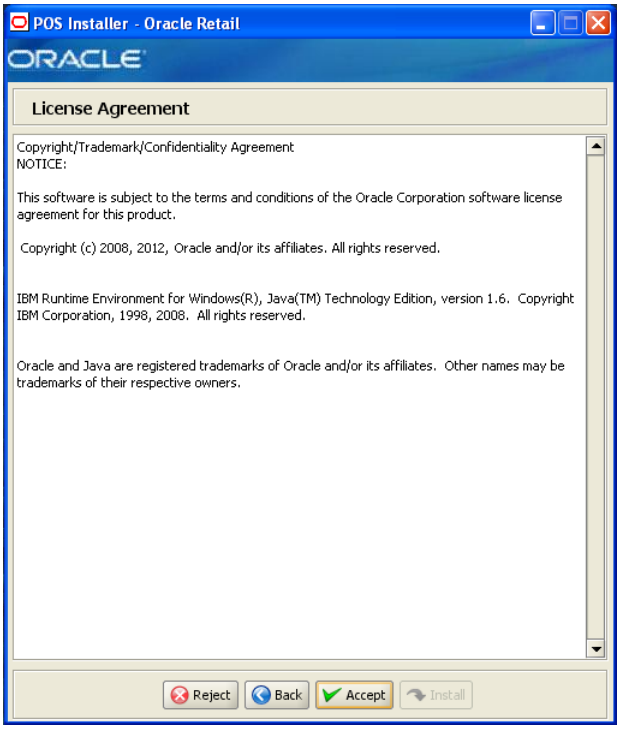
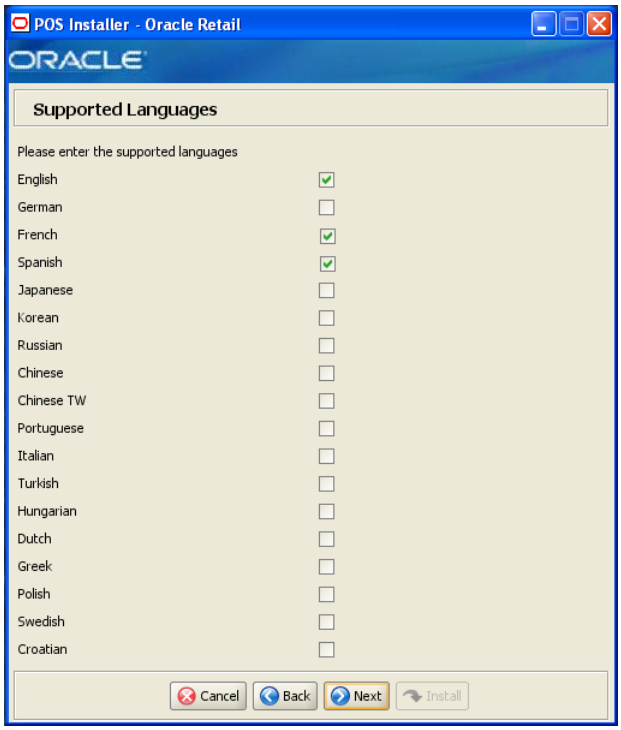


Figure A–3 License Agreement



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

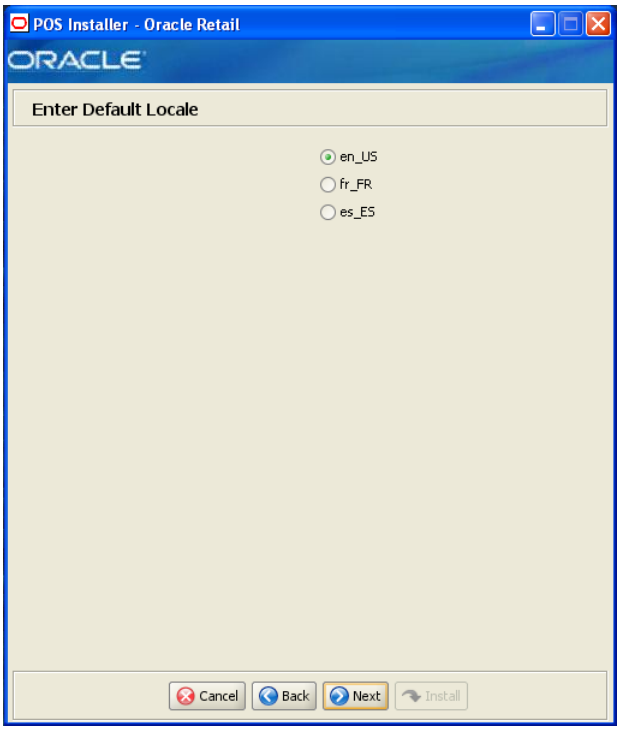
Figure A–4 Supported Languages



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

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

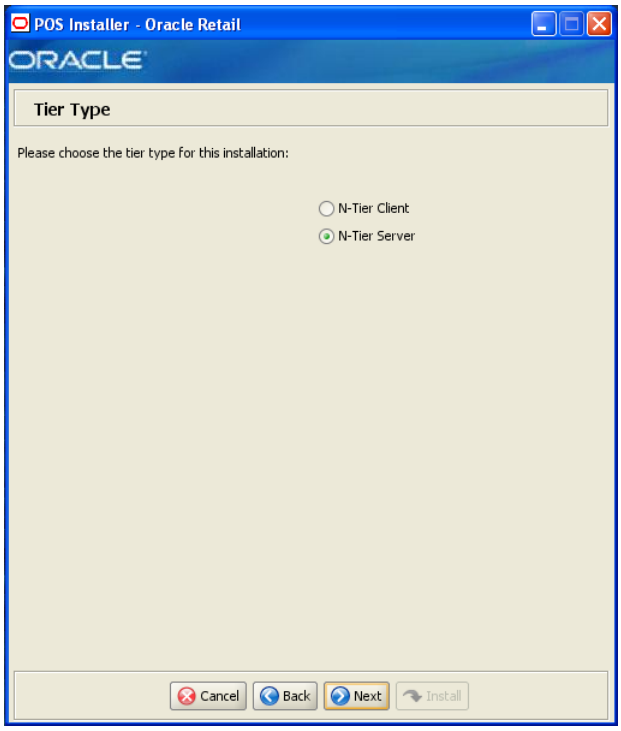
Figure A–5 Enter Default Locale



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

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

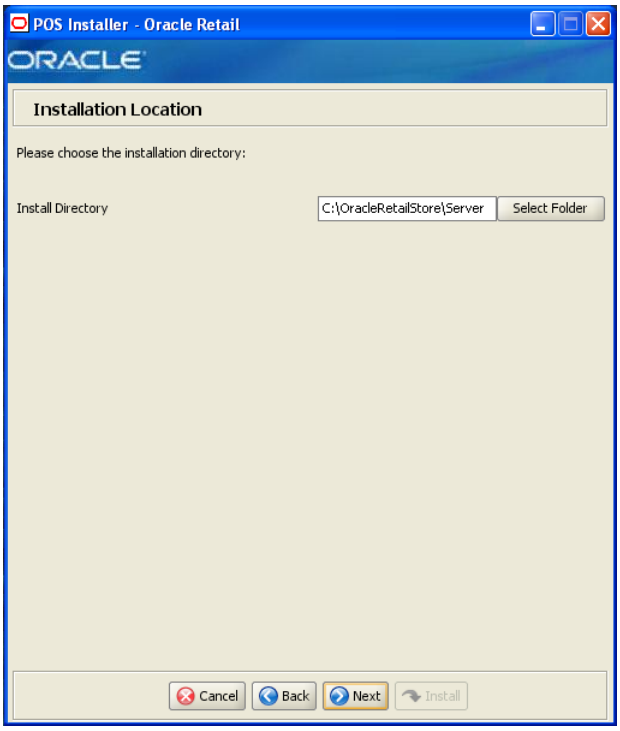
Figure A–6 Tier Type



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

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

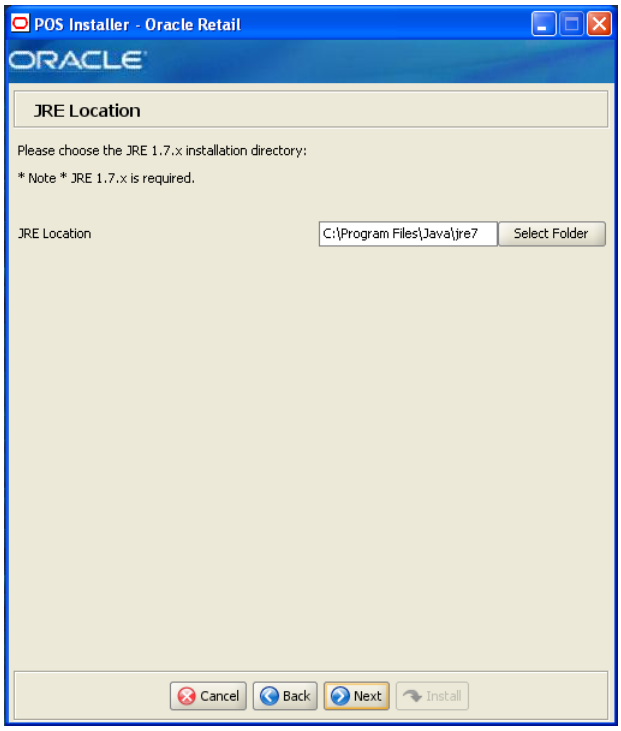
Figure A–7 Installation Location



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

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

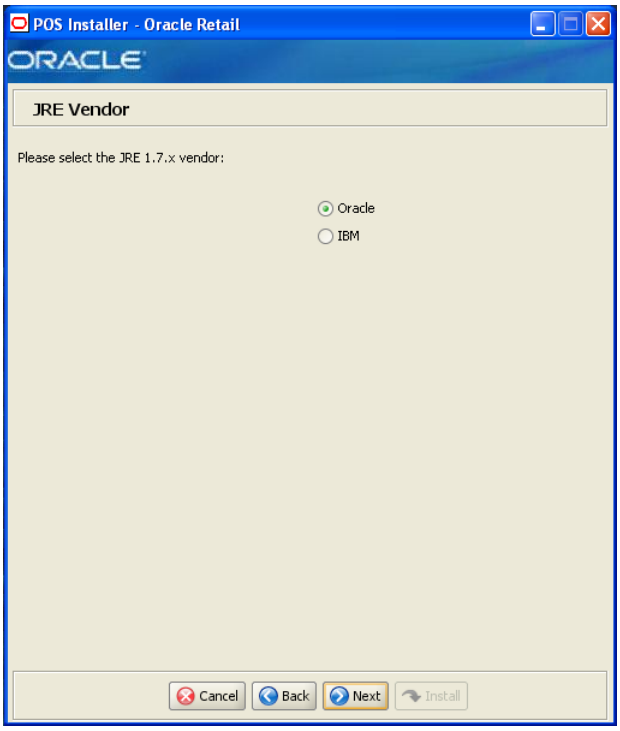
Figure A–8 JRE Location



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

Details	Content
Field Title	JRE Location
Field Description	Enter the location where the JRE is installed.
Example	`C:\Program Files\Java\jre7`

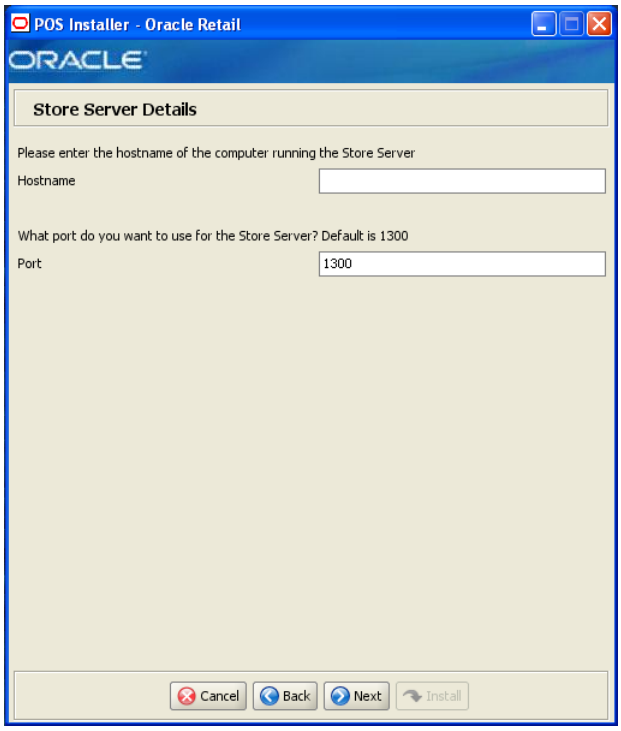
Figure A–9 JRE Vendor



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

Details	Content
Field Title	Please select the JRE 1.7.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

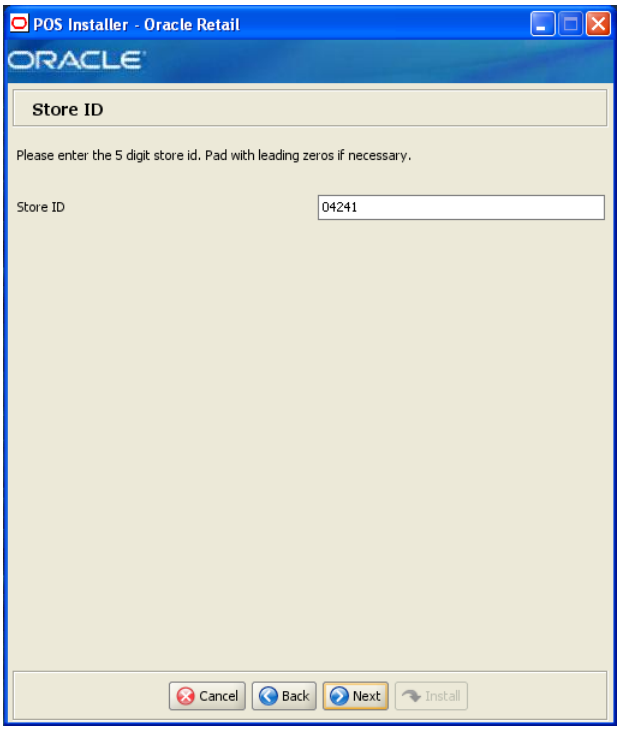


The fields on this screen are described in the following tables.

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

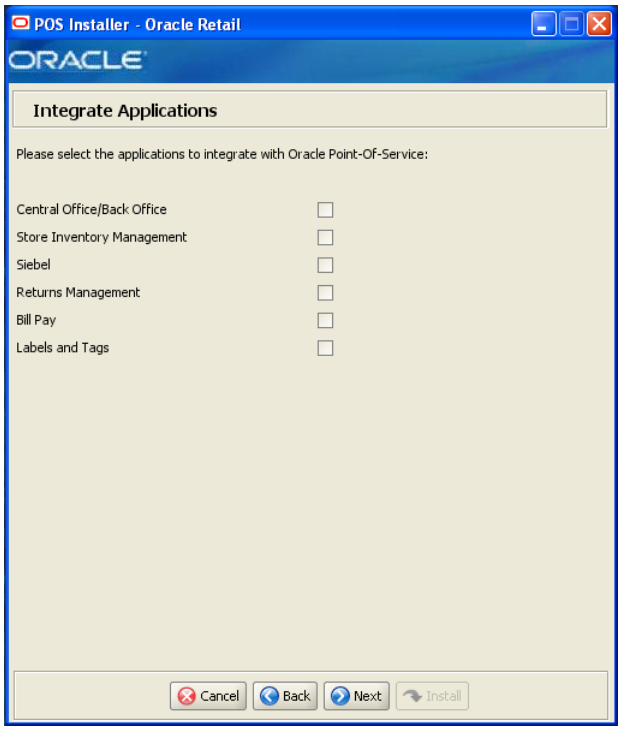
Figure A–11 Store ID



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

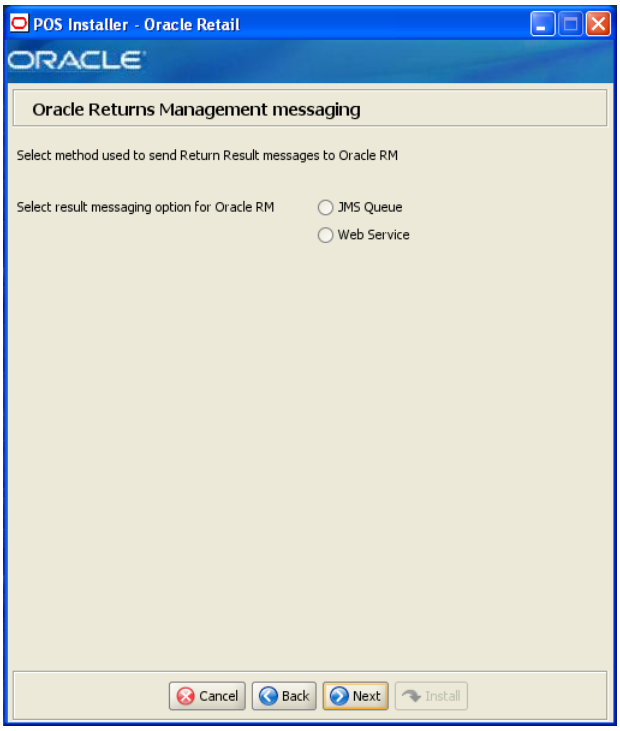
Figure A–12 Integrate Applications



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



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**.

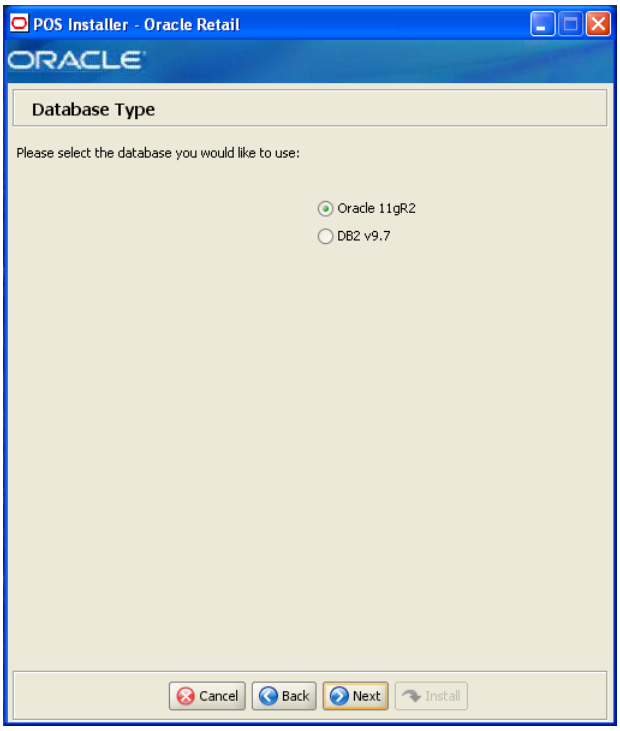
Figure A–14 Application Server Type

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**.

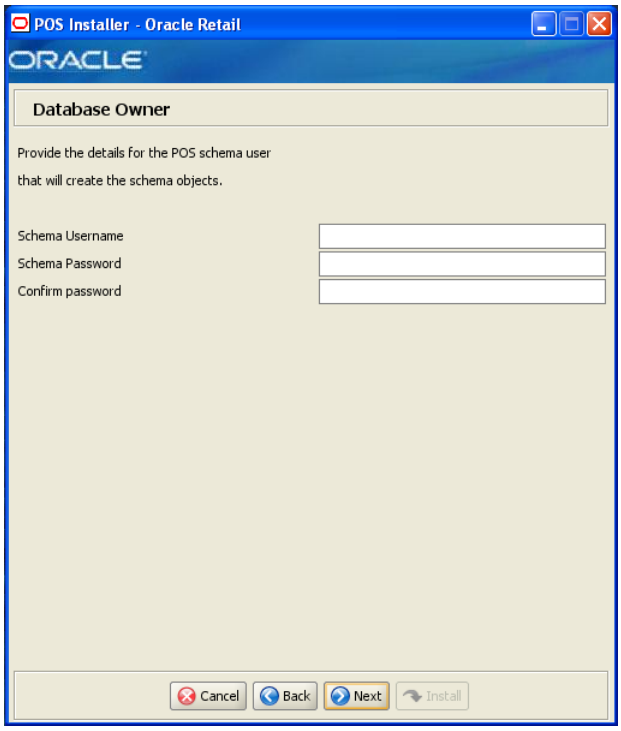
Figure A–15 Database Type



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



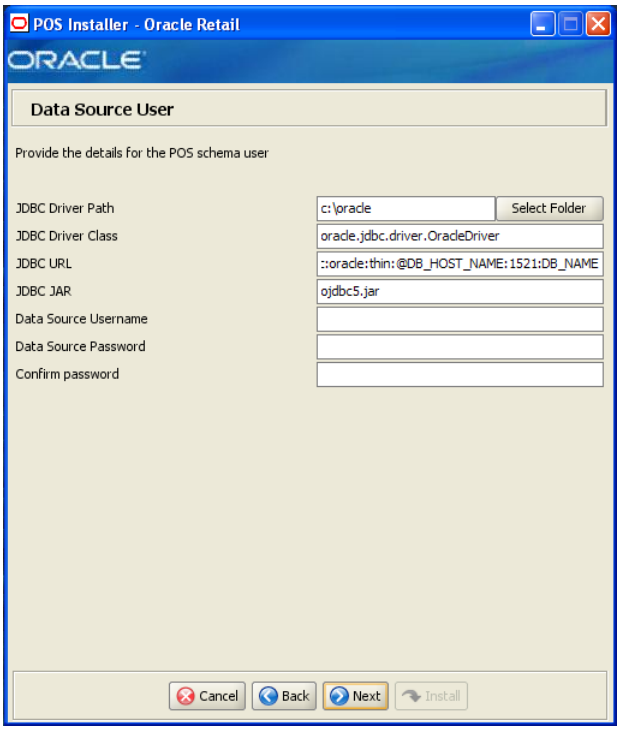
The fields on this screen are described in the following tables.

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



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

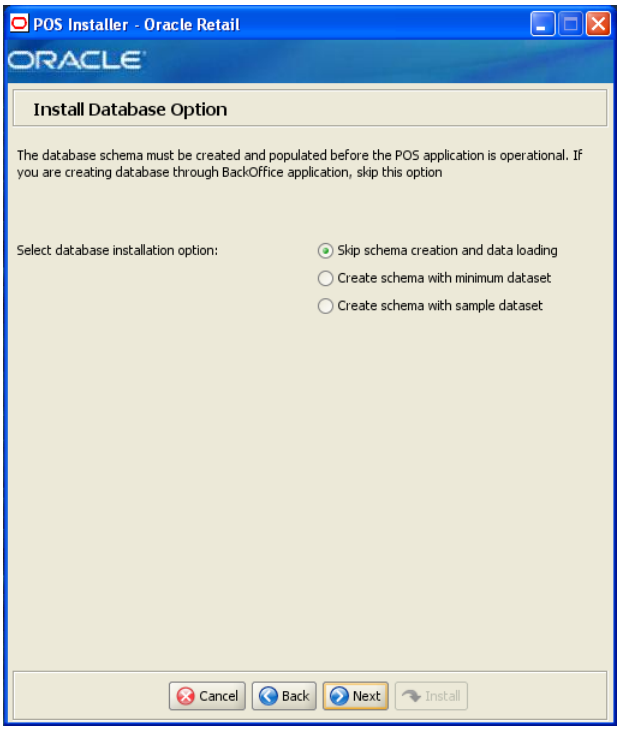
Details	Content
Field Description	Enter the name of the jar containing the database driver.
Example	`ojdbc5.jar`

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



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

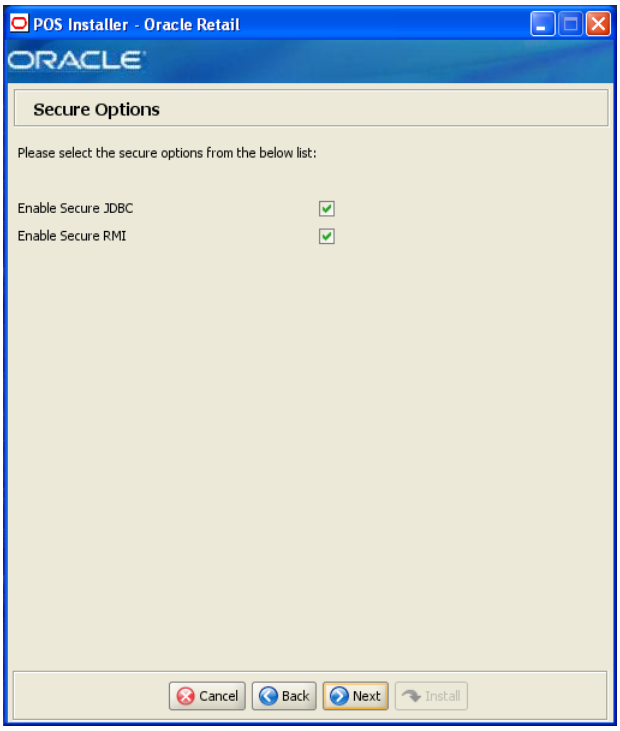
Figure A–19 Sample Dataset

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

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

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

Figure A–20 Secure Options

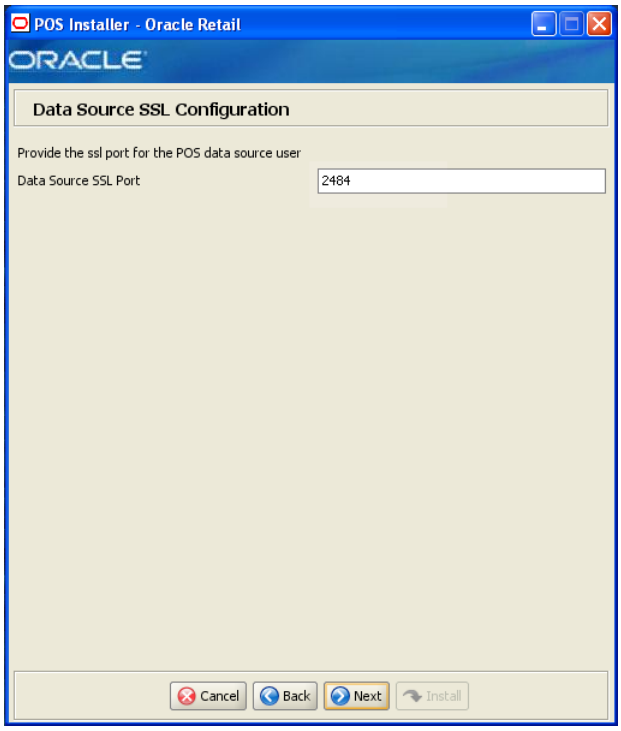


The fields on this screen are described in the following tables.

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

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

Figure A–21 Data Source SSL Configuration

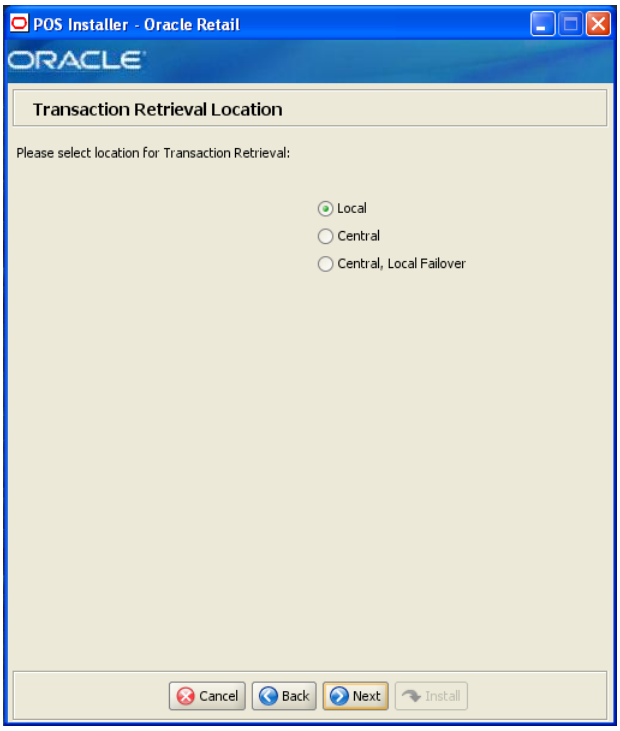


This screen is only displayed if **Enable Secure JDBC** is selected on the Secure Options screen.

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

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

Figure A–22 Transaction Retrieval Location

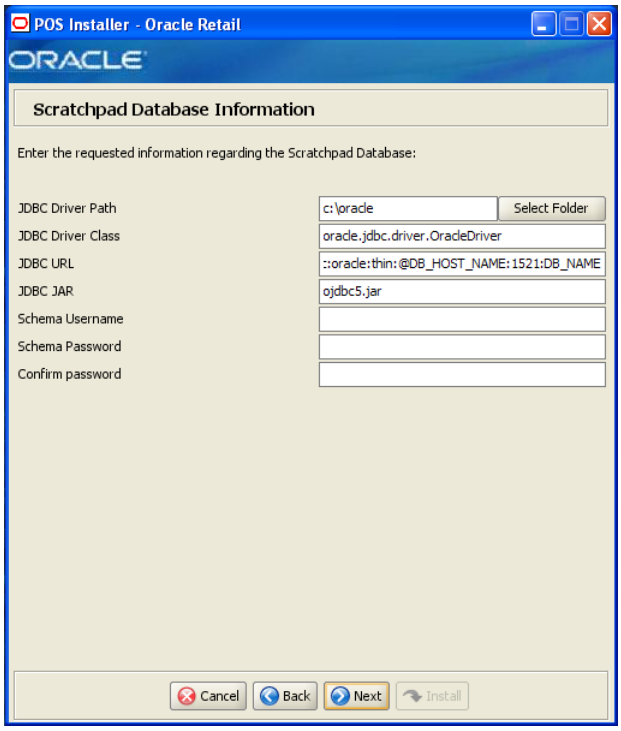


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

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

Figure A–23 Scratchpad Database Information



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

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

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`

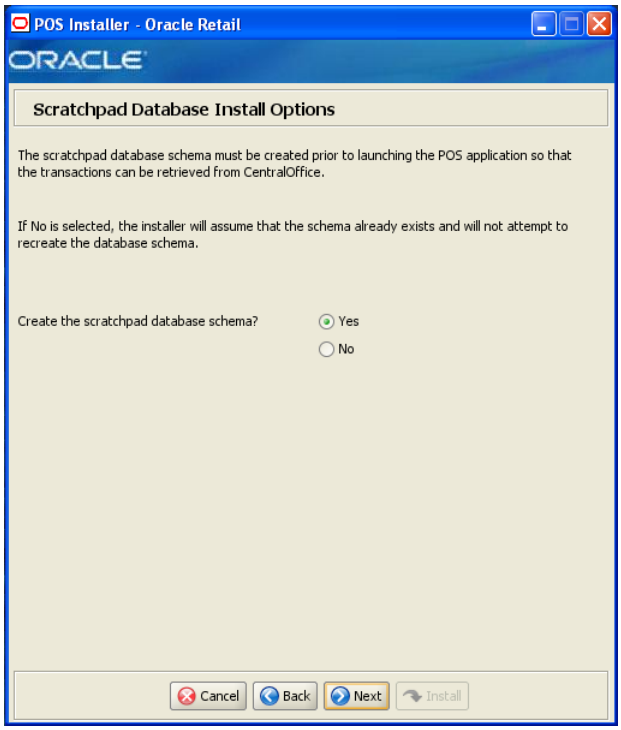
Details	Content
Field Title	JDBC JAR
Field Description	Enter the name of the jar containing the database driver.
Example	`ojdbc5.jar`

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

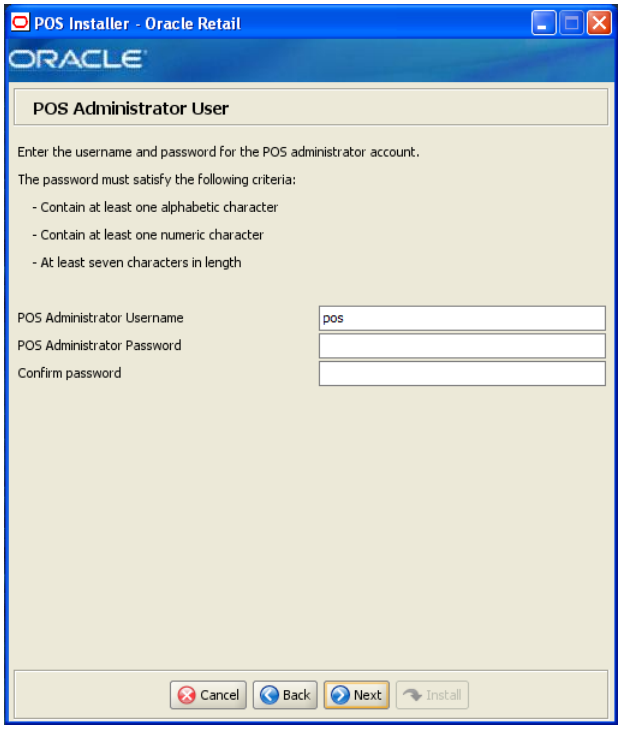


This screen is only displayed if **Central** or **Central, Local Failover** is selected on the Transaction Retrieval Location screen.

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



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

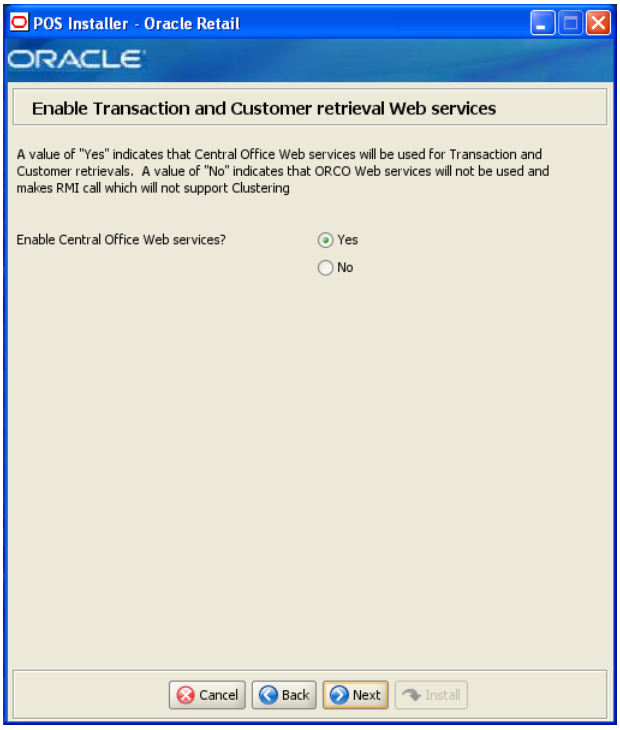
Details	Content
Field Title	POS Administrator Username
Field Description	Enter the user name used for performing Point-of-Service administrative functions.
Example	pos

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

Details	Content
Field Title	Confirm Password

Details	Content
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

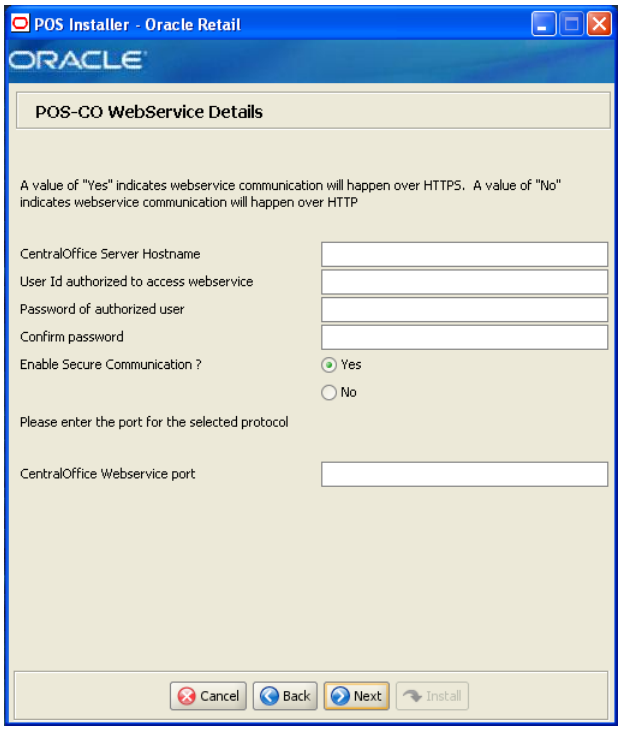


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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



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.

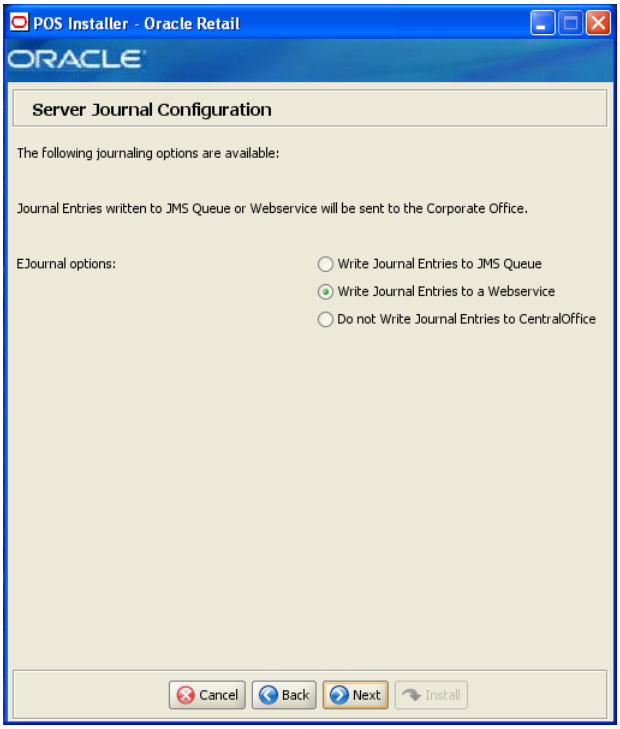
Details	Content
Field Title	Password of authorized user
Field Description	Enter the password of the authorized user.

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

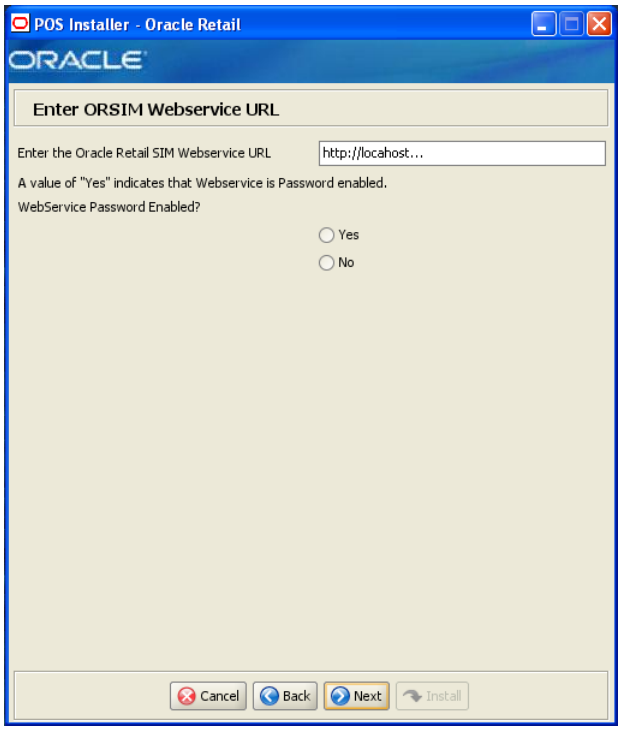


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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



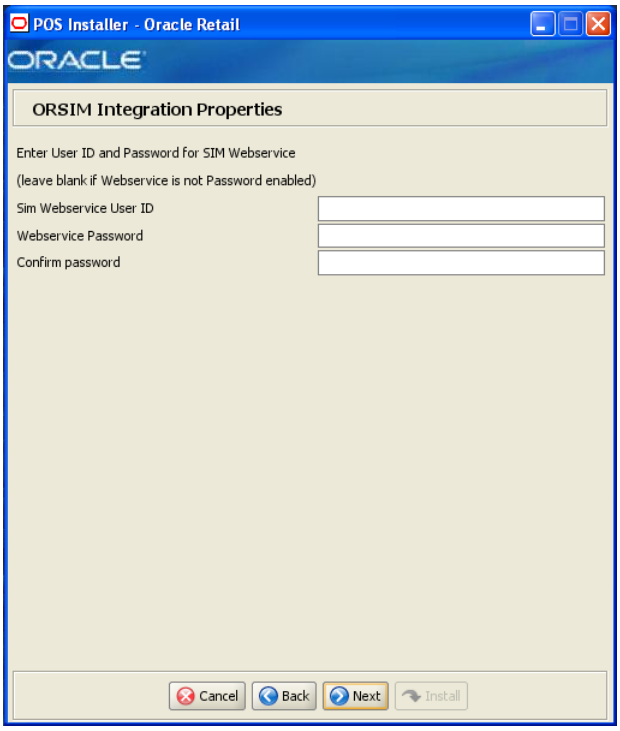
This screen is only displayed if **Store Inventory Management** is selected on the Integrate Applications screen.

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



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

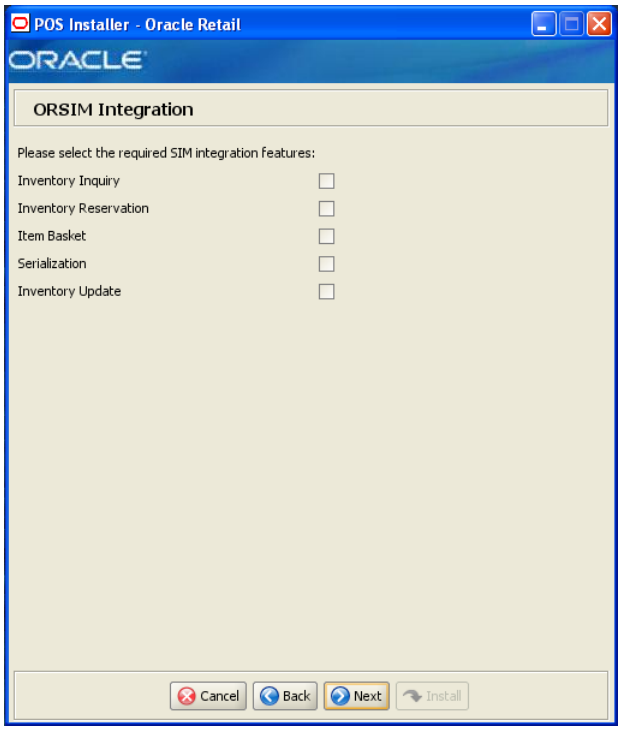
The fields on this screen are described in the following tables.

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

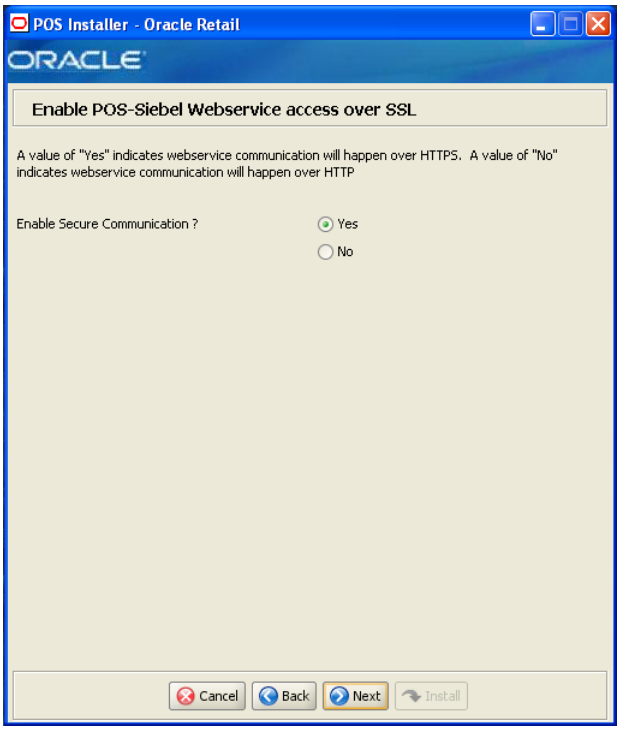


This screen is only displayed if **Store Inventory Management** is selected on the Integrate Applications screen.

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**.

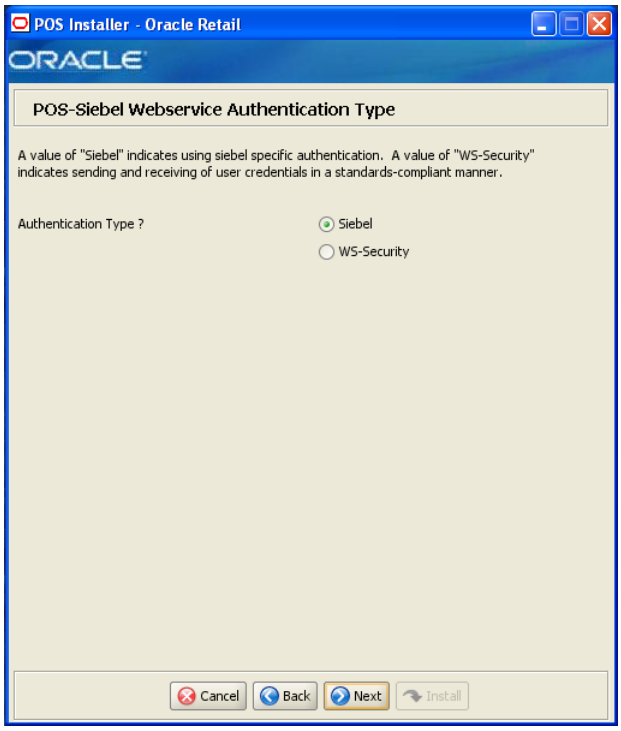
Figure A–32 Enable POS-Siebel Webservice Access Over SSL



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

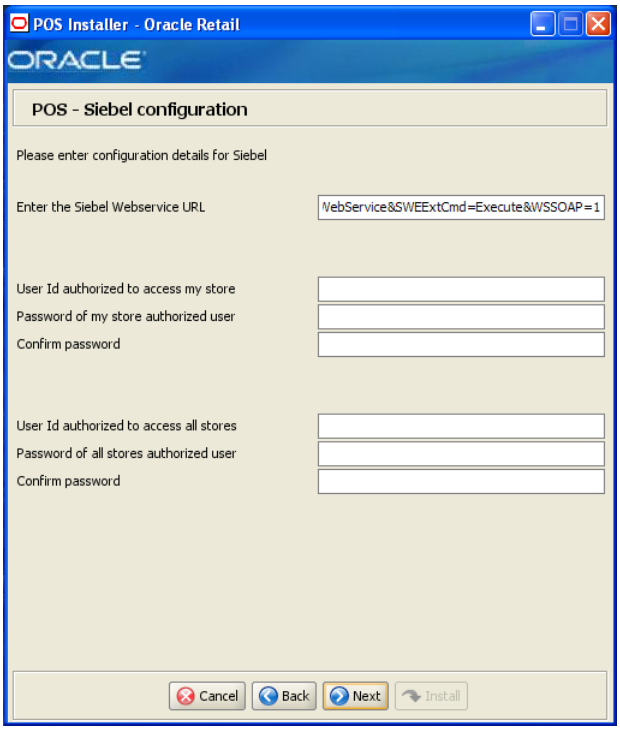


This screen is only displayed if **Siebel** is selected on the Integrate Applications screen.

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



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

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

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

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

Details	Content
Field Title	Confirm Password

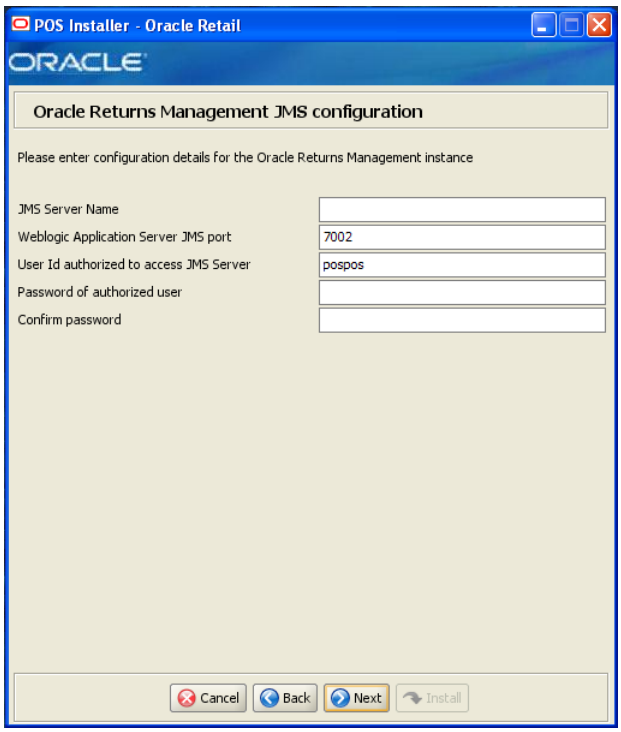
Details	Content
Field Description	Reentered password of my store authorized user used to confirm the password. **Note:** The passwords in the Password of my store authorized user and Confirm Password fields must match.

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

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

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

Figure A–35 Oracle Returns Management JMS Configuration



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

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

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

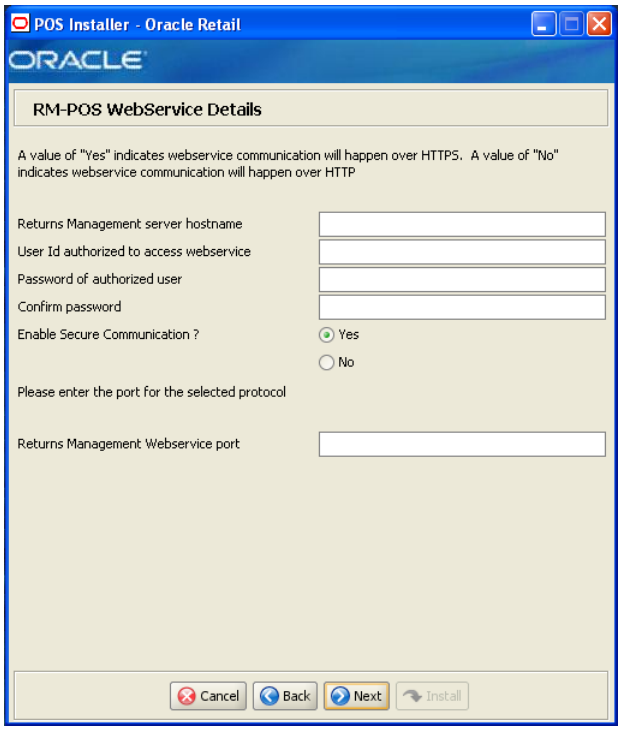
Details	Content
Field Title	Weblogic Application Server JMS port
Field Description	Enter the port number of the JMS server to use to send return result messages to Oracle Retail Returns Management.
Example	7002

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



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.

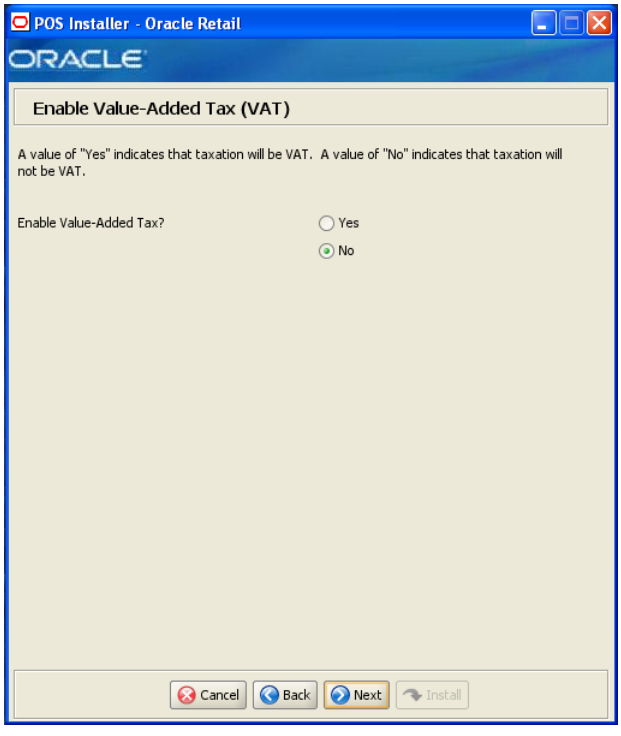
Details	Content
Field Title	Confirm Password

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

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

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

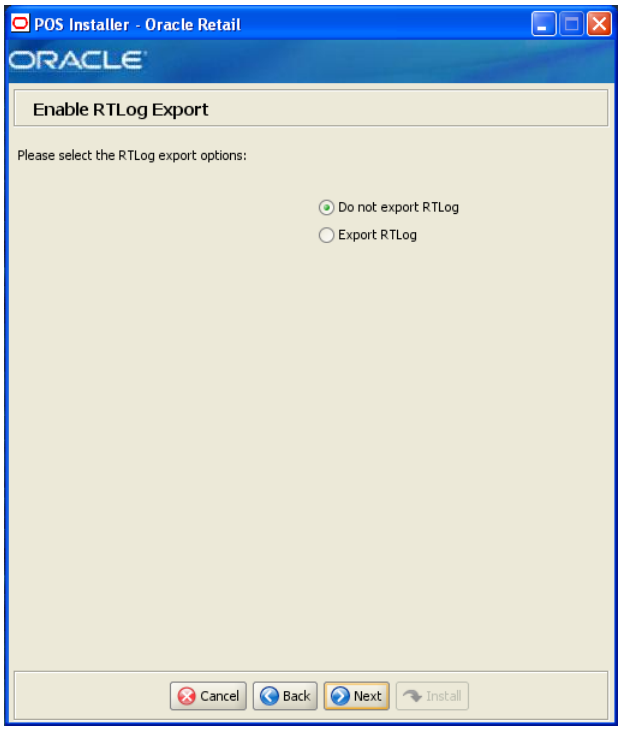
Figure A–37 Enable Value-Added Tax (VAT)



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

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

Figure A–38 Enable RTLog Export



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

Details	Content
Field Title	Please select RTLog export options
Field Description	Choose how the RTLog is to be exported. ■ To not export the log, choose **Do not export RTLog**. ■ To export the log, choose **Export RTLog**.
Example	Do not export RTLog

Figure A–39 Security Setup: Key Manager Settings

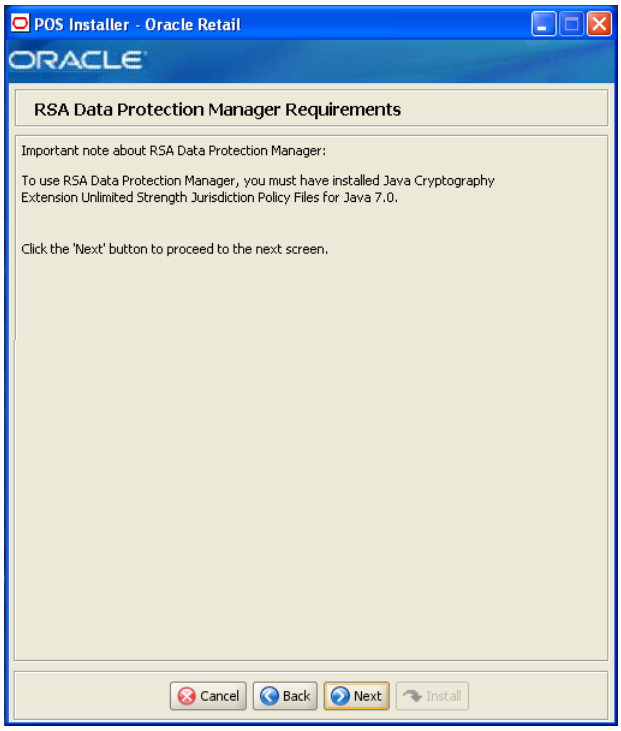
This screen is used to configure the Encryption Key Manager.

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

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

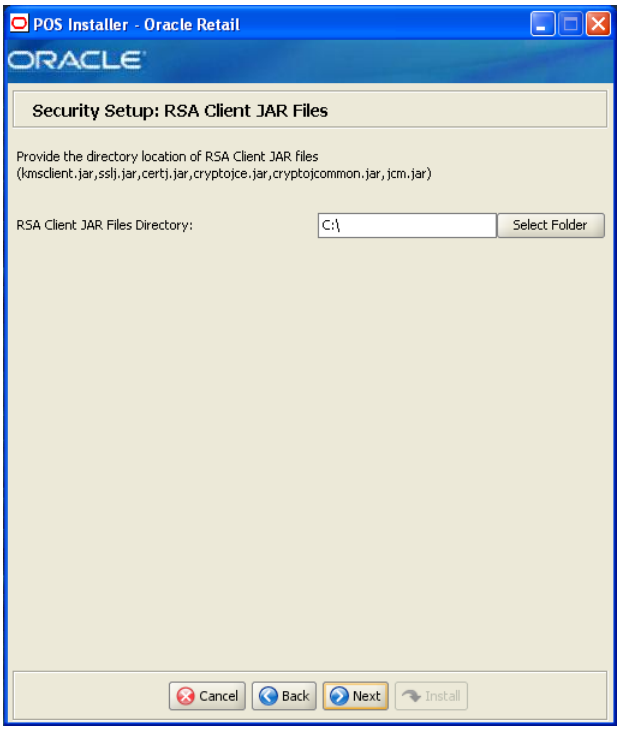
Details	Content
Field Title	Select Key Manager
Field Description	Provider for Key Manager: ■ To use the RSA Data Protection Manager, select **RSA Data Protection Manager**. The next screen displayed is Figure A–40. ■ To use the simulated key management package, select **Simulator**. The next screen displayed is Figure A–43.
Example	RSA Data Protection Manager

Figure A–40 RSA Data Protection Manager Requirements



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

Figure A–41 Security Setup: RSA Client JAR Files



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

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

Details	Content
Field Title	RSA Client JAR Files Directory
Field Description	Choose the directory where the following Key Manager jar files are located: ▪ certj.jar ▪ cryptojce.jar ▪ cryptojcommon.jar ▪ jcm.jar ▪ kmsclient.jar ▪ sslj.jar
Example	`C:\`

Figure A–42 RSA Client Configuration

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

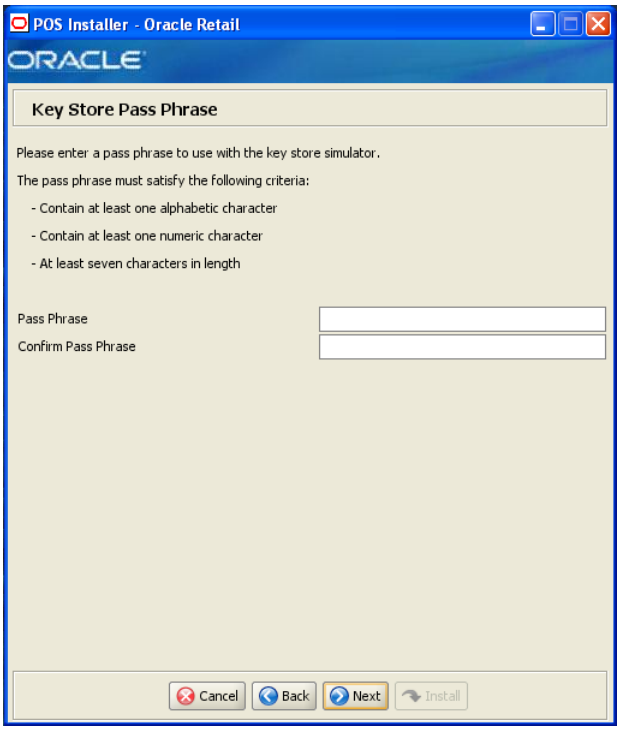
The fields on this screen are described in the following tables.

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

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

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

Figure A–43 Key Store Pass Phrase for Simulator Key Manager



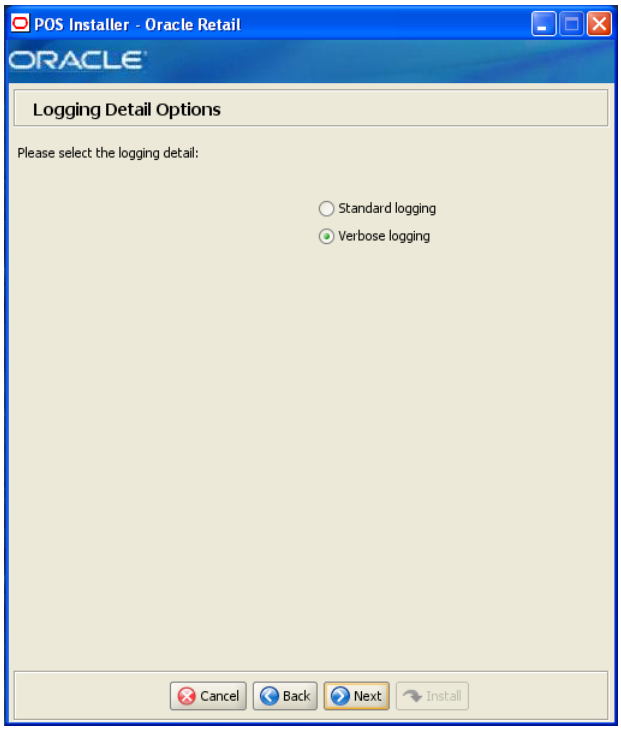
This screen is only displayed if **Simulator** is selected for the Key Manager on the Security Setup: Key Manager Settings screen.

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

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

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

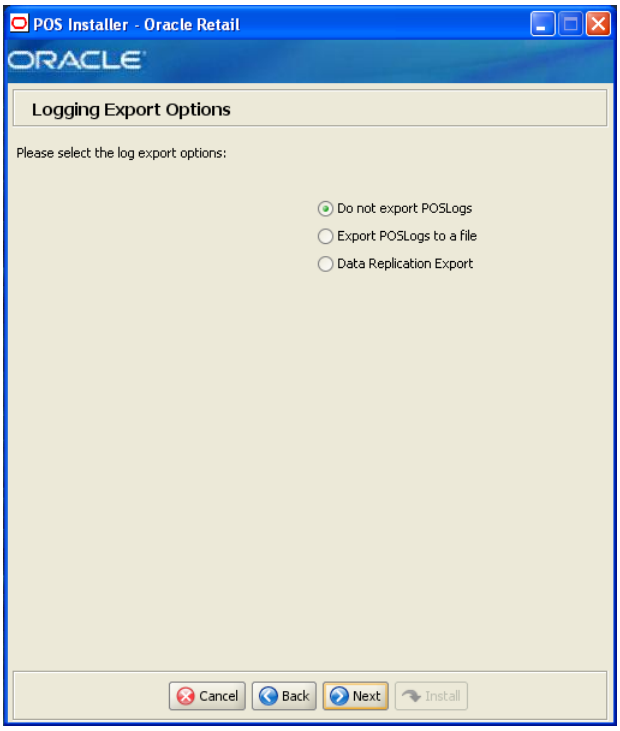
Figure A–44 Logging Detail Options



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

Details	Content
Field Title	Please select the logging detail
Field Description	Choose the level of client logging. ■ To only log some of the messages, choose **Standard Logging**. ■ To log all of the messages, choose **Verbose Logging**.
Example	Verbose logging

Figure A–45 Logging Export Options

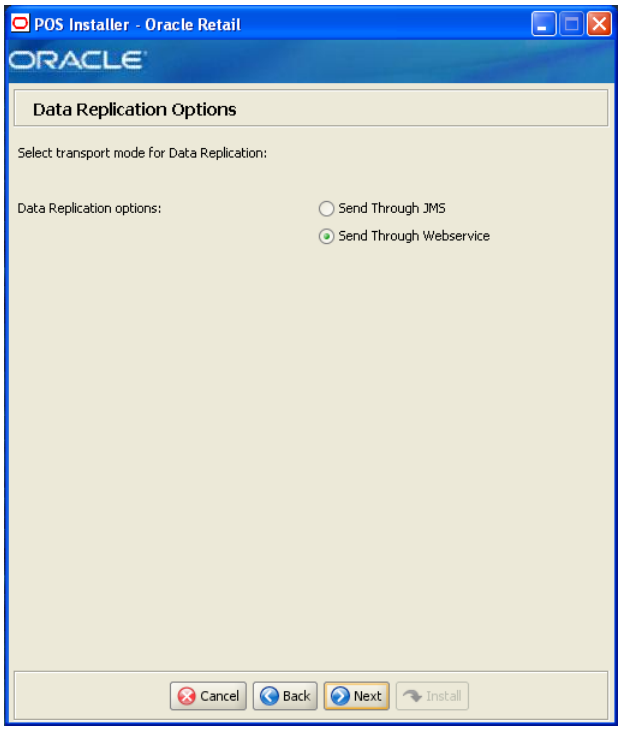


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

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

Figure A–46 Data Replication Options

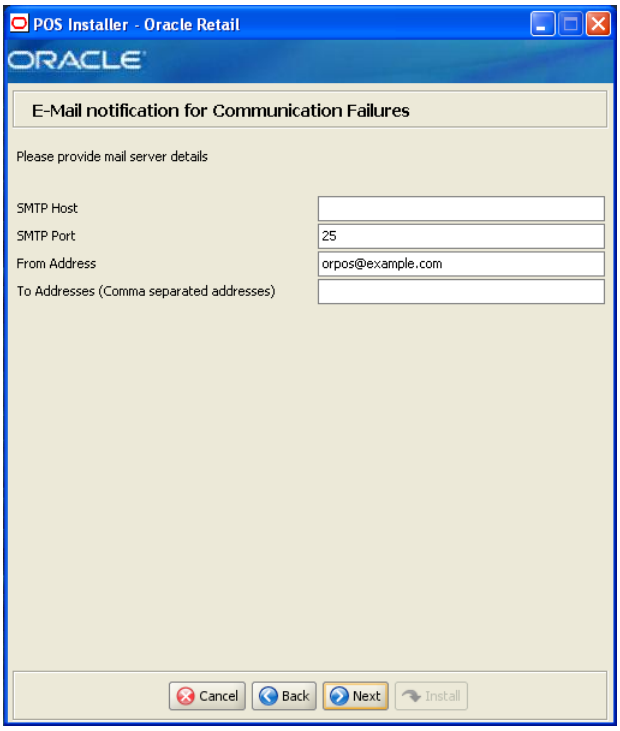


This screen is only displayed if **Data Replication Export** is selected on the Logging Export Options screen.

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

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

Figure A–47 E-mail Notification for Communication Failures



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

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

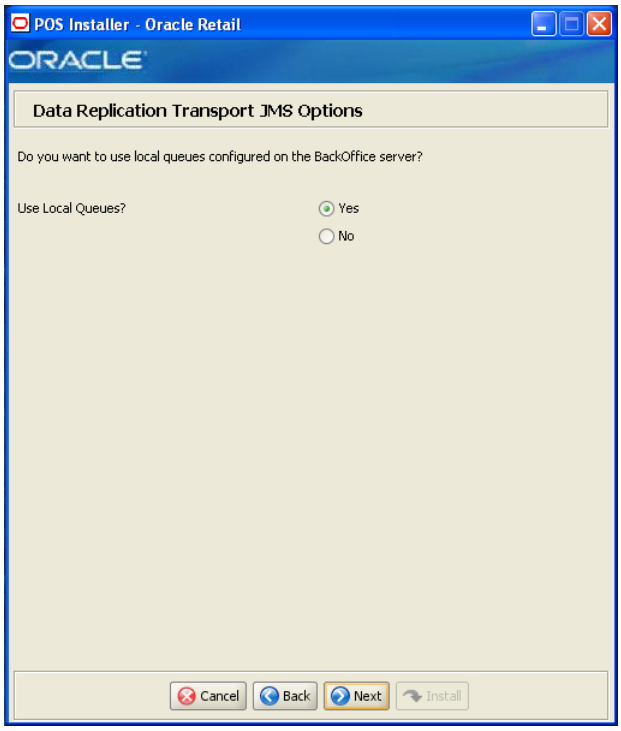
Details	Content
Field Title	SMTP host
Field Description	Host where the SMTP server is running.

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

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

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

Figure A–48 Data Replication Transport JMS Options

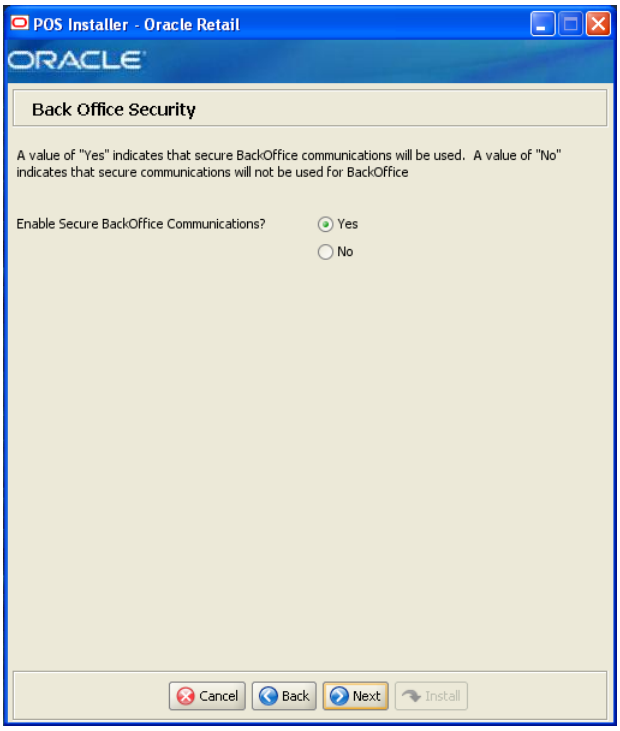


This screen is only displayed if **Send through JMS** is selected on the Data Replication Options screen.

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

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

Figure A–49 Back Office Security

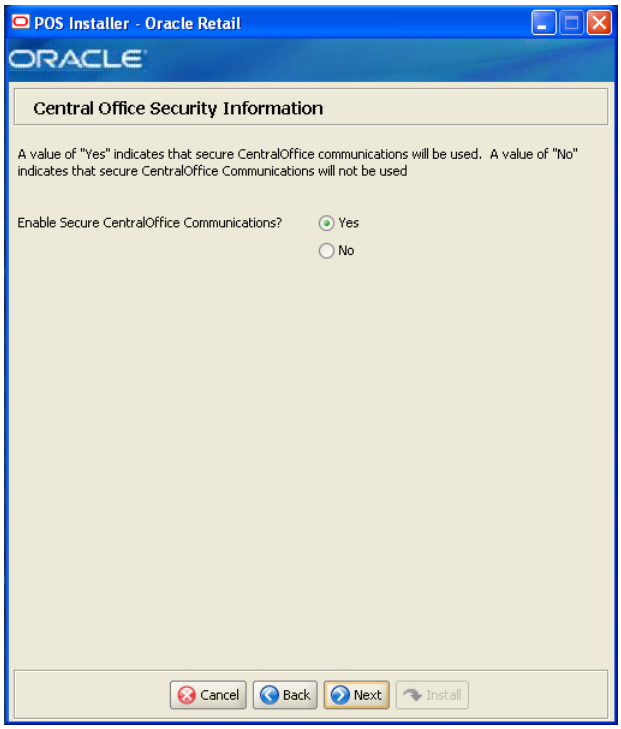


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

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–50 Central Office Security Information

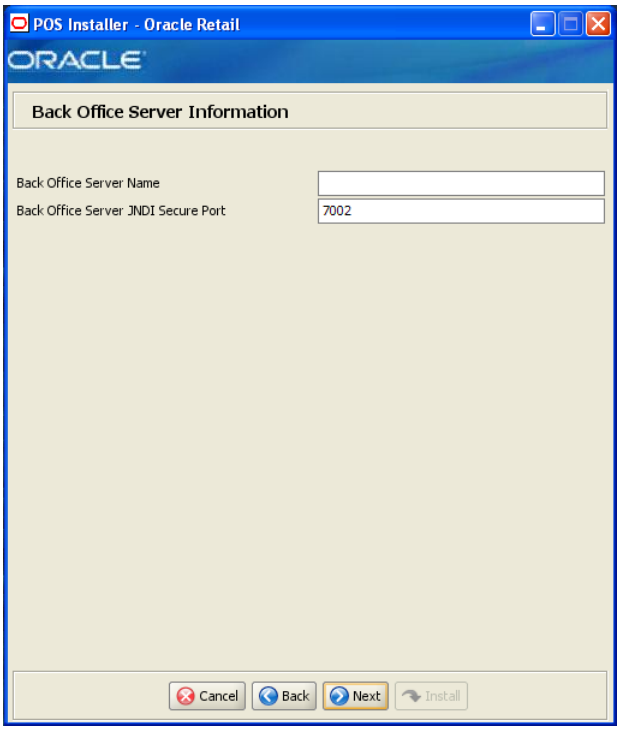


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

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–51 Back Office Server Information



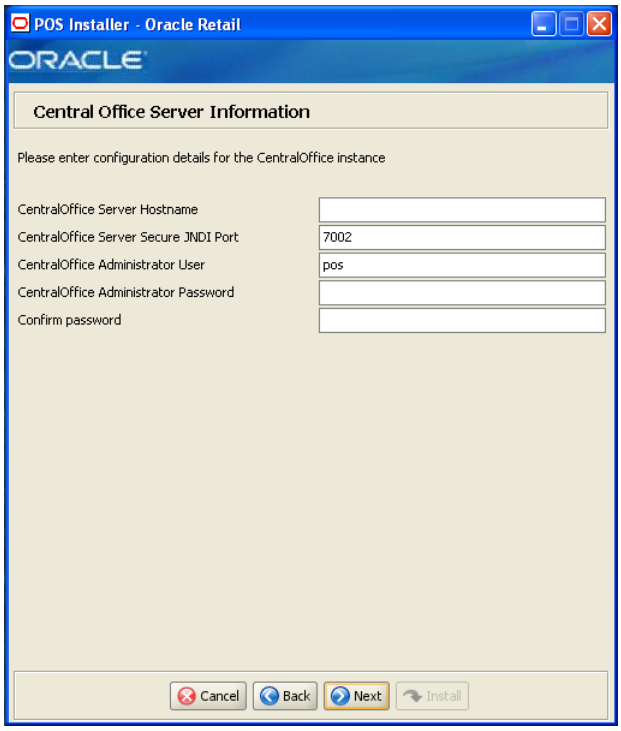
This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

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–52 Central Office Server Information



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

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

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

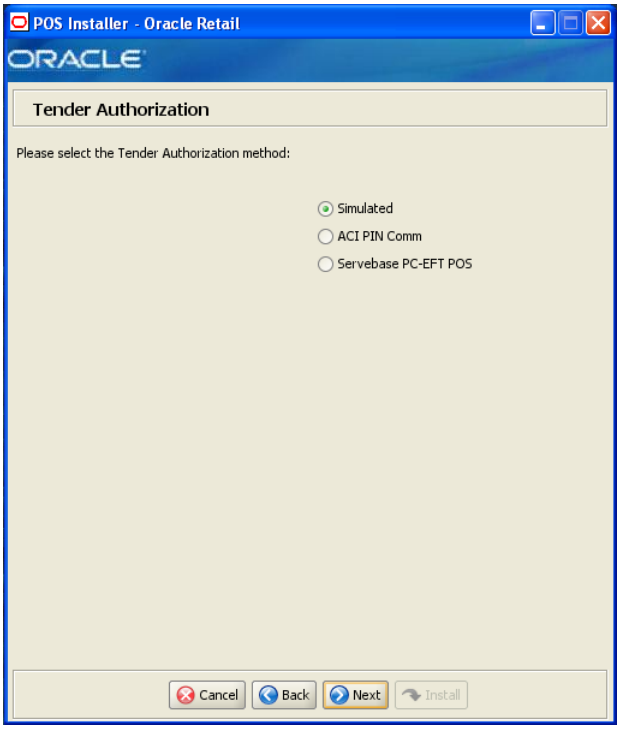
Details	Content
Field Title	Central Office Server Secure JNDI Port
Field Description	Enter the port number for the Central Office application. This is the port number that was selected when the Central Office domain was created.
Example	7002

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

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

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

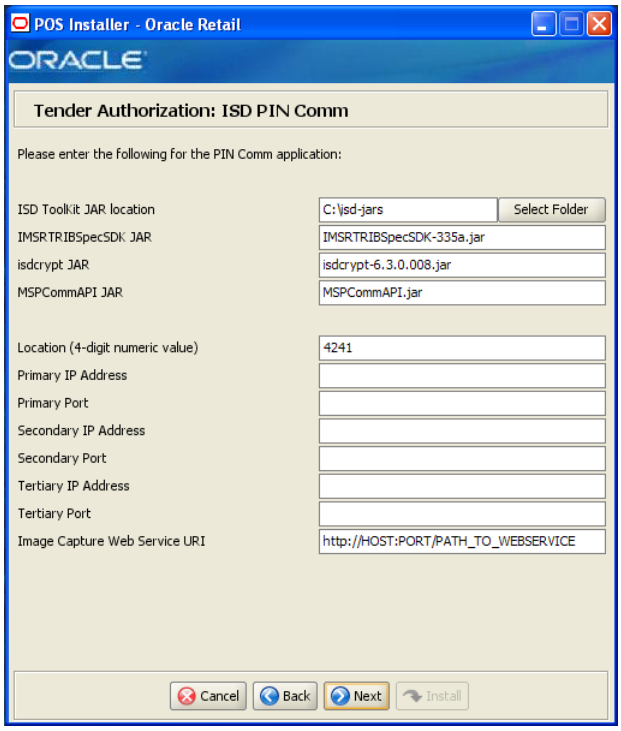
Figure A–53 Tender Authorization



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

Details	Content
Field Title	Please select the tender authorization method
Field Description	Choose where tender authorizations are sent. ▪ If approvals do not leave the store server and are based on values and certain numbers, choose **Simulated**. ▪ If approvals are sent to a third-party system to approve the authorizations, choose **ACI PIN Comm** or **Servebase PC_EFT POS**. **Note:** Demo installations should use the Simulated option.
Example	Simulated

Figure A–54 Tender Authorization: ISD PIN Comm



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

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

Details	Content
Field Title	ISD ToolKit JAR Location
Field Description	Enter the path to the ISD ToolKit JAR file.
Example	`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

Details	Content
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.

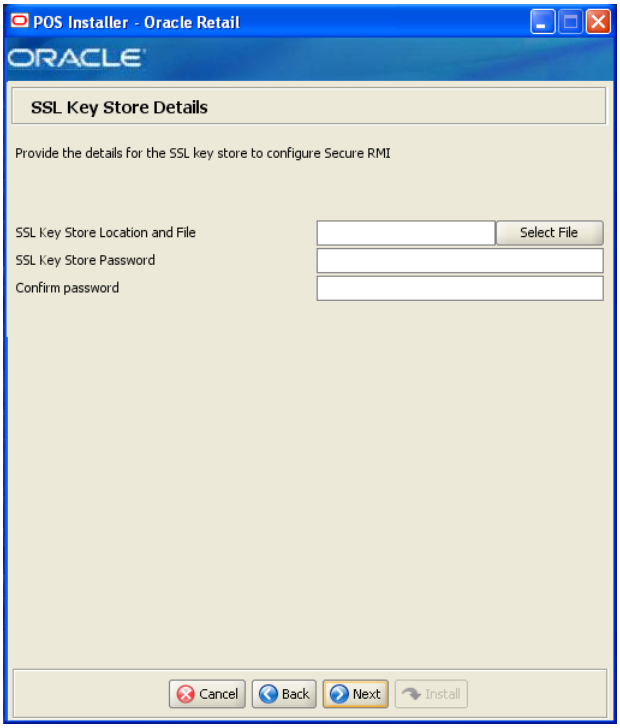
Details	Content
Field Title	Secondary Port
Field Description	Enter the secondary port number used for the communication between the store server and the tender authorizer.

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–55 SSL Key Store Details



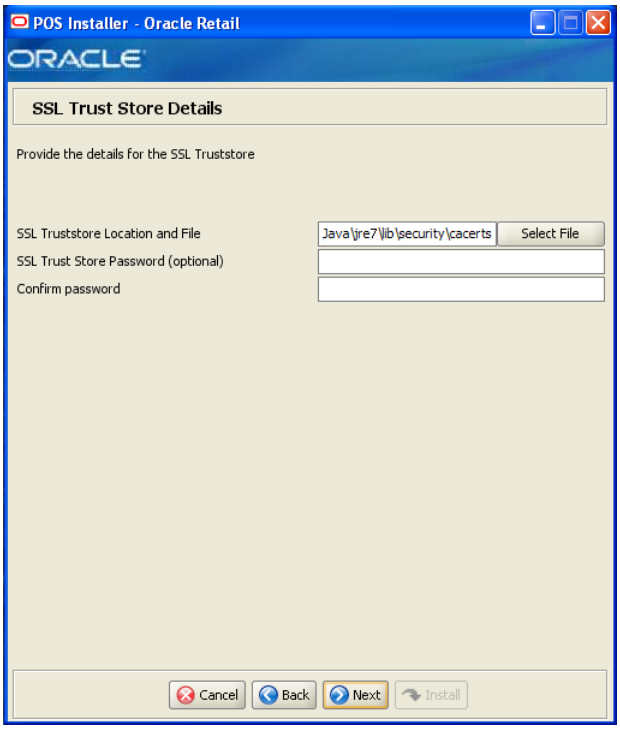
The fields on this screen are described in the following tables.

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

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

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

Figure A–56 SSL Trust Store Details



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

Details	Content
Field Title	SSL Truststore Location and File
Field Description	Enter the location and name of the truststore file.
Example	`C:\Program Files\Java\jre7\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–57 Installation Progress

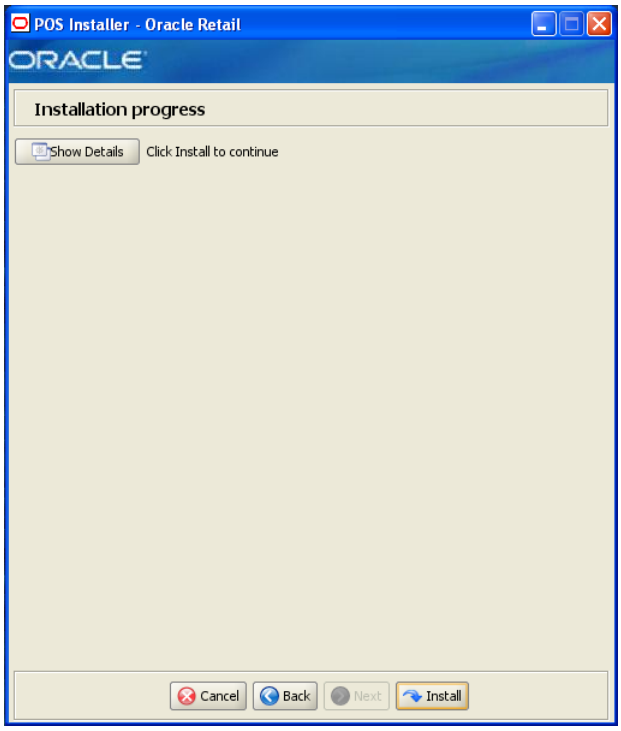


Figure A–58 Install Complete

B

Appendix: Installer Screens for Client Installation on the Oracle Stack

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

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

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

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

Figure B–1 Introduction

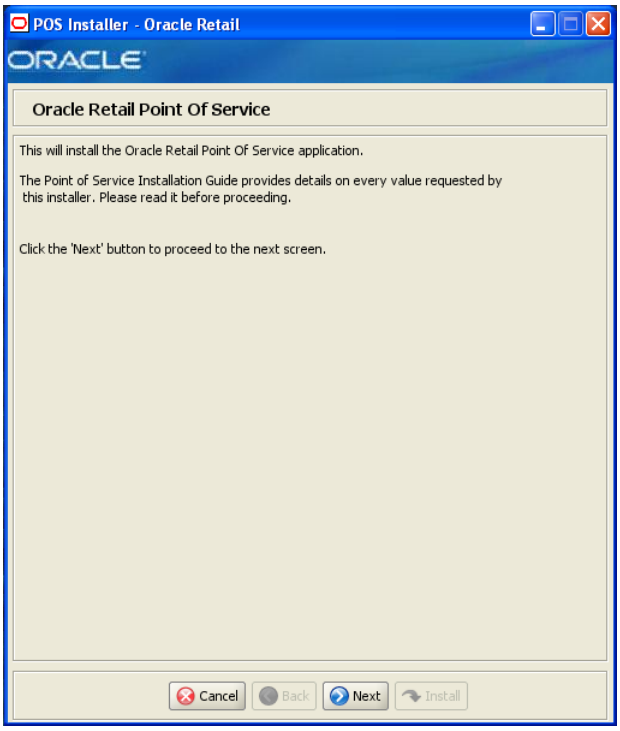
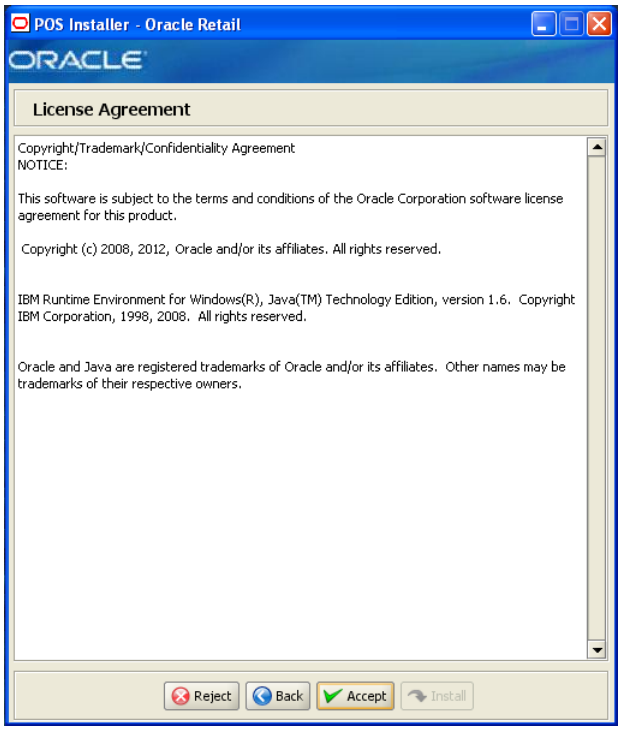


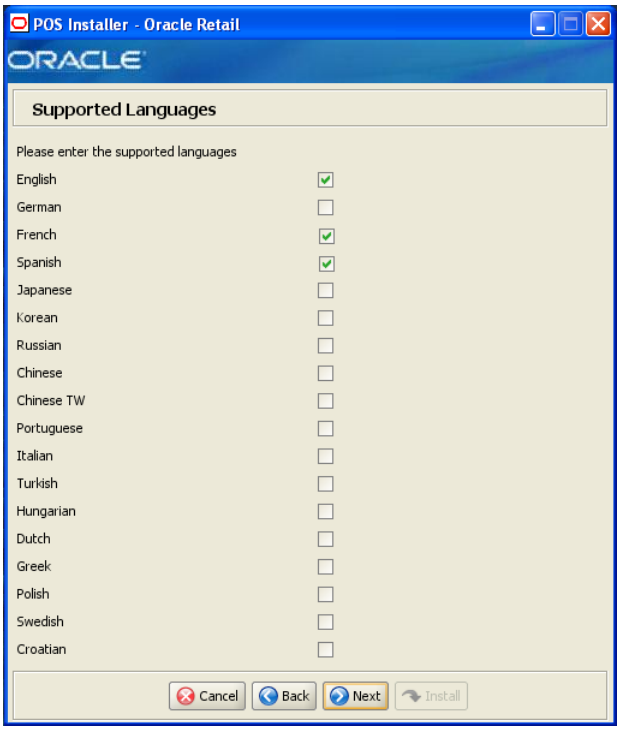
Figure B–2 Previous POS Install

Figure B–3 License Agreement



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

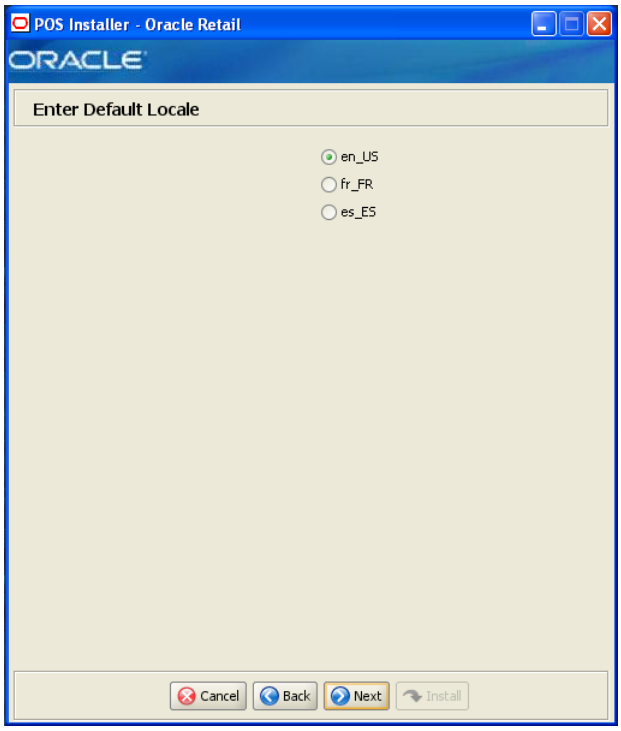
Figure B–4 Supported Languages



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

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

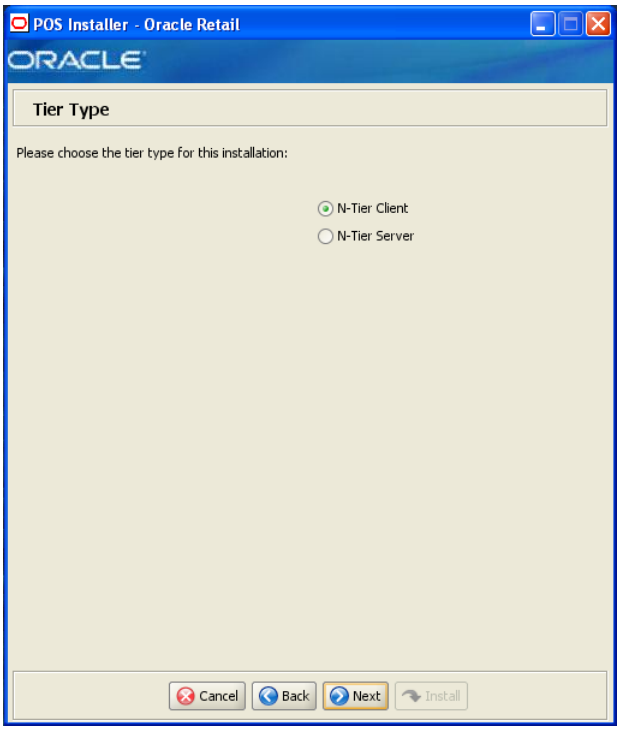
Figure B–5 Enter Default Locale



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

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

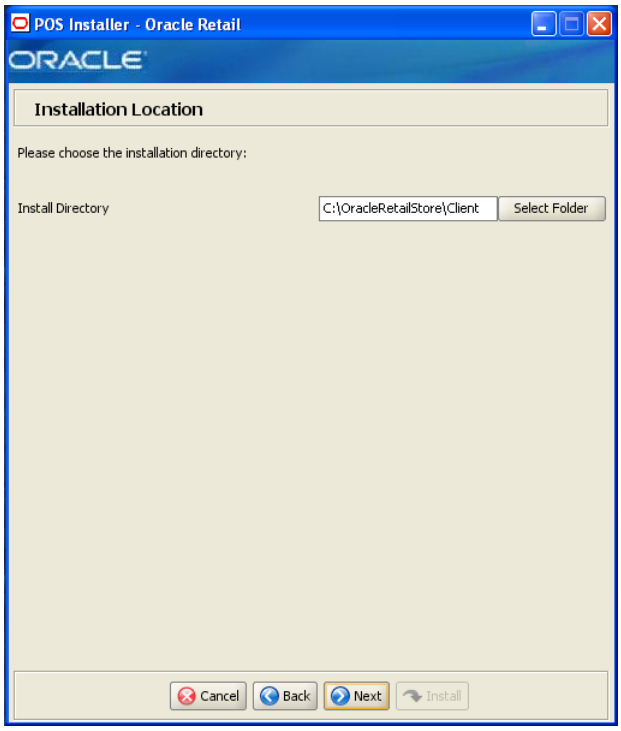
Figure B–6 Tier Type



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

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

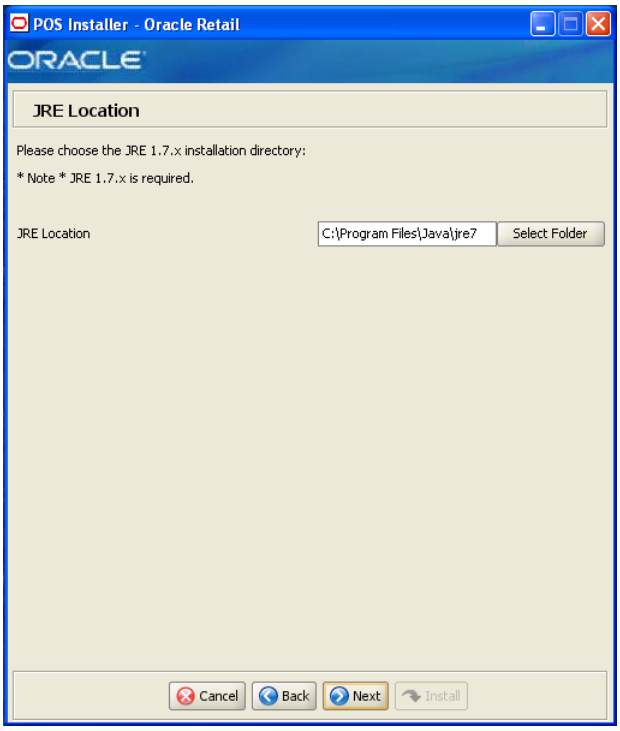
Figure B–7 Installation Location



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

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

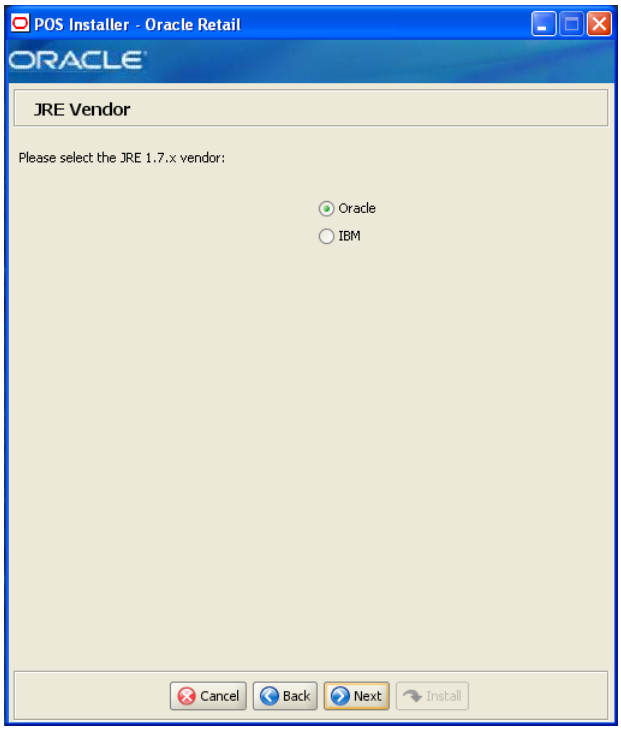
Figure B–8 JRE Location



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

Details	Content
Field Title	JRE Location
Field Description	Enter the location where the JRE is installed.
Example	`C:\Program Files\Java\jre7`

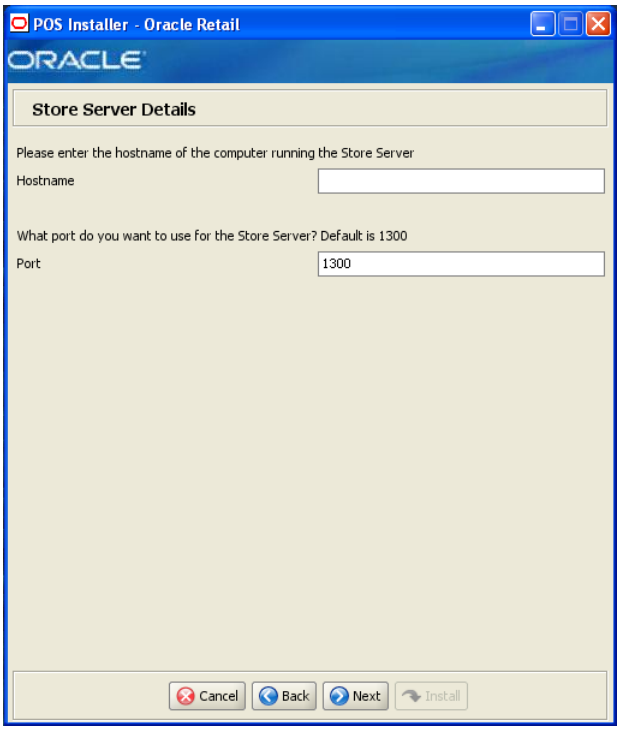
Figure B–9 JRE Vendor



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

Details	Content
Field Title	Please select the JRE 1.7.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

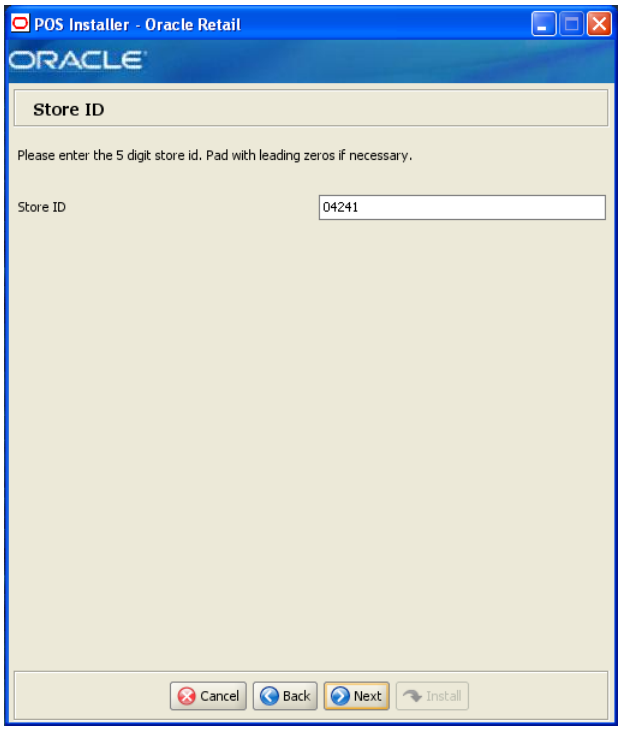


The fields on this screen are described in the following tables.

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

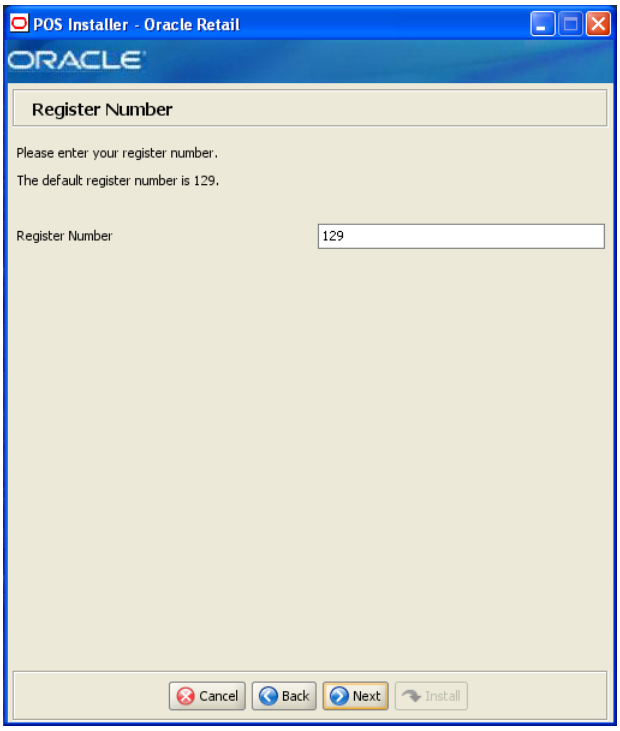
Figure B–11 Store ID



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

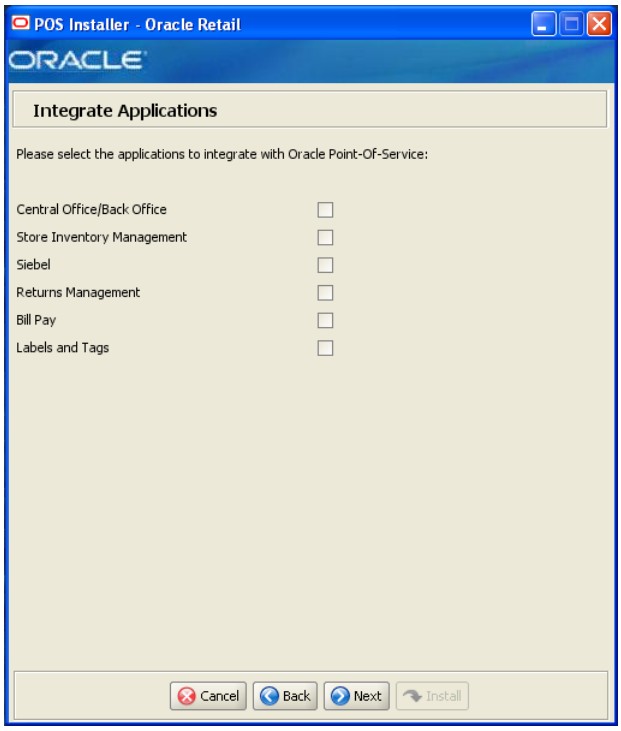
Figure B–12 Register Number



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



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

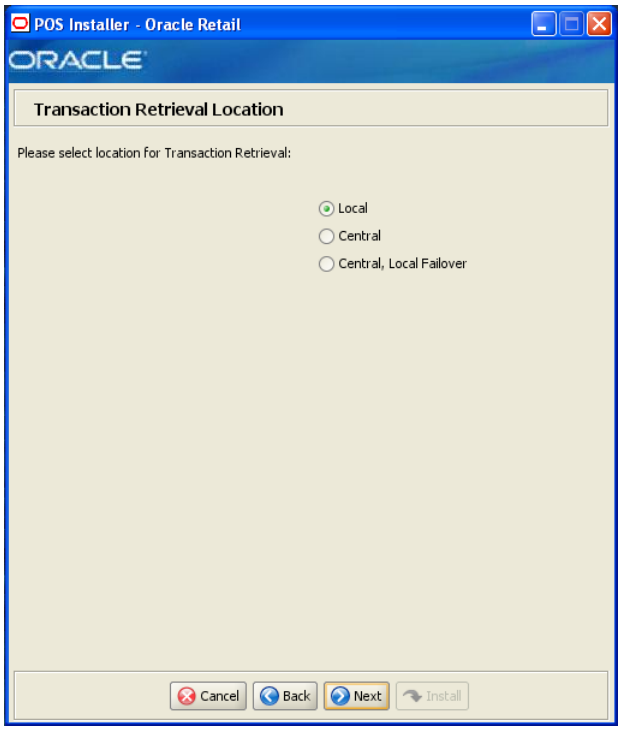
Figure B–14 Application Server Type

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

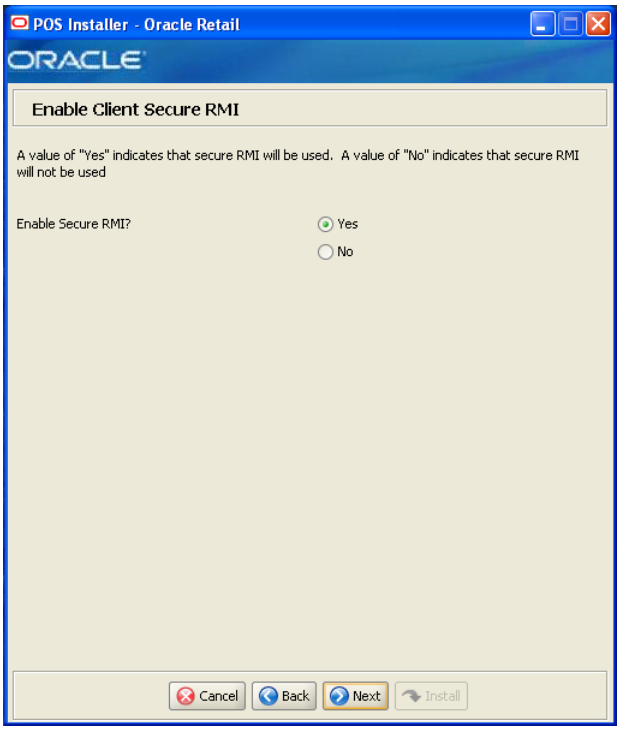


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

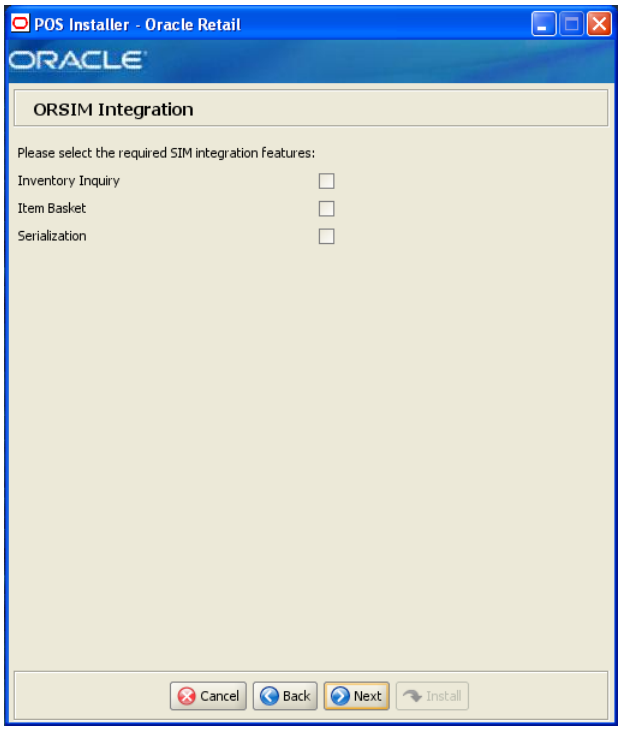
Figure B–16 Enable Client Secure RMI



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

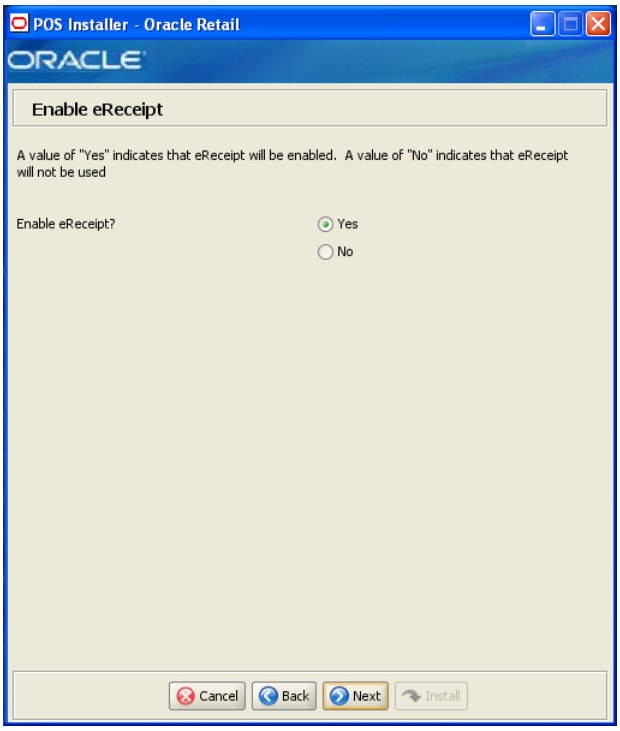


This screen is only displayed if **Store Inventory Management** is selected on the Integrate Applications screen.

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**.

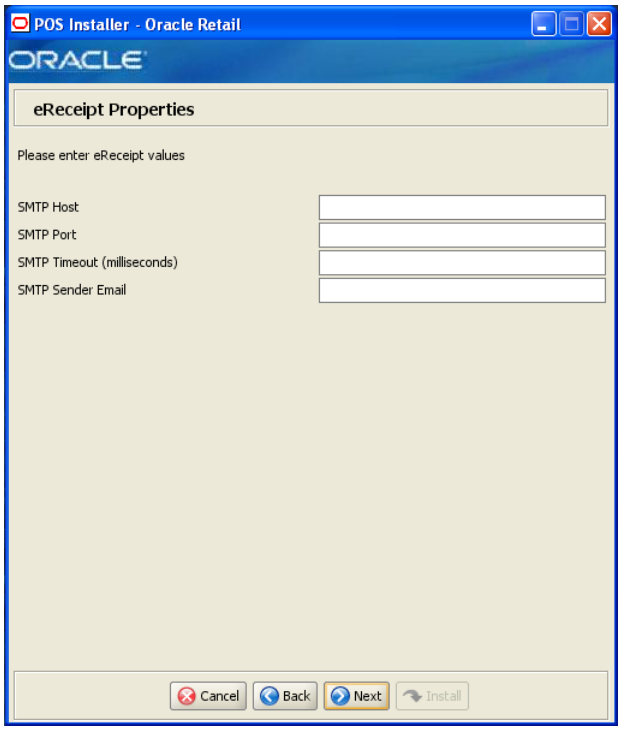
Figure B–18 Enable eReceipt



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



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.

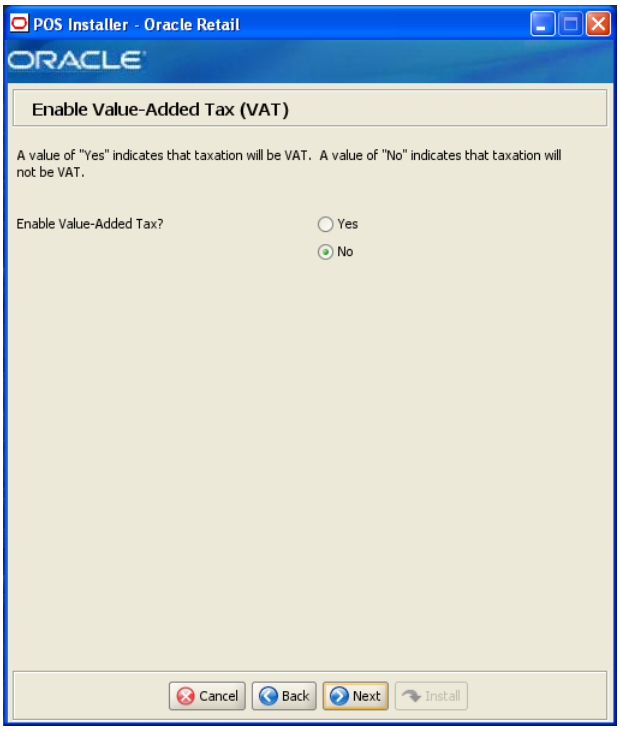
Details	Content
Field Title	SMTP Host
Field Description	Enter the host name for the SMTP server.

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)



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 Manager Settings

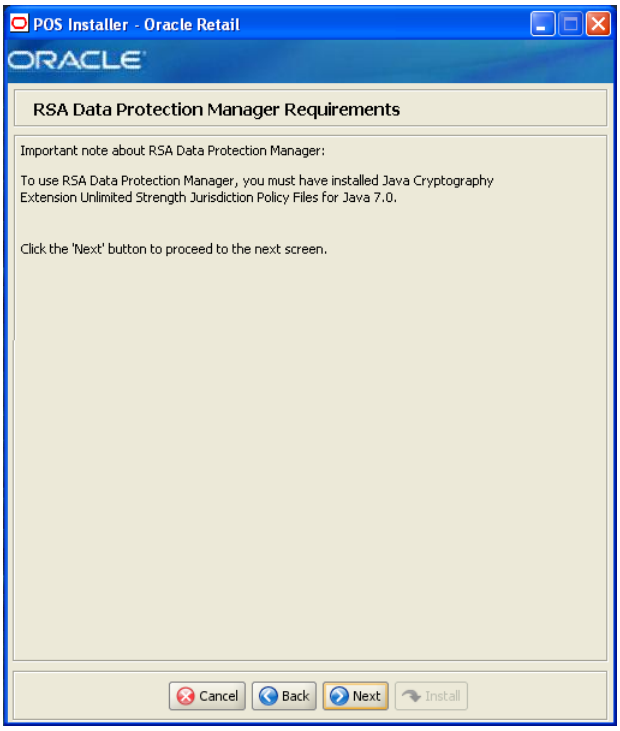
This screen is used to configure the Encryption Key Manager.

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

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

Details	Content
Field Title	Select Key Manager
Field Description	Provider for Key Manager: ■ To use the RSA Data Protection Manager package, select **RSA Data Protection Manager**. The next screen displayed is Figure B–22. ■ To use the simulated key management package, select **Simulator**. The next screen displayed is Figure B–25.
Example	RSA Data Protection Manager

Figure B–22 RSA Data Protection Manager Requirements



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

Figure B–23 Security Setup: RSA Client JAR Files

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

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

Details	Content
Field Title	RSA Client JAR Files Directory
Field Description	Choose the directory where the following Key Manager jar files are located: ■ certj.jar ■ cryptojce.jar ■ cryptojcommon.jar ■ jcm.jar ■ kmsclient.jar ■ sslj.jar
Example	`C:\`

Figure B–24 RSA Client Configuration

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

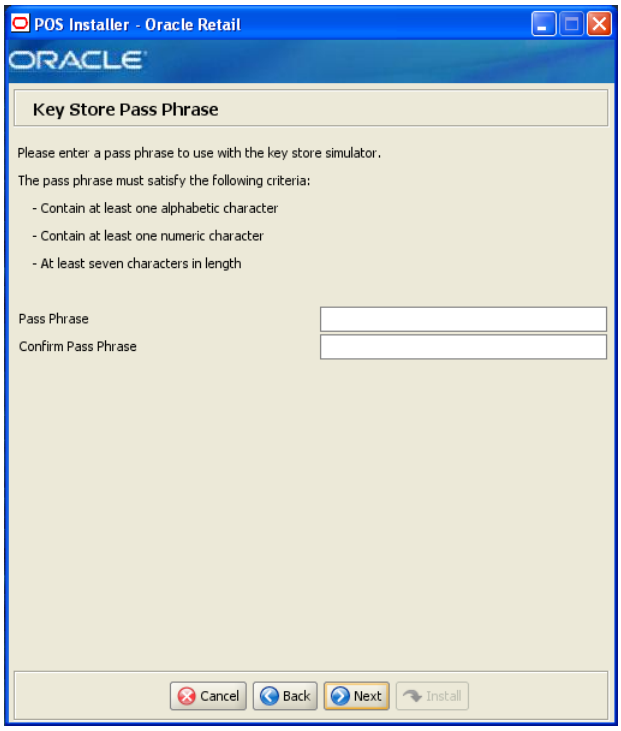
The fields on this screen are described in the following tables.

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

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

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

Figure B–25 Key Store Pass Phrase for Simulator Key Manager



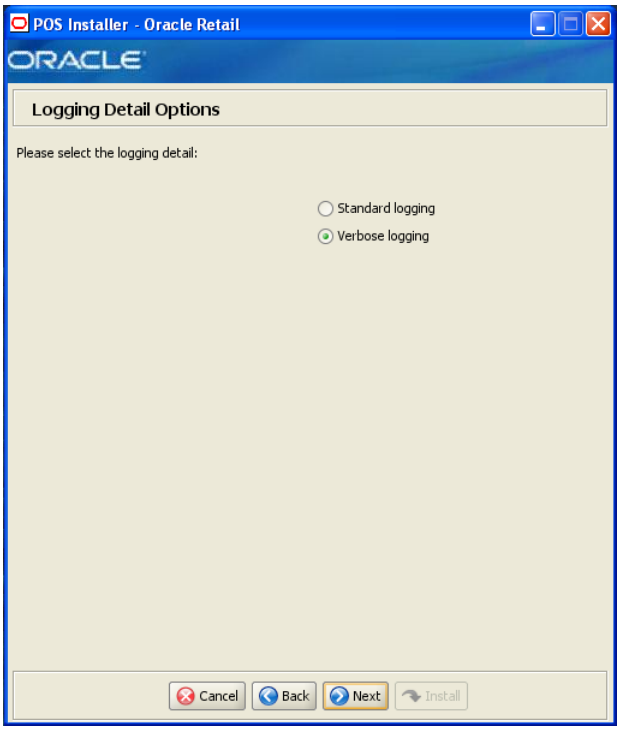
This screen is only displayed if **Simulator** is selected for the Key Manager on the Security Setup: Key Manager Settings screen.

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

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

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

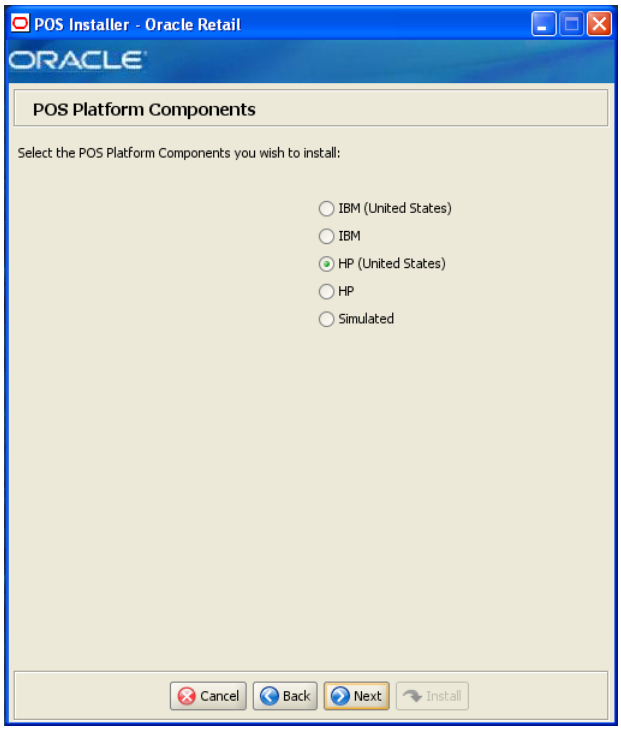
Figure B–26 Logging Detail Options



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

Details	Content
Field Title	Please select the logging detail
Field Description	Choose the level of client logging. ▪ To only log some of the messages, choose **Standard Logging**. ▪ To log all of the messages, choose **Verbose Logging**.
Example	Verbose logging

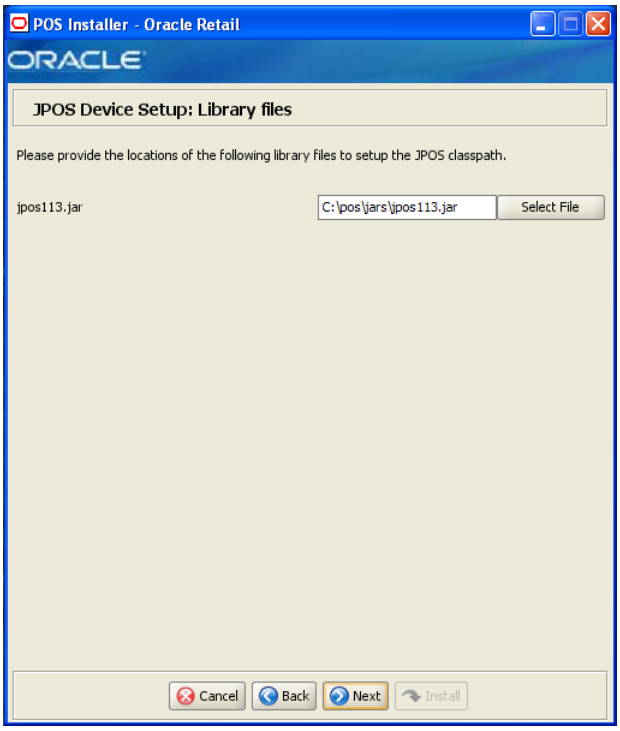
Figure B–27 POS Platform Components



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

Details	Content
Field Title	Select the POS Platform Components you wish to install
Field Description	From the platform components, choose the type of register and whether the devices are intended for use in or outside the United States: ▪ To use an 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)

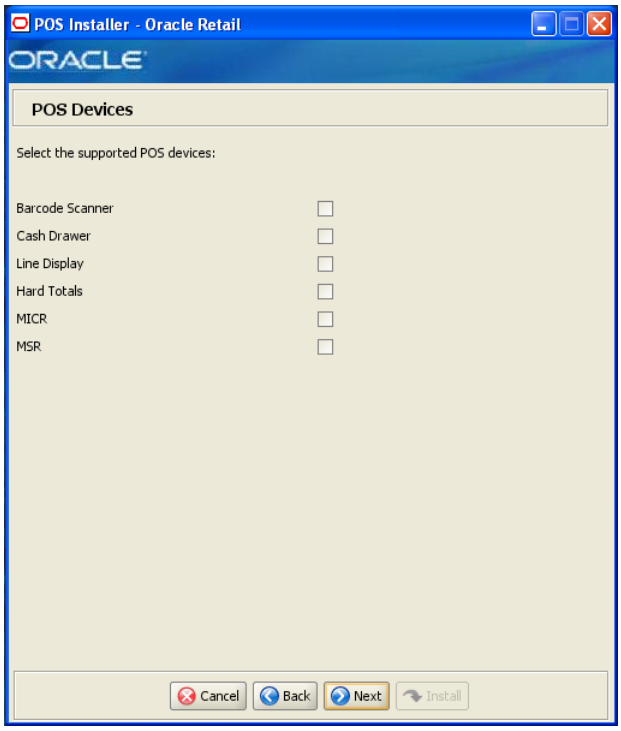
Figure B–28 JPOS Device Setup: Library Files



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–29 POS Devices

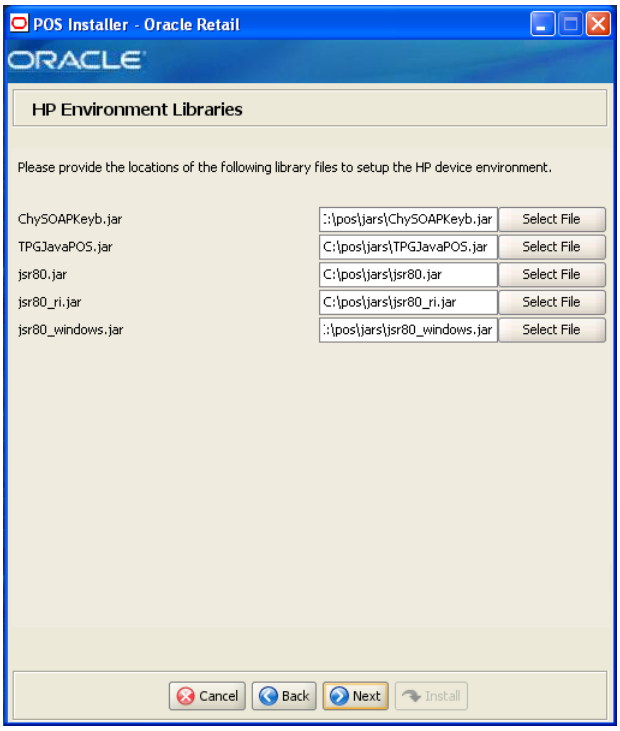


This screen is only displayed if any component other than **Simulated** is selected on the POS Platform Components screen.

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

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

Figure B–30 HP Environment Libraries



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

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

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`

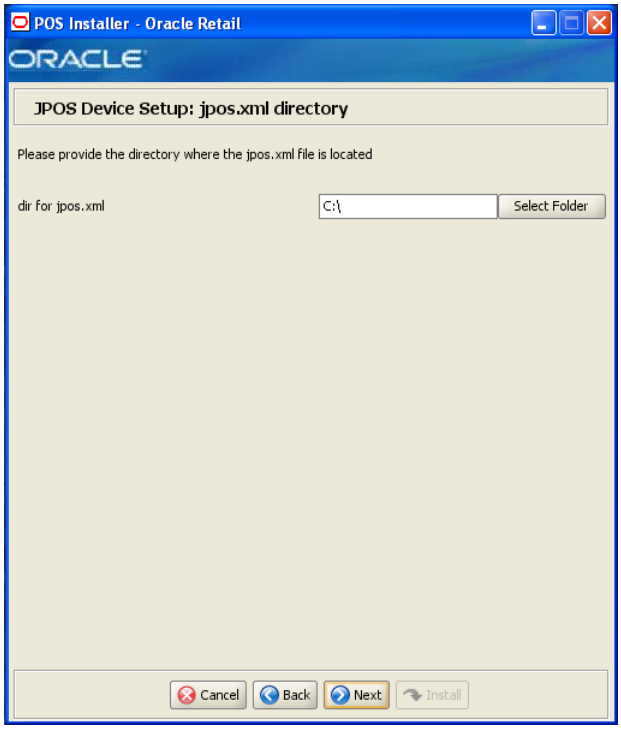
Details	Content
Field Title	jsr80.jar
Field Description	Enter the location of the jar file.
Example	`C:\pos\jars\jsr80.jar`

Details	Content
Field Title	jsr80_ri.jar

Details	Content
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–31 JPOS Device Setup: jpos.xml directory

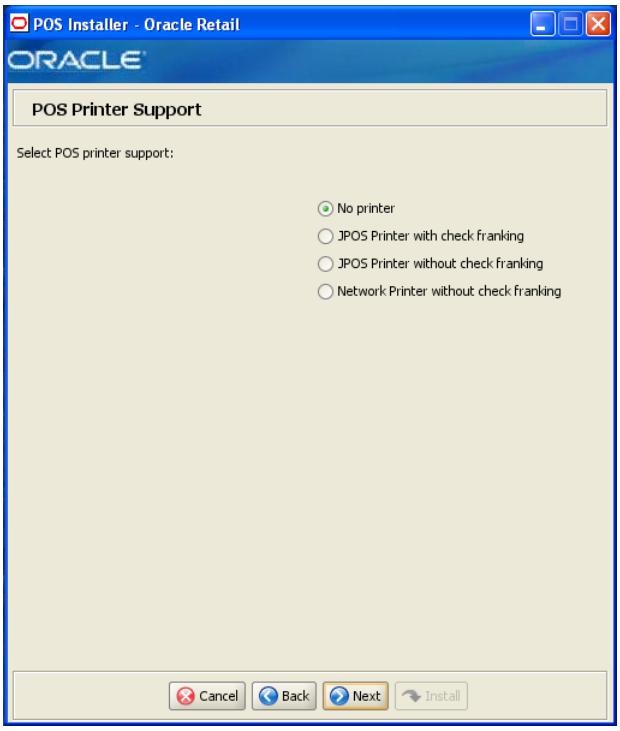


This screen is only displayed if any component other than **Simulated** is selected on the POS Platform Components screen.

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

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

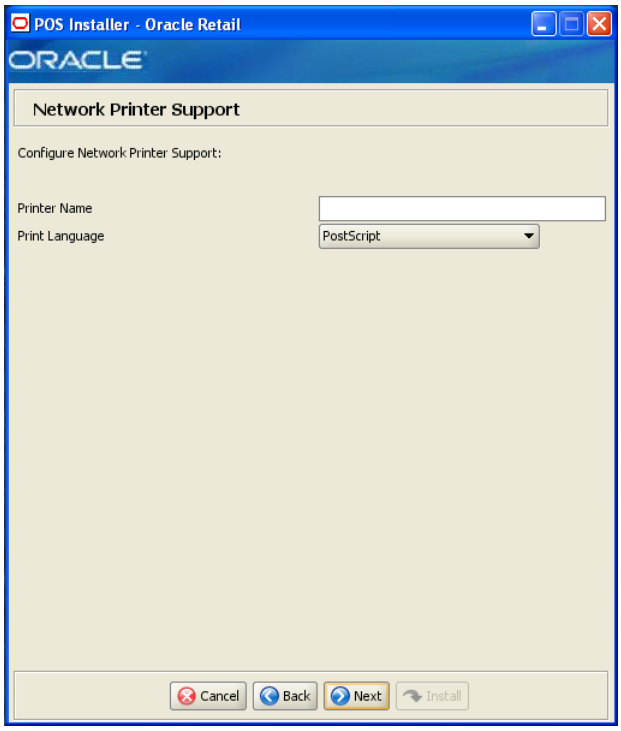
Figure B–32 POS Printer Support



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

Details	Content
Field Title	Select POS Printer Support
Field Description	Choose what is supported for a printer attached to the register or select a network printer.
Example	No Printer

Figure B–33 Network Printer Support Configuration



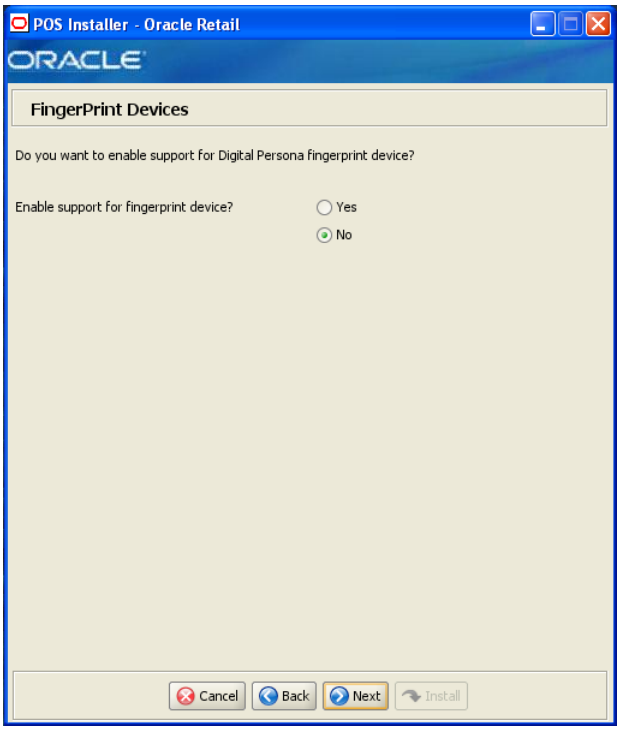
This screen is only displayed if **Network Printer without check franking** is selected on the POS Printer Support screen.

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

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

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

Figure B–34 Fingerprint Devices

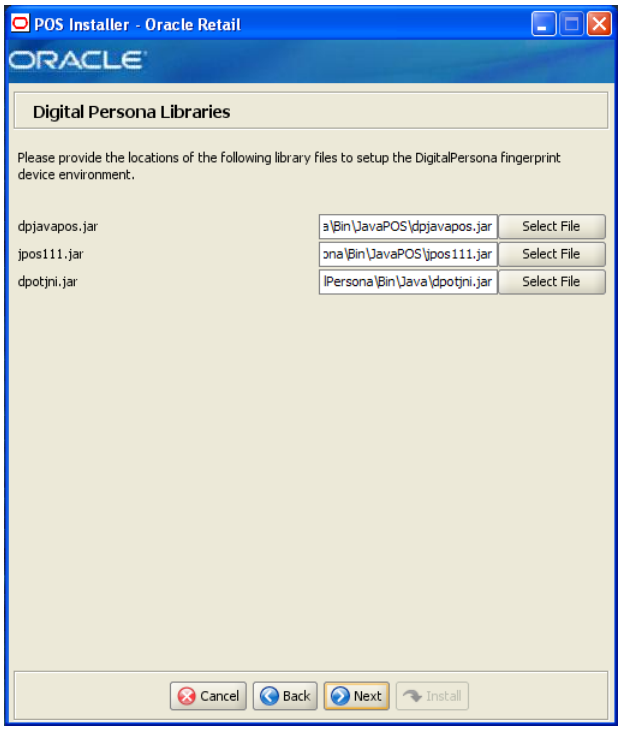


This screen is only displayed if **HP (United States)** or **HP** is selected on the POS Platform Components screen.

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–35 Digital Persona Libraries



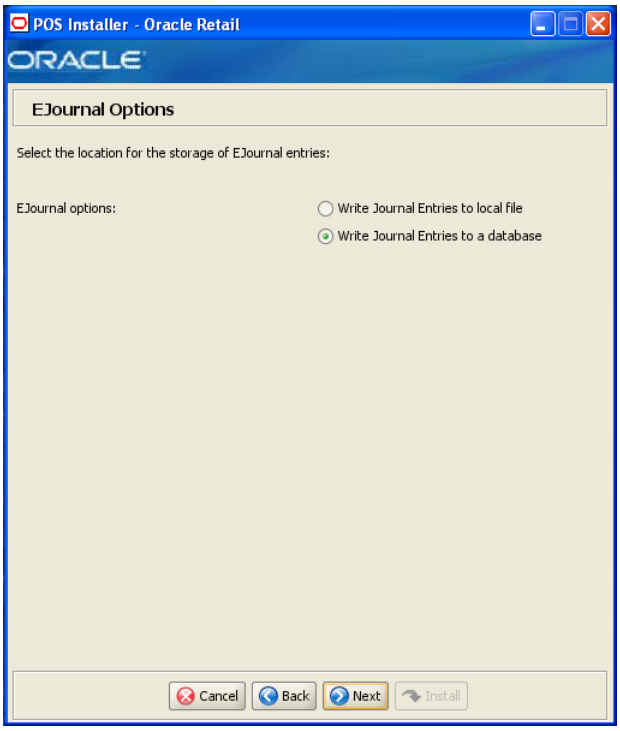
This screen is only displayed if **Yes** is selected on the Fingerprint Devices screen. The fields on this screen are described in the following tables.

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

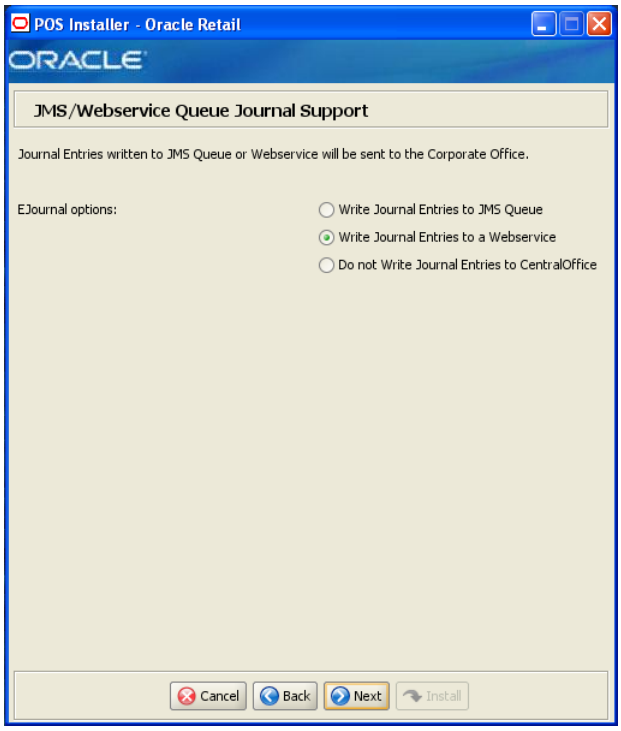
Figure B–36 EJournal Options



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

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

Figure B–37 JMS /Webservice Queue Journal Support

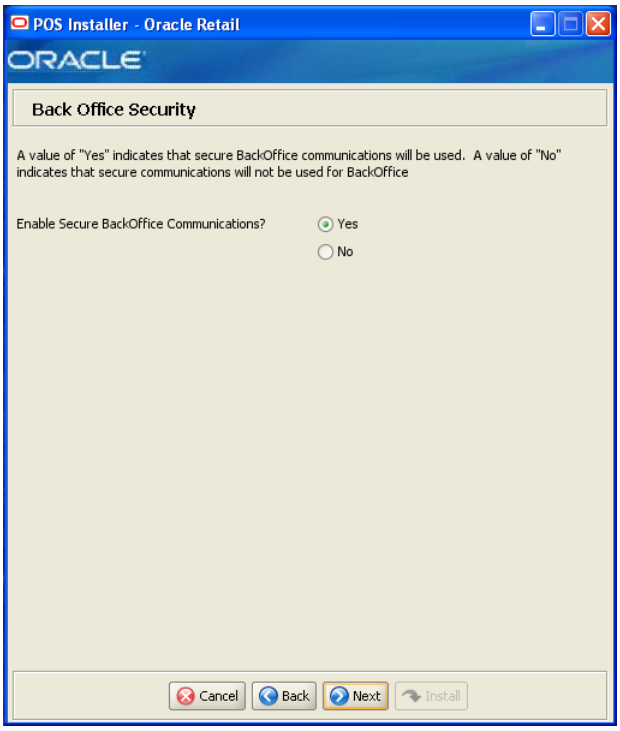


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

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

Figure B–38 Back Office Security

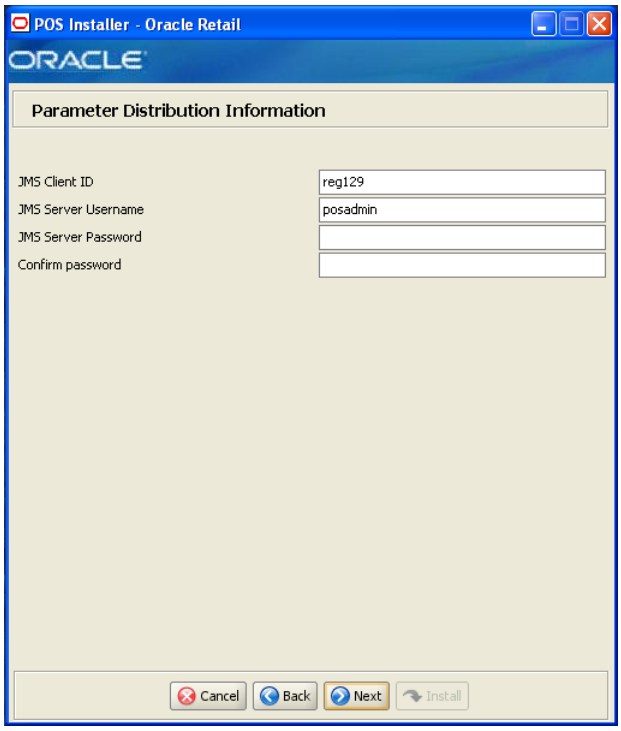


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

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–39 Parameter Distribution Information



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

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

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

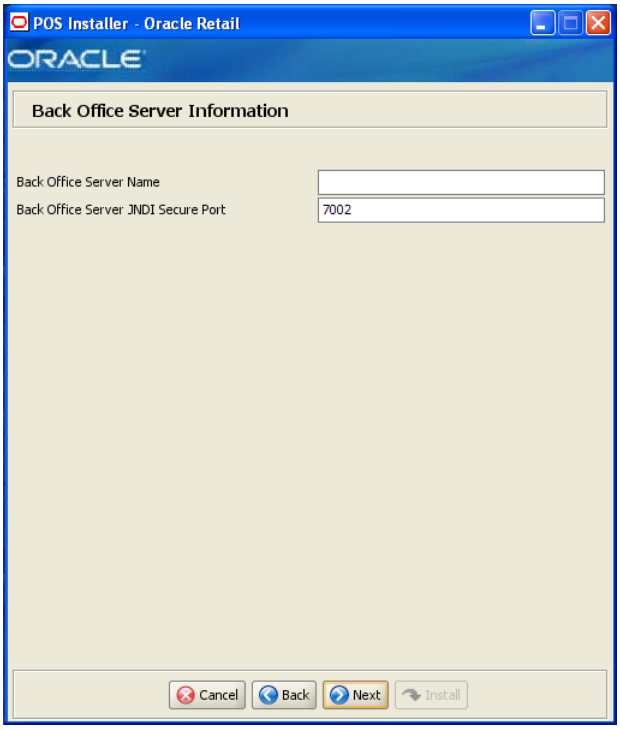
Details	Content
Field Title	JMS Username
Field Description	Identifier of the JMS user for receiving parameter updates.
Example	posadmin

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

Details	Content
Field Title	Confirm Password

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

Figure B–40 Back Office Server Information



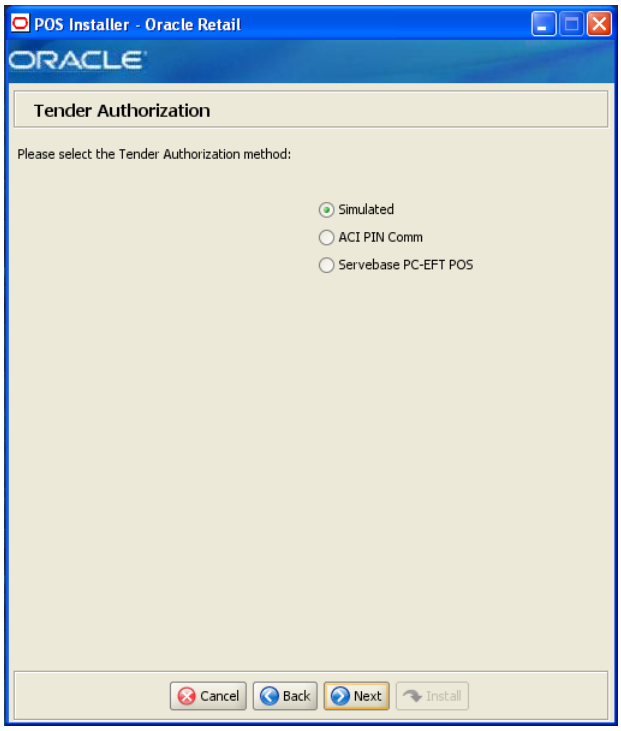
This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

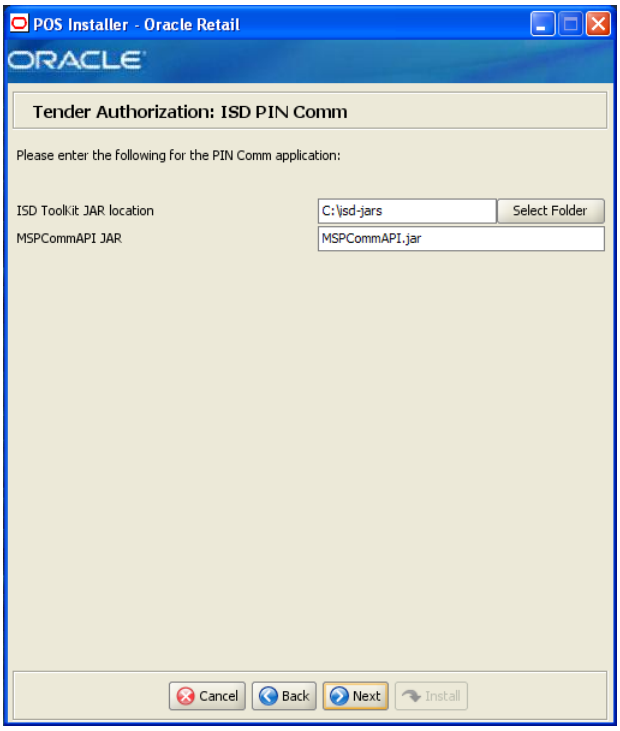
Figure B–41 Tender Authorization



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

Details	Content
Field Title	Please select the tender authorization method
Field Description	Choose where tender authorizations are sent. ▪ If approvals do not leave the store server and are based on values and certain numbers, choose **Simulated**. ▪ If approvals are sent to a third-party system to approve the authorizations, choose **ACI PIN Comm** or **Servebase PC_EFT POS**. **Note:** Demo installations should use the Simulated option.
Example	Simulated

Figure B–42 Tender Authorization: ISD PIN Comm



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

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

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

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

Figure B–43 Tender Authorization: Servebase PC-EFT

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

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

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

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

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

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

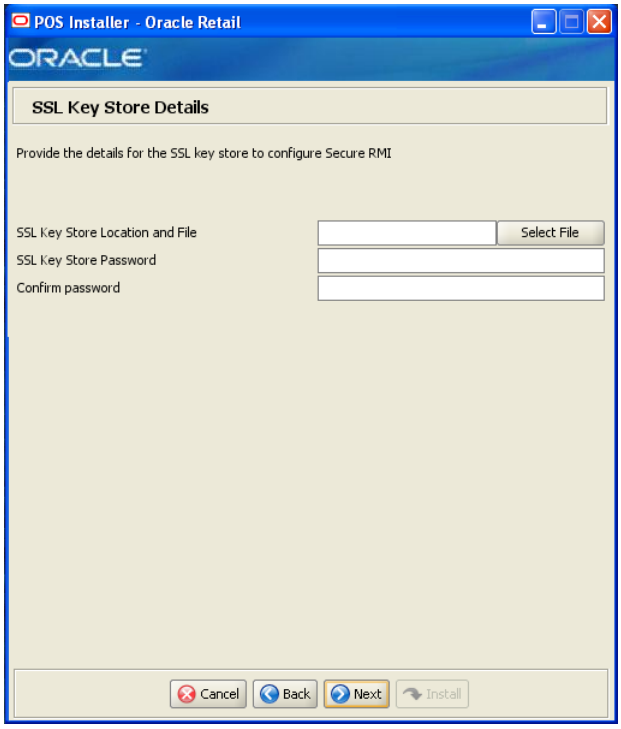
Details	Content
Field Title	Site
Field Description	Enter the site to access the PXP Solutions application.

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

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

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

Figure B–44 SSL Key Store Details



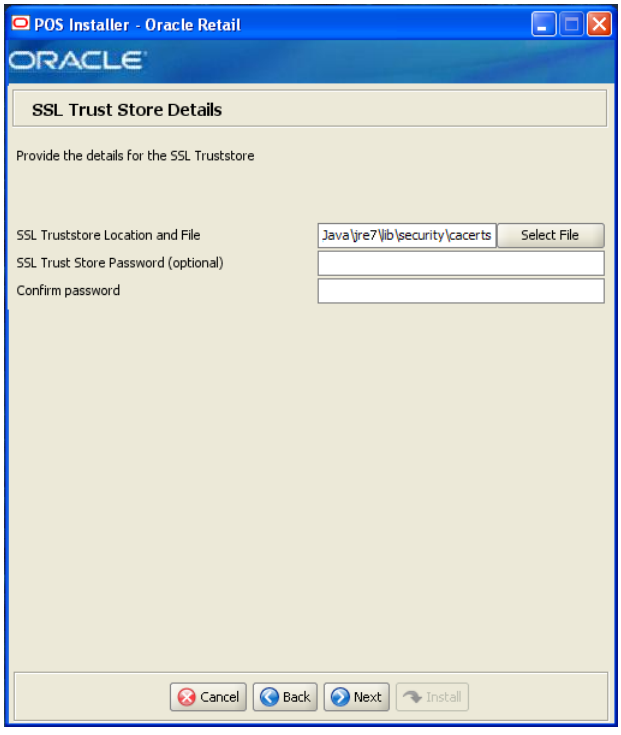
The fields on this screen are described in the following tables.

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

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

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

Figure B–45 SSL Trust Store Details



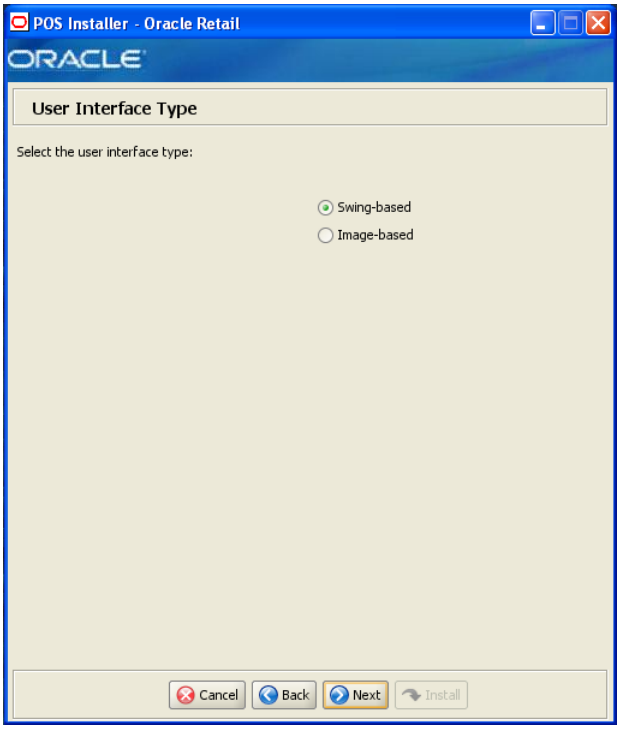
The fields on this screen are described in the following tables.

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\jre7\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–46 User Interface Type



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

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

Figure B–47 Installation Progress

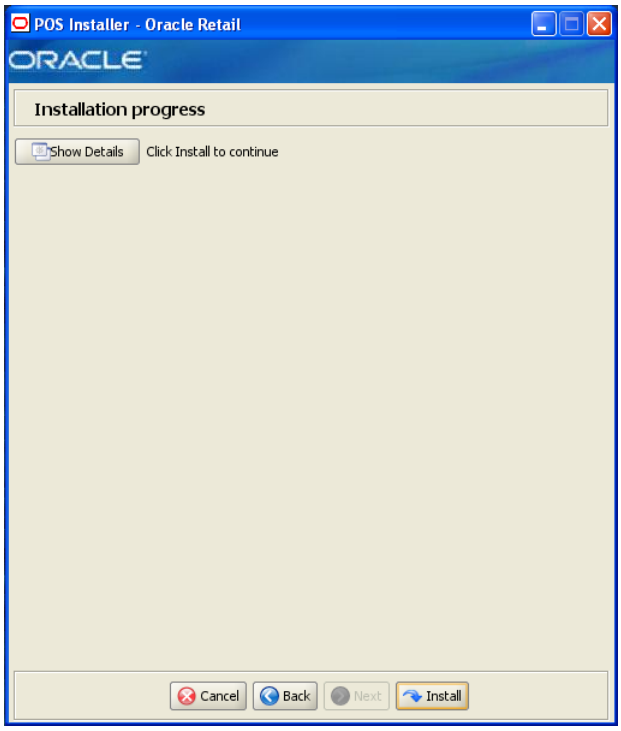


Figure B–48 Install Complete

C

Appendix: Installer 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

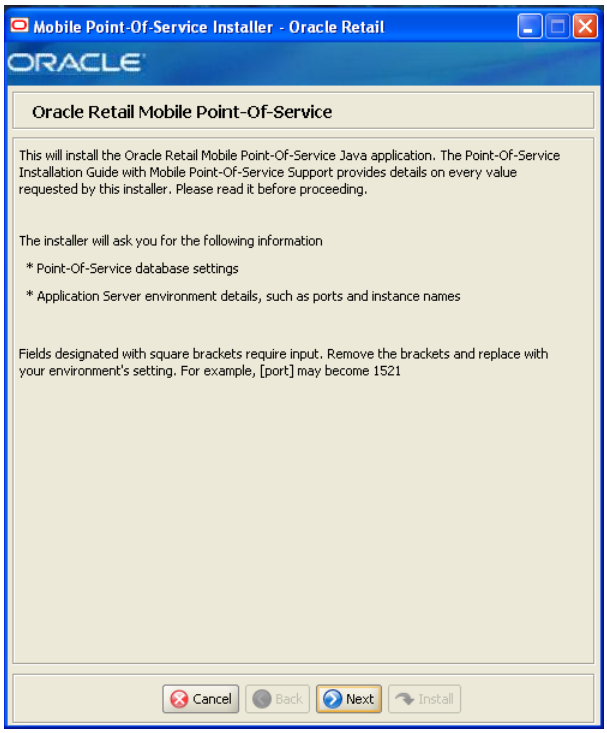


Figure C–2 Requirements

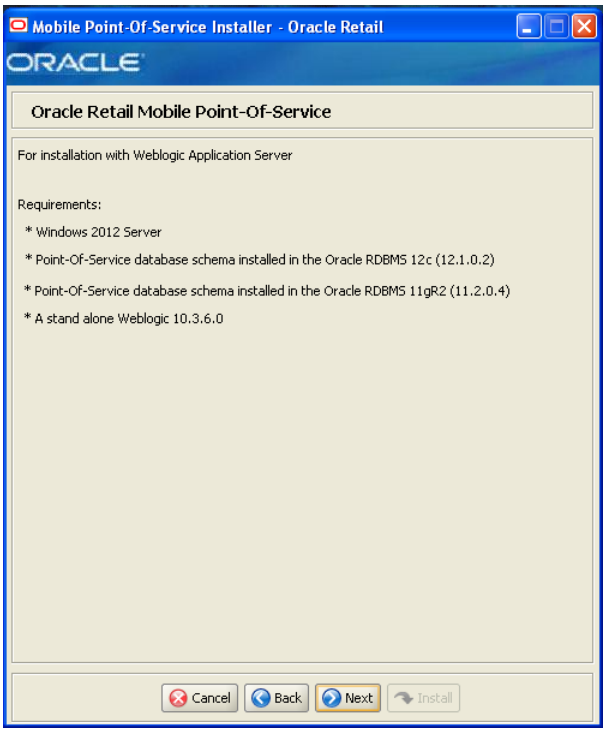
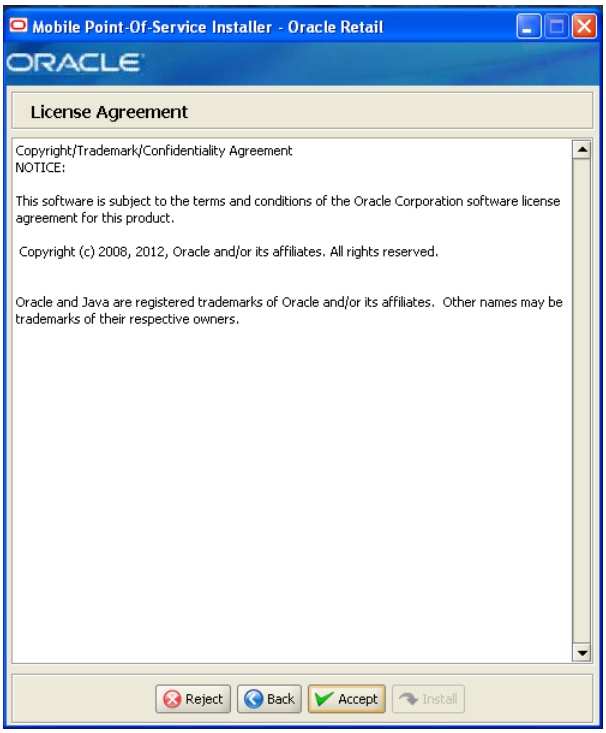
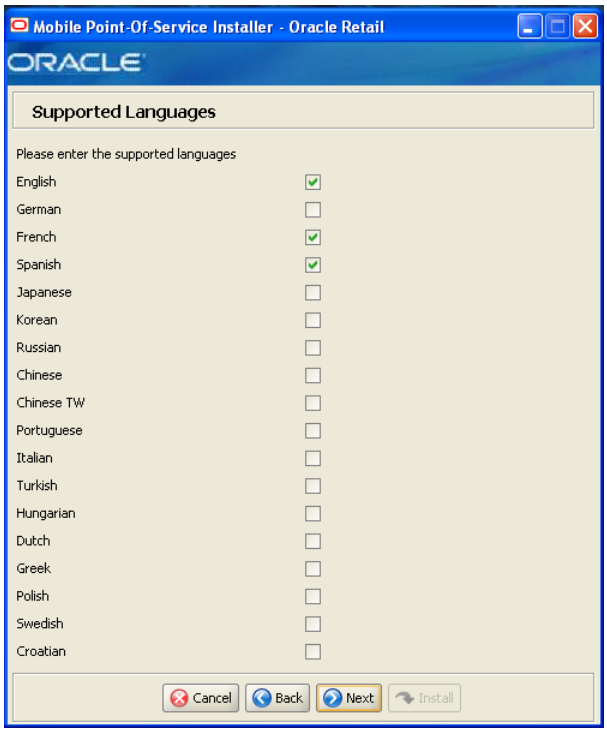


Figure C–3 License Agreement



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

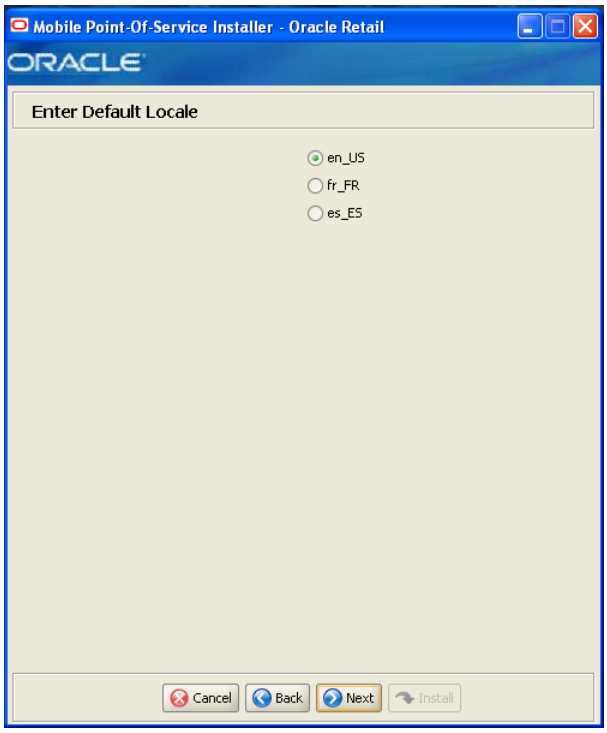
Figure C–4 Supported Languages



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

Details	Content
Field Title	Please enter the supported languages
Field Description	Select the languages that will be available for the 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

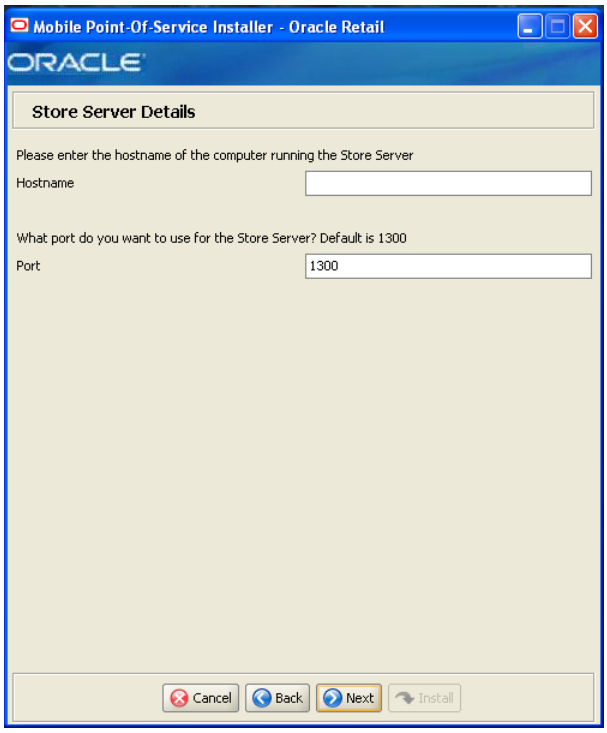
Figure C–5 Enter Default Locale



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

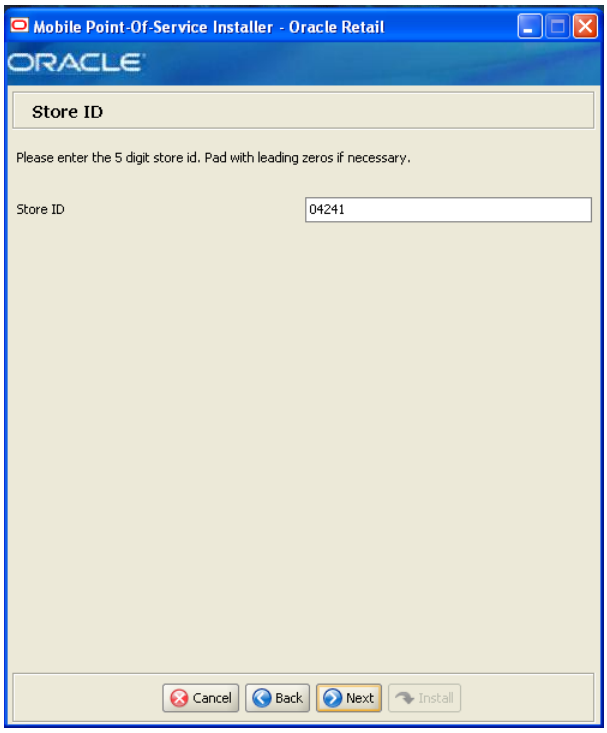


The fields on this screen are described in the following tables.

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

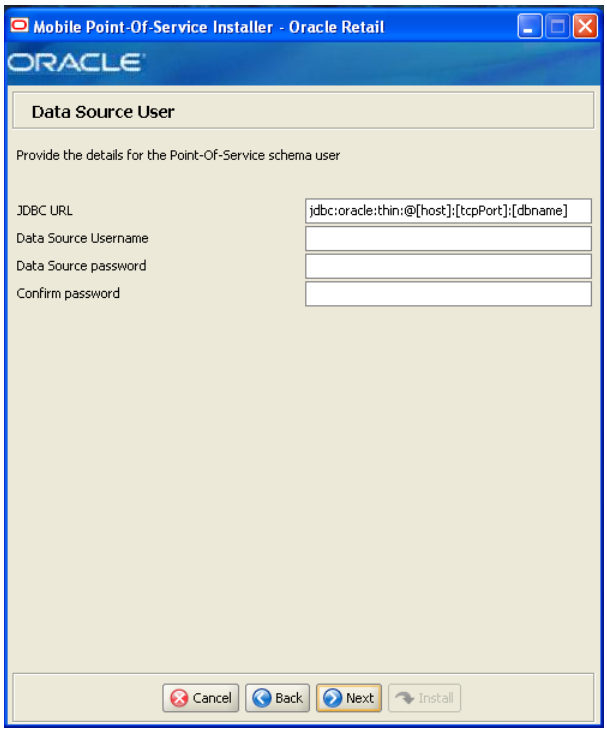
Figure C–7 Store ID



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



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

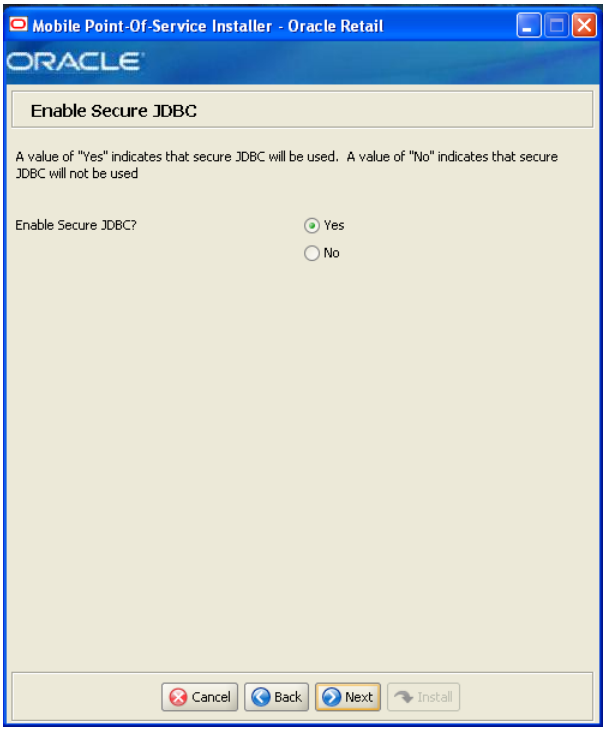
Details	Content
Field Title	JDBC URL
Field Description	Enter the URL used by the Mobile Point-of-Service application to access the database schema. For the expected syntax, see Appendix E.
Example	`jdbc:oracle:thin:@DB_HOST_NAME:1521:DB_NAME`

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.

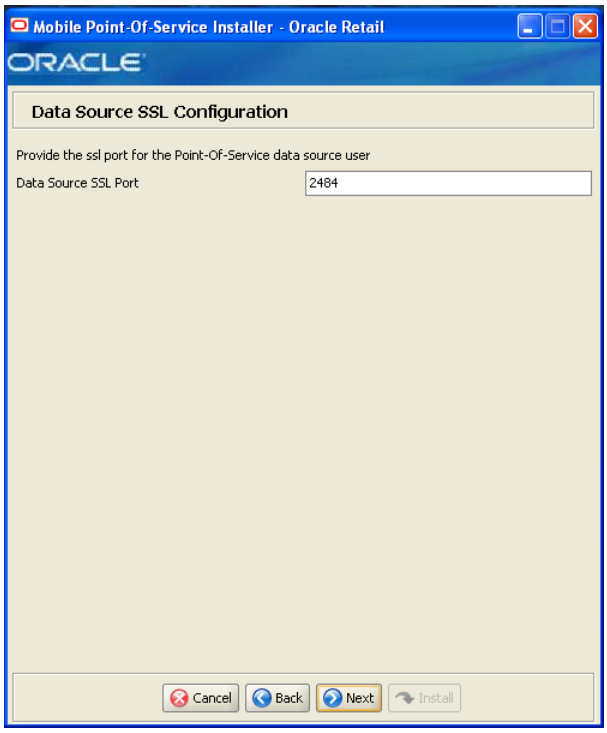
Figure C–9 Enable Secure JDBC



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

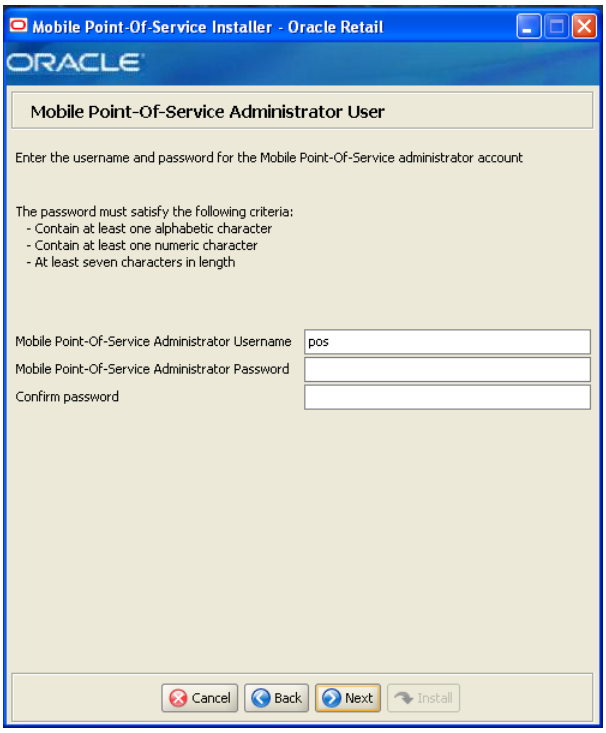
Figure C–10 Data Source SSL Configuration



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



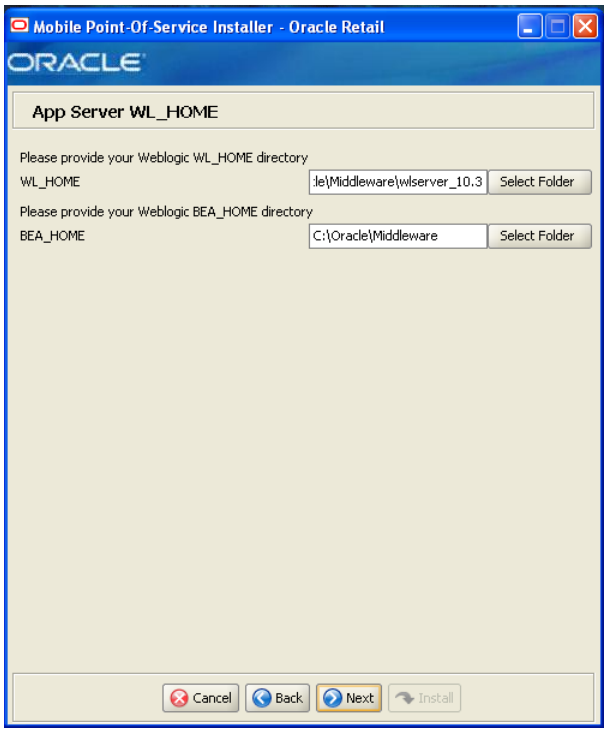
The fields on this screen are described in the following tables.

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

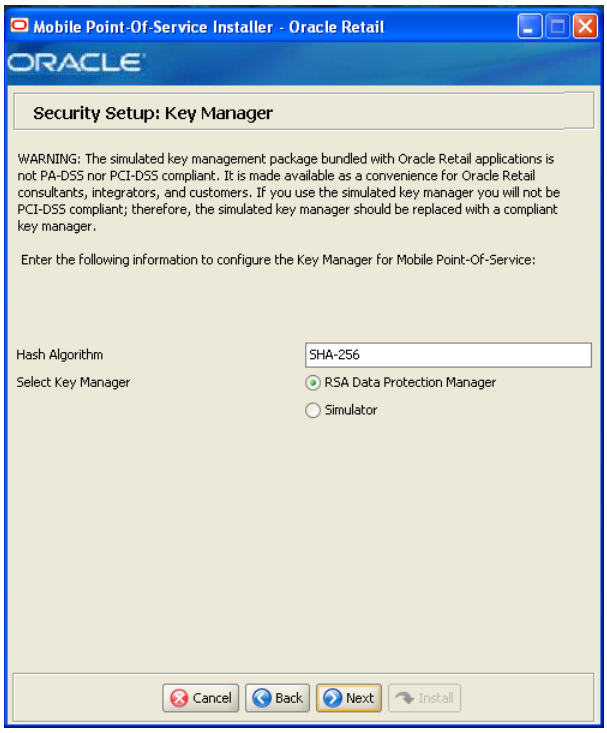


The fields on this screen are described in the following tables.

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 Manager



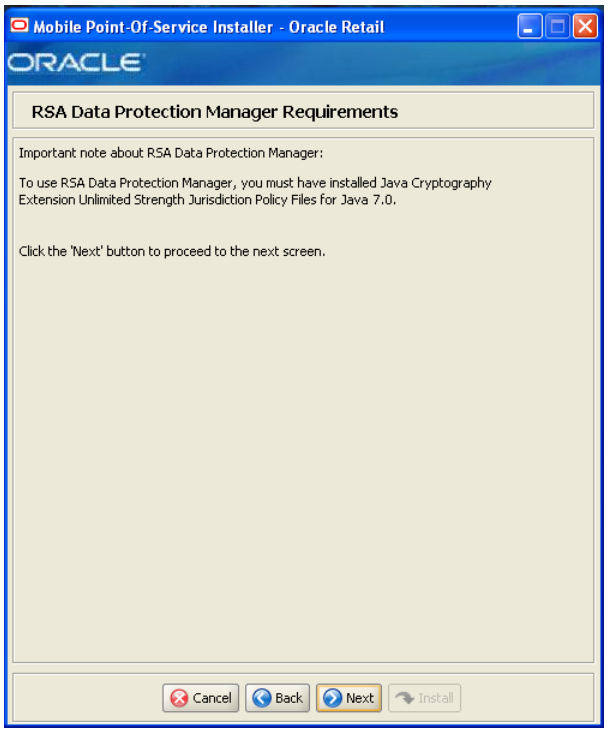
This screen is used to configure the Encryption Key Manager.

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

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

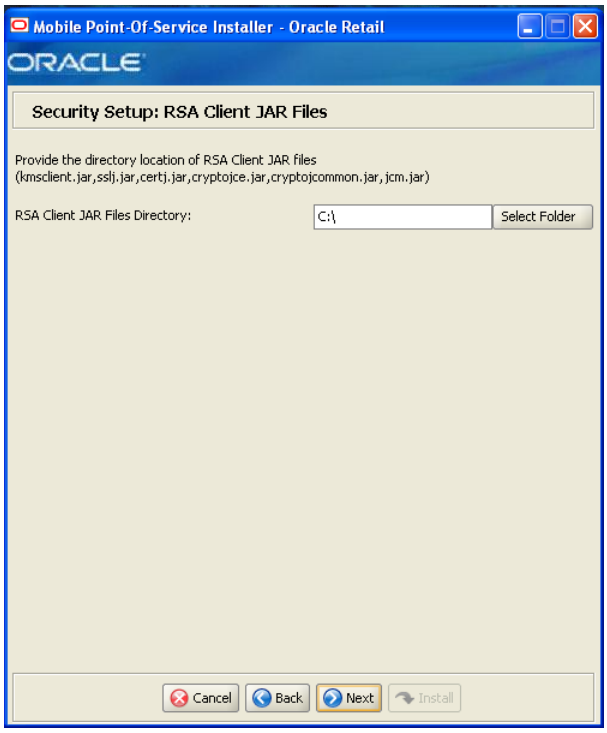
Details	Content
Field Title	Select Key Manager
Field Description	Provider for Key Manager: ▪ To use the RSA Data Protection Manager, select **RSA Data Protection Manager**. The next screen displayed is Figure C–14. ▪ To use the simulated key management package, select **Simulator**. The next screen displayed is Figure C–17.
Example	RSA Data Protection Manager

Figure C–14 RSA Data Protection Manager Requirements



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

Figure C–15 Security Setup: RSA Client JAR Files

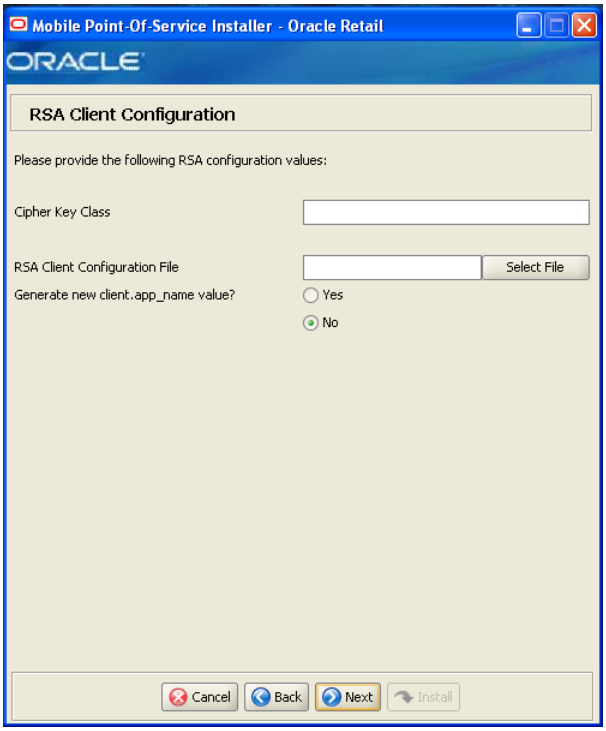


This screen is only displayed if **RSA Data Protection Manager** is selected for the Key Manager on the Security Setup: Key Manager screen.

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

Details	Content
Field Title	RSA Client JAR Files Directory
Field Description	Choose the directory where the following Key Manager jar files are located: ▪ certj.jar ▪ cryptojce.jar ▪ cryptojcommon.jar ▪ jcm.jar ▪ kmsclient.jar ▪ sslj.jar
Example	C:\

Figure C–16 RSA Client Configuration



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

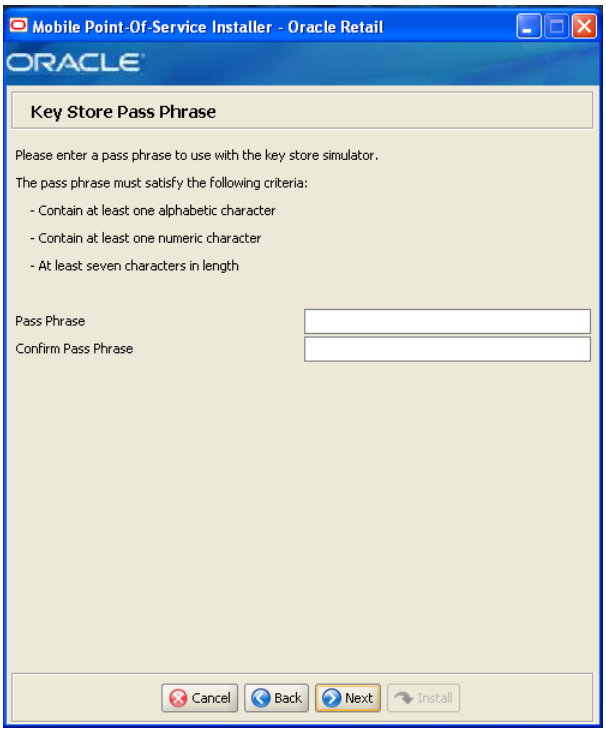
The fields on this screen are described in the following tables.

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

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

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

Figure C–17 Key Store Pass Phrase for Simulator Key Manager



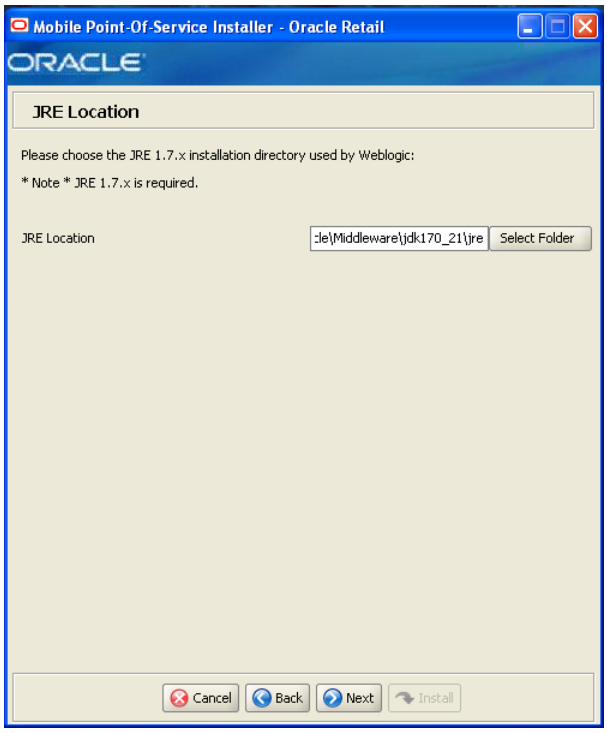
This screen is only displayed if **Simulator** is selected for the Key Manager on the Security Setup: Key Manager screen.

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.

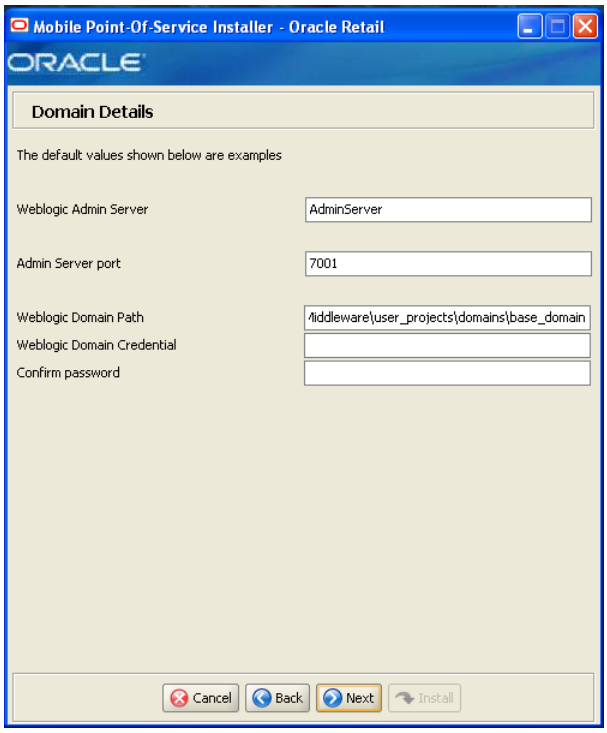
Figure C–18 JRE Location



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

Details	Content
Field Title	JRE Location
Field Description	Enter the location where the JRE is installed.
Example	`C:\Oracle\Middleware\jdk170_21\jre`

Figure C–19 Domain Details



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

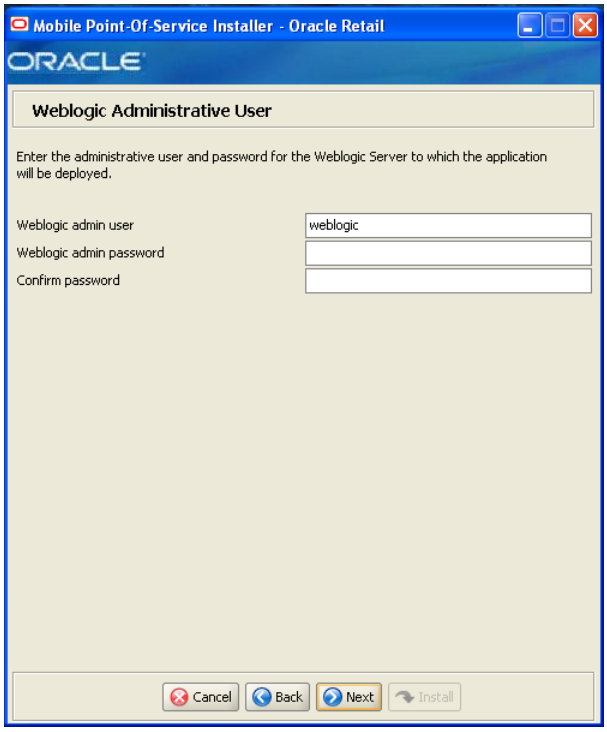
Details	Content
Field Title	Admin Server port
Field Description	Port used by the administration server. This port was selected when the administration domain was created.
Example	7001

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–20 Weblogic Administrative User



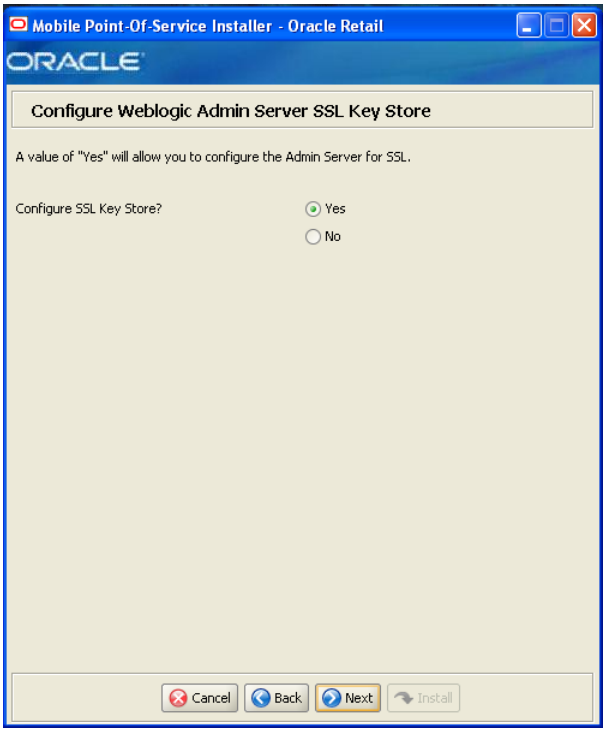
The fields on this screen are described in the following tables.

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–21 Configure Weblogic Admin Server SSL Key Store

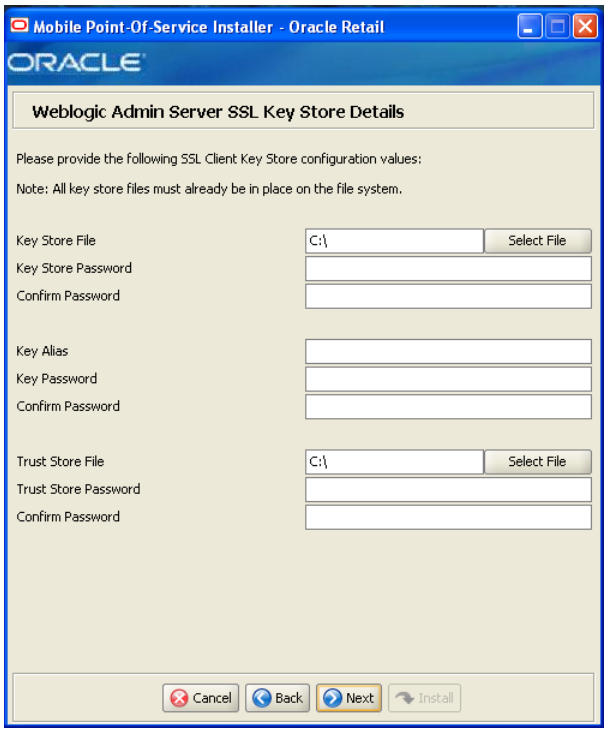


This screen is only displayed if **Deploy to Admin Server** is selected on the Weblogic Deploy Server Type screen.

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–22 Weblogic Admin Server SSL Key Store Details



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.

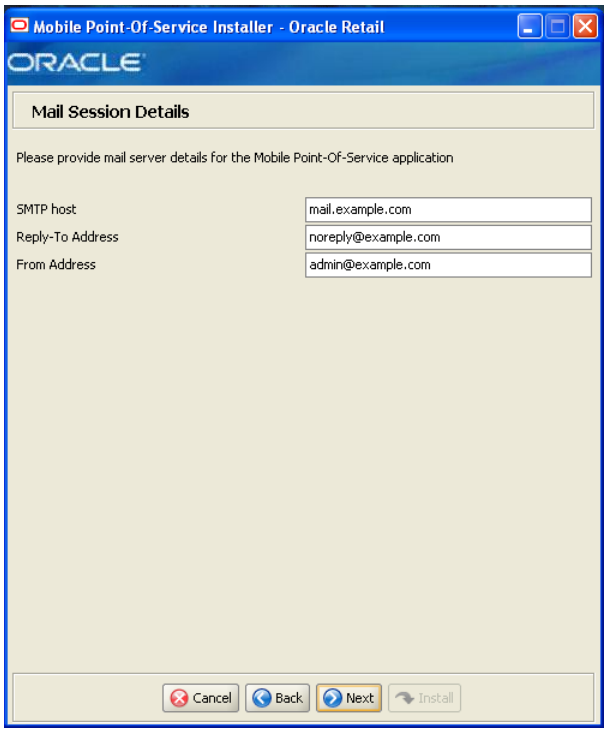
Details	Content
Field Title	Confirm Password
Field Description	Reentered Key Password used to confirm the password. **Note:** The passwords in the Key Password and Confirm Password fields must match.

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–23 Mail Session Details



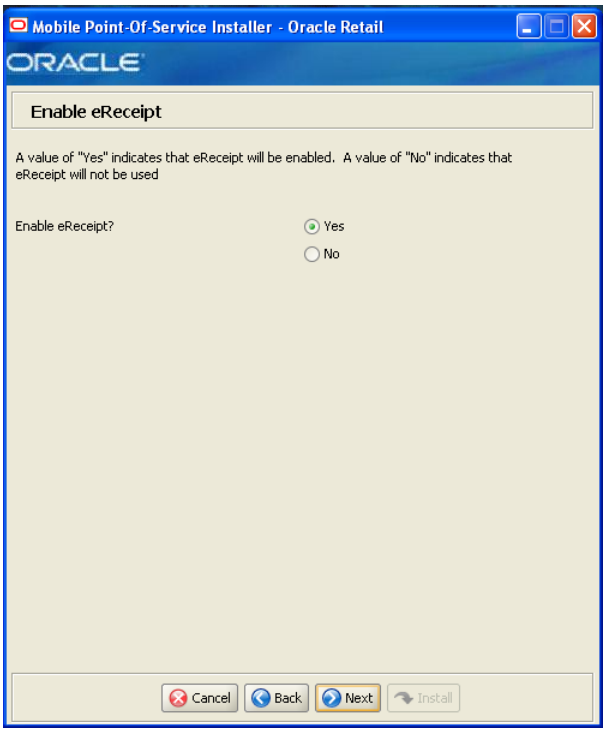
The fields on this screen are described in the following tables.

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

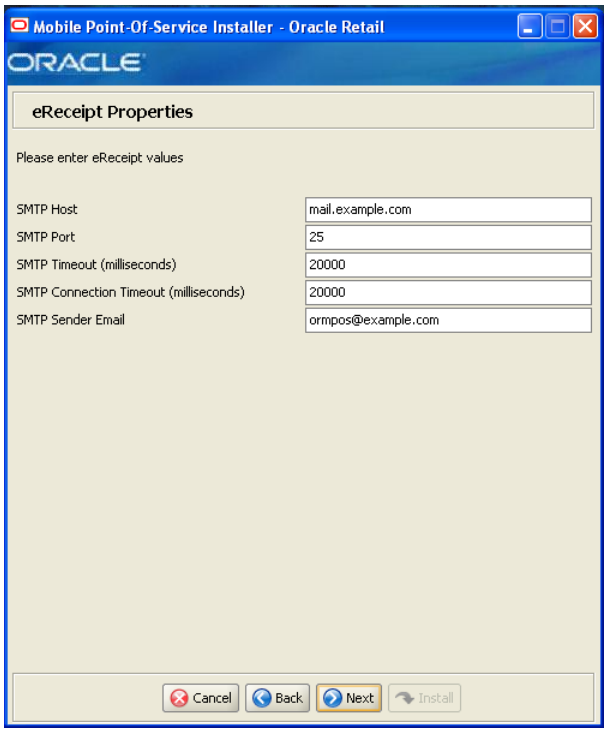
Figure C–24 Enable eReceipt



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

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

Figure C–25 eReceipt Properties



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

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

Details	Content
Field Title	SMTP Host
Field Description	Enter the host name for the SMTP server.
Example	mail.example.com

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

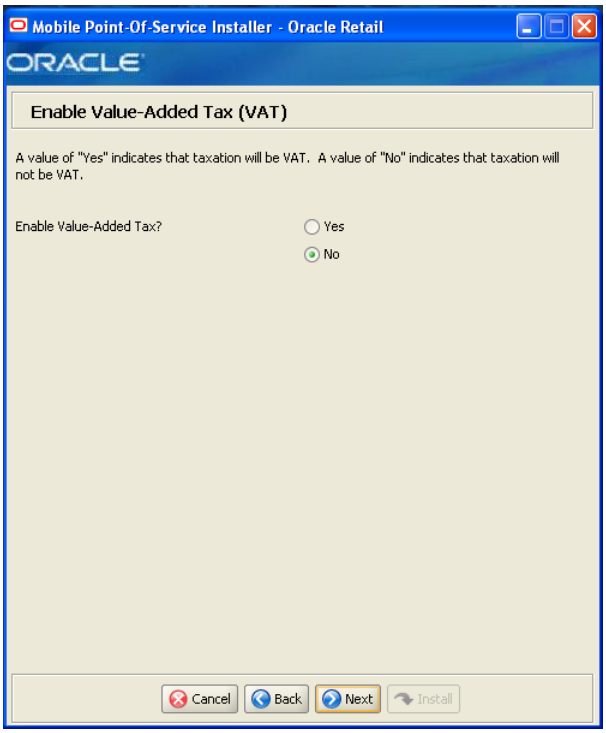
Details	Content
Field Title	SMTP Timeout (milliseconds)
Field Description	Enter the amount of time to wait for the SMTP server.
Example	20000

Details	Content
Field Title	SMTP Connection Timeout (milliseconds)

Details	Content
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–26 Value-Added Tax (VAT)



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

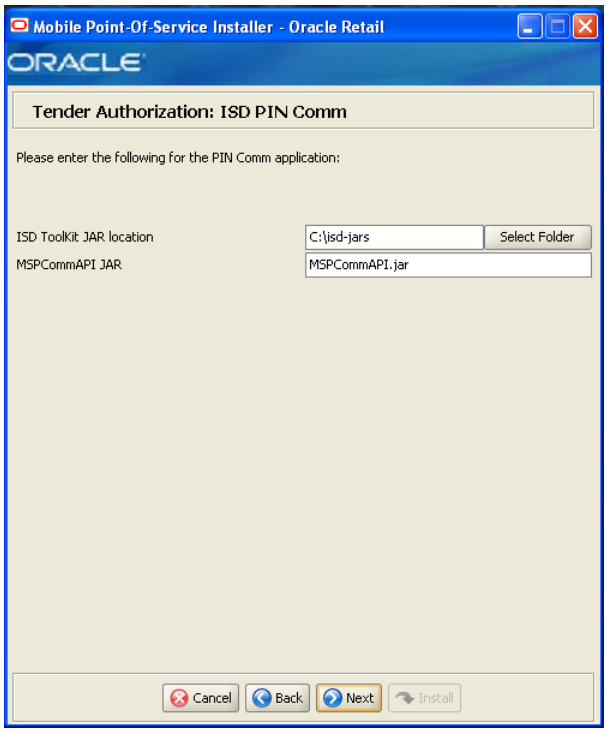
Details	Content
Field Title	Enable Value-Added Tax?
Field Description	Select Yes if Value-Added Tax is used.
Example	No

Figure C–27 Tender Authorization

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

Details	Content
Field Title	Please select the tender authorization method
Field Description	Choose where tender authorizations are sent. ▪ If approvals do not leave the store server and are based on values and certain numbers, choose **Simulated**. ▪ If approvals are sent to a third-party system to approve the authorizations, choose **ACI PIN Comm** or **Servebase PC_EFT POS**. **Note:** Demo installations should use the Simulated option.
Example	Simulated

Figure C–28 Tender Authorization: ISD PIN Comm



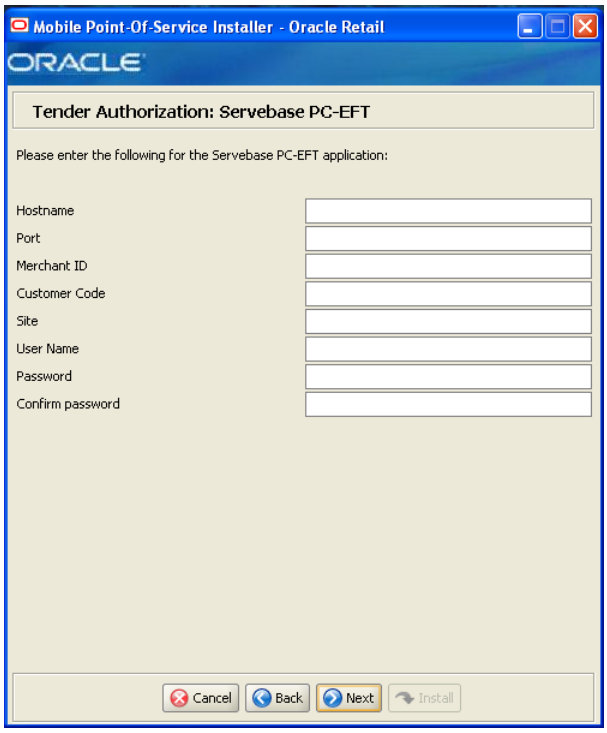
This screen is only displayed if **ACI PIN Comm** is selected for the Tender Authorization.

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

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

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

Figure C–29 Tender Authorization: Servebase PC-EFT



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

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

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

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

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

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

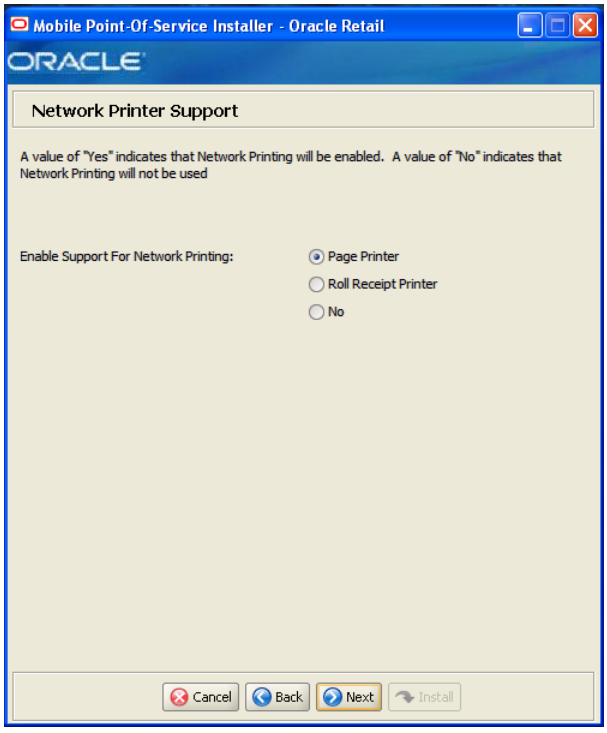
Details	Content
Field Title	Site
Field Description	Enter the site to access the PXP Solutions application.

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

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

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

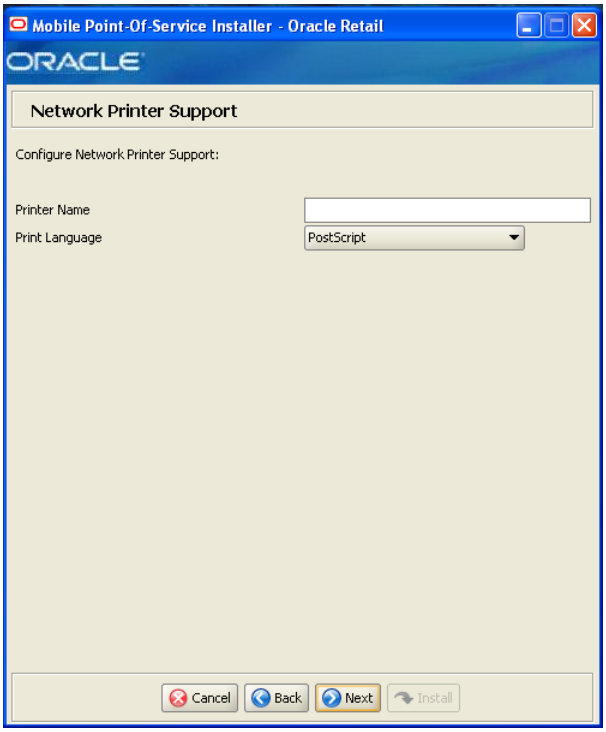
Figure C–30 Network Printer Support



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

Details	Content
Field Title	Enable Support for Network Printing
Field Description	Choose the type of network printing: ■ To use a network printer, select **Page Printer**. ■ To use a receipt printer with a paper roll, select **Roll Receipt Printer**. ■ To not enable network printing, select **No**.
Example	Page Printer

Figure C–31 Network Printer Support Configuration for Page Printer



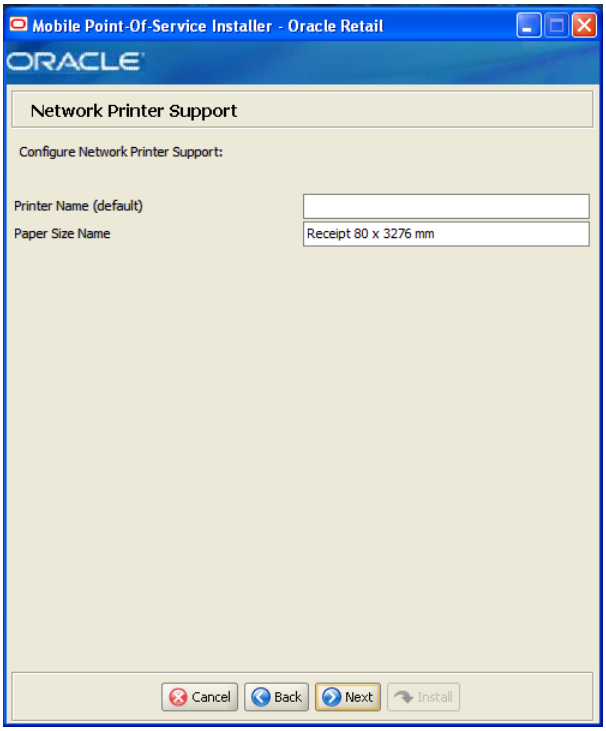
This screen is only displayed if **Page Printer** is selected on the Network Printer Support screen.

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–32 Network Printer Support Configuration for Roll Receipt Printer



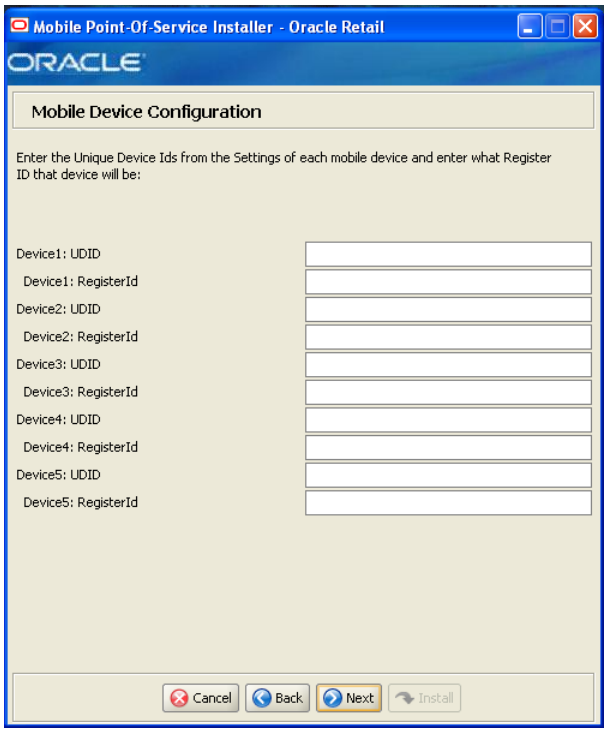
This screen is only displayed if **Roll Receipt Printer** is selected on the Network Printer Support screen.

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

Details	Content
Field Title	Printer Name (default)
Field Description	Enter the printer name.

Details	Content
Field Title	Paper Size Name
Field Description	Enter the name for the paper size for the printer.
Example	Receipt 80 x 3276 mm

Figure C–33 Mobile Device Configuration



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*.

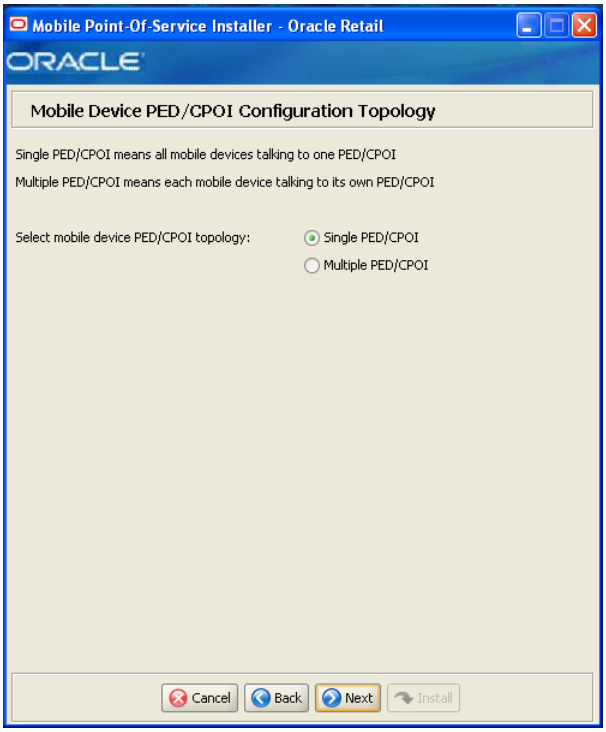
The fields on this screen are described in the following tables. Enter the following information for each mobile device.

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

Details	Content
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.

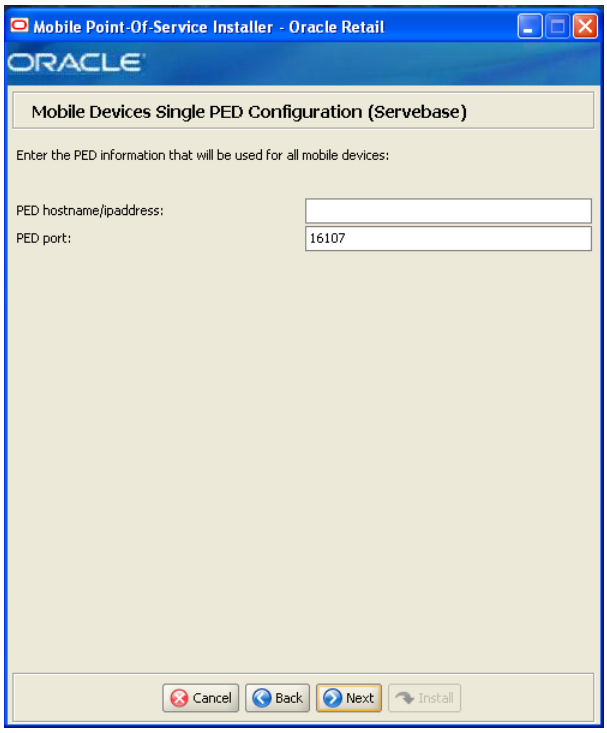
Figure C–34 Mobile Device PED/CPOI Configuration Topology



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–35 Mobile Devices Single PED Configuration (PXP Solutions)



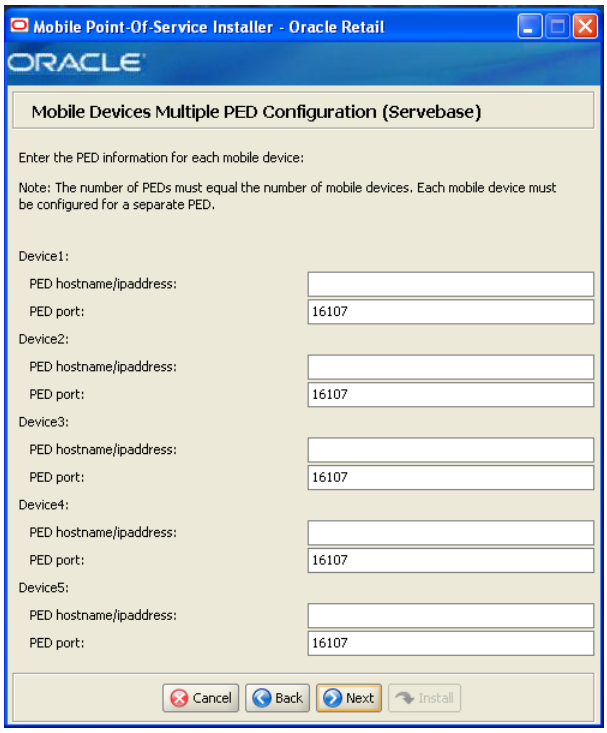
This screen is only displayed if **Servebase PC-EFT POS** is selected on the Tender Authorization screen and **Single PED/CPOI** is selected on the Mobile Device PED/CPOI Configuration Topology screen.

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–36 Mobile Devices Multiple PED Configuration (PXP Solutions)



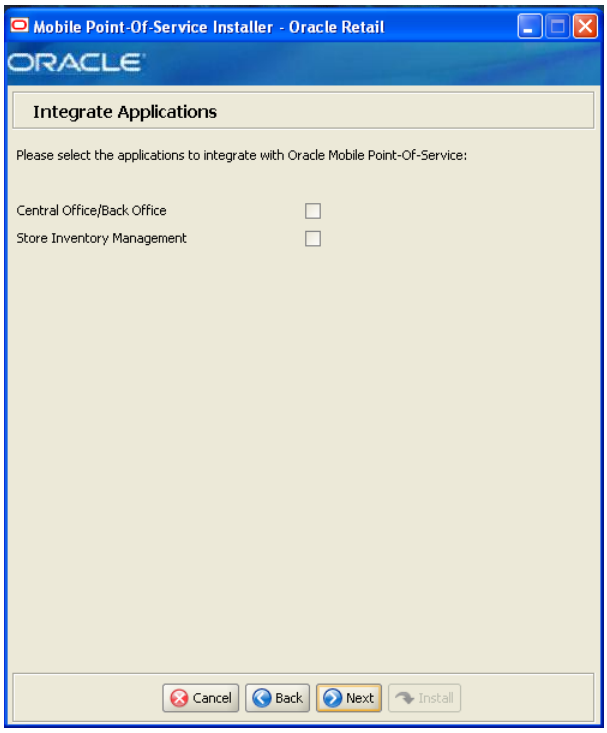
This screen is only displayed if **Servebase PC-EFT POS** is selected on the Tender Authorization screen and **Multiple PED/CPOI** is selected on the Mobile Device PED/CPOI Configuration Topology screen.

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

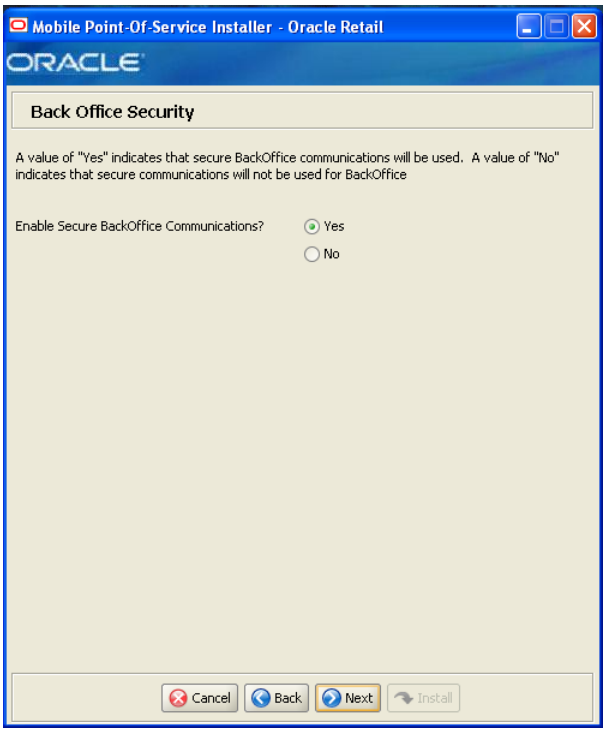
Figure C–37 Integrate Applications



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

Details	Content
Field Title	Please select the applications to integrate with Oracle 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–38 Back Office Security

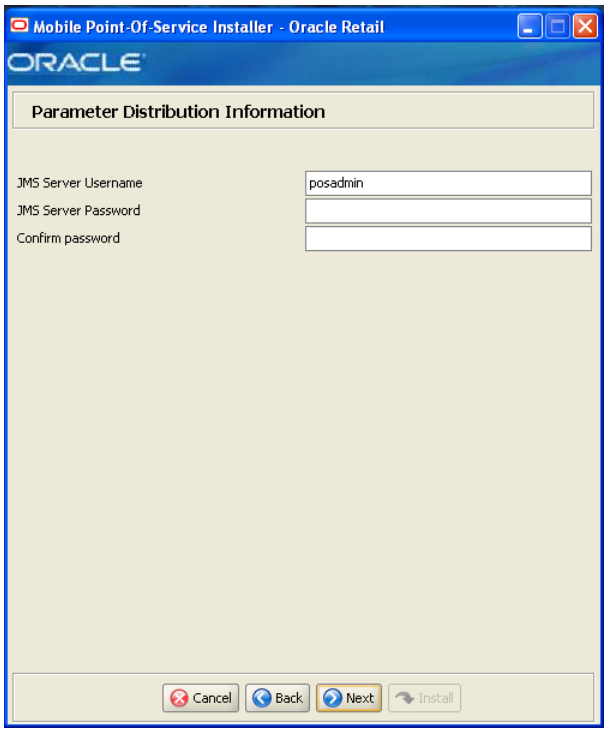


This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

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–39 Parameter Distribution Information



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

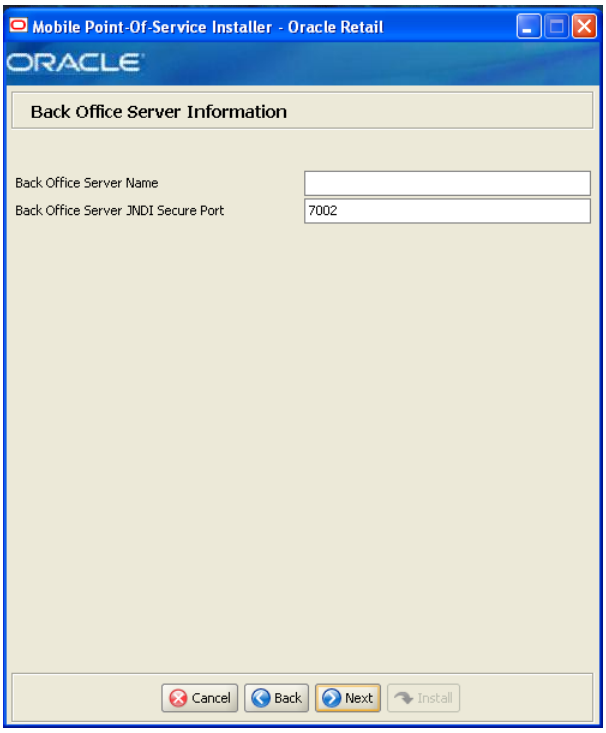
The fields on this screen are described in the following tables.

Details	Content
Field Title	JMS 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–40 Back Office Server Information



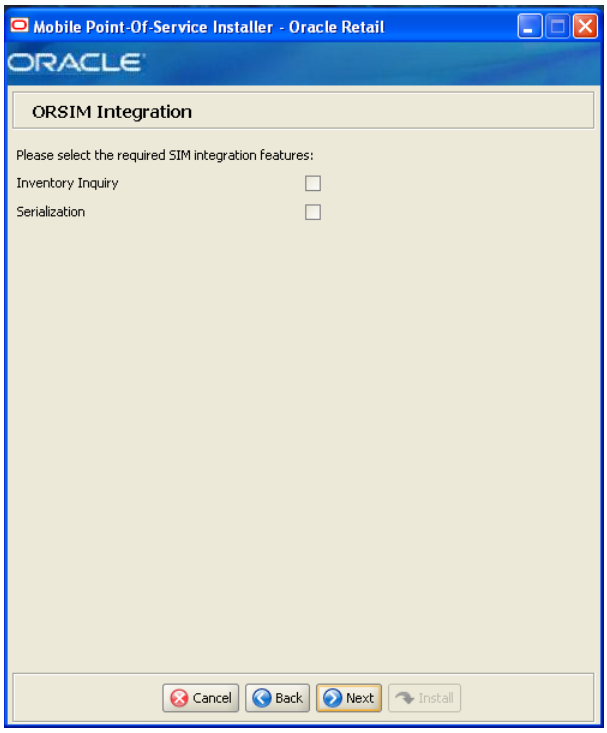
This screen is only displayed if **Central Office/Back Office** is selected on the Integrate Applications screen.

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

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–41 ORSIM Integration

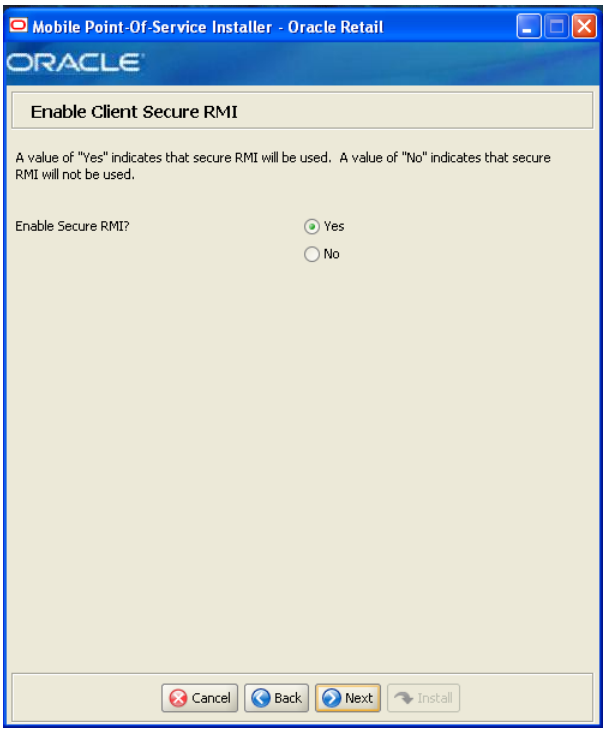


This screen is only displayed if **Store Inventory Management** is selected on the Integrate Applications screen.

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

Details	Content
Field Title	Please select the required SIM integration features
Field Description	Select the Oracle Retail Store Inventory Management (SIM) features that will be used in Mobile Point-of-Service: ■ To inquire about inventory using SIM, select **Inventory Inquiry**. ■ To enable serialization using SIM, select **Serialization**.

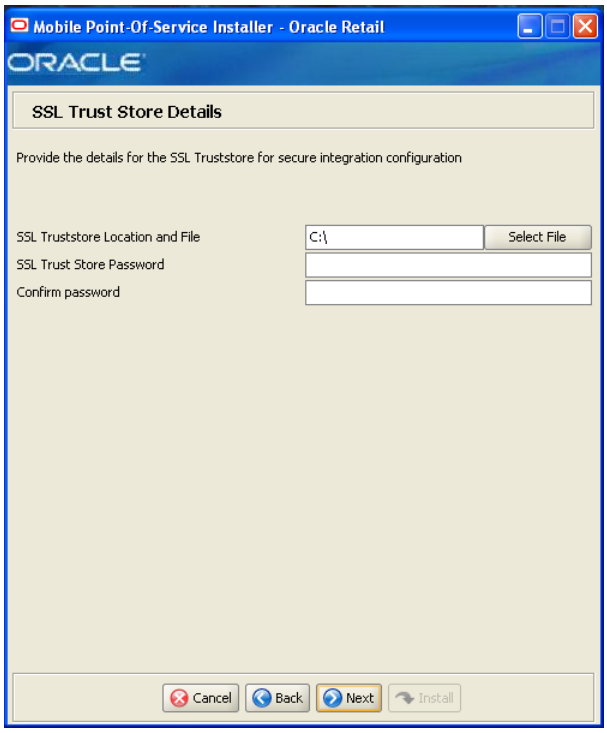
Figure C–42 Enable Client Secure RMI



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–43 SSL Trust Store Details



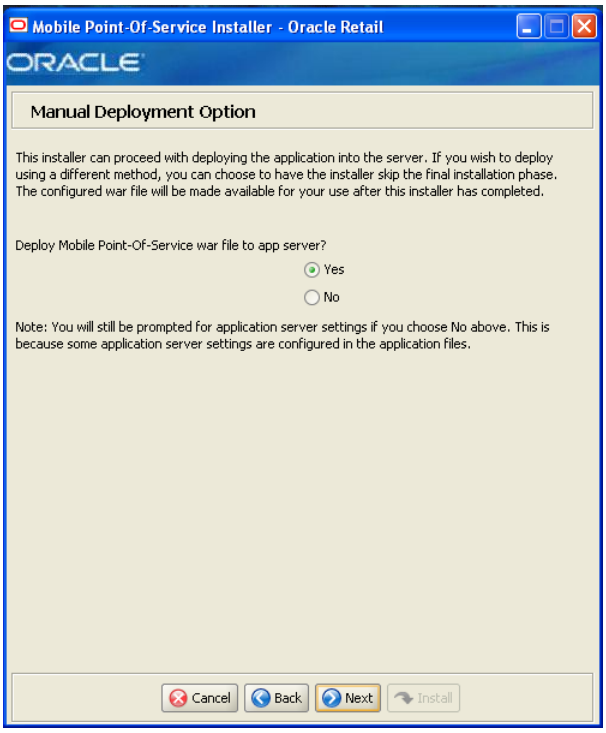
The fields on this screen are described in the following tables.

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

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.

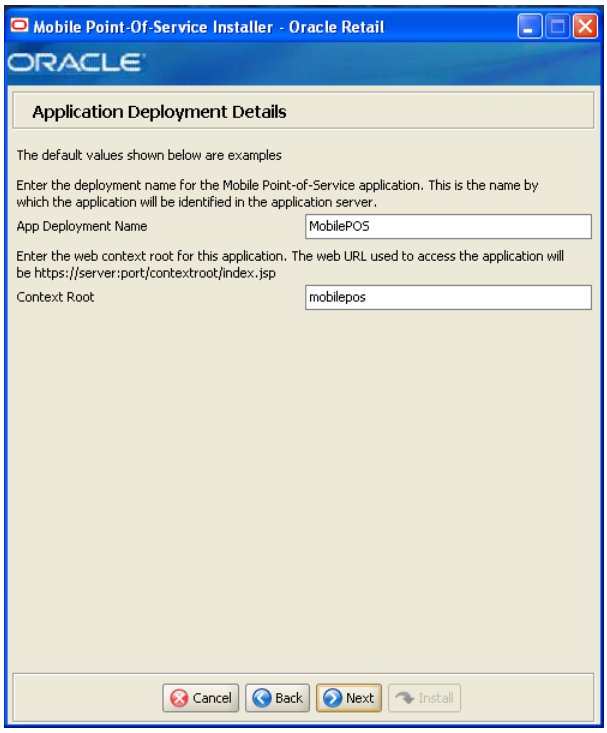
Figure C–44 Manual Deployment Option



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–45 Application Deployment Details

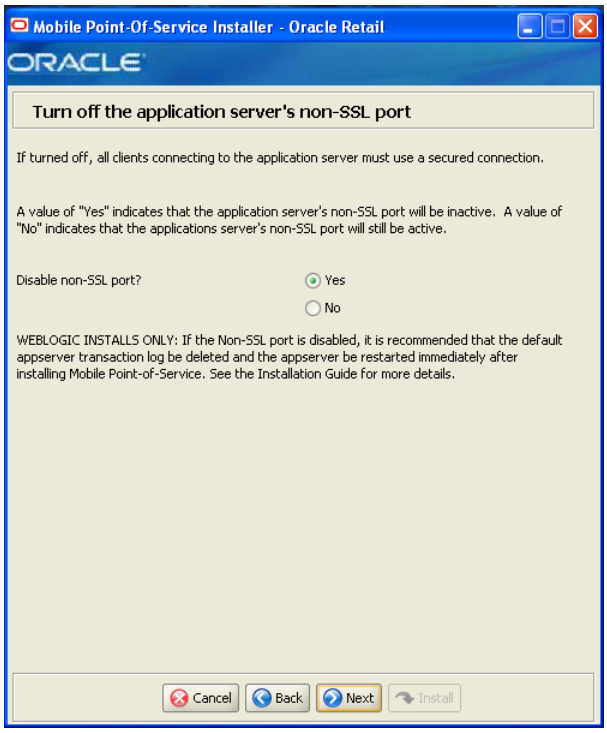


The fields on this screen are described in the following tables.

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

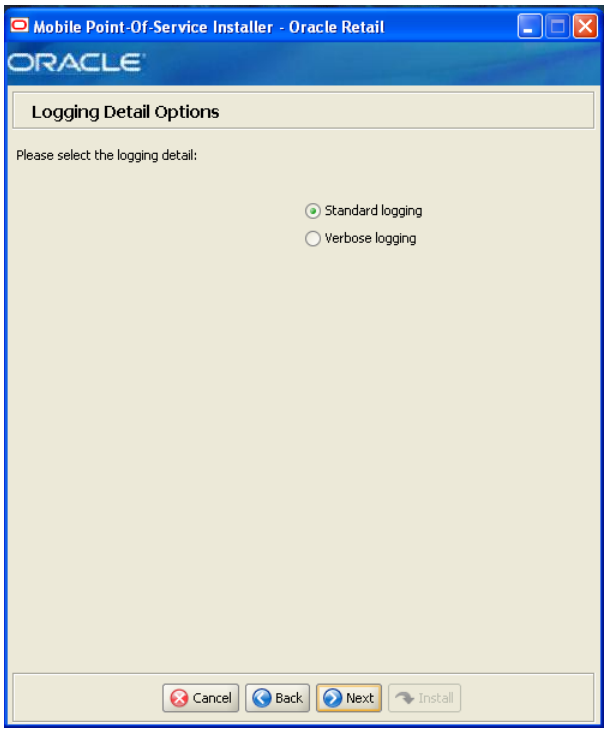
Figure C–46 Turn Off the Application Server's Non-SSL Port



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–47 Logging Detail Options



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

Details	Content
Field Title	Please select the logging detail
Field Description	Choose the level of 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–48 Installation Progress

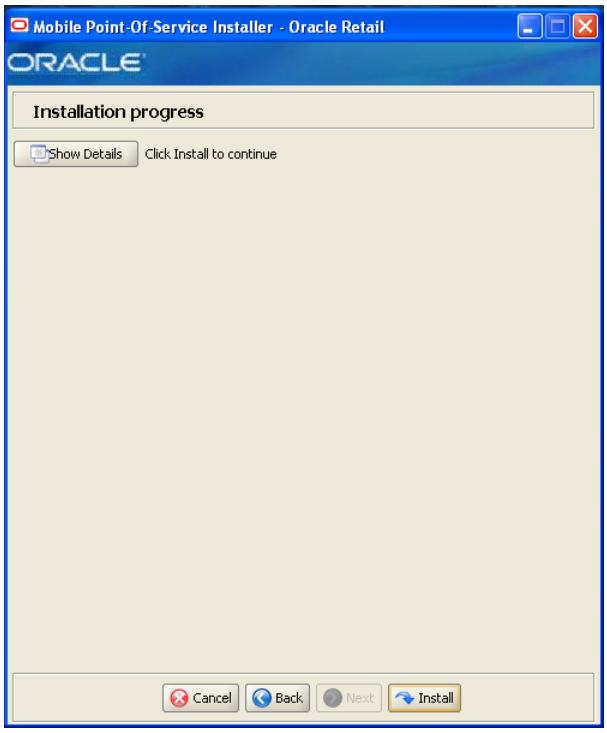


Figure C–49 Install Complete

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.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.
- The following is correct in the <*POS_install_directory*>\<*client*>\pos\bin\posenv.bat file:

  ```
  SET FP_PATH=C:\DigitalPersona\Bin;C:\DigitalPersona\Bin\Java
  SET PATH=%FP_PATH%;%PATH%
  ```

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 12c Database

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

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

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

For example, `jdbc:oracle:thin:@myhost:1525:myservice`

Add the following entry to the listener.ora:

USE_SID_AS_SERVICE_listener=on

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*.

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)