Oracle® Retail Point-of-Service

Installation Guide

Release 14.1.2

E65746-02

March 2016

ORACLE®

Oracle Retail Point-of-Service Installation Guide, Release 14.1.2

E65746-02

Primary Author: Bernadette Goodman

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

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

Contents

2 Secure Configuration

3 Installation on Microsoft Windows Server and Embedded POSReady

4 Installation on Novell SLEPOS

5 Installation of Mobile Point-of-Service

I Appendix: Installation Order

List of Figures

List of Tables

Send Us Your Comments

Oracle Retail Point-of-Service Installation Guide, Release 14.1.2

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 document in the Oracle Retail Point-of-Service Release 14.1.2 documentation set:

- *Oracle Retail Point-of-Service Release Notes*

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, 14.1) or a later patch release (for example, 14.1.2). 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.

Convention	Meaning
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 that must be met before Oracle Retail Point-of-Service can be installed.

> **Note:** These are the configurations that were tested for this release. While Point-of-Service may work in other configurations, these configurations were 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 Database Server Requirements

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

Table 1–1 Database Server Requirements

Supported on	Stack 1	Stack 2
Operating System	Microsoft Windows 2012 Server R2 Standard Edition (64-bit)	Novell SLEPOS11 SP3 (64-bit)
Database	Oracle Database 12c Standard Edition 12.1.0.2 (64-bit) **Note:** Oracle Retail Point-of-Service is not certified with Real Application Clusters (RAC).	Oracle Database 12c Standard Edition 12.1.0.2 (64-bit) **Note:** Oracle Retail Point-of-Service is not certified with Real Application Clusters (RAC).

> **Note:** It is recommended that separate tablespaces are used for tables and indexes. This may improve performance when accessing the database.

Required Setting for Database Installation

During database creation, the database must be set to AL32UTF8.

Check Supported Store Server Software Requirements

Table 1–2 lists the general requirements for a store server capable of running Point-of-Service and the versions supported for this release.

Table 1–2 Store Server Requirements

Supported on	Stack 1	Stack 2
Operating System	Microsoft Windows 2012 Server R2 Standard Edition (64-bit)	Novell SLEPOS11 SP3 (64-bit)
JDK/JRE	Oracle Java 7 or later within the Java 7 code line	Oracle Java 7 or later within the Java 7 code line

Check Supported Client Hardware and Software Requirements

Table 1–3 and Table 1–4 list 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 1–3 Client Requirements for Stack 1

Supported on			
Register	NCR 82XRT	Toshiba TcxWave 6140-E10	Dell Venue 11 Pro Tablet
Operating System	Microsoft Windows Embedded POSReady 7 (32-bit)	Microsoft Windows Embedded POSReady 7 (32-bit)	Microsoft Windows 8.1 Mobile (32-bit)
JVM	Oracle Java 7 JRE or later within the Java 7 code line (32-bit)	IBM Java 1.7 JRE or later within the Java 1.7 code line (32-bit)	Oracle Java 7 JRE or later within the Java 7 code line (32-bit)
Persistent Storage	Apache Derby 10.10.1.1	Apache Derby 10.10.1.1	Apache Derby 10.10.1.1
Cash drawer	NCR 2181	4510 Wide Cash Drawer	APG Cash Drawer
Pole Display	NCR 2X20	IBM PN 96Y4948	NA
Keyboard	NCR Keyboard (compact)	IBM 93Y1251	Dell Keyboard
Scanner	NCR 9208	Symbol Scanner LS4208	Symbol Scanner LS4208
Payment Device (ACI)	Verifone MX915	Verifone MX880	Verifone MX915
Payment Device (AJB)	Verifone MX915	NA	NA

Table 1–3 (Cont.) Client Requirements for Stack 1

Supported on			
Payment Locale	Europay, MasterCard, and Visa (EMV) and non-EMV **Note:** EMV is AJB only.	non-EMV	non-EMV
Receipt Printer	NCR Printer (Two-sided thermal printers with form input)	IBM 4610-2CR Thermal/Impact	Epson TMH 60000IV
Biometric Device	Digital Persona U are U 4500 Fingerprint READER v 2.02	Included	NA

Table 1–4 Client Requirements for Stack 2

Supported on	
Register	IBM SurePOS 700 (742/743)
Operating System	Novell SLEPOS11 SP3 (32-bit)
JVM	IBM Java 1.7 JRE or later within the Java 1.7 code line (32-bit)
Persistent Storage	Apache Derby 10.10.1.1
Cash drawer	IBM Cash Drawer
Pole Display	IBM Pole Display
Keyboard	IBM Keyboard
Scanner	Symbol Scanner LS2208 and LS4209
Payment Device (ACI)	Verifone MX915 and MX880
Payment Locale	non-EMV
Receipt Printer	IBM Printer
Biometric Device	Digital Persona U are U 4500 Fingerprint READER v 2.02

Install DigitalPersona Software

Registers that support a DigitalPersona fingerprint device require the installation of DigitalPersona Windows SDK (uareusdk220.zip).

The installer 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 are examples of how to set the PATH variable:

- Microsoft Windows:

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

- Novell SLEPOS:

```
FP_PATH=/opt/DigitalPersona/Bin:/opt/DigitalPersona/Bin/Java
```

```
PATH=$FP_PATH:$PATH; export PATH
```

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

Table 1–5 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 1–5 Mobile Point-of-Service Server Requirements

Supported on	Stack 1	Stack 2
Operating System	Microsoft Windows 2012 Server R2 Standard Edition (64-bit)	Novell SLEPOS11 SP3 (64-bit)
J2EE Application Server	Oracle WebLogic 10.3.6.0 Standard Edition (32-bit) **Note:** To install Oracle WebLogic with the supported version, use the Oracle WebLogic generic installer. For more information, see the Oracle WebLogic installation documentation.	Oracle WebLogic 10.3.6.0 Standard Edition (32-bit) **Note:** To install Oracle WebLogic with the supported version, use the Oracle WebLogic generic installer. For more information, see the Oracle WebLogic installation documentation.
J2EE Application Server JVM	Oracle Java 7 or later within the Java 7 code line	Oracle Java 7 or later within the Java 7 code line
Messaging Provider	included in Oracle WebLogic Server (32-bit)	included in Oracle WebLogic Server (32-bit)

Table 1–6 lists the general requirements for mobile devices capable of running Mobile Point-of-Service and the versions supported for this release. The devices are supported on both stacks.

Table 1–6 Mobile Point-of-Service Device Requirements

Supported on	Stack 1 and 2			
Device	Apple iPod Touch (5th Generation)	Apple iPad mini (2nd Generation)	Motorola MC 40	Motorola Tablet (ET1)
Operating System	Apple iOS 8.4	Apple iOS 8.4	Android 4.1.1	Android 4.1.1
Sled **Note:** Mobile Point-of-Service can be run without a sled, but this is not suitable for a production environment.	Verifone PAYware Mobile e315	Verifone PAYware Mobile e335	Built-in; for scanning only	Built-in; for scanning only
Payment Device (ACI)	NA	NA	Verifone MX915 and MX880 Equinox L5300	Verifone MX915 and MX880 Equinox L5300
Payment Device (AJB)	Verifone MX915	Verifone MX915	NA	NA
Payment Locale	EMV and non-EMV	EMV and non-EMV	non-EMV	non-EMV
Network Printer	Programmable Logical Control System (PLCS) and Postscript - Epson TM-T88v	PLCS and Postscript - Epson TM-T88v	PLCS and Postscript - Epson TM-P60	PLCS and Postscript - Epson TM-T88v

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 Supported Oracle Retail Products

Table 1–7 lists the Oracle Retail products that are supported.

Table 1–7 Supported Oracle Retail Products

Integrates with	Version
Oracle Retail Back Office	14.1.2
Oracle Retail Central Office	14.1.2
Oracle Retail Merchandising System	14.1.2
Oracle Retail Price Management	14.1.2
Oracle Retail Returns Management	14.1.2
Oracle Retail Sales Audit	14.1.2
Oracle Retail Store Inventory Management	14.1.2 (on Oracle WebLogic Server)

Check Additional Oracle Technologies

Table 1–8 lists the Oracle technologies used by Oracle Retail Point-of-Service and the required versions.

Table 1–8 Additional Oracle Technologies

Integrates with	Version
Siebel	8.1.1.3

Check Java Key Manager Requirement

If you are using the RSA Data Protection Manager, you must use version 3.5.2.2.

Oracle Retail Point-of-Service requires that a Java Key Manager system is available prior to installation. Specific information for configuring the Key Manager is entered on the Security Setup: Key Manager installer windows.

If you are using the RSA Data Protection Manager, you must obtain specific jar files, obtain the lockbox files for the operating system you are using, and install the Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files 7.0. For Microsoft Windows, see "Obtain the Files Needed for the RSA Data Protection Manager" in Chapter 3. For Novell SLEPOS, see "Obtain the Files Needed for the RSA Data Protection Manager" in Chapter 4.

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 in the Key Store Pass Phrase installer window.

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 on Microsoft Windows, see "Secure Communication" in Chapter 3. For Novell SLEPOS, see "Secure Communication"in Chapter 4.

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.

Tender Authorization Testing for Point-of-Service

Tender authorization testing was done with ACI PINComm and AJB,. 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 PINComm

The following ACI versions were used for testing:

- PINComm 6.5.0.006 and toolkit 346 (IMSRTRIBSpecSDK-346.jar)
- SAF/TOR 6.5.0.010 and toolkit 346 (IMSRTRIBSpecSDK-346.jar)

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

Table 1–9 ACI PINComm Authorization Set Tested with Point-of-Service

Transaction Type	Transaction Type Message Sent from ACI PINComm to Point-of-Service
Check Tender	■ Check Sale Approval ■ Check Sale Authorization Offline ■ Check Sale Authorization Timeout ■ Check Sale Decline ■ Check Sale Post Void ■ Check Sale Referral
Credit Card Tender	■ Credit Card Return Approval ■ Credit Card Return Authorization Offline ■ Credit Card Return Authorization Timeout ■ Credit Card Return Decline ■ Credit Card Return Post Void ■ Credit Card Return Referral ■ Credit Card Sale Approval ■ Credit Card Sale Authorization Offline ■ Credit Card Sale Authorization Timeout ■ Credit Card Sale Decline ■ Credit Card Sale Partial Approval ■ Credit Card Sale Post Void ■ Credit Card Sale Referral

Table 1–9 (Cont.) ACI PINComm Authorization Set Tested with Point-of-Service

Transaction Type	Transaction Type Message Sent from ACI PINComm to Point-of-Service
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
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

Table 1–9 (Cont.) ACI PINComm Authorization Set Tested with Point-of-Service

Transaction Type	Transaction Type Message Sent from ACI PINComm to Point-of-Service
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

AJB

The AJB Fipay software version used for testing was 19444.

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

Table 1–10 AJB Authorization Set Tested with Point-of-Service

Transaction Type	Transaction Type Message Sent from AJB to Point-of-Service
Check Tender	■ Check Sale Approval ■ Check Sale Authorization Offline ■ Check Sale Decline ■ Check Sale Post Void ■ Check Sale Referral
Credit Card Tender	■ Credit Card Return Approval ■ Credit Card Return Authorization Offline ■ Credit Card Return Decline ■ Credit Card Return Post Void ■ Credit Card Return Referral ■ Credit Card Sale Approval ■ Credit Card Sale Authorization Offline ■ 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 Decline ■ Debit Card Sale Partial Approval ■ Debit Card Post Void

Table 1–10 (Cont.) AJB Authorization Set Tested with Point-of-Service

Transaction Type	Transaction Type Message Sent from AJB to Point-of-Service
Gift Card Issue	■ Gift Card Issue Approval ■ Gift Card Issue Authorization Offline ■ Gift Card Issue Decline
Gift Card Redeem	■ Gift Card Redeem Approval ■ Gift Card Redeem Authorization Offline ■ Gift Card Redeem Decline
Gift Card Refund Issue new gift card or reload to existing gift card	■ Gift Card Issue Approval as a Refund ■ Gift Card Issue Authorization Offline as a Refund ■ Gift Card Issue Decline as a Refund ■ Gift Card Reload Approval as a Refund ■ Gift Card Reload Authorization Offline as a Refund ■ Gift Card Reload Decline as a Refund
Gift Card Reload	■ Gift Card Reload Approval ■ Gift Card Reload Authorization Offline ■ Gift Card Reload Decline
Gift Card Tender	■ Gift Card Post Void ■ Gift Card Sale Approval ■ Gift Card Sale Authorization Offline ■ Gift Card Sale Decline ■ Gift Card Sale Referral
House Account Inquiry, Temporary Pass, Payment	■ House Account Search Authorization Offline ■ House Account Search Not Found ■ House Account Search Referral ■ House Account Search Success
House Account Tender	■ House Account Return Approval ■ House Account Return Authorization Offline ■ House Account Return Decline ■ House Account Return Post Void ■ House Account Return Referral ■ House Account Sale Approval ■ House Account Sale Authorization Offline ■ House Account Sale Decline ■ House Account Sale Post Void

Tender Authorization Testing for Mobile Point-of-Service

Tender authorization testing was done with ACI PINComm and AJB. For each payment application, the version used for the testing and the transaction types and messages that were tested are listed below.

ACI PINComm

Note: Testing with ACI PINComm was done only with the Motorola mobile devices.

The following ACI versions were used for testing:

- PINComm 6.5.0.006 and toolkit 346 (IMSRTRIBSpecSDK-346.jar)
- SAF/TOR 6.5.0.010 and toolkit 346 (IMSRTRIBSpecSDK-346.jar)

Table 1–11 shows the transaction types and messages that were tested.

Table 1–11 ACI PINComm Authorization Set Tested with Mobile Point-of-Service

Transaction Type	Transaction Type Message Sent from ACI PINComm to Mobile Point-of-Service
Credit Card Tender	■ Credit Card Return Approval ■ Credit Card Return Authorization Offline ■ Credit Card Return Authorization Timeout ■ 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 Refund Issue new gift card or reload to existing gift card	■ Gift Card Issue Approval as a Refund ■ Gift Card Issue Authorization Offline as a Refund ■ Gift Card Issue Decline as a Refund ■ Gift Card Reload Approval as a Refund ■ Gift Card Reload Authorization Offline as a Refund ■ Gift Card Reload Decline as a Refund
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

AJB

Note: Testing with AJB was done only with the Apple mobile devices.

The AJB Fipay software version used for testing was 19444.

Table 1–11 shows the transaction types and messages that were tested.

Table 1–12 AJB Authorization Set Tested with Mobile Point-of-Service

Transaction Type	Transaction Type Message Sent from AJB 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

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 3.0.

Operating System

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

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

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 benchmarks at the following links:

- Microsoft Windows Server 2012

  http://benchmarks.cisecurity.org/en-us/?route=downloads.browse.category.benchmarks.os.windows.2012

- SUSE Linux (SLEPOS)

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

- Apple iOS

  http://benchmarks.cisecurity.org/downloads/browse/index.cfm?category=benchmarks.mobile.iphone

- Google Android

  http://benchmarks.cisecurity.org/downloads/browse/index.cfm?category=benchmarks.mobile.android

Infrastructure/Middleware

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

Database

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

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

For information about secure configuration of Oracle Database, see the *Oracle Database 2 Day + Security Guide*. The guide is available at the following link on the Oracle Technology Network web site:

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

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 Data Protection Manager

The Oracle Retail POS Suite applications are designed to be easily integrated with an external key management service, selected by the retailer, for encryption and decryption of sensitive data. The Oracle Retail POS Suite 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 Data Protection Manager. 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 Data Protection 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 Data Protection 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 14.1.2 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 14.1.2 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 8.2.3, 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.

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. For information about securing this interface protocol, 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 in the installer windows 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 Microsoft Windows Server and Embedded POSReady

This chapter provides information about the installation procedures for Oracle Retail Point-of-Service. This chapter covers installing the server on Microsoft Windows Server and clients on Microsoft Windows Embedded POSReady. For a list of tested components and supported versions, 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 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;
```

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 TO <data_source_role>;
```

> **Note:** After the product is installed successfully, the CREATE SYNONYM privilege must be revoked from the data source role. Before the installer exits, it prompts for a database administrator to revoke the privilege.

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 connection user access to the application database objects.

Installing Point-of-Service

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

Determining Tier Type

Machines and logical components of the Oracle Retail Point-of-Service application are defined in Table 3–1:

Table 3–1 Server Tier Logical Components

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

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

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

Installing the Database

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

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

Required Settings for the Database

During database creation, the database must be set to AL32UTF8.

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 NCR Register"
- "Configuring Devices for an IBM SurePOS Register"
- "Configuring a Device for ACI PINComm"

Expand the Point-of-Service Distribution

To extract the Point-of-Service files:

1. Extract the Point-of-Service 14.1.2 distribution zip file.
2. Create a new staging directory for the Point-of-Service application distribution `ORPOS-14.1.2.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-14.1.2.zip` to *<staging_directory>* and extract its contents. The following files and directories should be created under *<staging_directory>*`\ORPOS-14.1.2`:

```
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
revokesyn.sql
wallet.xml
```

For the remainder of this chapter, <*staging_directory*>\ORPOS-14.1.2 is referred to as <*INSTALL_DIR*>.

Obtain the JRE Required for Client Install

This release requires Oracle Java 7 JRE for the client install:

- NCR register:

  This release requires Oracle Java 7 JRE for client installs on NCR registers. The download is available at the following web site:

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

- IBM SurePOS register:

  This release requires IBM JRE 1.7 for client installs on IBM SurePOS registers. It is distributed by IBM with JavaPOS 1.13.

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 in the Secure Options window. See Figure A–17.
  - 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 in the Enable Client Secure RMI window. See Figure B–23.
  - 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*.

Enable Order Integration

Point-of-Service supports processing orders thorough an external order management system and Commerce Anywhere. To enable order integration:

1. In the Integration Applications window, select **Orders**. See Figure A–13 and Figure B–17.
2. Select the order type. See Figure A–14 and Figure B–18:
   - To use an external order management system, select **External Order**.
   - To use Commerce Anywhere, select **Commerce Anywhere**.

External Order Management System

You provide the information for accessing the web service for the external order management system. For more information on integrating with an external order management system, see the *Oracle Retail POS Suite Implementation Guide, Volume 4 - Point-of-Service External Order*.

Commerce Anywhere

Commerce Anywhere enables retailers to integrate with e-commerce and order management solutions for processing customer transactions in stores and through web applications.

You provide the information for accessing the web services for Commerce Anywhere.

For more information on Commerce Anywhere, see the following documents available through My Oracle Support. Access My Oracle Support at the following URL:

https://support.oracle.com

Oracle Retail Commerce Anywhere Technical Integration Solution (Doc ID: 1598187.1)

This set of architectural diagrams and related business processes depict the Commerce Anywhere solution and its major integration points. The conceptual representation that is depicted is intended to support an integrated implementation of an Oracle Retail Commerce Anywhere solution that includes Oracle Retail Merchandising System, Oracle Retail Store Inventory Management, Oracle Retail Warehouse Management System, Oracle Retail POS Suite, and Oracle Retail Advanced Inventory Planning.

Oracle Retail Commerce Anywhere Functional White Papers (Doc ID: 1598177.1)

This library contains a collection of white papers that outline functional aspects of the Commerce Anywhere solution in Oracle Retail applications. One document provides an overview of the solution from an enterprise perspective, and it is accompanied by product specific-papers addressing Oracle Retail Merchandising System, Oracle Retail Store Inventory Management, Oracle Retail Warehouse Management System, Oracle Retail POS Suite, and Oracle Retail Advanced Inventory Planning.

Database Install Options

In the Install Database Option window, you select whether the installer creates and populates the database schema or if you want to do this manually. See Figure A–20.

> **Caution:** If the database schema is already created and populated, select **Skip schema creation and data loading**. Selecting one of the other options will result in the loss of the data already in the database. If the database schema was created and populated using Point-of-Service, 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 in the Sample Dataset installer window. See Figure A–21. You can obtain the `sample-dataset-14.1.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 in the window. You choose this option if you want to create and populate the database schema manually or the database schema was created using Back Office.

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 the RSA Data Protection Manager

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

- "Obtain the RSA Client Configuration File"
- "Obtain the RSA Data Protection Manager Jar Files"
- "Obtain the RSA Libraries for Lockbox"
- "Install the Java Cryptography Extension (JCE)"

Obtain the RSA Client Configuration File

You must provide the installer with the name and location of the configuration property file in the RSA Client Configuration window. See Figure A–66 and Figure B–32. For detailed information on the content of this file, see the Java client documentation provided by your provider for the RSA Data Protection Manager.

Obtain the RSA Data Protection Manager Jar Files

You must obtain the required jar files from your RSA Data Protection Manager provider. You provide the location of the jar files in the RSA Client JAR Files window.

See Figure A–65 and Figure B–31. The directory for the jar files must contain only the RSA Java client jar files.

Obtain the RSA Libraries for Lockbox

Lockbox is an RSA feature the provides protection for RSA configuration information. Obtain these libraries from your RSA Data Protection Manager.

You must also update the path variable, PATH, for the lockbox libraries.

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 window 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

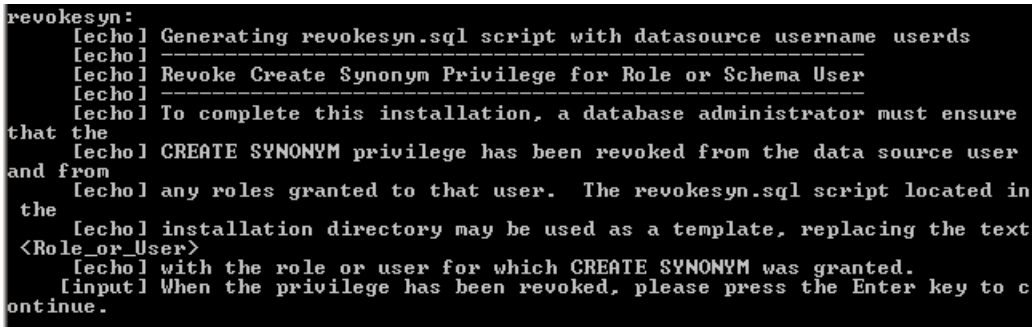
   In the log file name, `yyyyMMddHHmm` is the timestamp of the install.

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

   ```
   install.cmd
   ```

5. If this is a server install, after the installation is successfully completed, the CREATE SYNONYM privilege must be revoked. In the installer console window, it prompts for a database administrator to run the revokesyn SQL script to revoke the privilege. The script is found in the *<INSTALL_DIR>* directory.

Figure 3–1 Installer Prompt to Run revokesyn



   For information on granting this privilege, see "Create the Database Schema Owner and Data Source Users".

6. If this is a client install and you are using a DigitalPersona fingerprint device on and IBM SurePOS register, 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\\jpos113.jar
     input.dpfingerprint.dpotjni = C:\\DigitalPersona\\Bin\\Java\\dpuareu.jar
     ```

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

Resolve Errors Encountered During Application Installation

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

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

Configure Devices for Fiscal Printing

The fiscal printer JPOS API does not support barcode printing. The implementation for this release uses an Epson-specific directIO command to print the barcode. The directIO command is configured in the DeviceContext.xml file. The command and its parameters control the barcode alignment (position in the receipt), barcode width, and barcode type.

To configure the fiscal printing device for barcode printing, make the changes to the following file:

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

Update the following entry in that file:

```
<property name="barcodeDirectIO">
    <map>
        <entry key="command" value="1075" />
        <entry key="parameters" value="011203075210073" />
    </map>
</property>
```

The following table describes the parameters entry in the preceding example:

Value	Description
01	Operator. Any two digit number can be used.
120	Left margin (120 at 180 dpi equals 17 mm, plus offset of 3 mm, equals 20 mm).
03	Dot width of each bar (3 at 180 dpi equals 4 mm).
075	Height in dots of the barcode (120 at 180 dpi equals 17 mm).
2	Human Readable Interpretation (HRI) numerical representation text placement (0 = none, 1 = above, 2 = below, and 3 = both above and below).
1	Font for text that can be printed above and below the barcode. HRI numerical representation text font (1, 2, or 3).
00	Always set to 00.
73	Barcode type.

The left margin and dot width in the example are configured for a 13-digit transaction ID. To accommodate the 26-digit transaction ID, the left margin needs to be reduced to 080 and dot width to 02.

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

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

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

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

Resolve Misprinted Character Problems in eReceipts

To resolve misprinted character problems in eReceipts:

1. Verify that the operating system is installed with a fixed-width font capable of cleanly displaying the misprinted character. For example on Microsoft Windows, MS Gothic can be used to display Chinese characters and Courier New can be used to display Russian characters.

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

2. In the style-sheet used by the Point-of-Service client for eReceipts, specify the best font available for the language on the operating system. Point-of-Service uses Extensible Style-sheet Language Formatting Objects (XSL-FO) to transform each line of receipt data into PDF output. The style-sheet used for eReceipts specifies the Courier font family. To specify a different font, such as SimSun or Courier New, replace the reference to Courier with the new font name in the following files:

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

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

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

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

Resolve Misprinted Character Problems in Network Printed Receipts and Reports

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

1. Verify that the operating system is installed with a fixed-width font capable of cleanly displaying the misprinted character. For example on Microsoft Windows, MS Gothic can be used to display Chinese characters and Courier New can be used to display Russian characters.

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

2. In the style-sheet used by the Point-of-Service client for network printing, specify the best font available for the language on the operating system. Point-of-Service uses Extensible Style-sheet Language Formatting Objects (XSL-FO) to transform each line of receipt or report data into the type of output designated for the configured network printer. The style-sheet used for network printing specifies the Courier font family. To specify a different font, such as MS Gothic or Courier New, replace the reference to Courier with the new font name in the following file:

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

Enable Dashboard and Browser Functionality in the Client Installation

Point-of-Service provides the capabilities to display a dashboard in the Main Options screen and access a web site from a register using the **Browser** button in the Main Options screen. JavaFX, which comes bundled with Oracle Java, is required for both the dashboard and browser functionality.

Accessing Web Sites Through a Secure HTTP Connection

If a web site is accessed through a secure HTTP connection, an SSL certificate is required. The SSL certificate of the web site, which you want to access through the Point-of-Service embedded browser, should be imported in the trust store of the Point-of-Service client.

Set up the Security for Tender Authorization for ACI

Either the server or client can host communication with ACI PINComm. If ACI PINComm was selected in the Tender Authorization window, you must update the security for the JRE on either the server or client where the communication is hosted. For more information, see "Install the Java Cryptography Extension (JCE)".

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

Table 3–3 (Cont.) <POS_install_directory>\pos Subdirectories

Name	Contents
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.

To run Point-of-Service:

1. Start the store server:

   `<INSTALL_DIR>\Server\pos\bin\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:

   `<INSTALL_DIR>\Client\pos\bin\ClientConduit.bat`

3. Verify the installation on each register by logging in to Point-of-Service. On the Main Options screen, select a component and complete the login. For more information, see the *Oracle Retail Point-of-Service User Guide*.

   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 on Novell SLEPOS

This chapter provides information about the installation procedures for Oracle Retail Point-of-Service. This chapter covers installing the server and clients on Novell SLEPOS. For a list of tested components and supported versions, 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 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;
```

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 TO <data_source_role>;
```

> **Note:** After the product is installed successfully, the CREATE SYNONYM privilege must be revoked from the data source role. Before the installer exits, it prompts for a database administrator to revoke the privilege.

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 connection 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 4–1:

Table 4–1 Server Tier Logical Components

Machine	Description
Store Server	The machine that runs the server component of Oracle Retail Point-of-Service. There is at least one store server for each store. This component runs as a service. This machine may also house the Back Office Server and other Oracle Retail POS Suite components such as the OracleRetailStore database.

Table 4–1 (Cont.) Server Tier Logical Components

Machine	Description
Point-of-Service Clients	The machines that execute the Point-of-Service transactions; they are typically cash registers.
Database Server	The machine that houses the OracleRetailStore databases. This machine may or may not be the same as the store server.
JMS Server	The machine that houses the JMS server software.

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

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

Installing the Database

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

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

Required Settings for the Database

During database creation, the database must be set to AL32UTF8.

Installing Point-of-Service on Machines

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

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

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

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

Updating Device Configuration

Instructions for configuring peripheral devices are in Appendix H:

- "Configuring Devices for an NCR Register"
- "Configuring Devices for an IBM SurePOS Register"
- "Configuring a Device for ACI PINComm"

Expand the Point-of-Service Distribution

To extract the Point-of-Service files:

1. Extract the Point-of-Service 14.1.2 distribution zip file.
2. Create a new staging directory for the Point-of-Service application distribution `ORPOS-14.1.2.zip` file, for example, `/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-14.1.2.zip` to *<staging_directory>* and extract its contents. The following files and directories should be created under *<staging_directory>*`/ORPOS-14.1.2`:

```
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
revokesyn.sql
wallet.xml
```

For the remainder of this chapter, *<staging_directory>*`/ORPOS-14.1.2` is referred to as *<INSTALL_DIR>*.

Obtain the JRE Required for Client Install

This release requires IBM JRE 1.7 for client installs on IBM SurePOS registers. It is distributed by IBM with JavaPOS 1.13.

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 in the Secure Options window. See Figure A–17.
  - 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 in the Enable Client Secure RMI window. See Figure B–23.
  - 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*.

Enable Order Integration

Point-of-Service supports processing orders thorough an external order management system and Commerce Anywhere. To enable order integration:

1. In the Integration Applications window, select **Orders**. See Figure A–13 and Figure B–17.
2. Select the order type. See Figure A–14 and Figure B–18:
   - To use an external order management system, select **External Order**.
   - To use Commerce Anywhere, select **Commerce Anywhere**.

External Order Management System

You provide the information for accessing the web service for the external order management system. For more information on integrating with an external order management system, see the *Oracle Retail POS Suite Implementation Guide, Volume 4 - Point-of-Service External Order*.

Commerce Anywhere

Commerce Anywhere enables retailers to integrate with e-commerce and order management solutions for processing customer transactions in stores and through web applications.

You provide the information for accessing the web services for Commerce Anywhere.

For more information on Commerce Anywhere, see the following documents available through My Oracle Support. Access My Oracle Support at the following URL:

https://support.oracle.com

Oracle Retail Commerce Anywhere Technical Integration Solution (Doc ID: 1598187.1)

This set of architectural diagrams and related business processes depict the Commerce Anywhere solution and its major integration points. The conceptual representation that is depicted is intended to support an integrated implementation of an Oracle Retail Commerce Anywhere solution that includes Oracle Retail Merchandising System, Oracle Retail Store Inventory Management, Oracle Retail Warehouse Management System, Oracle Retail POS Suite, and Oracle Retail Advanced Inventory Planning.

Oracle Retail Commerce Anywhere Functional White Papers (Doc ID: 1598177.1)

This library contains a collection of white papers that outline functional aspects of the Commerce Anywhere solution in Oracle Retail applications. One document provides an overview of the solution from an enterprise perspective, and it is accompanied by product specific-papers addressing Oracle Retail Merchandising System, Oracle Retail Store Inventory Management, Oracle Retail Warehouse Management System, Oracle Retail POS Suite, and Oracle Retail Advanced Inventory Planning.

Database Install Options

In the Install Database Option window, you select whether the installer creates and populates the database schema or if you want to do this manually. See Figure A–20.

Caution: If the database schema is already created and populated, select **Skip schema creation and data loading**. Selecting one of the other options will result in the loss of the data already in the database. If the database schema was created and populated using Point-of-Service, 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 in the Sample Dataset installer window. See Figure A–21. You can obtain the `sample-dataset-14.1.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 in the window. You

choose this option if you want to create and populate the database schema manually or the database schema was created using Back Office.

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 the RSA Data Protection Manager

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

- "Obtain the RSA Client Configuration File"
- "Obtain the RSA Data Protection Manager Jar Files"
- "Obtain the RSA Libraries for Lockbox"
- "Install the Java Cryptography Extension (JCE)"

Obtain the RSA Client Configuration File

You must provide the installer with the name and location of the configuration property file in the RSA Client Configuration window. See Figure A–66 and Figure B–32. For detailed information on the content of this file, see the Java client documentation provided by your provider for the RSA Data Protection Manager.

Obtain the RSA Data Protection Manager Jar Files

You must obtain the required jar files from your RSA Data Protection Manager provider. You provide the location of the jar files in the RSA Client JAR Files window. See Figure A–65 and Figure B–31. The directory for the jar files must contain only the RSA Java client jar files.

Obtain the RSA Libraries for Lockbox

Lockbox is an RSA feature the provides protection for RSA configuration information. Obtain these libraries from your RSA Data Protection Manager.

You must also update the path variable, LD_LIBRARY_PATH, for the lockbox libraries.

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
     mv local_policy.jar local_policy.jar.bak
     mv US_export_policy.jar US_export_policy.jar.bak
     ```

   - On the client:

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

2. Download version 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 window 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.

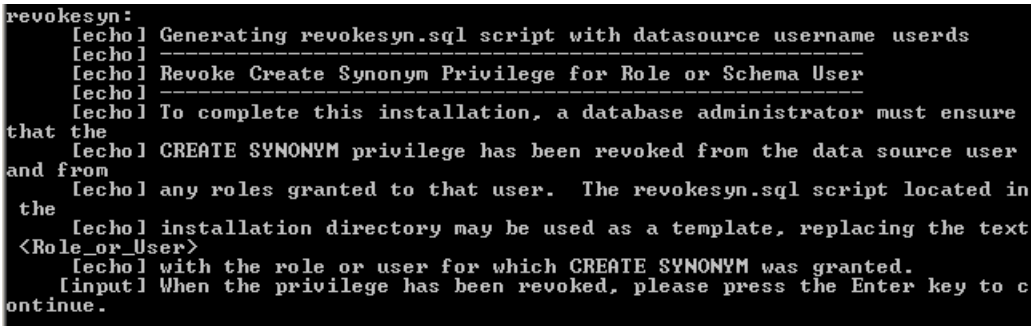
3. When installing the store server, set the account of the user running the installer to run as an administrator. Set the account using Microsoft Windows 2008 Server.
4. Run the `install.cmd` script. This will launch the installer. After installation is complete, a detailed installation log file is 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 server install, after the installation is successfully completed, the CREATE SYNONYM privilege must be revoked. In the installer console window, it prompts for a database administrator to run the revokesyn SQL script to revoke the privilege. The script is found in the *<INSTALL_DIR>* directory.

Figure 4–1 Installer Prompt to Run revokesyn



For information on granting this privilege, see "Create the Database Schema Owner and Data Source Users".

6. If this is a client install and you are using a DigitalPersona fingerprint device on an IBM SurePOS register, 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 =
     //opt//DigitalPersona//Bin//JavaPOS//dpjavapos.jar
     input.dpfingerprint.jpos = //opt//DigitalPersona//Bin//JavaPOS//jpos113.jar
     input.dpfingerprint.dpotjni = //opt//DigitalPersona//Bin//Java//dpuareu.jar
     ```

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

Resolve Errors Encountered During Application Installation

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

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

Configure Devices for Fiscal Printing

The fiscal printer JPOS API does not support barcode printing. The implementation for this release uses an Epson-specific directIO command to print the barcode. The directIO command is configured in the DeviceContext.xml file. The command and its parameters control the barcode alignment (position in the receipt), barcode width, and barcode type.

To configure the fiscal printing device for barcode printing, make changes to the following file:

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

Update the following entry in that file:

```
<property name="barcodeDirectIO">
    <map>
        <entry key="command" value="1075" />
        <entry key="parameters" value="011203075210073" />
    </map>
</property>
```

The following table describes the parameters entry in the preceding example:

Value	Description
01	Operator. Any two digit number can be used.
120	Left margin (120 at 180 dpi equals 17 mm, plus offset of 3 mm, equals 20 mm).
03	Dot width of each bar (3 at 180 dpi equals 4 mm).
075	Height in dots of the barcode (120 at 180 dpi equals 17 mm).
2	Human Readable Interpretation (HRI) numerical representation text (0 = none, 1 = above, 2 = below, and 3 = both above and below).
1	Font for text that can be printed above and below the barcode. HRI numerical representation text font (1, 2, or 3).
00	Always set to 00.
73	Barcode type.

The left margin and dot width in the example are configured for a 13-digit transaction ID. To accommodate the 26-digit transaction ID, the left margin needs to be reduced to 080 and dot width to 02.

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

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

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

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

Resolve Misprinted Character Problems in eReceipts

To resolve misprinted character problems in eReceipts:

1. Verify that the operating system is installed with a fixed-width font capable of cleanly displaying the misprinted character. For example on Microsoft Windows,

MS Gothic can be used to display Chinese characters and Courier New can be used to display Russian characters.

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

2. In the style-sheet used by the Point-of-Service client for eReceipts, specify the best font available for the language on the operating system. Point-of-Service uses Extensible Style-sheet Language Formatting Objects (XSL-FO) to transform each line of receipt data into PDF output. The style-sheet used for eReceipts specifies the Courier font family. To specify a different font, such as SimSun or Courier New, replace the reference to Courier with the new font name in the following files:
   - *<POS_install_directory>*/*<client>*/pos/receipts/printing/templates/xsl/ipp_default.xsl
   - *<POS_install_directory>*/*<client>*/pos/receipts/printing/templates/xsl/ipp_image_receipt.xsl

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

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

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

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

Resolve Misprinted Character Problems in Network Printed Receipts and Reports

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

1. Verify that the operating system is installed with a fixed-width font capable of cleanly displaying the misprinted character. For example on Microsoft Windows, MS Gothic can be used to display Chinese characters and Courier New can be used to display Russian characters.

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

2. In the style-sheet used by the Point-of-Service client for network printing, specify the best font available for the language on the operating system. Point-of-Service uses Extensible Style-sheet Language Formatting Objects (XSL-FO) to transform each line of receipt or report data into the type of output designated for the configured network printer. The style-sheet used for network printing specifies the Courier font family. To specify a different font, such as MS Gothic or Courier New, replace the reference to Courier with the new font name in the following file:

   <POS_install_directory>/*<client>*/pos/receipts/printing/templates/xsl/ipp_

```
default.xsl
```

Enable Dashboard and Browser Functionality in the Client Installation

Point-of-Service provides the capabilities to display a dashboard in the Main Options screen and access a web site from a register using the **Browser** button in the Main Options screen. JavaFX is required for both the dashboard and browser functionality. If the version of IBM JRE you are using does not support JavaFX, contact IBM for assistance.

Accessing Web Sites Through a Secure HTTP Connection

If a web site is accessed through a secure HTTP connection, an SSL certificate is required. The SSL certificate of the web site, which you want to access through the Point-of-Service embedded browser, should be imported in the trust store of the Point-of-Service client.

Set up the Security for Tender Authorization for ACI

Either the server or client can host communication with ACI PINComm. If ACI PINComm was selected in the Tender Authorization window, you must update the security for the JRE on either the server or client where the communication is hosted. For more information, see "Install the Java Cryptography Extension (JCE)".

Results of a Point-of-Service Installation

The default root directory for OracleRetailStore applications on Windows for the store server is `/OracleRetailStore/Server`. For the client, the default directory is `/OracleRetailStore/Client`. In this guide, these directories are referred to as *<POS_install_directory>*. The subdirectories listed in Table 4–2 are created:

Table 4–2 <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 4–3:

Table 4–3 <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.

To run Point-of-Service:

1. Start the store server:

   `<INSTALL_DIR>/Server/pos/bin/StoreServerConduit.sh`

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

2. Start the registers.

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

   `<INSTALL_DIR>/Client/pos/bin/ClientConduit.sh`

3. Verify the installation on each register by logging in to Point-of-Service. On the Main Options screen, select a component and complete the login. For more information, see the *Oracle Retail Point-of-Service User Guide*.

   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.

5

Installation of Mobile Point-of-Service

This chapter provides information about the installation procedures for the Mobile Point-of-Service server. For a list of tested components and supported versions, 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".

Update Oracle WebLogic for RSA

If using the RSA Data Protection Manager, WebLogic needs to be updated for the RSA jars and log4j jar. The RSA jar files must be obtained from your provider for the RSA Data Protection Manager. The following RSA and log4j jar files need to be added:

- cryptojce.jar
- cryptojcommon.jar
- jcm.jar
- jcmFIPS.jar
- kmsclient.jar
- LB.jar
- LBJNI.jar
- sslj.jar
- log4j-1.2.17.jar

To set up the jars to use RSA Data Protection Manager:

1. Copy the RSA jar files and the log4j.jar file to the appropriate directories.
2. Set the CLASSPATH:
   - To set the CLASSPATH for Microsoft Windows, edit commEnv.cmd in the *<WebLogic_HOME>*\wlserver_10.3\common\bin directory:

     ```
     PRE_CLASSPATH=%MODULES_DIR%\javax.persistence_
     2.1.0.v201304241213.jar;%MODULES_DIR%/eclipselink.jar;<RSA_JARS_
     LOCATION>\cryptojce.jar;<RSA_JARS_LOCATION>\cryptojcommon.jar;<RSA_JARS_
     LOCATION>\jcm.jar;<RSA_JARS_LOCATION>\jcmFIPS.jar;<RSA_JARS_
     ```

```
LOCATION>\kmsclient.jar;<RSA_JARS_LOCATION>\LB.jar;<RSA_JARS_
LOCATION>\LBJNI.jar;<RSA_JARS_LOCATION>\sslj.jar;<APACHE_JARS_
LOCATION>\log4j-1.2.17.jar
```

- To set the CLASSPATH for Novell SLEPOS, edit commEnv.sh in the <*WebLogic_HOME*>/wlserver_10.3/common/bin directory:

```
PRE_CLASSPATH="${MODULES_DIR}/javax.persistence_
2.1.0.v201304241213.jar:${MODULES_DIR}/eclipselink.jar:<RSA_JARS_
LOCATION>/cryptojce.jar:<RSA_JARS_LOCATION>/cryptojcommon.jar:<RSA_JARS_
LOCATION>/jcm.jar:<RSA_JARS_LOCATION>/jcmFIPS.jar:<RSA_JARS_
LOCATION>/kmsclient.jar:<RSA_JARS_LOCATION>/LB.jar:<RSA_JARS_
LOCATION>/LBJNI.jar:<RSA_JARS_LOCATION>/sslj.jar:<APACHE_JARS_
LOCATION>/log4j-1.2.17.jar"
```

3. After setting the variable, look on the console and make sure the jars are added to the CLASSPATH. If they are not added, shut down WebLogic and add the jars to the WEBLOGIC_CLASSPATH variable in the same file. Put the jar files ahead of the WebLogic jar files.

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

You can skip this section if you are manually 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.

Server Name Considerations

Each server instance in your WebLogic environment must have a unique name, regardless of the domain in which it resides. Within a domain, each server, machine, virtual host, and any other resource type must be named uniquely and must not use the same name as the domain.

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.

Enabling Trust Between WebLogic Server Domains

The WebLogic Server enables you to establish global trust between two or more domains. You do this by specifying the same Domain Credential for each of the domains. By default, the Domain Credential is randomly generated and therefore, no two domains have the same Domain Credential. During installation, the WebLogic domain credential is configured to the value entered in the Domain Details installer window. For more information, see Figure C–19.

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

Secure Sockets Layer

Mobile Point-of-Service is accessed through a secure HTTP connection. Enable the Secure Sockets Layer (SSL) when creating the domain and set the listen port and SSL

list port number so that the numbers are unique for each domain in your configuration.

Verify that the domain's administrative server is started and in running mode.

General Steps for Creating a New Domain

In addition to specific steps previously described, you can use the following steps to create a new domain using the WebLogic Configuration Wizard:

1. Log on to the server, which is running your WebLogic installation, as the user who owns the WebLogic installation.
2. Launch the Weblogic Configuration Wizard.
3. Select **Create a new WebLogic Domain**. The domain can be a basic WebLogic server domain.
4. Choose a unique name for the new domain. In the remainder of this installation guide, <*ormpos-domain*> is used for the name.
5. Configure the administrator user name and password.
6. Configure the server start mode and JDK.
7. Configure the Administration Server.

Before launching the Mobile Point-of-Service installer:

1. Start the Administration Server.
2. Verify that the domain's Administration Server is started and in running mode.

WebLogic Domain Startup Mode

WebLogic can be run in production mode or development mode.

Boot Identity Files

When a domain is created in development mode using the Configuration Wizard, a boot identity file, named `boot.properties`, is created in the Administration Server's root directory. The boot identity file contains an encrypted version of the user name and password which lets you bypass the login prompt during instantiations of the server. In production mode, WebLogic prompts for credentials on the command line.

To install the Mobile Point-of-Service server on a domain using production mode, you must first create a boot identity file so that the Administration Server can bypass the prompt for user name and password when the installer restarts the server.

Consult your WebLogic documentation for more information and options for creating boot identity files. Following is an example of one method, that can be used after domain creation, to create the boot identity file:

1. Start the Administration Server at least once and provide the user credentials on the command line.
2. Create the Administration Server's security directory, if it does not already exist.

   `<WEBLOGIC_INSTALL_DIR>/user_projects/domains/<ormpos-domain>/servers/<AdminServerName>/security`

3. Place the following two lines in a file named `boot.properties` in the `security` directory:

   `password=<password>`

```
username=<username>
```

Note: There should be no spaces on either side of the equal sign.

4. Stop and restart the Administration Server to verify that the credential prompts are bypassed.

Expand the Mobile Point-of-Service Distribution

To extract the Mobile Point-of-Service files:

1. Extract the Mobile Point-of-Service 14.1.2 distribution zip file.
2. Create a new staging directory for the Mobile Point-of-Service application distribution `ORMPOS-14.1.2.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-14.1.2.zip` to *<staging_directory>* and extract its contents. The following files and directories should be created under *<staging_directory>*`\ORMPOS-14.1.2`:

```
ant\
ant-ext\
antinstall\
connectors\
installer-resources\
mobilepos\
.postinstall.cmd
.postinstall.sh
.preinstall.cmd
.preinstall.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-14.1.2` is referred to as *<INSTALL_DIR>*.

Set Up for Integration with Central Office

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

Enable Commerce Anywhere Integration

Commerce Anywhere enables retailers to integrate with e-commerce and order management solutions for processing customer transactions in stores and through web applications.

In the Enable Commerce Anywhere installer window, you select whether integration with Commerce Anywhere is enabled. See Figure C–39.

For more information on Commerce Anywhere, see the following documents available through My Oracle Support. Access My Oracle Support at the following URL:

`https://support.oracle.com`

Oracle Retail Commerce Anywhere Technical Integration Solution (Doc ID: 1598187.1)

This set of architectural diagrams and related business processes depict the Commerce Anywhere solution and its major integration points. The conceptual representation that is depicted is intended to support an integrated implementation of an Oracle Retail Commerce Anywhere solution that includes Oracle Retail Merchandising System, Oracle Retail Store Inventory Management, Oracle Retail Warehouse Management System, Oracle Retail POS Suite, and Oracle Retail Advanced Inventory Planning.

Oracle Retail Commerce Anywhere Functional White Papers (Doc ID: 1598177.1)

This library contains a collection of white papers that outline functional aspects of the Commerce Anywhere solution in Oracle Retail applications. One document provides an overview of the solution from an enterprise perspective, and it is accompanied by product specific-papers addressing Oracle Retail Merchandising System, Oracle Retail Store Inventory Management, Oracle Retail Warehouse Management System, Oracle Retail POS Suite, and Oracle Retail Advanced Inventory Planning.

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 in the Enable Secure JDBC window, 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 Client 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–49.

Register Accountability

Accountability determines whether one or more than one operator can be assigned to a till on a given business day. Each register associated with a mobile device must be configured to use register accountability.

This configuration is stored in the Accountability Code column (cd_act) of the Workstation database table (as_ws). Run the following SQL statement for each register ID associated with a Unique Vendor Identifier (UVID). In this example, the register ID is 200, the store id is 04241, and the accountability code is 0 (Register).

update as_ws set cd_act='0' where id_ws='200' and id_str_rt='04241';

A register is associated with a UVID in the Mobile Device Configuration window. See Figure C–35.

Obtain the Files Needed for the RSA Data Protection Manager

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

- "Obtain the RSA Client Configuration File"
- "Obtain the RSA Data Protection Manager Jar Files"
- "Obtain the RSA Libraries for Lockbox"
- "Install the Java Cryptography Extension (JCE)"

Obtain the RSA Client Configuration File

You must provide the installer with the name and location of the configuration property file in the RSA Client Configuration window. See Figure C–16. For detailed information on the content of this file, see the Java client documentation provided by your provider for the RSA Data Protection Manager.

Obtain the RSA Data Protection Manager Jar Files

You must obtain the required jar files from your RSA Data Protection Manager provider. You provide the location of the jar files in the RSA Client JAR Files window. See Figure C–15. The directory for the jar files must contain only the RSA Java client jar files.

Obtain the RSA Libraries for Lockbox

Lockbox is an RSA feature the provides protection for RSA configuration information. Obtain these libraries from your RSA Data Protection Manager.

You must also update the path variable for the lockbox libraries. For Microsoft Windows, update the PATH variable. For Novell SLEPOS, update the LD_LIBRARY_PATH variable.

Install the Java Cryptography Extension (JCE)

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

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

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

2. Download version 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 window 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 2012 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.

Disable Non-SSL Port

You can choose to disable the non-SSL port in the Turn Off the Application Server's Non-SSL Port window. See Figure C–54. If you select **Yes** in the window, 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 window. See Figure C–52.

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:

  Note: The application server's non-SSL listen port must be enabled before running the ant target described here. The non-SSL listen port can be enabled using the WebLogic Admin Console. After these steps are completed, the non-SSL listen port can be disabled so the server can only be reached on the SSL listen port.

  1. 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.
  2. Update the following property in the `ant.install.properties` file.

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

  3. Run the following ant target:

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

- To deploy from the application server console:

  1. 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.
  2. Run the following target:

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

3. 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 for iOS and Android. The following information is included:

- "Setting Up the Mobile POS Application Xcode Project"
- "Setting Up the Mobile POS Application Android Project"
- "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 14.1 distribution zip file.

The `ORMPOS-14.1.2_client.zip` file in the distribution zip file contains the Xcode projects used for building the Mobile POS Handheld iOS application that runs on iPod Touch (5th Generation) devices and Mobile POS Tablet iOS application that runs on iPad mini 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-14.1.2_client.zip` file.
2. Copy the `ORMPOS-14.1.2_client.zip` file into the new directory.
3. Unzip the file into the new directory.
4. Open the `mobilepos` directory, created in Step 3, by using `mobilepos-14.1.2.xcodeproj`.
5. Having obtained the Provisioning from Apple, change the Bundle Identifier and Team fields on XCode for each of the targets (mobilepos/mpft).
6. Navigate to the build settings and change the code signing to point to the iPhone Distribution obtained from Apple.

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. For the tablet, in the `mobilepos/www/tablet/js` directory. For the handheld, in the `mobilepos/www/handheld/js` directory.
- CSS files for the tablet, in the `mobilepos/www/tablet/css` directory. CSS files for the handheld, in the `mobilepos/www/handheld/css` directory.
- Translation bundles for the tablet, in the `mobilepos/www/tablet/js/translations` directory. Translation bundles for the handheld, in the `mobilepos/www/handheld/js/translations` directory.

Adding new JavaScript and CSS files to the project requires referencing those files in the `mobilepos/www/tablet/index.html` file for the tablet. For the handheld, reference those files in the `mobilepos/www/handheld/index.html` file.

Install the PhoneGap Library

Mobile POS also has an external dependency on the PhoneGap library, specifically PhoneGap 2.9.0.

To install the PhoneGap library:

1. Download the PhoneGap 2.9.0 package from the following web site:

   `http://phonegap.com/install`

2. Unzip the PhoneGap 2.9.0 package that was downloaded in Step 1. This creates a directory named `phonegap-2.9.0`.
3. In Finder, navigate to `phonegap-2.9.0/lib/ios/Cordovalib`.
4. Double-click `CordovaLib.xcodeproj` to open the `CordovaLib` project in Xcode.
5. Within Xcode, click on the `CordovaLib` project in the Project Navigator.
6. Click the `CordovaLib` target in the main panel.
7. Click the Build Settings tab.
8. Select Product, Destination, and then iOS Device or the name of an attached iOS device.
9. Perform a clean and build of the product. This creates the PhoneGap 2.9.0 library, `libCordova.a`.
10. In the Project Navigator, expand the Products folder. Right click on `libCordova.a` and select **Show in Finder**. A new Finder window opens showing a directory with `libCordova.a` and a directory named `include`.
11. Copy `include` and `libCordova.a` to the `mobilepos/lib/PhoneGap` directory.
12. Navigate to `phonegap-2.9.0/lib/ios/Cordovalib` and copy the `cordova.js` file. Place it into the `mobilepos/www/js` directory.
13. Restart the mobilepos-14.1.2.xcodeproj file in the mobilepos directory. This opens the project in Xcode.
14. Do a clean-build to each of the targets against IOSDevice.

Install the VeriFone VX600 Sled Framework

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

1. Obtain the supported version of the VeriFone framework, 1.0.4.257, 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 `mobilepos/lib/NullSled` directory. This overwrites the existing VMF.framework.
4. Restart the mobilepos-14.1.2.xcodeproj file in the mobilepos directory. This opens the project in Xcode.
5. Do a clean-build to each of the targets against IOSDevice.

Install the AJB Framework Library

To install the AJB Framework library:

1. Get the AJB.framework build 100 from AJB Software Design Inc. Following is the primary sales contact for obtaining the AJB Framework:

   Pat Polillo

   e-mail: ppolillo@ajbsoftware.com

   phone: 905-238-4462
2. After unzipping theAJB framework provided by AJB, copy AJB.Framework to mobilepos. Drag the AJB.framework file on to the XCode Project Navigator section and drop it in the `mobilepos/Frameworks` directory. This should prompt you to select the targets to which references need to be added. Select both mobilepos and MPFT.
3. Under the mobilepos/Frameworks/MobilePOS.framework, uncomment the following line from MobilePOS.h:

   ```
   #import "AJBPaymentProvider.h"
   ```
4. Under mobilepos/mobilepos/Classes, uncomment the following lines from AppDelegate.m:

   ```
   #import "AJBPaymentProvider.h"
   self.paymentProvider = [[AJBPaymentProvider alloc] init]; under runCustomtartUp
   ```
5. Under mobilepos/mobilepos/Plugins, uncomment the following lines from PaymentAcquisitionPlugin.m:

   ```
   #import <AJB/FiPaySled.h>
   #import "AJBPaymentProvider.h"
   ```

   From the isDeviceConnected function, uncomment all commented out lines. After uncommenting everything, it should look like the following:

   ```
   - (void) isDeviceConnected:(NSMutableArray *)arguments
   withDict:(NSMutableDictionary *)options
   {
       NSString *callback = [arguments pop];

      AppDelegate *appDelegate = (AppDelegate*)[[UIApplication sharedApplication]
   delegate];
       if (appDelegate.paymentProvider != nil &&

           [appDelegate.paymentProvider isMemberOfClass:[AJBPaymentProvider
   class]]) {
   ```

```
        AJBPaymentProvider *app =
 (AJBPaymentProvider*)appDelegate.paymentProvider;

        if (app.isDeviceConnected) {

            CDVPluginResult* pluginResult = [CDVPluginResult
resultWithStatus:CDVCommandStatus_OK];
            [self writeJavascript: [pluginResult
toSuccessCallbackString:callback]];
            return;

        } else {

            CDVPluginResult* pluginResult = [CDVPluginResult
resultWithStatus:CDVCommandStatus_ERROR];
            [self writeJavascript: [pluginResult
toErrorCallbackString:callback]];
            return;

        }
    }
    else {
        CDVPluginResult* pluginResult = [CDVPluginResult
resultWithStatus:CDVCommandStatus_OK];
        [self writeJavascript: [pluginResul toSuccessCallbackString:callback]];
        return;
    }

}
```

6. Go to finder and navigate to `mobilepos/mobilepos/classes`. Drag the AJBPaymentProvider.m on the Xcode under `mobilepos/mobilepos/classes`. This should prompt you to select the targets to which references need to be added. Select both mobilepos and MPFT. Once done, AJBPaymentProvider.m must be seen added to "compile Sources" under the respective targets(mobilepos/mpft) "Build Phases" tab.
7. From project navigator, Select mobilepos. For each of the targets, navigate to the Info tab. Under Custom iOS Target Properties, change the value of ActivePaymentFramework from blank to AJBPaymentProvider.
8. Right-click mobilepos/mobilepos/Resources/targets/mobilepos/Settings.bundle/Root.plist and open it as source code. Text needs to be added for each of the targets to configure the AJB payment host and port.

   In Root.plist, add the text before the following code:

```
<dict>
    <key>Title</key>
    <string>Sled</string>
    <key>Type</key>
    <string>PSGroupSpecifier</string>
</dict>
```

   Add the text, shown in the following example, for each of the targets to configure the AJB payment host and port. Add the text before the code shown in the previous example:

```
<dict>
    <key>Title</key>
```

```
    <string>Payment Server</string>
    <key>Type</key>
    <string>PSGroupSpecifier</string>
</dict>
<dict>
    <key>AutocapitalizationType</key>
    <string>None</string>
    <key>AutocorrectionType</key>
    <string>No</string>
    <key>IsSecure</key>
    <false/>
    <key>Key</key>
    <string>payment_host</string>
    <key>KeyboardType</key>
    <string>URL</string>
    <key>Title</key>
    <string>Payment Host</string>
    <key>Type</key>
    <string>PSTextFieldSpecifier</string>
</dict>
<dict>
    <key>IsSecure</key>
    <false/>
    <key>Key</key>
    <string>payment_port</string>
    <key>KeyboardType</key>
    <string>NumberPad</string>
    <key>Title</key>
    <string>Payment Port</string>
    <key>Type</key>
    <string>PSTextFieldSpecifier</string>
</dict>
<dict>
    <key>IsSecure</key>
    <false/>
    <key>Key</key>
    <string>payment_idle_timeout</string>
    <key>KeyboardType</key>
    <string>NumberPad</string>
    <key>Title</key>
    <string>Idle Timeout (seconds)</string>
    <key>Type</key>
    <string>PSTextFieldSpecifier</string>
</dict>
```

9. Do a clean-build to each of the targets against IOSDevice.

Verify the Build Settings

To verify the build settings:

1. Double-click the `mobilepos-14.1.2.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. 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 14.1.2.

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 for iOS".

Configuring and Deploying the MPOS UI Certificate for iOS

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 *Managing Your Team* section in the *App Distribution 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 *Managing Your Team* section in the *App Distribution 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 *Managing Your Team* section in the *App Distribution 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 identifier from the Organizer. This is a 40-digit hexadecimal number. Send this identifier 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 *Managing Your Team* section in the *App Distribution 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, under the iOS device attached, there is Provisioning Profiles. If the provision is not in the list, add one by clicking Add at the bottom and pointing it to the provisioning file. The team administrator is notified of this development certificate request.
2. 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 *Managing Your Team* section in the *App Distribution 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. 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, there should be Debug and Release options. Click the value next to Debug and choose the newly installed iOS developer identity from the list.
3. Make sure the project is built for debug and not release. In the Xcode scheme editor, click the build target and select **Edit Scheme**.
4. Click **Run <*project name*>**. In the Info tab, choose **Debug** for the Build Configuration setting.
5. 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 *Managing Your Team* section in the *App Distribution 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 *Managing Your Team* section in the *App Distribution 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 *Managing Your Team* section in the *App Distribution 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 **Distribute**. 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 Concerning Certificates

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 8 are listed here:

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

  To access the list of trusted certificates for Android, select Settings, Security, and then Trusted Credentials.

- 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".

Setting Up the Mobile POS Application Android Project

This section describes how to set up the Mobile POS Android project included in the Mobile Point-of-Service Release 14.1.2 distribution zip file.

Set Up the Development Environment

Android SDK and Eclipse IDE, with the ADT plug-in, are prerequisites for setting up the MPOS Android project. The Android SDK and ADT plug-in installers, installation instructions, and system requirements are available in the Android developer portal at the following web site:

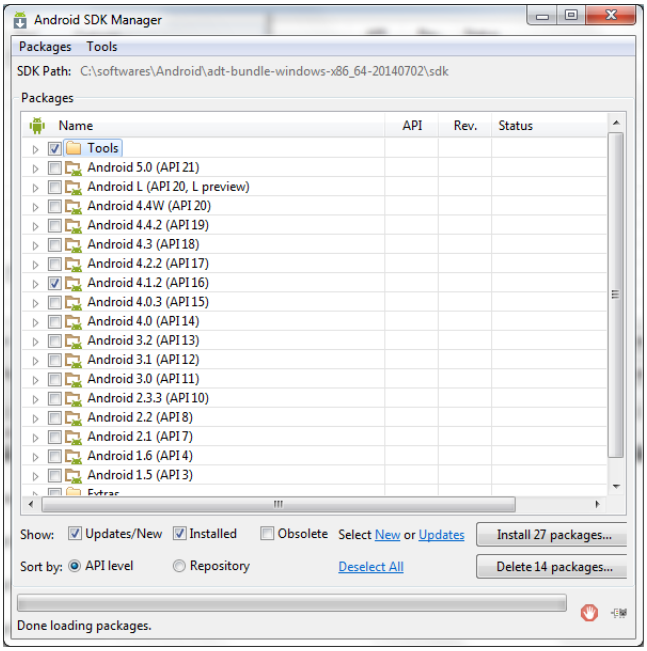
http://developer.android.com

Note: Java 7 JDK or later within the Java 7 code line is required for compiling the MPOS projects.

Update Android SDK Manager

Install Android SDK 4.1.2 (API16) using the Android SDK manager. Launch the SDK manager from the Eclipse tool bar or SDK manager installation folder.

Figure 5–1 Android SDK Manager Installation Window



The Intel x86 Emulator Accelerator (HAXM Installer) package, available under Extras, can be installed to speed up the Android application emulation. For more information on system requirements and installation steps, see the following web site:

https://software.intel.com/en-us/android/articles/intel-hardware-accelerated-execution-manager

Install the Android Project

To install the Android project:

1. Create a directory to hold the extracted contents of the `ORMPOS-14.1.2_client_android.zip` file. The file contains projects for both MPOS editions (handheld and tablet).
2. Copy the `ORMPOS-14.1.2_client_android.zip` file into the new directory.
3. Extract the file into the new directory. The following directories are created:

   ```
   mobilepos
   MobilePOS_Android_Framework
   mpft
   www
   ```

4. Open the `mobilepos` or `mpft` directory created in Step 3.
5. The `mobilepos` and `mpft` directory structures are both a typical Android 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 Android Java. For best practices in extending, adding, and changing functionality and presentation in Mobile Point-of-Service, 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. For the tablet, in the `mobilepos/www/tablet/js` directory. For the handheld, in the `mobilepos/www/handheld/js` directory.
- CSS files for the tablet, in the `mobilepos/www/tablet/css` directory. CSS files for the handheld, in the `mobilepos/www/handheld/css` directory.
- Translation bundles for the tablet, in the `mobilepos/www/tablet/js/translations` directory. Translation bundles for the handheld, in the `mobilepos/www/handheld/js/translations` directory.

Adding new JavaScript and CSS files to the project requires referencing those files in the `mobilepos/www/tablet/index.html` file for the tablet. For the handheld, reference those files in the `mobilepos/www/handheld/index.html` file.

Install the PhoneGap Library for Android

Mobile POS has an external dependency on the PhoneGap library, specifically PhoneGap 2.9.0.

To install the PhoneGap library:

1. Download the PhoneGap 2.9.0 package from the following web site:

   `http://phonegap.com/install`

2. Extract the PhoneGap 2.9.0 package that was downloaded in Step 1. This creates a directory named `phonegap-2.9.0`.
3. Navigate to `phonegap-2.9.0/lib/android`.
4. Rename `cordova.js` to `cordova-android-2.9.0.js`.
5. Copy `cordova-android-2.9.0.js` and place it into the extracted `www/js` directory.
6. Copy the `cordova-2.9.0.jar` to the extracted `Mobilepos_Android_Framework/libs` directory.

Import the Android Project into the Workspace

To import the Android project:

1. The MPOS Handheld and Tablet projects use business logic code available in the `www` folder. Create a symbolic link from the Android project assets directory to the `www` directory:
   a. Open a command prompt as an administrator.
   b. Change to the mobilepos assets directory:

      cd <*MPOS_EXTRACT*>/mobilepos/assets

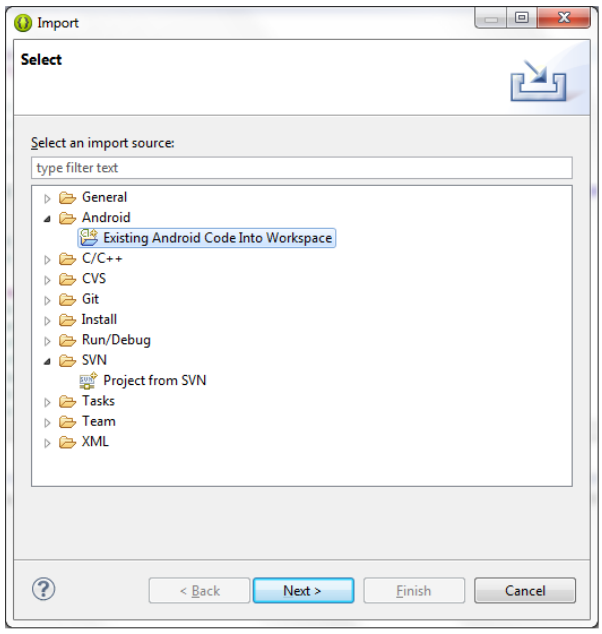
   c. Run the following command to create a symbolic link from `mobile/assets` to `www`:

      Microsoft Windows: mklink /D www <*path to www directory*>

      Linux: ln -s <*path to www directory*> www

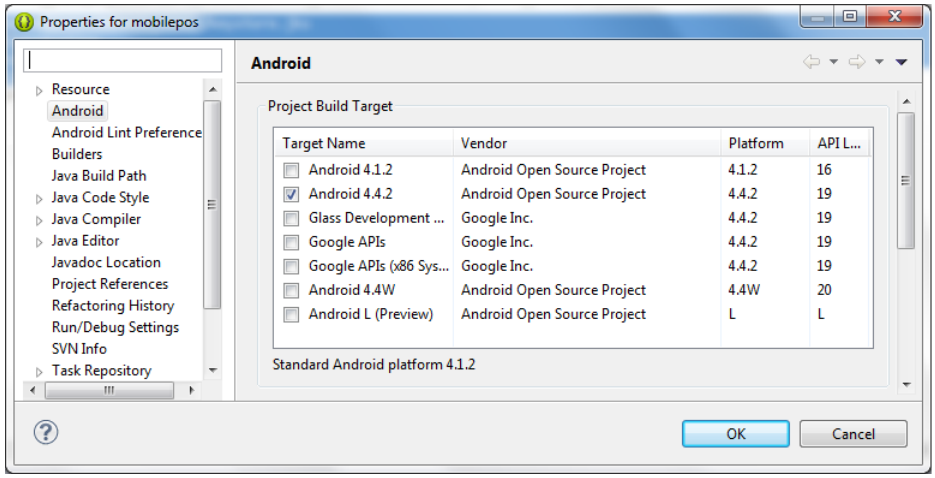
   d. Repeat Steps b and c for the `mpft` project.
2. Launch Eclipse ADT. Select File, Import, Android, and then Existing Android Code into Workspace.

Figure 5–2 Import Android Project Select Window



3. Select the directory to which the MPOS Android distribution file was extracted.
4. To complete the import, click **Finish**.
5. Set the Project Build Target to Android 4.4.2 for the mobilepos and mpft projects. From Eclipse Navigator, right-click mobilepos/mpft. Select Properties and then Android. Select Android 4.4.2. Click **OK**.

Figure 5–3 Set Project Build Target for Android



6. Clean build the projects. There should not be any compilation errors.

Deploying Mobile Point-of-Service to the Motorola MC40/ET1

This section describes the steps for deploying Mobile Point-of-Service to the Motorola tablet.

Install the Motorola USB Driver To install the USB driver to the Android development workstation:

1. Download the USB driver from the Motorola support web site using one of the following URLs:

   https://launchpad.motorolasolutions.com/Android/AndroidDrv010100.zip

   https://atgsupportcentral.motorolasolutions.com/ewa/pub/getFile.do?fileName=ssi/emb/downloads/AndroidDrv010201.zip

2. Extract the driver and run the executable.
3. After installation, reboot your machine as prompted.

Direct Deploy to the Device To directly deploy the application to the device:

1. Connect the ET1/MC40 to the development machine using the data cable.
2. Right click on the `mobilepos` project. Choose Run As and then Android application.
3. Select the connected device and run the application.

   The application throws an Invalid Server Settings error when the application is launched for the first time.
4. Press the Android home button. Go to Settings, Accounts, and then MPOS 14.1.2 or MPFT 14.1. Configure the MPOS application settings. For more information, see "Configuring the Mobile Point-of-Service Application on a Mobile Device".

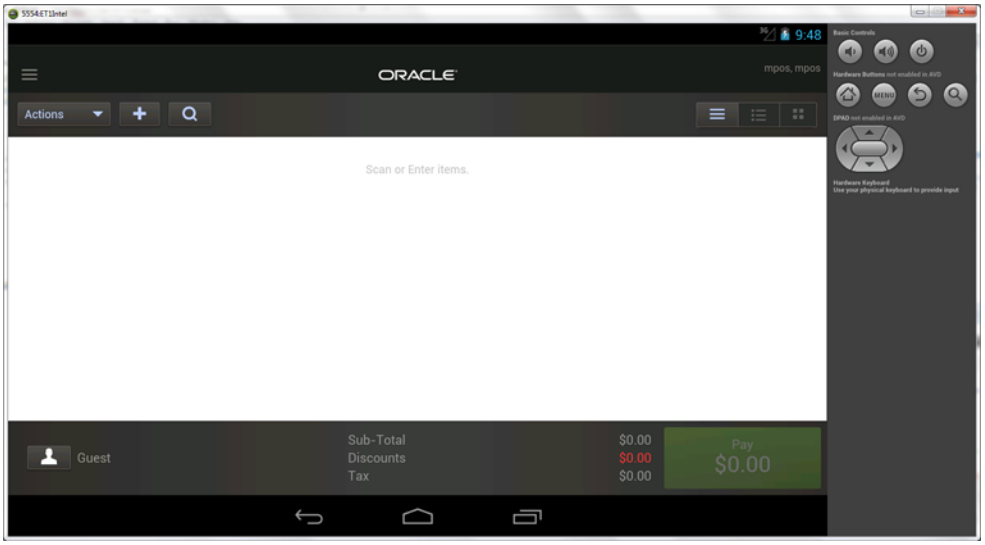
Deploy MPOS to Android Emulator To run the application on Android emulators:

1. Launch AVD Manager in Eclipse and create a device definition similar to the Android device used for running MPOS.
2. Create a virtual device using the device definition created in the Step 1. Set the target as Android 4.1.2.

   Note: Enter an SD card size in the virtual device definition, for example, 100.

3. Launch the emulator created in Step 2.
4. Right click on the `mobilepos/mpft` project and choose Run As and then Android application. The application is uploaded and installed to the Android emulator.

Figure 5–4 Android Emulator Screen



Create the Application for Distribution

To create the MPOS Android application installers:

1. Create the ANDROID_HOME environment variable with the value <*Android_SDK_DIR*>.
2. Open the `build.xml` file in the `<Android_SDK_DIR>/tools/ant` directory and change the properties java.target and java.source values from 1.5 to 1.7.
3. Android requires that all applications be digitally signed with a certificate before they can be installed. Generate a keystore.jks signing the installers and copy it to the `<Android_SDK_ DIR>\sdk` folder. For more information, see "Additional Notes Concerning Certificates" and the following web site:

   `http://developer.android.com/tools/publishing/app-signing.html`

4. After generating the keystore, the `ant.properties` file needs to be modified. Open the `ant.properties` file under the `mobilepos/mpft` project and set the values for the following properties:

   key.store=${env.ANDROID_HOME}/<*Keystore_Name*>

   key.alias= <*Alias_Name*>

   key.store.password=<*Keystore_Password*>Key.alias.password=<*Alias_Password*>

5. Open `<MPOS_EXTRACT>\MobilePOS_Android_Framework\local.properties` and update `sdk.dir` to point to the SDK installation directory, for example:

   sdk.dir=D:\\Android\\android-sdk

6. Open a command prompt and change directory to `mobilepos`, for example:

   `<MPOS_EXTRACT>\mobilepos\build.xml`

7. Set the ANT_HOME environment variable and run `ant clean release`.

   The signed and unsigned installers are created under the `dist` folder. The final mobile installation file will be similar to `<MPOS Application>-release.apk`.

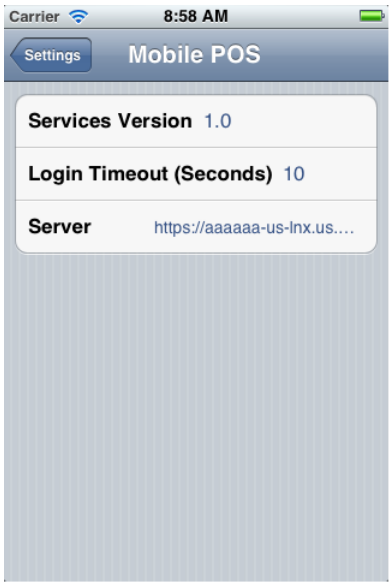
Note: The Eclipse ADT Android Tools also can be used for creating the MPOS Android application installers.

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. Get the UVID of the device. For more information, see "Obtaining the UVID after Installation". A register is associated with a UVID in the Mobile Device Configuration window. See Figure C–35.
2. Open the Settings screen for the Mobile POS application.

Figure 5–5 Mobile POS Settings Screen



3. 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/services`

4. When using AJB for payment authorization:
   a. For the payment host, enter the host name of the AJB FIPAY server.
   b. For the payment port, enter the default AJB port plus the register ID assigned to the device.

Note: Mobile POS Android applications only support payment using CPOI devices. The payment host and payment port fields are not used.

Sending Log Files in E-Mail

If the device log files are to be sent in e-mail from the device, an e-mail account needs to be set up on the device. For information on setting up the e-mail account, consult the documentation for the device.

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 Windows for Server Installation

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

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

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

> **Note:** The paths shown in the window examples in this appendix use the path format for Microsoft Windows. In the table describing those fields, example paths for both Microsoft Windows and Novell SLEPOS are shown.

Figure A–1 Introduction

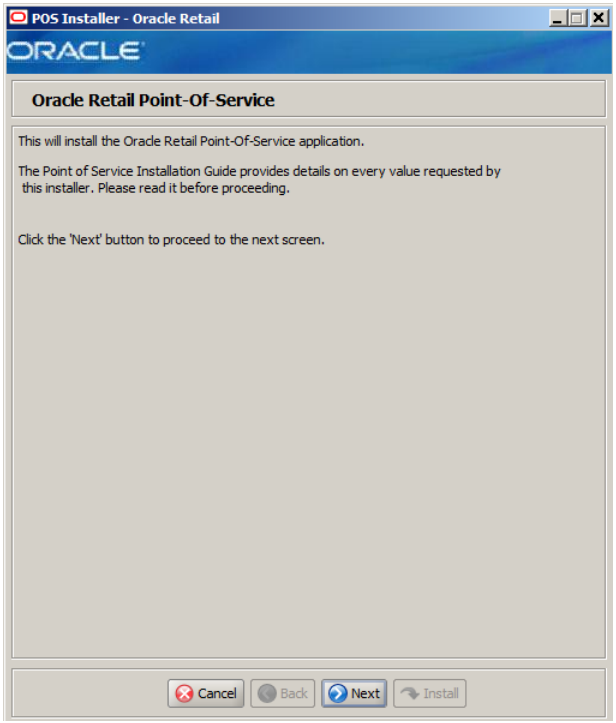


Figure A–2 Previous POS Install

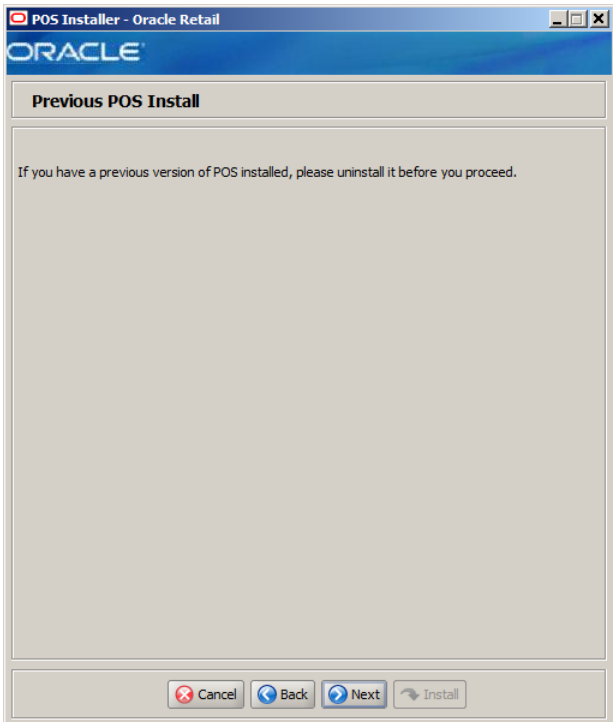
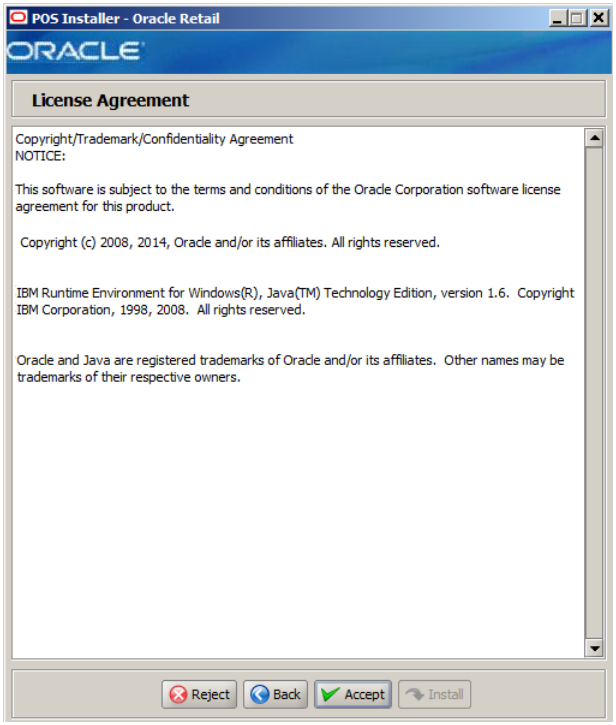
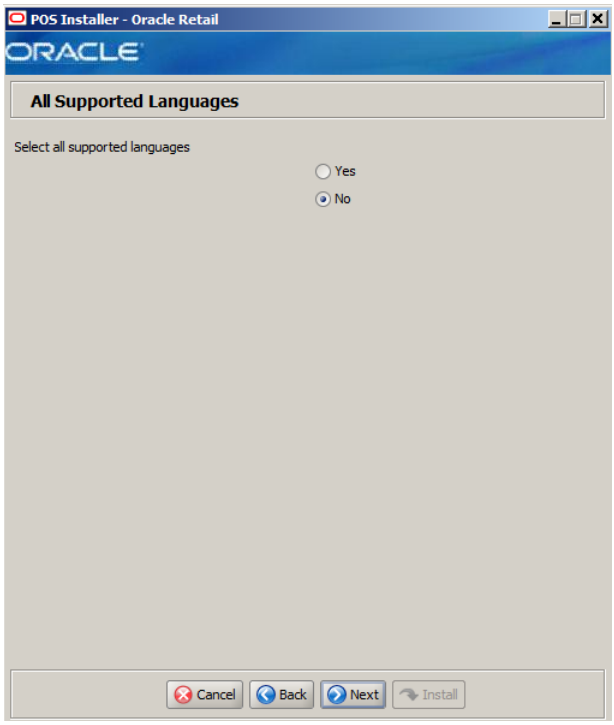


Figure A–3 License Agreement



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

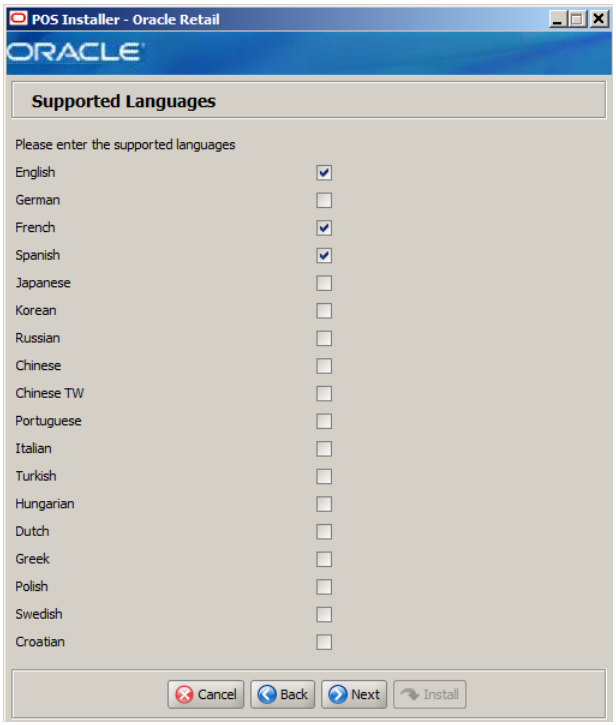
Figure A–4 All Supported Languages



The field in this window is described in the following table:

Details	Content
Field Title	Select all supported languages
Field Description	Choose whether all languages are initially selected on the Supported Languages screen: ▪ To have all available languages initially selected, select **Yes**. ▪ To have only English initially selected, select **No**.
Example	No

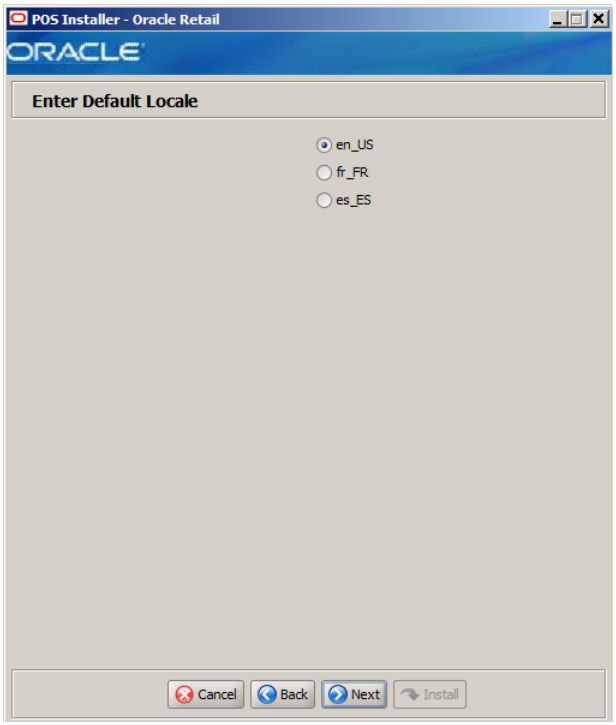
Figure A–5 Supported Languages



The field in this window 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 in this window determine the available choices in the Enter Default Locale window.
Example	English, French, and Spanish

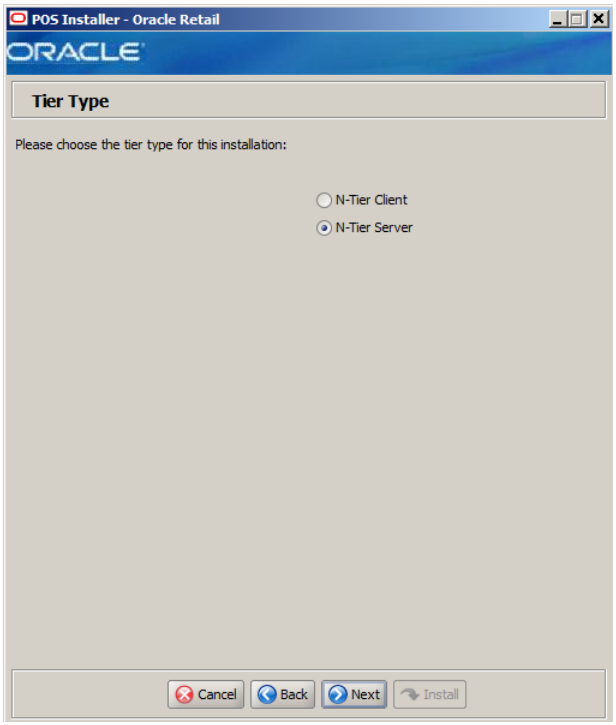
Figure A–6 Enter Default Locale



The field in this window 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 in the Supported Languages window. For each selected language, the default locale for that language is displayed in the Enter Default Locale window. For example, if English, French, and Italian are selected in the Supported Languages window, en_US, fr_FR, and it_IT are the available choices for the default locale.
Example	en_US

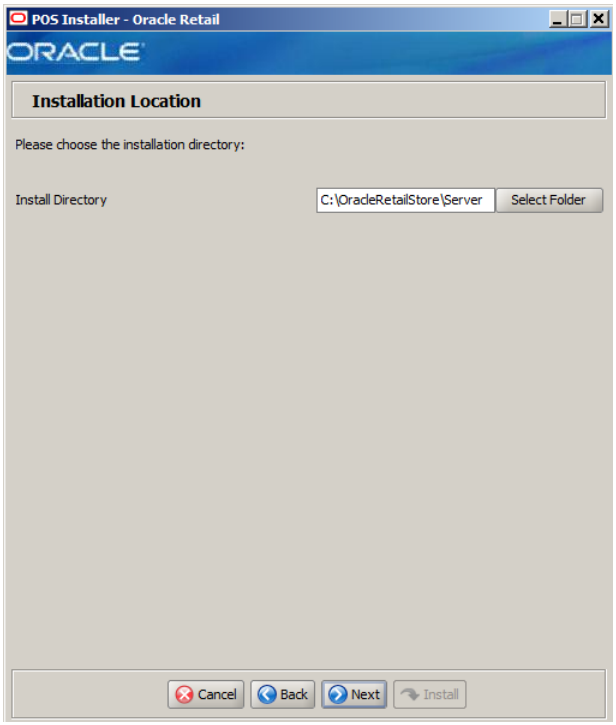
Figure A–7 Tier Type



The field in this window 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

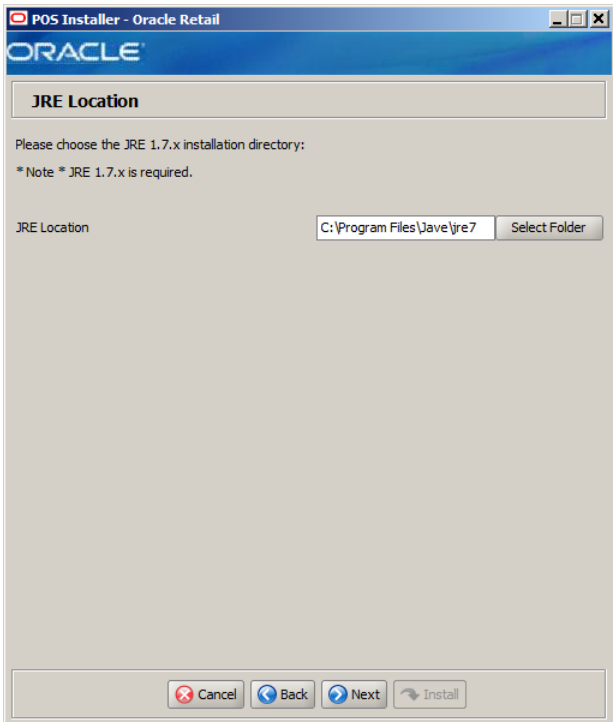
Figure A–8 Installation Location



The field in this window 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. **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	■ Microsoft Windows: C:\OracleRetailStore\Server ■ Novell SLEPOS: /opt/OracleRetailStore/Server

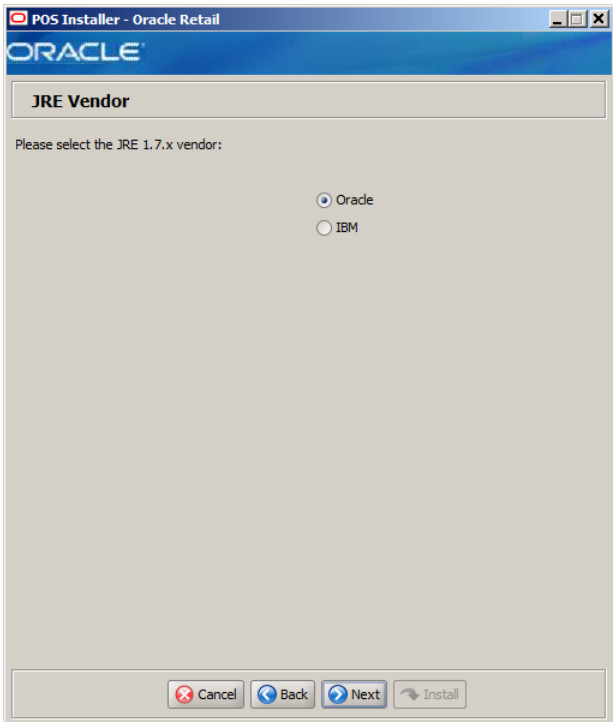
Figure A–9 JRE Location



The field in this window is described in the following table:

Details	Content
Field Title	JRE Location
Field Description	Enter the location where the JRE is installed.
Example	▪ Microsoft Windows: C:\Program Files\Java\jre7 ▪ Novell SLEPOS: /opt/Java/jre7

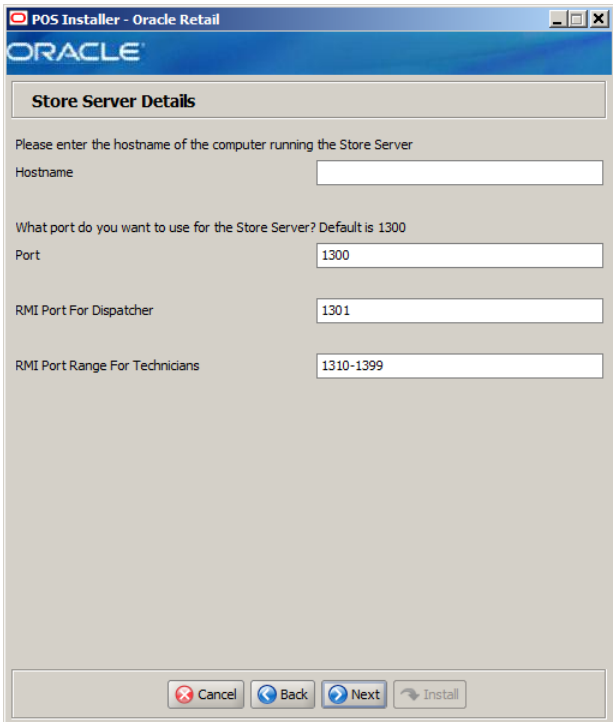
Figure A–10 JRE Vendor



The field in this window 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 in the JRE Location window: ■ Oracle ■ IBM Choose **Oracle**.

Figure A–11 Store Server Details



The fields in this window are described in the following tables:

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

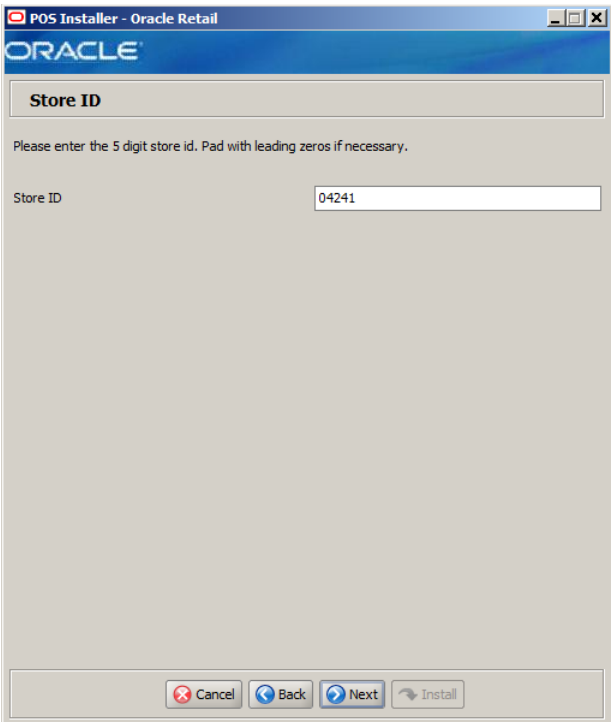
Details	Content
Field Title	Port
Field Description	Enter the port number of the store server host computer used for JNDI lookups by remote clients.
Example	1300

Details	Content
Field Title	RMI Port For Dispatcher
Field Description	Enter the port number of the store server host computer used for RMI communication to this installation's Point-of-Service dispatcher.
Example	1301

Details	Content
Field Title	RMI Port Range For Technicians
Field Description	Enter the range of port numbers enabled for RMI communication to this installation's technicians.

Details	Content
Example	1310-1399

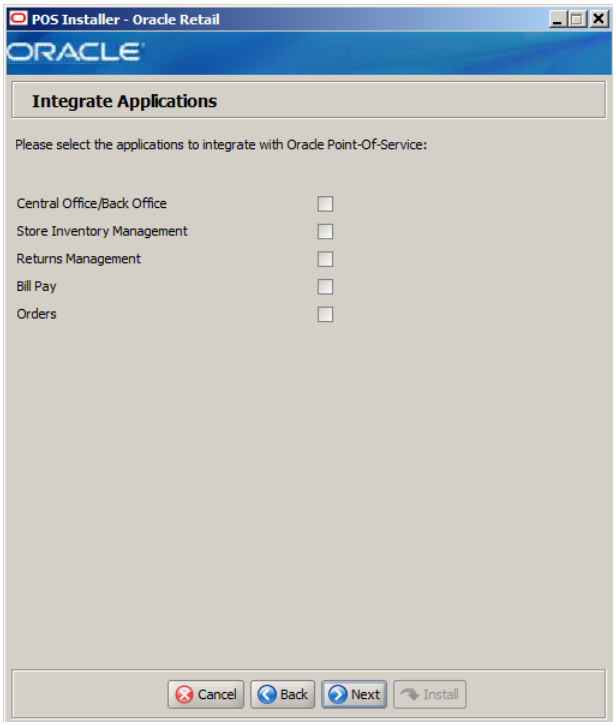
Figure A–12 Store ID



The field in this window is described in the following table:

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

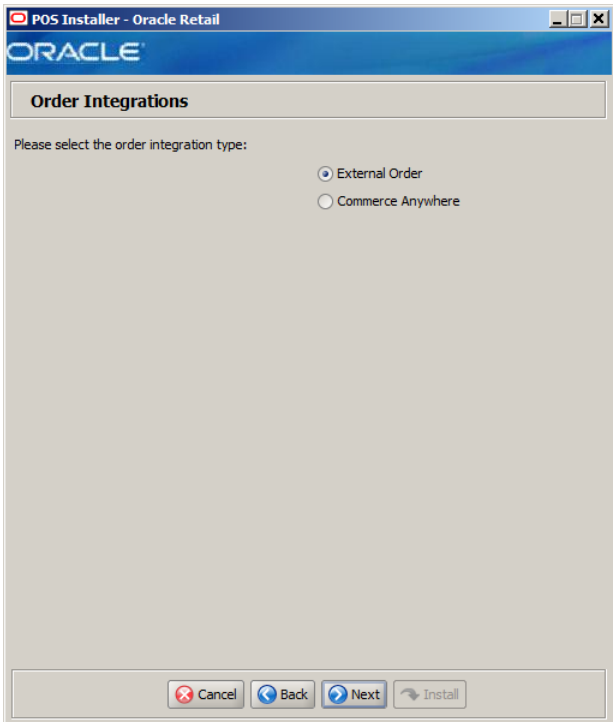
Figure A–13 Integrate Applications



The field in this window 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 ▪ Returns Management ▪ Bill Pay ▪ Orders

Figure A–14 Order Integrations

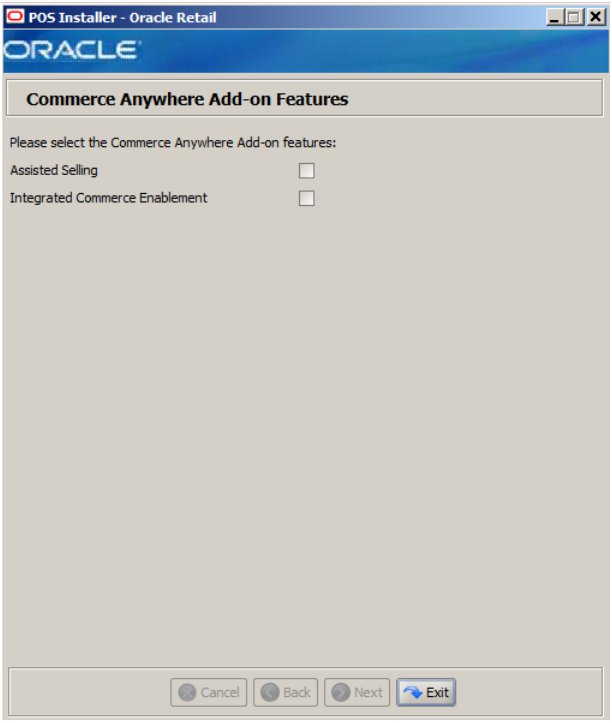


This window is only displayed if **Orders** is selected in the Integrate Applications window.

The field in this window is described in the following table:

Details	Content
Field Title	Please select the order integration type
Field Description	Select the type of orders to be used: ■ External Order ■ Commerce Anywhere
Example	External Order

Figure A–15 Commerce Anywhere Add-on Features

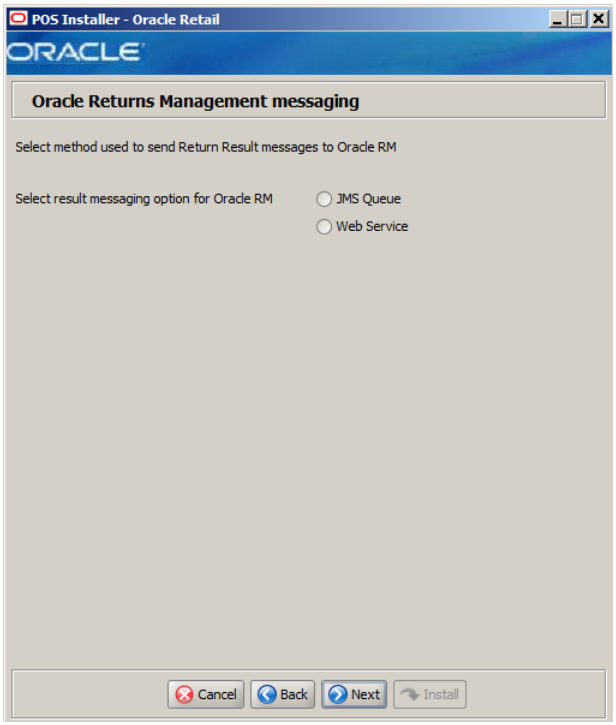


This window is only displayed if **Commerce Anywhere** is selected in the Order Integrations window.

The field in this window is described in the following table:

Details	Content
Field Title	Please select the Commerce Anywhere Add-on features
Field Description	Select the Commerce Anywhere features that will be used in Mobile Point-of-Service: ▪ To use the Assisted Selling Application (ASA), select **Assisted Selling**. **Note:** This feature is not tested in Release 14.1. ▪ To use integrated commerce, select **Integrated Commerce Enablement**.

Figure A–16 Oracle Returns Management Messaging

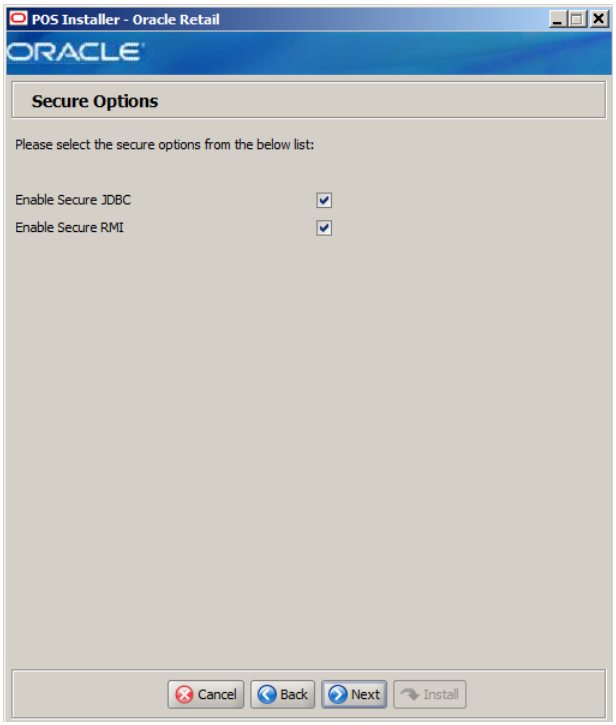


This window is only displayed if **Returns Management** is selected in the Integrate Applications window.

The field in this window 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–17 Secure Options

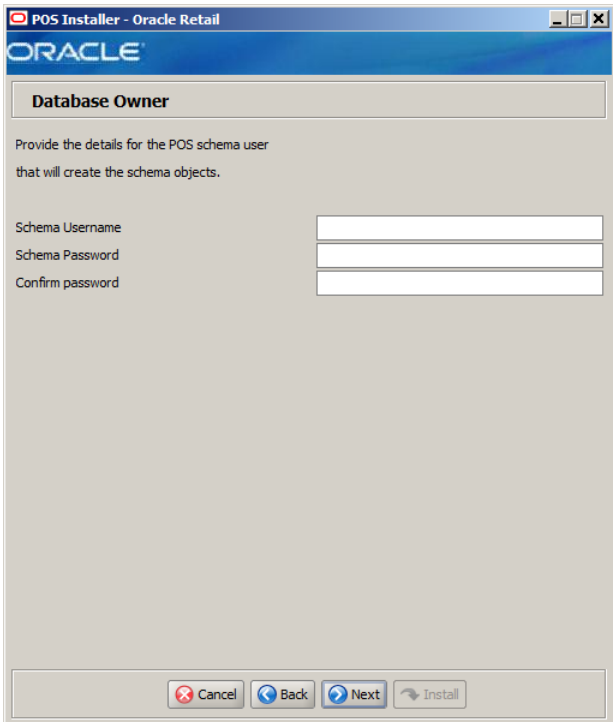


The fields in this window are described in the following tables:

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–18 Database Owner



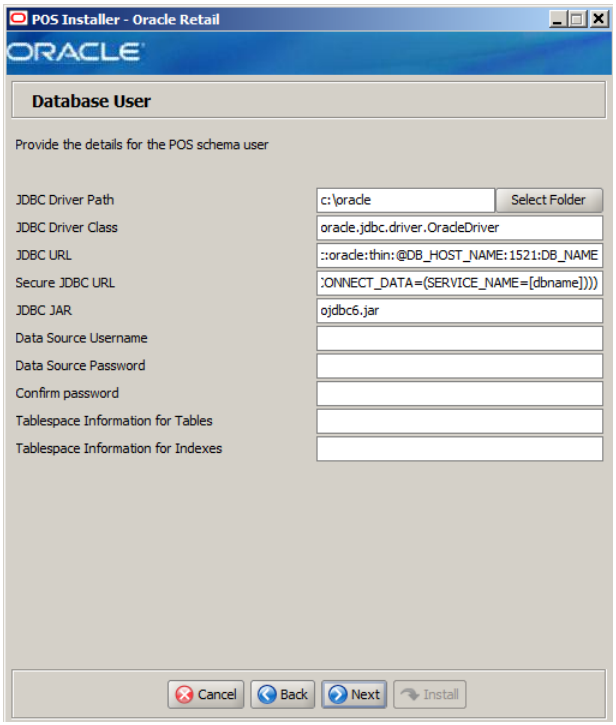
The fields in this window are described in the following tables:

Details	Content
Field Title	Schema Username
Field Description	Schema user name that manages the objects in the schema. This user has Create, Drop, and Alter privileges in the schema, that is, Data Definition Language (DDL) execution privileges. For information on creating this user, see "Create the Database Schema Owner and Data Source Users" in Chapter 3. **Note:** This user creates the database objects used by Point-of-Service.

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

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

Figure A–19 Database Source User



The fields in this window 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. **Note:** The ojdbc6.jar file can be found in the <*INSTALL-DIR*>\product\server\common\db\lib
Example	▪ Microsoft Windows: C:\oracle ▪ Novell SLEPOS: /opt/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	URL used by the Point-of-Service application to access the database schema. For the expected syntax, see Appendix E. **Note:** If Enable Secure JDBC is selected in the Secure Options window, this URL is only used by the installer.

Details	Content
Example	jdbc:oracle:thin:@DB_HOST_NAME:1521:DB_NAME

Details	Content
Field Title	Secure JDBC URL
Field Description	Secure URL containing the specific parameters used by Point-of-Service to access the database schema. See Appendix E for the expected syntax. This field is only displayed if Enable Secure JDBC is selected in the Secure Options window.
Example	jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=[host])(PORT=[tcpsPort]))(CONNECT_DATA=(SERVICE_NAME=[dbname])))

Details	Content
Field Title	JDBC JAR
Field Description	Enter the name of the jar containing the database driver.
Example	ojdbc6.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.

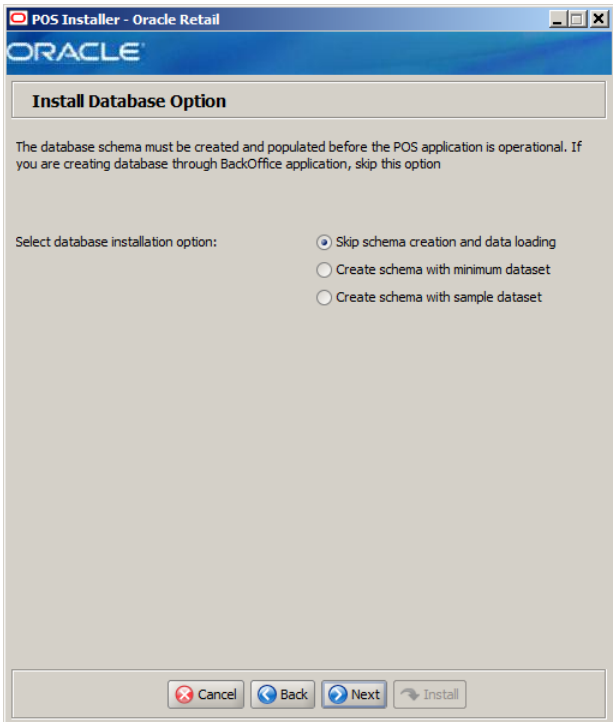
Details	Content
Field Title	Confirm Password
Field Description	Reentered Data Source Password used to confirm the password. **Note:** The passwords in the Data Source Password and Confirm Password fields must match.

Details	Content
Field Title	Tablespace Information for Tables

Details	Content
Field Description	Name of the tablespace, associated with the data source user, which is used for tables. If this field is blank, tables are installed in the default tablespace.

Details	Content
Field Title	Tablespace Information for Indexes
Field Description	Name of the tablespace, associated with the data source user, which is used for indexes. If this field is blank, indexes are installed in the default tablespace.

Figure A–20 Install Database Option

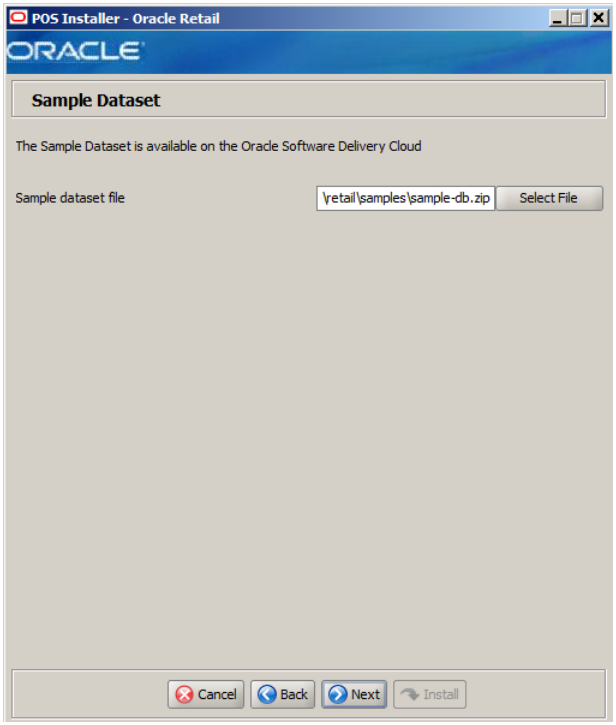


The field in this window is described in the following table:

Details	Content
Field Title	Select database installation option

Details	Content
Field Description	The database schema must be created and populated before starting Point-of-Service. This window gives you the option to have the installer create and populate the database schema or leave the database schema unmodified. **Caution:** If the database schema is already created and populated, select **Skip schema creation and data loading**. Selecting one of the other options will result in the loss of the data already in the database. If the database schema was created and populated using Back Office, reports data, and Back Office parameters will be lost. ▪ To have the installer leave the database schema unchanged, select **Skip schema creation and data loading**. ▪ To have the installer create and populate the database schema with the minimum dataset, select **Create schema with minimum dataset**. ▪ To have the installer create and populate the database schema with the sample dataset, select **Create schema with sample dataset**. For more information, see "Database Install Options" in Chapter 3.
Example	Skip schema creation and data loading

Figure A–21 Sample Dataset



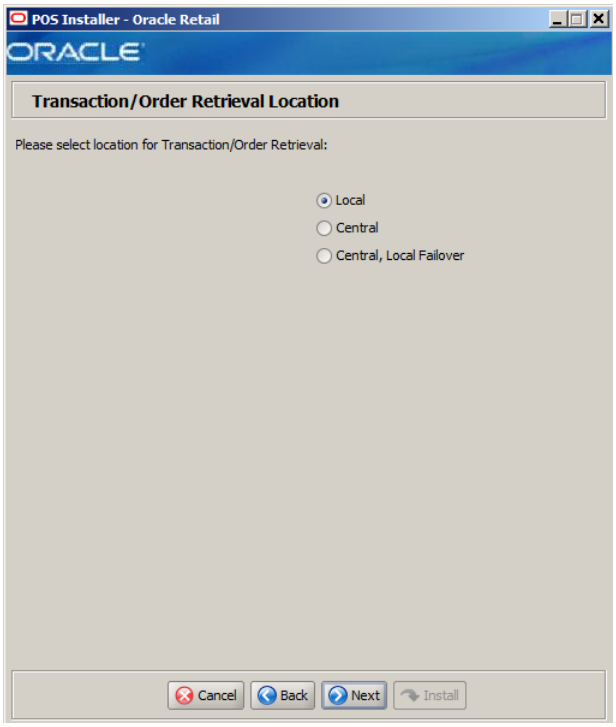
This window is only displayed when **Create schema with sample dataset** is selected in the Install Database Option window.

The field in this window is described in the following table:

Details	Content
Field Title	Sample dataset file

Details	Content
Field Description	Enter the path to the sample dataset to be loaded into the database schema. You can obtain the sample-dataset-14.1.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	▪ Microsoft Windows: C:\oracle\retail\samples\sample-db.zip ▪ Novell SLEPOS: /oracle/retail/samples/sample-db.zip

Figure A–22 Transaction Retrieval Location



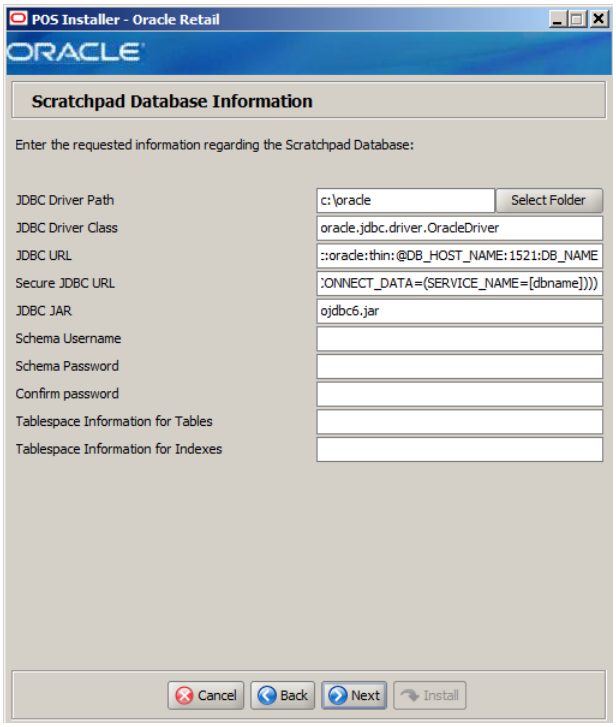
This window is only displayed if **Central Office/Back Office** is selected in the Integrate Applications window.

The field in this window is described in the following table:

Details	Content
Field Title	Please select location for Transaction Retrieval

Details	Content
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 window is only displayed if **Central** or **Central, Local Failover** is selected in the Transaction Retrieval Location window.

The fields in this window 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	■ Microsoft Windows: C:\oracle ■ Novell SLEPOS: /opt/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	URL used by the Point-of-Service application to access the database schema. For the expected syntax, see Appendix E. **Note:** If Enable Secure JDBC is selected in the Secure Options window, this URL is only used by the installer.
Example	jdbc:oracle:thin:@DB_HOST_NAME:1521:DB_NAME

Details	Content
Field Title	Secure JDBC URL
Field Description	Secure URL containing the specific parameters used by Point-of-Service to access the database schema. See Appendix E for the expected syntax. This field is only displayed if Enable Secure JDBC is selected in the Secure Options window.
Example	jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=[host])(PORT=[tcpsPort]))(CONNECT_DATA=(SERVICE_NAME=[dbname])))

Details	Content
Field Title	JDBC JAR
Field Description	Enter the name of the jar containing the database driver.
Example	ojdbc6.jar

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

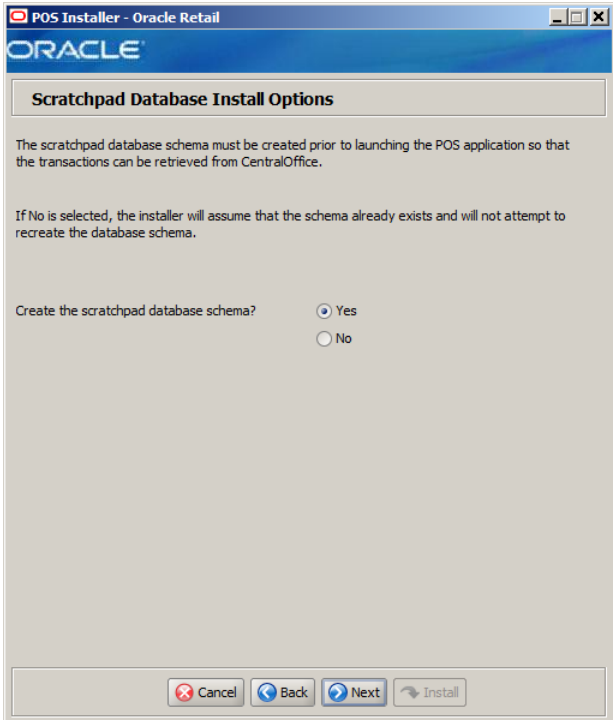
Details	Content
Field Title	Schema Password
Field Description	Password for the database owner.

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.

Details	Content
Field Title	Tablespace Information for Tables
Field Description	Name of the tablespace, associated with the data source user, which is used for tables. If this field is blank, tables are installed in the default tablespace.

Details	Content
Field Title	Tablespace Information for Indexes
Field Description	Name of the tablespace, associated with the data source user, which is used for indexes. If this field is blank, indexes are installed in the default tablespace.

Figure A–24 Scratchpad Database Install Options

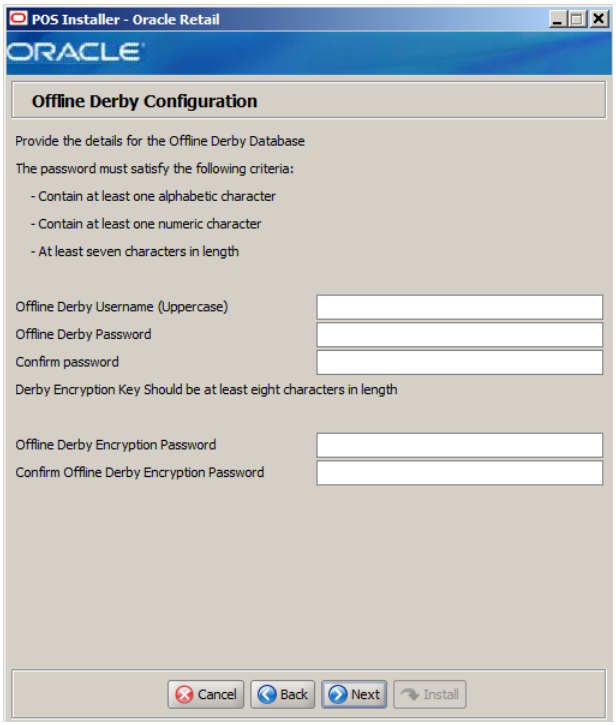


This window is only displayed if **Central** or **Central, Local Failover** is selected in the Transaction Retrieval Location window.

The field in this window 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 Offline Derby Configuration



The fields in this window are described in the following tables:

Details	Content
Field Title	Offline Derby Username (Uppercase)
Field Description	Enter the user name used for offline Derby processing. The user name must be in uppercase characters.

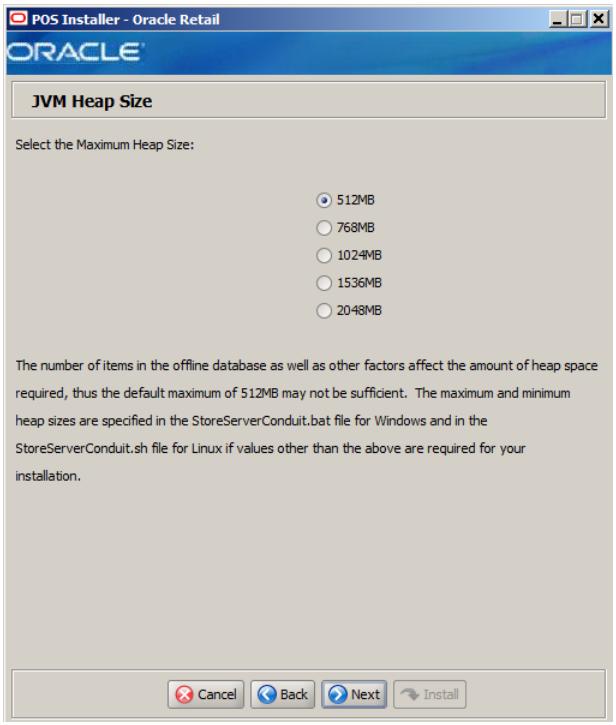
Details	Content
Field Title	Offline Derby Password
Field Description	Enter the password for the offline Derby user.

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

Details	Content
Field Title	Offline Derby Encryption Password
Field Description	Enter the encryption password for the offline Derby user.

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

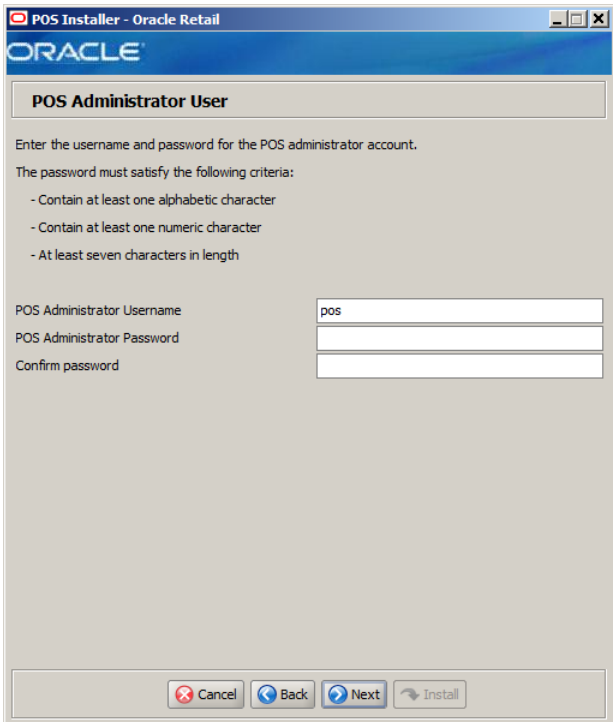
Figure A–26 JVM Heap Size



The field in this window is described in the following table:

Details	Content
Field Title	Select the Maximum Heap Size
Field Description	Select the maximum heap size for the offline database. **Note:** The number of items in the offline database, as well as other factors, affect the amount of heap size required.
Example	512MB

Figure A–27 POS Administrator User



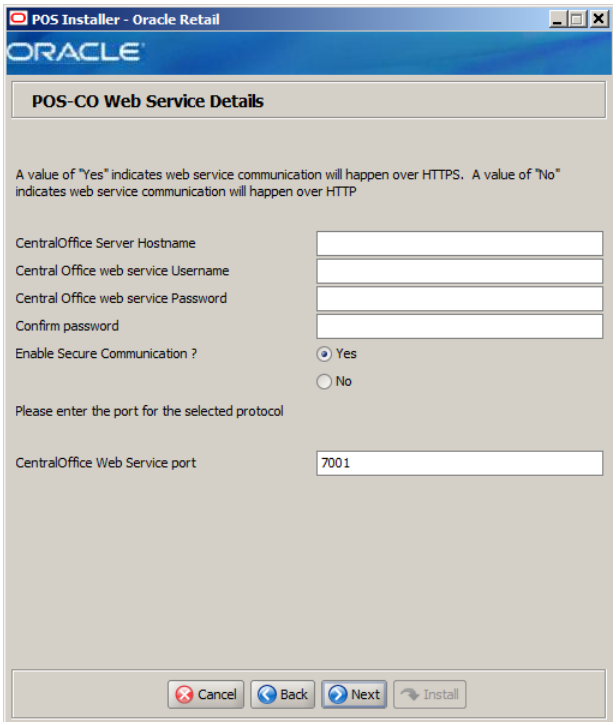
The fields in this window are described in the following tables:

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 Password
Field Description	Enter the password for the administrator user.

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

Figure A–28 POS-CO WebService Details



This window is only displayed if **Central Office/Back Office** is selected in the Integrate Applications window.

The fields in this window 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	Central Office web service Username
Field Description	Enter the user ID that is used to access the web service. **Note:** The same Web Service Username that was entered when installing Central Office must be entered here. For more information, see the *Oracle Retail Central Office Installation Guide*.

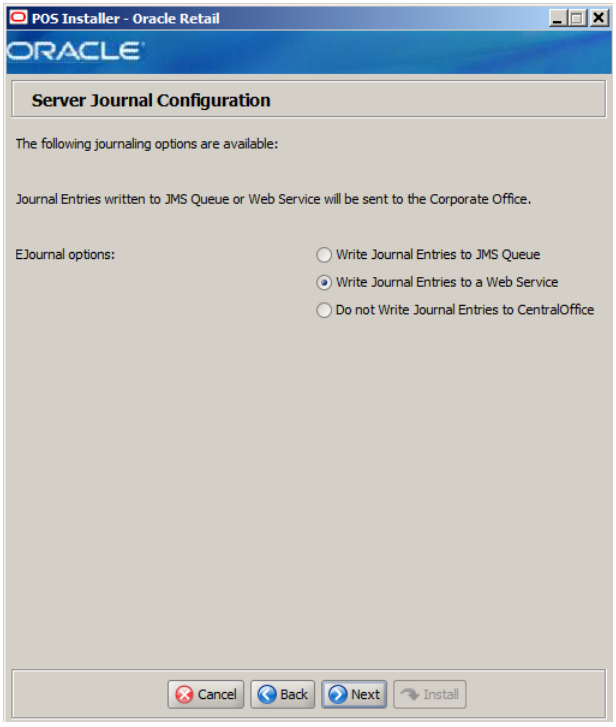
Details	Content
Field Title	Central Office web service Password
Field Description	Enter the password of the authorized user. **Note:** The same Web Service Password that was entered when installing Central Office must be entered here. For more information, see the *Oracle Retail Central Office Installation Guide*.

Details	Content
Field Title	Confirm Password
Field Description	Reentered Central Office web service Password used to confirm the password. **Note:** The passwords in the Central Office web service Password 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 Webs Service Port
Field Description	Enter the port number for the Central Office web service.

Figure A–29 Server Journal Configuration



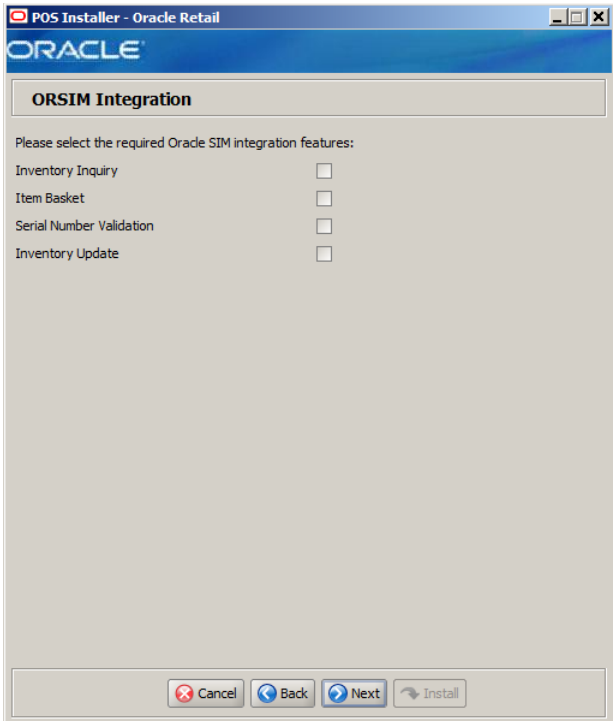
This window is only displayed if **Central Office/Back Office** is selected in the Integrate Applications window.

The field in this window is described in the following table:

Details	Content
Field Title	EJounal options

Details	Content
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 Web Service ■ Do not Write Journal Entries to CentralOffice
Example	Write Journal Entries to a Web Service

Figure A–30 ORSIM Integration

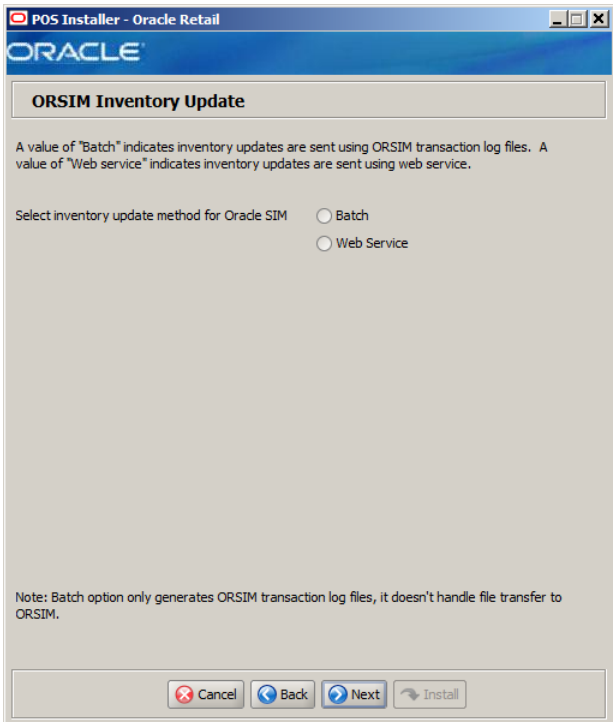


This window is only displayed if **Store Inventory Management** is selected in the Integrate Applications window.

The field in this window 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 validation of serial numbers using SIM, select **Serial Number Validation**. ■ To update inventory using SIM, select **Inventory Update**.

Figure A–31 ORSIM Inventory Update

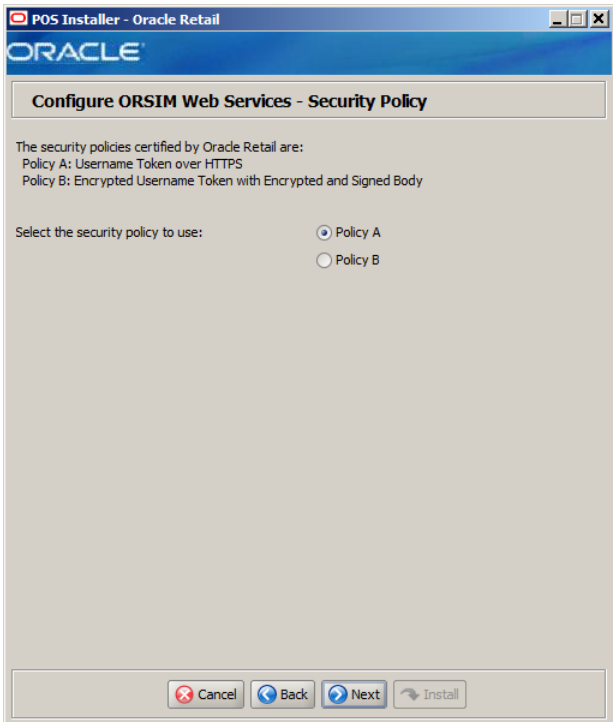


This window is only displayed if **Inventory Update** is selected in the ORSIM Integration window.

The field in this window is described in the following table:

Details	Content
Field Title	Select inventory update method for Oracle SIM
Field Description	Select the inventory update method used for SIM: ▪ To use batch, select **Batch**. ▪ To use a web service, select **Web Service**.

Figure A–32 Configure ORSIM Web Services - Security Policy

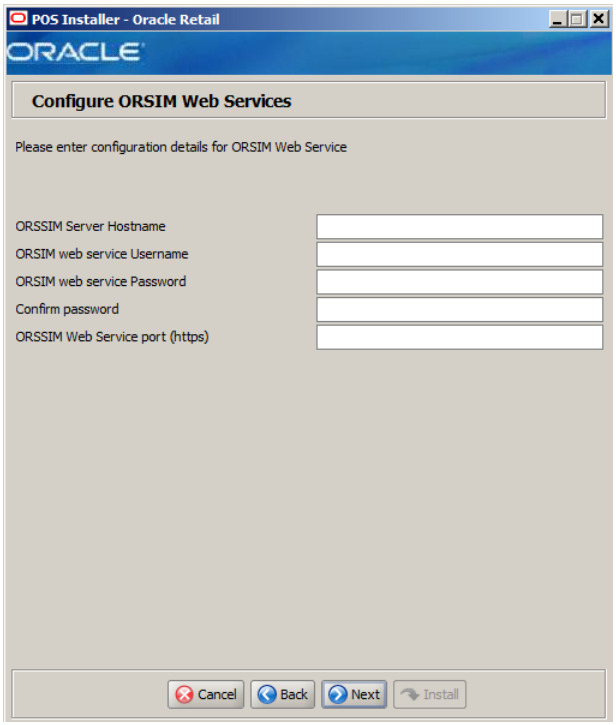


This window is only displayed if any features are selected in the ORSIM Integration window.

The field in this window is described in the following table:

Details	Content
Field Title	Select the security policy to use
Field Description	Select the security policy certified by Oracle: ■ To use a user name token over https, select **Policy A**. ■ To use an encrypted user name token with an encrypted and signed body, select **Policy B**.
Example	Policy A

Figure A–33 Configure ORSIM Web Services for Policy A



This window is only displayed **Policy A** is selected in the Configure ORSIM Web Services - Security Policy window.

The fields in this window are described in the following tables:

Details	Content
Field Title	ORSIM Server Hostname
Field Description	Enter the host name for the Oracle Retail Store Inventory Management web server.

Details	Content
Field Title	ORSIM Web Service Username
Field Description	Enter the user ID used to access the Oracle Retail Store Inventory Management web service.

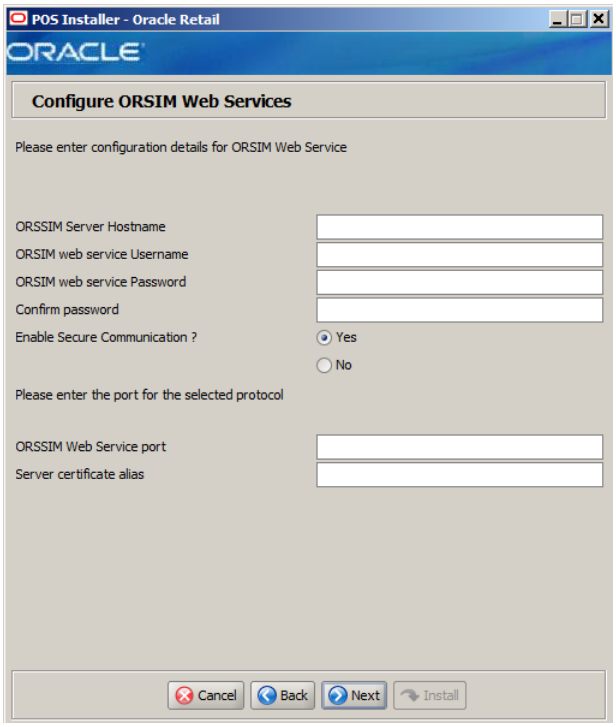
Details	Content
Field Title	ORSIM Web Service Password
Field Description	Enter the password used to access Oracle Retail Store Inventory Management web service.

Details	Content
Field Title	Confirm Password

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

Details	Content
Field Title	ORSIM Web Service Port (https)
Field Description	Enter the port number used to access Oracle Retail Store Inventory Management web service.

Figure A–34 Configure ORSIM Web Services for Policy B



This window is only displayed **Policy B** is selected in the Configure ORSIM Web Services - Security Policy window.

The fields in this window are described in the following tables:

Details	Content
Field Title	ORSIM Server Hostname
Field Description	Enter the host name for the Oracle Retail Store Inventory Management web server.

Details	Content
Field Title	ORSIM Web Service Username
Field Description	Enter the user ID used to access the Oracle Retail Store Inventory Management web service.

Details	Content
Field Title	ORSIM Web Service Password
Field Description	Enter the password used to access Oracle Retail Store Inventory Management web service.

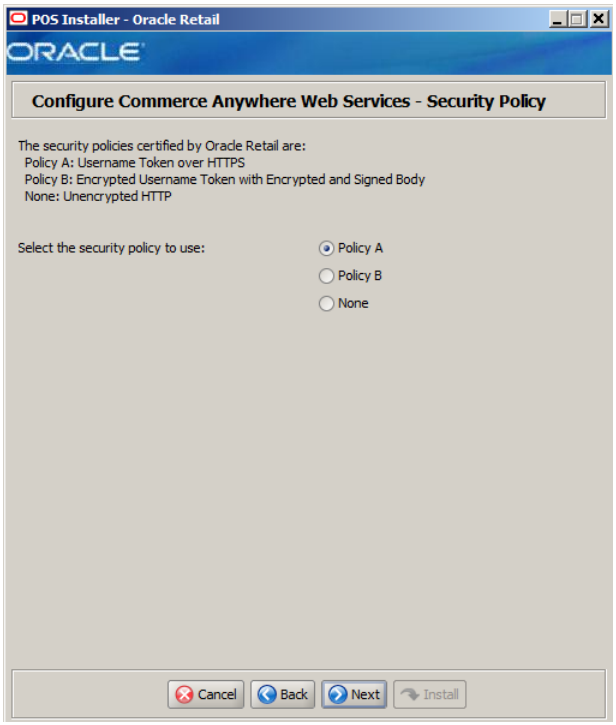
Details	Content
Field Title	Confirm Password
Field Description	Reentered ORSIM Web Service Password used to confirm the password. **Note:** The passwords in the WebService Password and Confirm Password fields must match.

Details	Content
Field Title	Enable Secure Communication?
Field Description	Select **Yes** for web service communication with Oracle Retail Store Inventory Management using HTTPS.
Example	Yes

Details	Content
Field Title	ORSIM Web Service Port
Field Description	Enter the port number used to access the Oracle Retail Store Inventory Management web service.

Details	Content
Field Title	Server Certificate Alias
Field Description	Enter the alias for the server certificate used to access the Oracle Retail Store Inventory Management web service.

Figure A–35 Configure Commerce Anywhere Web Services - Security Policy

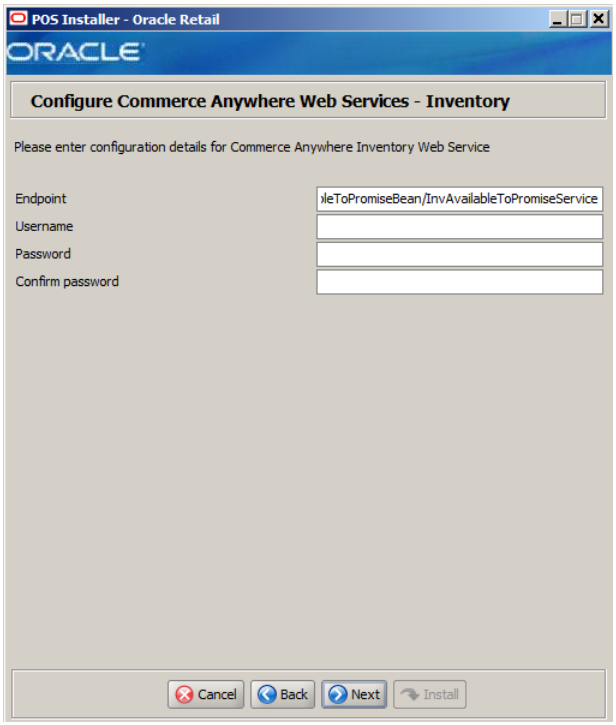


This window is only displayed if **Orders** in the Integrate Applications window and then **Commerce Anywhere** is selected in the Order Integrations window.

The field in this window is described in the following table:

Details	Content
Field Title	Select the security policy to use
Field Description	Select the security policy certified by Oracle: ■ To use a user name token over https, select **Policy A**. ■ To use an encrypted user name token with an encrypted and signed body, select **Policy B**. ■ To use un-encrypted http, select **None**.
Example	Policy A

Figure A–36 Configure Commerce Anywhere Web Services - Inventory for Policy A



This window is only displayed if **Policy A** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The fields in this window are described in the following tables:

Details	Content
Field Title	Endpoint
Field Description	Entry point to the Commerce Anywhere Inventory web service.
Example	https://HOST[:PORT]/InvAvailableToPromiseBean/InvAvailableToPromiseService

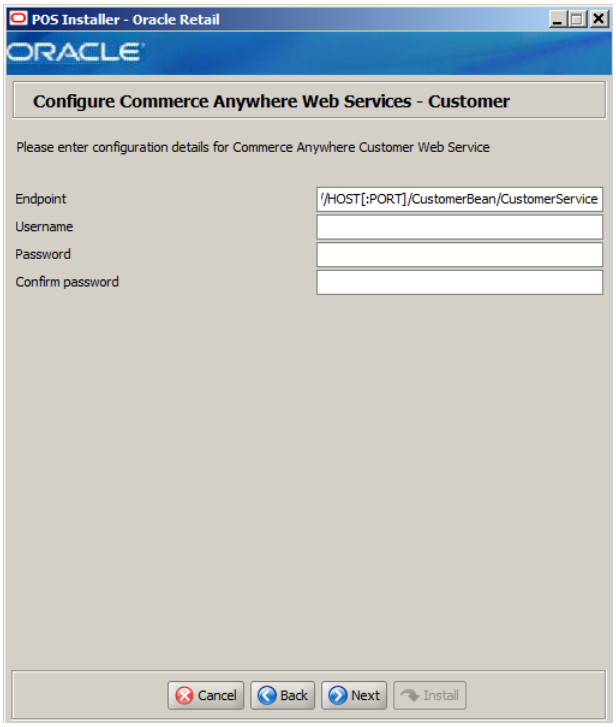
Details	Content
Field Title	Username
Field Description	User name for the Commerce Anywhere Customer Inventory web service.

Details	Content
Field Title	Password
Field Description	Password for the user.

Details	Content
Field Title	Confirm Password

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

Figure A–37 Configure Commerce Anywhere Web Services - Customer for Policy A



This window is only displayed if **Policy A** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The fields in this window are described in the following tables:

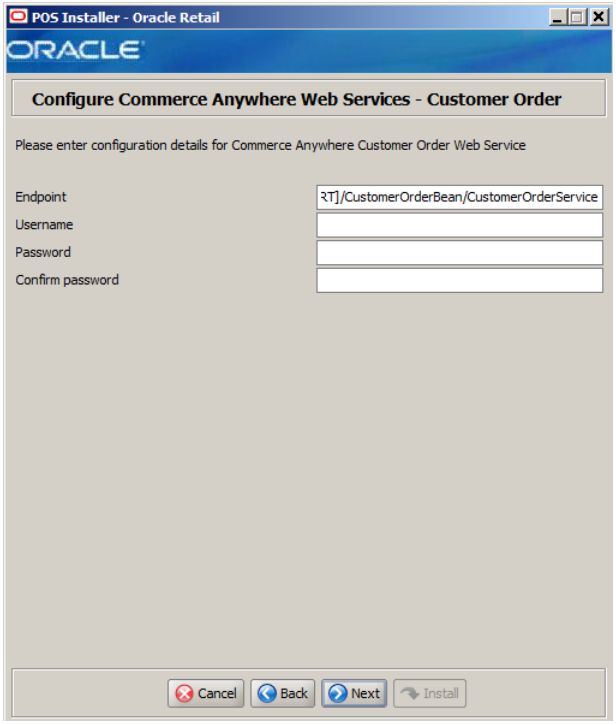
Details	Content
Field Title	Endpoint
Field Description	Entry point to the Commerce Anywhere Customer web service.
Example	https://HOST[:PORT]/CustomerBean/CustomerService

Details	Content
Field Title	Username
Field Description	User name for the Commerce Anywhere Customer web service.

Details	Content
Field Title	Password
Field Description	Password for the user.

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 A–38 Configure Commerce Anywhere Web Services - Customer Order for Policy A



This window is only displayed if **Policy A** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The fields in this window are described in the following tables:

Details	Content
Field Title	Endpoint
Field Description	Entry point to the Commerce Anywhere Customer Order web service.
Example	https://HOST[:PORT]/CustomerOrderBean/CustomerOrderService

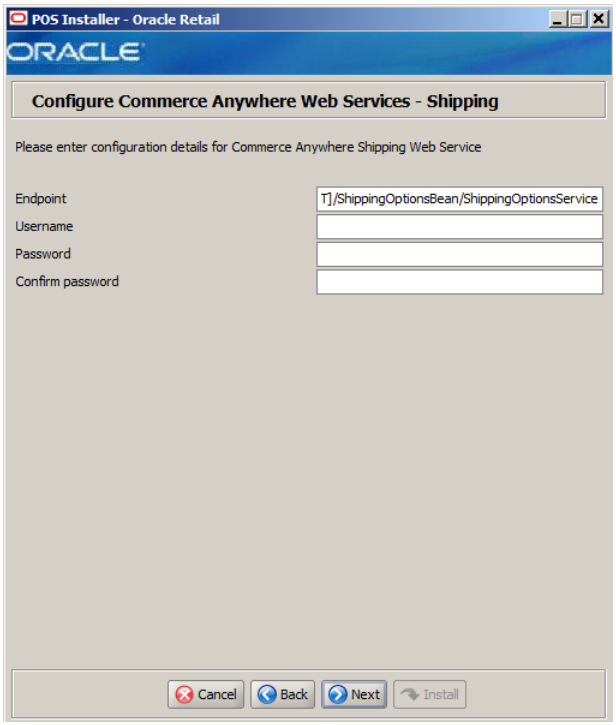
Details	Content
Field Title	Username
Field Description	User name for the Commerce Anywhere Customer Order web service.

Details	Content
Field Title	Password

Details	Content
Field Description	Password for the user.

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 A–39 Configure Commerce Anywhere Web Services - Shipping for Policy A



This window is only displayed if **Policy A** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The fields in this window are described in the following tables:

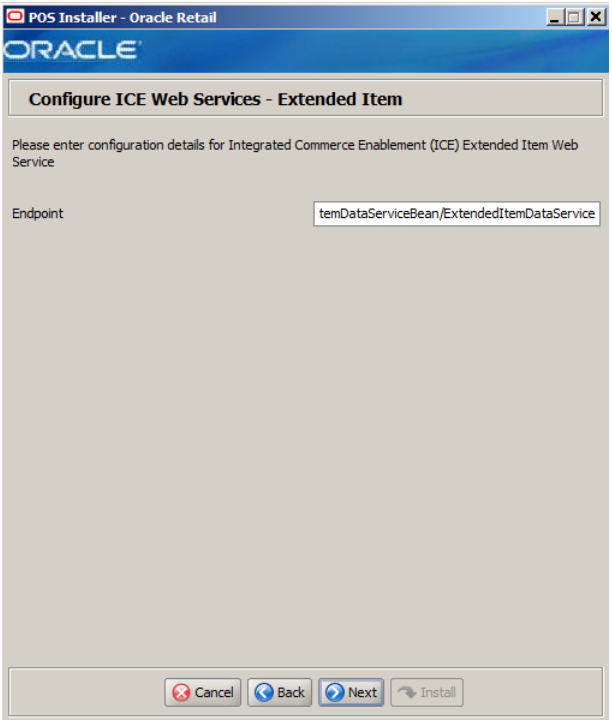
Details	Content
Field Title	Endpoint
Field Description	Entry point to the Commerce Anywhere Shipping web service.
Example	https://HOST[:PORT]/ShippingOptionsBean/ShippingOptionsService

Details	Content
Field Title	Username
Field Description	User name for the Commerce Anywhere Shipping web service.

Details	Content
Field Title	Password
Field Description	Password for the user.

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 A–40 Configure ICE Web Services - Extended Item for Policy A

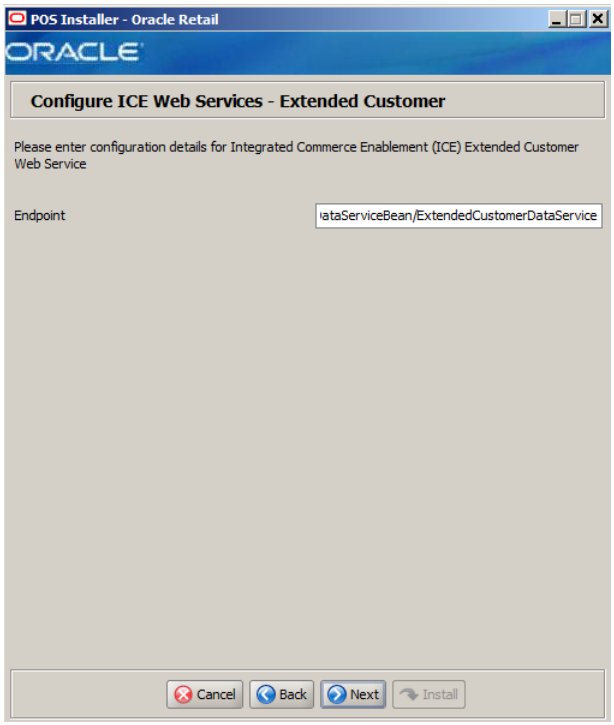


This window is only displayed if **Orders** is selected in the Integrate Application window and then **Integrated Commerce Enablement** is selected in the Order Integrations window and **Policy A** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The field in this window is described in the following table:

Details	Content
Field Title	Endpoint
Field Description	Entry point to the ICE Extended Item web service.
Example	https://HOST[:PORT]/ExtendedItemDataServiceBean/ExtendedItem DataService

Figure A–41 Configure ICE Web Services - Extended Customer for Policy A

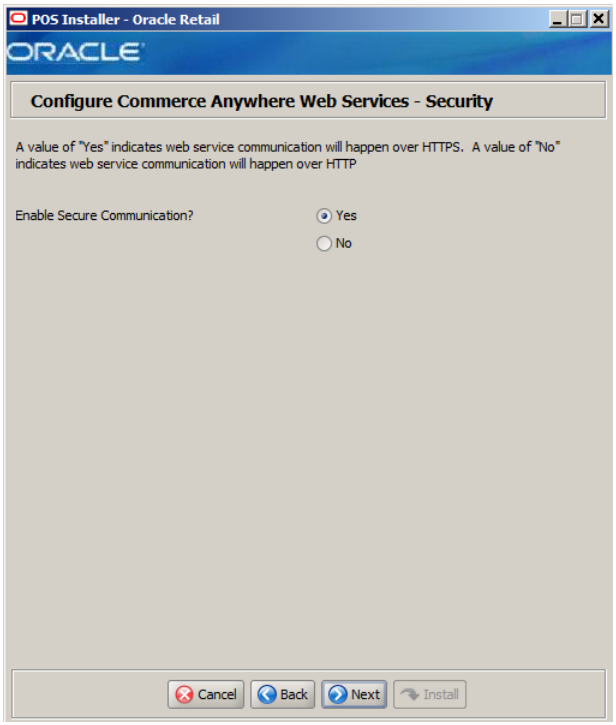


This window is only displayed if **Orders** is selected in the Integrate Application window and then **Integrated Commerce Enablement** is selected in the Order Integrations window and **Policy A** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The field in this window is described in the following table:

Details	Content
Field Title	Endpoint
Field Description	Entry point to the ICE Extended Customer web service.
Example	https://HOST[:PORT]/ExtendedCustomerDataServiceBean/ExtendedCustomerDataService

Figure A–42 Configure Commerce Anywhere Web Services - Security for Policy B

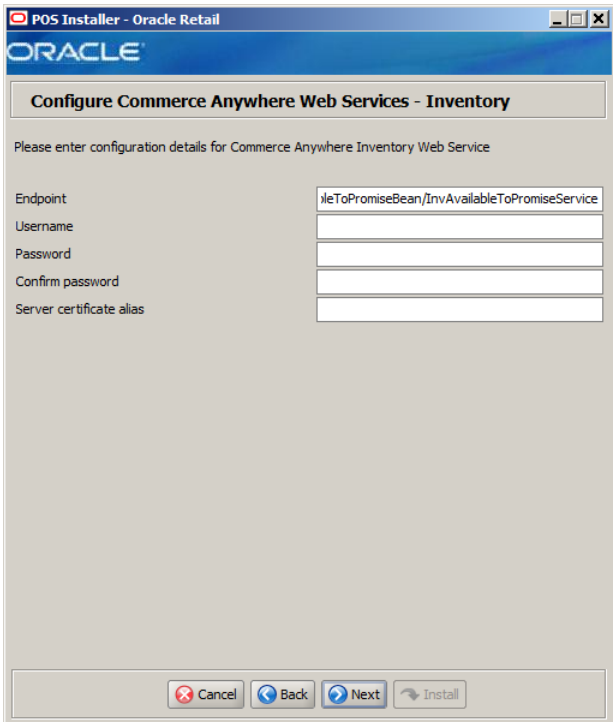


This window is only displayed if **Policy B** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The field in this window is described in the following table:

Details	Content
Field Title	Enable Secure Communication?
Field Description	Select **Yes** for web service communication with Commerce Anywhere using HTTPS.
Example	Yes

Figure A–43 Configure Commerce Anywhere Web Services - Inventory for Policy B



This window is only displayed if **Policy B** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The fields in this window are described in the following tables:

Details	Content
Field Title	Endpoint
Field Description	Entry point to the Commerce Anywhere Inventory web service.
Example	https://HOST[:PORT]/InvAvailableToPromiseBean/InvAvailableToPromiseService

Details	Content
Field Title	Username
Field Description	User name for the Commerce Anywhere Customer Inventory web service.

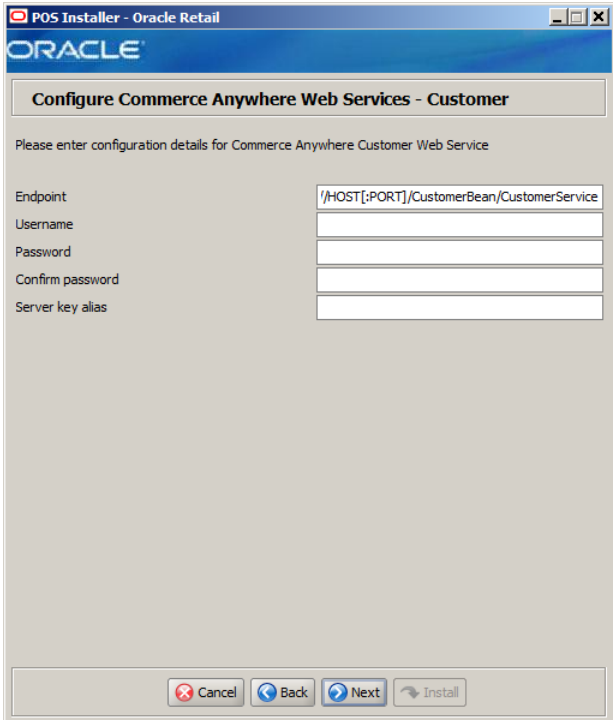
Details	Content
Field Title	Password
Field Description	Password for the user.

Details	Content
Field Title	Confirm Password

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

Details	Content
Field Title	Server certificate alias
Field Description	Alias used for the server key.

Figure A–44 Configure Commerce Anywhere Web Services - Customer for Policy B



This window is only displayed if **Policy B** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The fields in this window are described in the following tables:

Details	Content
Field Title	Endpoint
Field Description	Entry point to the Commerce Anywhere web service.
Example	https://HOST[:PORT]/CustomerBean/CustomerService

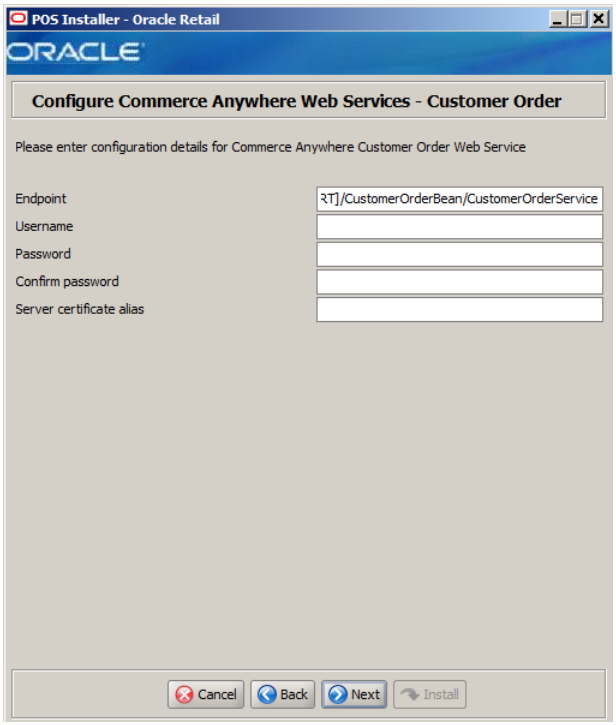
Details	Content
Field Title	Username
Field Description	User name for the Commerce Anywhere Customer web service.

Details	Content
Field Title	Password
Field Description	Password for the user.

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.

Details	Content
Field Title	Server certificate alias
Field Description	Alias used for the server key.

Figure A–45 Configure Commerce Anywhere Web Services - Customer Order for Policy B



This window is only displayed if **Policy B** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The fields in this window are described in the following tables:

Details	Content
Field Title	Endpoint
Field Description	Entry point to the Commerce Anywhere Customer Order web service.

Details	Content
Example	https://HOST[:PORT]/CustomerOrderBean/CustomerOrderService

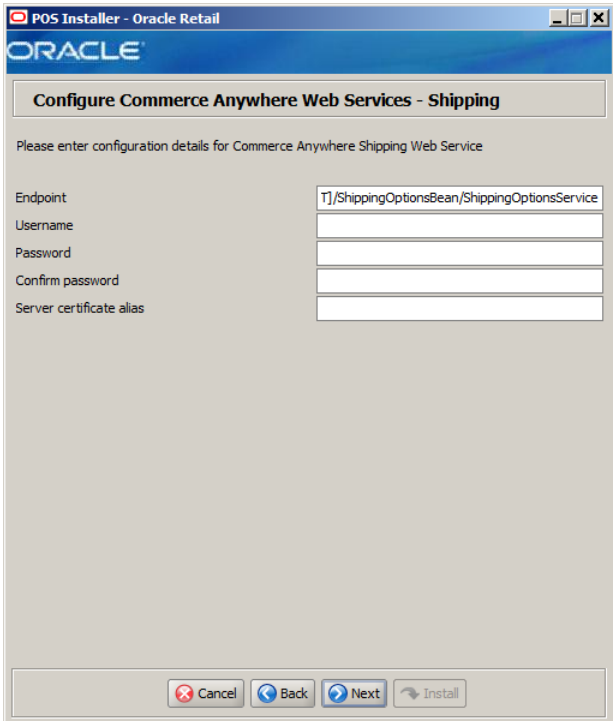
Details	Content
Field Title	Username
Field Description	User name for the Commerce Anywhere Customer Order web service.

Details	Content
Field Title	Password
Field Description	Password for the user.

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.

Details	Content
Field Title	Server certificate alias
Field Description	Alias used for the server key.

Figure A–46 Configure Commerce Anywhere Web Services - Shipping for Policy B



This window is only displayed if **Policy B** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The fields in this window are described in the following tables:

Details	Content
Field Title	Endpoint
Field Description	Entry point to the Commerce Anywhere Shipping web service.
Example	https://HOST[:PORT]/ShippingOptionsBean/ShippingOptionsService

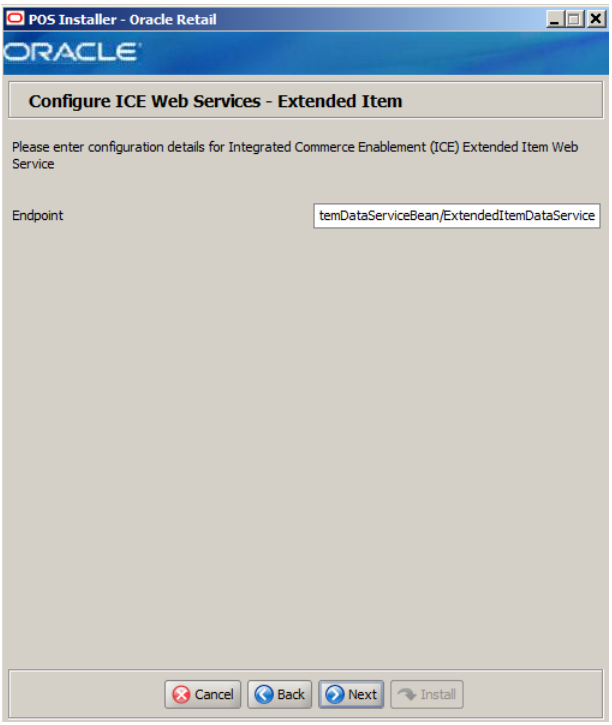
Details	Content
Field Title	Username
Field Description	User name for the Commerce Anywhere Shipping web service.

Details	Content
Field Title	Password
Field Description	Password for the user.

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.

Details	Content
Field Title	Server certificate alias
Field Description	Alias used for the server key.

Figure A–47 Configure ICE Web Services - Extended Item for Policy B

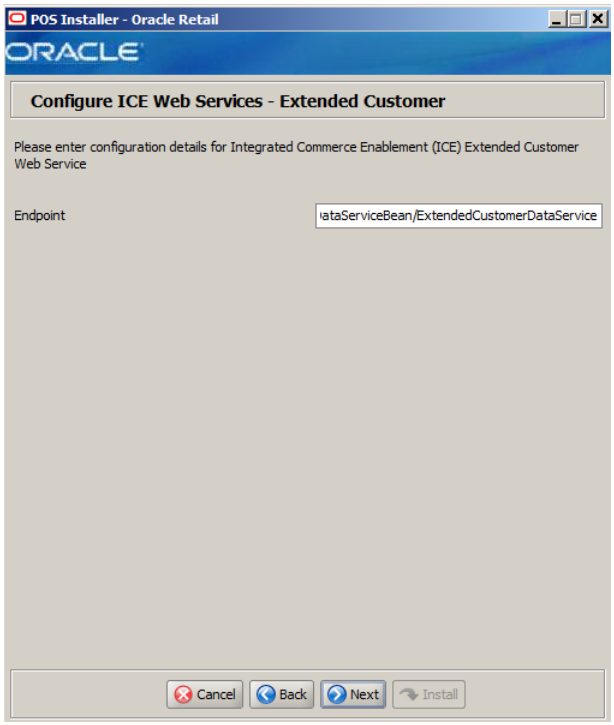


This window is only displayed if **Orders** is selected in the Integrate Application window and then **Integrated Commerce Enablement** is selected in the Order Integrations window and **Policy B** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The field in this window is described in the following table:

Details	Content
Field Title	Endpoint
Field Description	Entry point to the ICE Extended Item web service.
Example	https://HOST[:PORT]/ExtendedItemDataServiceBean/ExtendedItemDataService

Figure A–48 Configure ICE Web Services - Extended Customer for Policy B

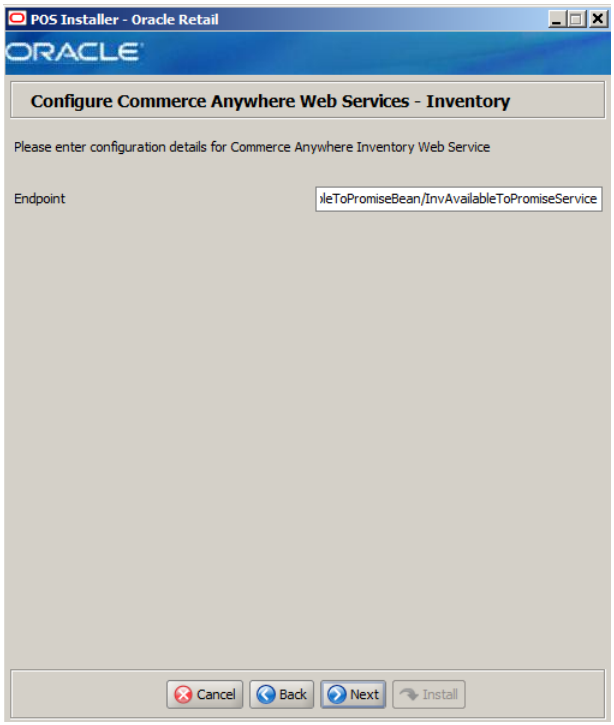


This window is only displayed if **Orders** is selected in the Integrate Application window and then **Integrated Commerce Enablement** is selected in the Order Integrations window and **Policy B** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The field in this window is described in the following table:

Details	Content
Field Title	Endpoint
Field Description	Entry point to the ICE Extended Customer web service.
Example	https://HOST[:PORT]/ExtendedCustomerDataServiceBean/ExtendedCustomerDataService

Figure A–49 Configure Commerce Anywhere Web Services - Inventory for Policy None

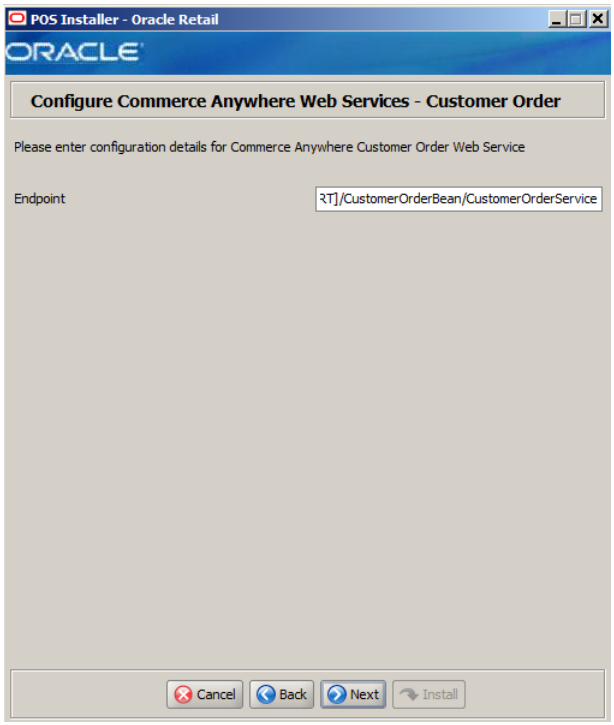


This window is only displayed if **None** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The field in this window is described in the following table:

Details	Content
Field Title	Endpoint
Field Description	Entry point to the Commerce Anywhere Inventory web service.
Example	http://HOST[:PORT]/InvAvailableToPromiseBean/InvAvailableToPromiseService

Figure A–50 Configure Commerce Anywhere Web Services - Customer for Policy None

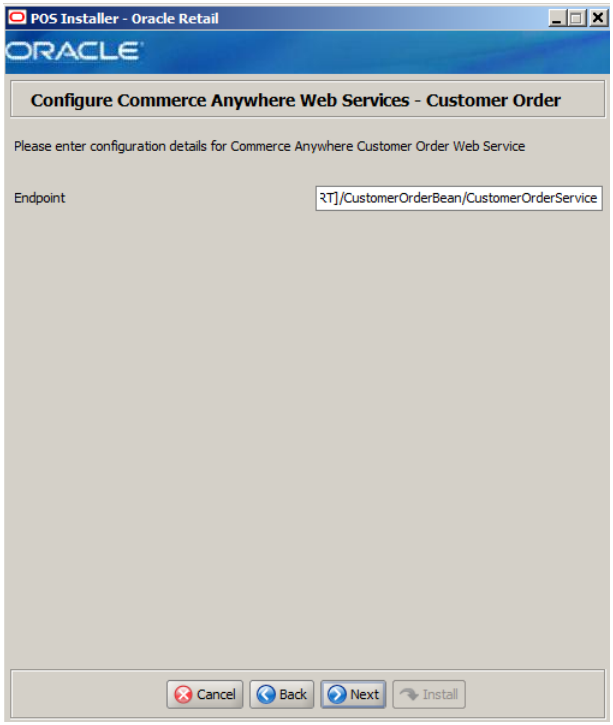


This window is only displayed if **None** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The field in this window is described in the following table:

Details	Content
Field Title	Endpoint
Field Description	Entry point to the Commerce Anywhere web service.
Example	http://HOST[:PORT]/CustomerBean/CustomerService

Figure A–51 Configure Commerce Anywhere Web Services - Customer Order for Policy None



This window is only displayed if **None** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The field in this window is described in the following table:

Details	Content
Field Title	Endpoint
Field Description	Entry point to the Commerce Anywhere Customer Order web service.
Example	http://HOST[:PORT]/CustomerOrderBean/CustomerOrderService

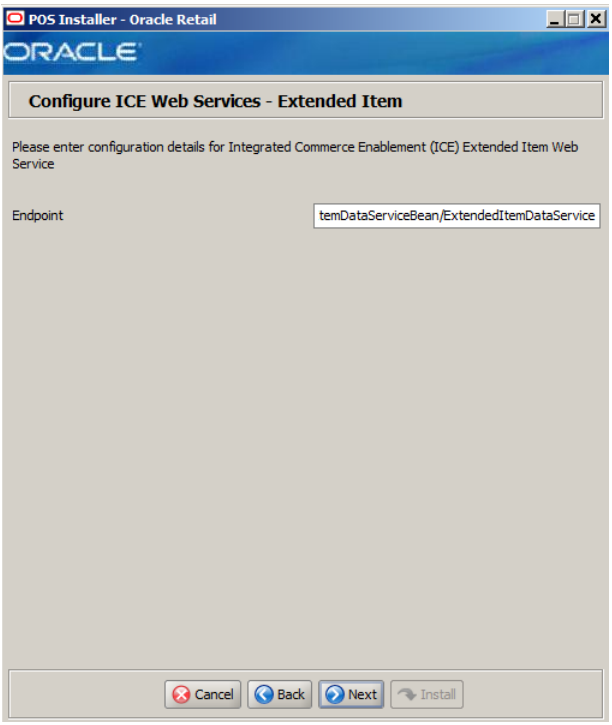
Figure A–52 Configure Commerce Anywhere Web Services - Shipping for Policy None

This window is only displayed if **None** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The fields in this window are described in the following tables:

Details	Content
Field Title	Endpoint
Field Description	Entry point to the Commerce Anywhere Shipping web service.
Example	http://HOST[:PORT]/ShippingOptionsBean/ShippingOptionsService

Figure A–53 Configure ICE Web Services - Extended Item for Policy None

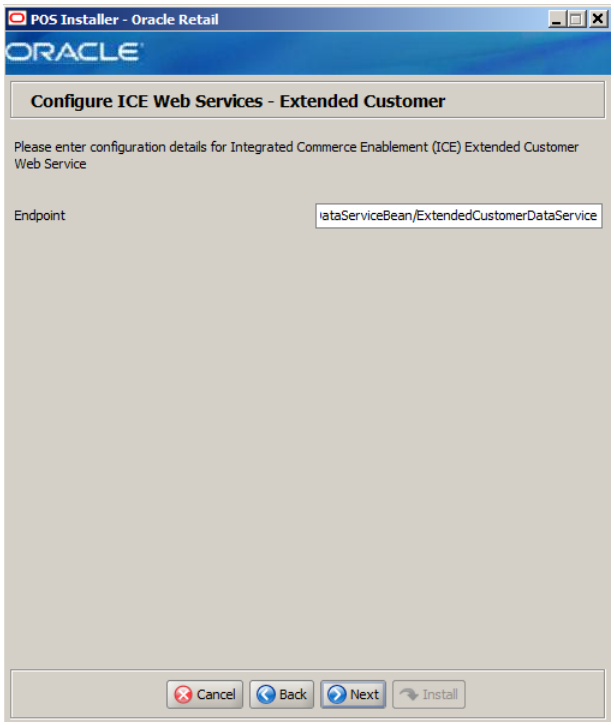


This window is only displayed if **Orders** is selected in the Integrate Application window and then **Integrated Commerce Enablement** is selected in the Order Integrations window and **None** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The field in this window is described in the following table:

Details	Content
Field Title	Endpoint
Field Description	Entry point to the ICE Extended Item web service.
Example	http://HOST[:PORT]/ExtendedItemDataServiceBean/ExtendedItemDataService

Figure A–54 Configure ICE Web Services - Extended Customer for Policy None

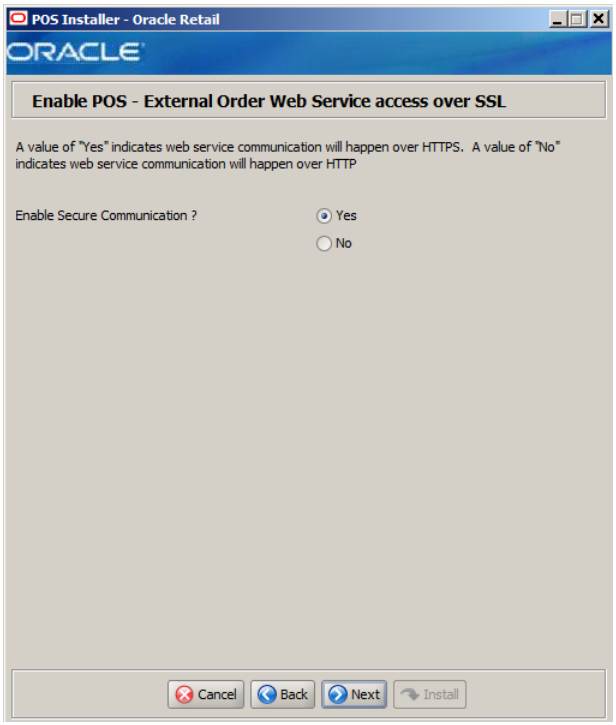


This window is only displayed if **Orders** is selected in the Integrate Application window and then **Integrated Commerce Enablement** is selected in the Order Integrations window and **None** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The field in this window is described in the following table:

Details	Content
Field Title	Endpoint
Field Description	Entry point to the ICE Extended Customer web service.
Example	http://HOST[:PORT]/ExtendedCustomerDataServiceBean/ExtendedCustomerDataService

Figure A–55 Enable POS - External Order Web Service Access Over SSL

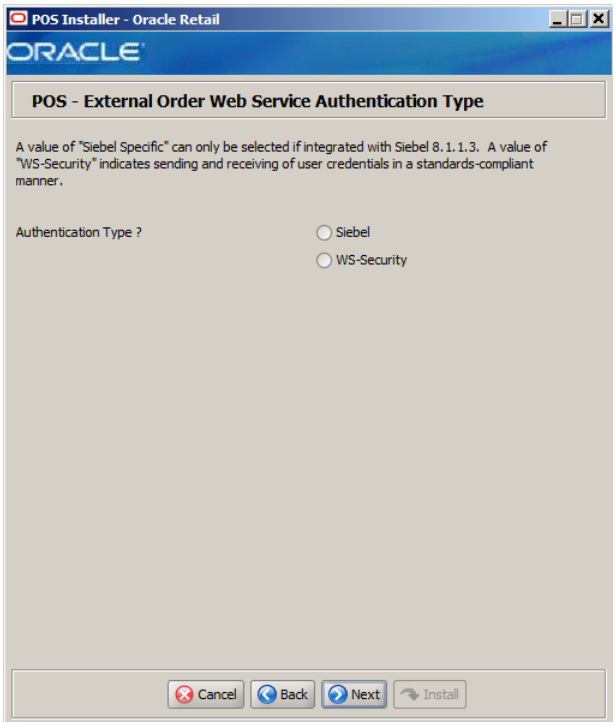


This window is only displayed if **Orders** and then **External Order** are selected in the Integrate Applications window.

The field in this window is described in the following table:

Details	Content
Field Title	Enable Secure Communication?
Field Description	Select Yes if web service communication with the external order management is using HTTPS.
Example	Yes

Figure A–56 POS - External Order Web Service Authentication Type

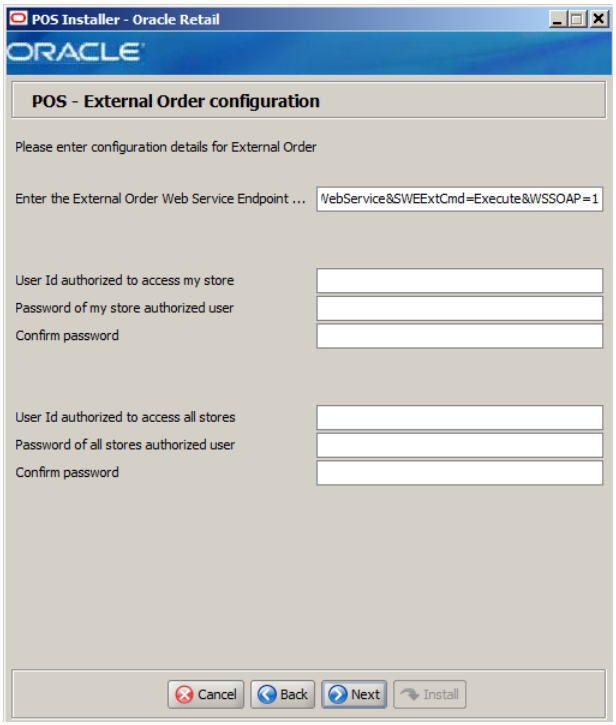


This window is only displayed if **Orders** and then **External Order** are selected in the Integrate Applications window.

The field in this window 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**. **Note:** Only select Siebel if Point-of-Service is integrated with Siebel 8.1.1.3 and is configured to use Siebel web service authentication.

Figure A–57 POS - External Order Configuration



This window is only displayed if **Orders** and then **External Order** are selected in the Integrate Applications window.

The fields in this window are described in the following tables:

Details	Content
Field Title	Enter the External Order Web Service Endpoint URL
Field Description	Enter the URL used by the Point-of-Service application to access the external order management system.
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

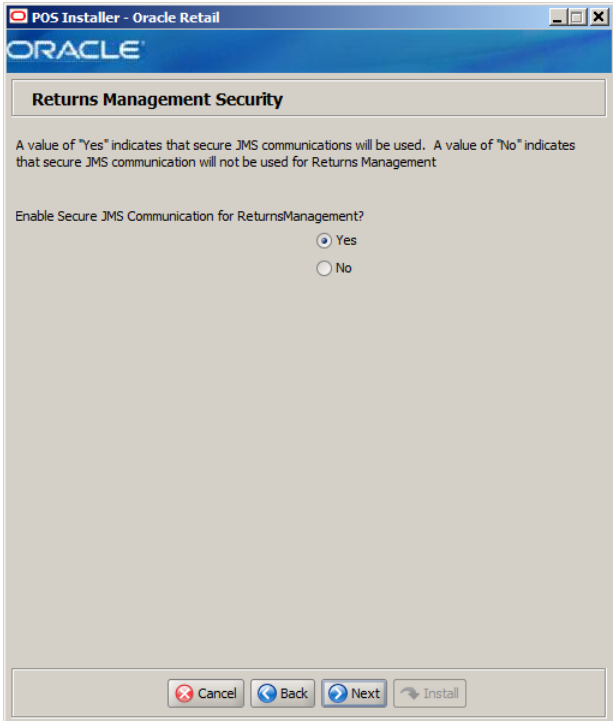
Details	Content
Field Description	Reentered password of my store authorized user used to confirm the password. **Note:** The passwords in the Password of my store authorized user and Confirm Password fields must match.

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–58 Returns Management Security

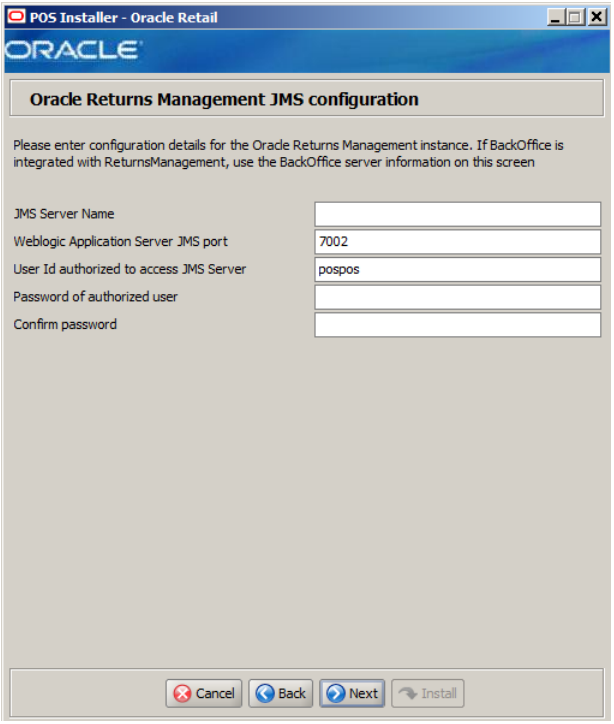


This window is only displayed if **Returns Management** is selected in the Integrate Applications window and **JMS Queue** is selected in the Oracle Returns Management Messaging window.

The field in this window is described in the following table:

Details	Content
Field Title	Enable Secure JMS Communication for Returns Management?
Field Description	Select whether secure JMS communication is used: ▪ To use secure communication, choose **Yes**. ▪ To not use secure communication, choose **No**.
Example	Yes

Figure A–59 Oracle Returns Management JMS Configuration



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

The fields in this window are 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

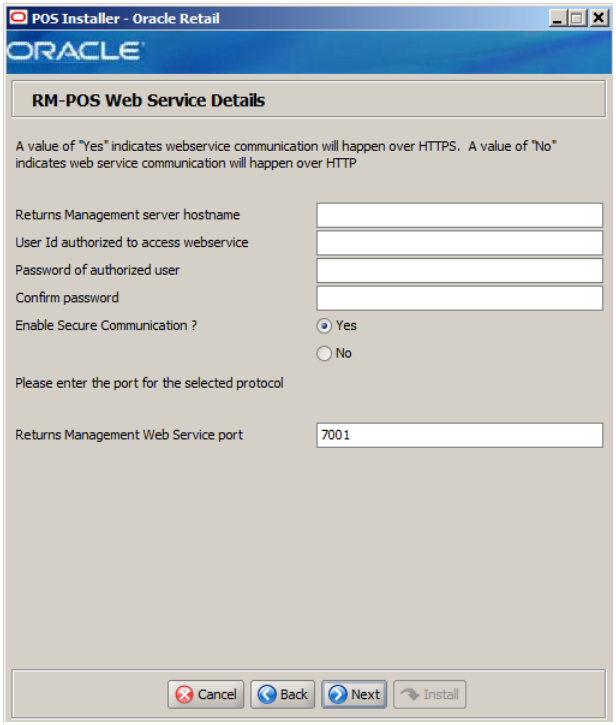
Details	Content
Field Description	Enter the port number of the JMS server to use to send return result messages to Oracle Retail Returns Management.
Example	7002

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–60 RM-POS Web Service Details



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

The fields in this window 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. **Note:** The same Web Service Username that was entered when installing Returns Management must be entered here. For more information, see the *Oracle Retail Returns Management Installation Guide*.

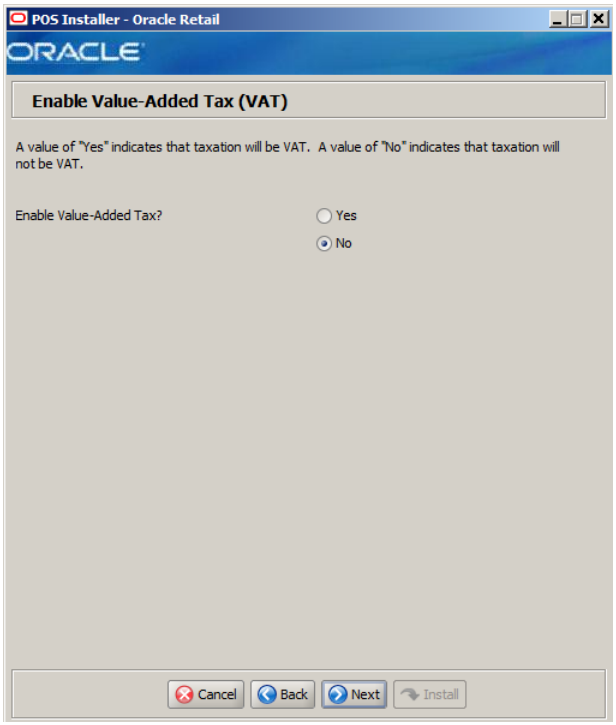
Details	Content
Field Title	Password of authorized user
Field Description	Enter the password of the authorized user. **Note:** The same Web Service Password that was entered when installing Returns Management must be entered here. For more information, see the *Oracle Retail Returns Management Installation Guide*.

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

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

Details	Content
Field Title	Returns Management Web Service port
Field Description	Enter the port number for the Oracle Retail Returns Management web service.
Example	7001

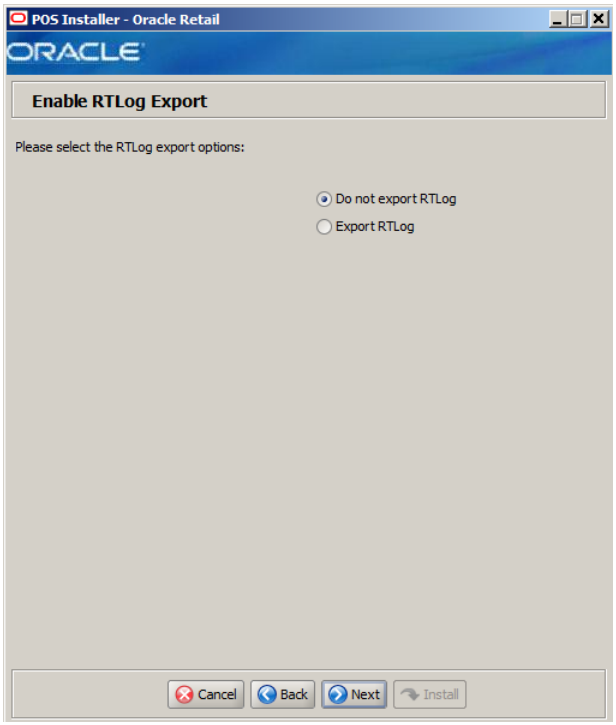
Figure A–61 Enable Value-Added Tax (VAT)



The field in this window 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

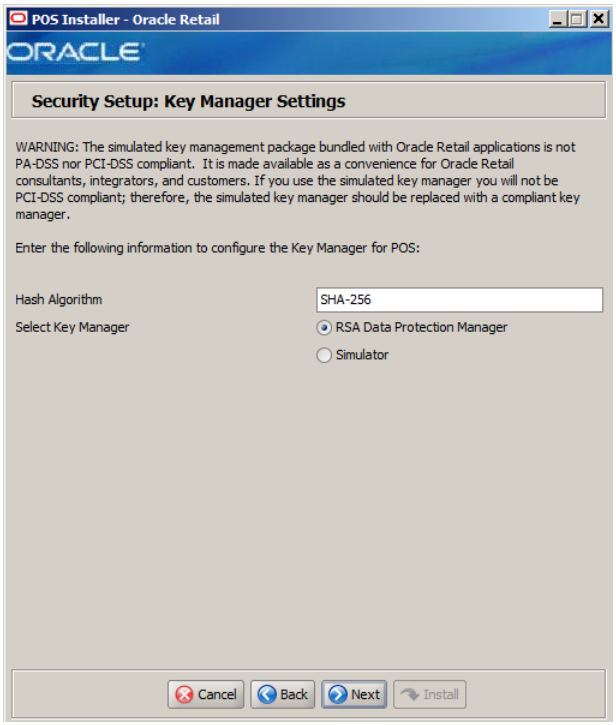
Figure A–62 Enable RTLog Export



The field in this window 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–63 Security Setup: Key Manager Settings



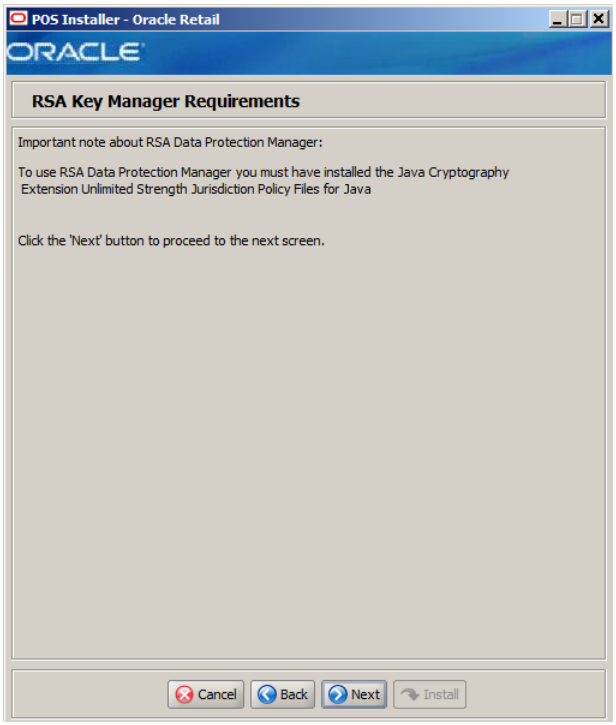
This window is used to configure the Encryption Key Manager.

The fields in this window 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

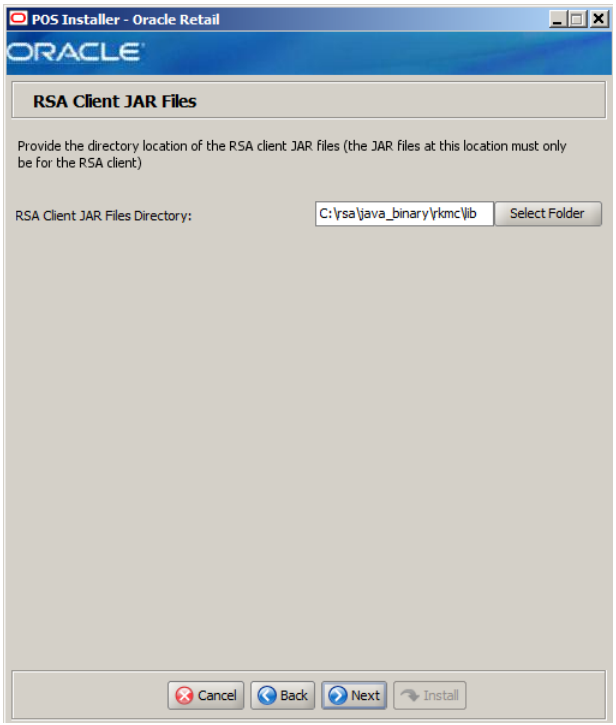
Details	Content
Field Title	Select Key Manager
Field Description	Provider for Key Store management: ■ RSA Data Protection Manager package, select **RSA Data Protection Manager**. The next window displayed is Figure A–64. ■ To use the simulated key management package, select **Simulator**. The next window displayed is Figure A–67.
Example	RSA Data Protection Manager

Figure A–64 RSA Key Manager Requirements



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

Figure A–65 RSA Client JAR Files

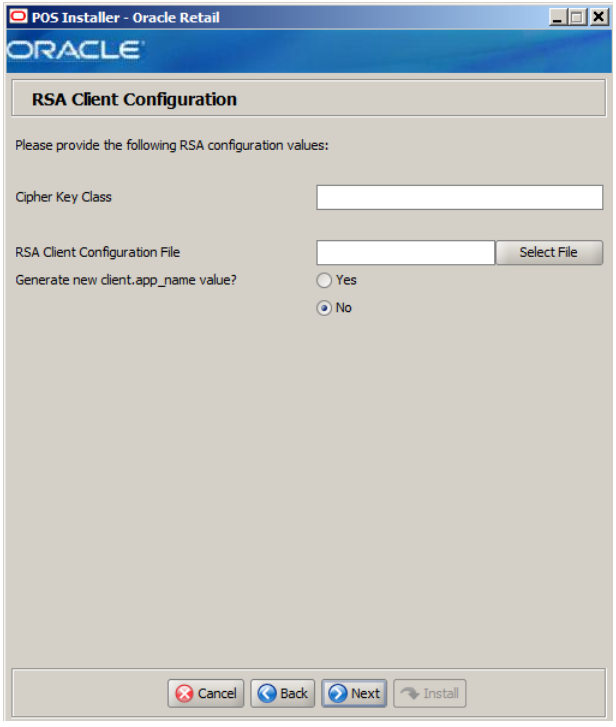


This window is only displayed if **RSA Data Protection Manager** is selected in the Security Setup: Key Manager window.

The field in this window is described in the following table:

Details	Content
Field Title	RSA Client JAR Files Directory
Field Description	Choose the directory where the following RSA client jar files are located: ▪ cryptojce.jar ▪ cryptojcommon.jar ▪ jcm.jar ▪ jcmFIPS.jar ▪ kmsclient.jar ▪ LB.jar ▪ LBJNI.jar ▪ sslj.jar
Example	▪ Microsoft Windows: C:\rsa\java_binary\rlmc\lib ▪ Novell SLEPOS: /opt/rsa/java_binary/rlmc/lib

Figure A–66 RSA Client Configuration



This window is only displayed if **RSA Data Protection Manager** is selected in the Security Setup: Key Manager window.

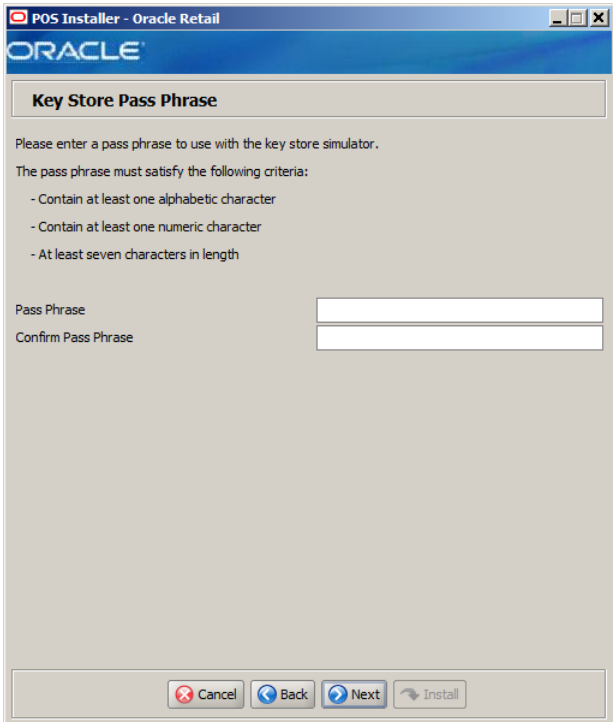
The fields in this window are described in the following tables:

Details	Content
Field Title	Cipher Key Class
Field Description	Enter the name of the cipher suite that define 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–67 Key Store Pass Phrase



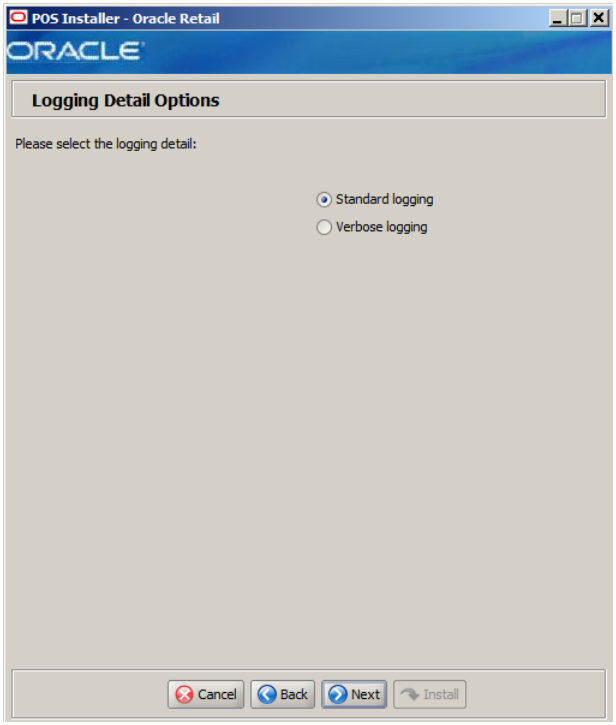
This window is only displayed if **Simulator** is selected in the Security Setup: Key Manager window.

The field in this window 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.

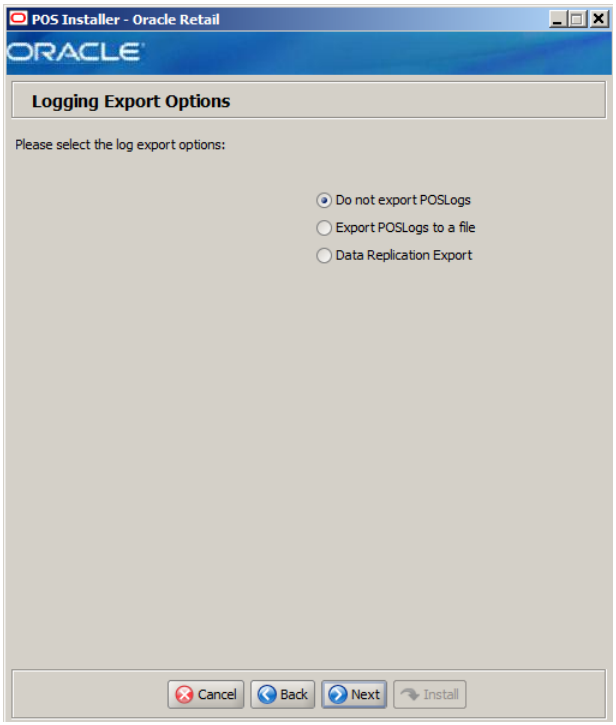
Figure A–68 Logging Detail Options



The field in this window 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	Standard logging

Figure A–69 Logging Export Options

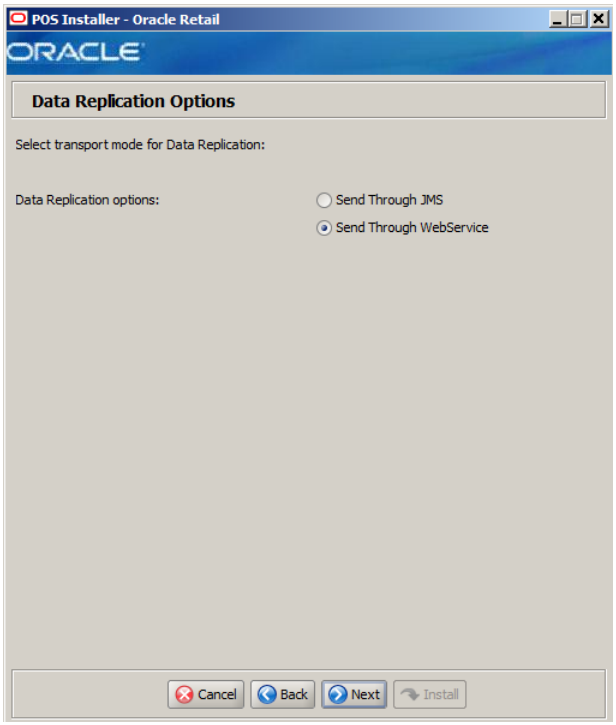


This window is only displayed if **Central Office/Back Office** is selected in the Integrate Applications window.

The field in this window 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–70 Data Replication Options

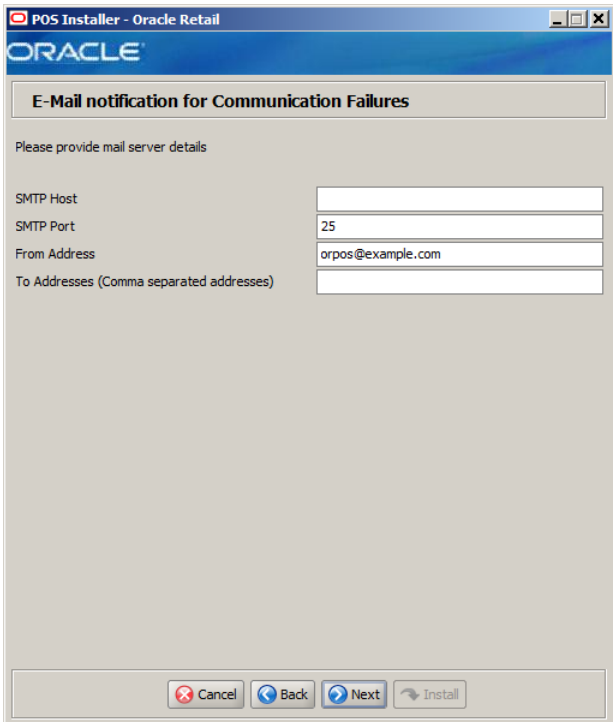


This window is only displayed if **Data Replication Export** is selected in the Logging Export Options window.

The field in this window 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–71 E-Mail Notification for Communication Failures



This window is only displayed if **Send through Webservice** is selected in the Data Replication Options window.

The fields in this window are described in the following tables:

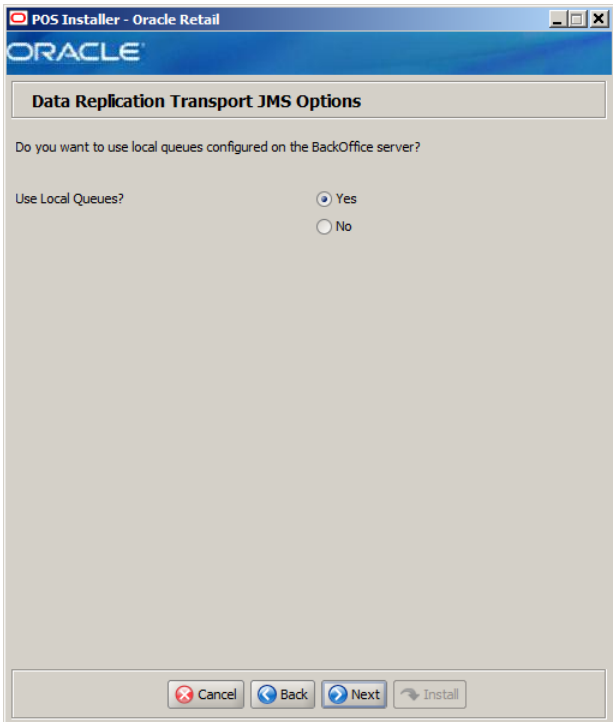
Details	Content
Field Title	SMTP host
Field Description	Host where the SMTP server is running.

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–72 Data Replication Transport JMS Options

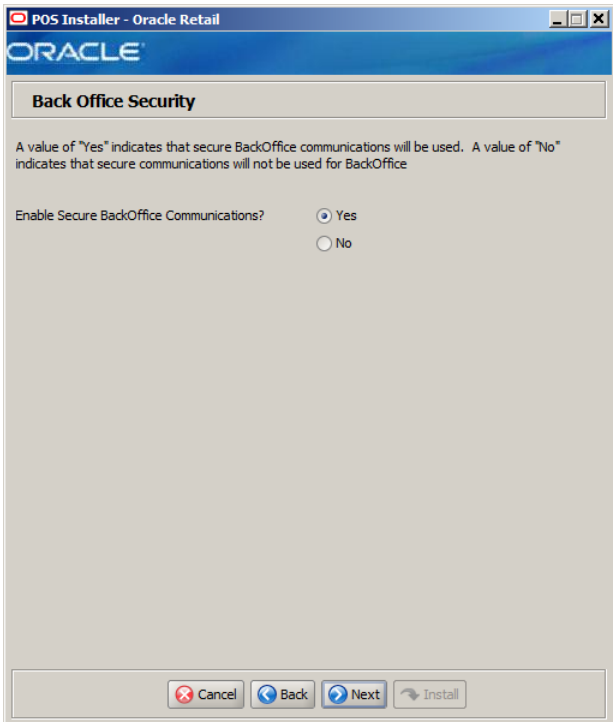


This window is only displayed if **Send through JMS** is selected in the Data Replication Options window.

The field in this window 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–73 Back Office Security

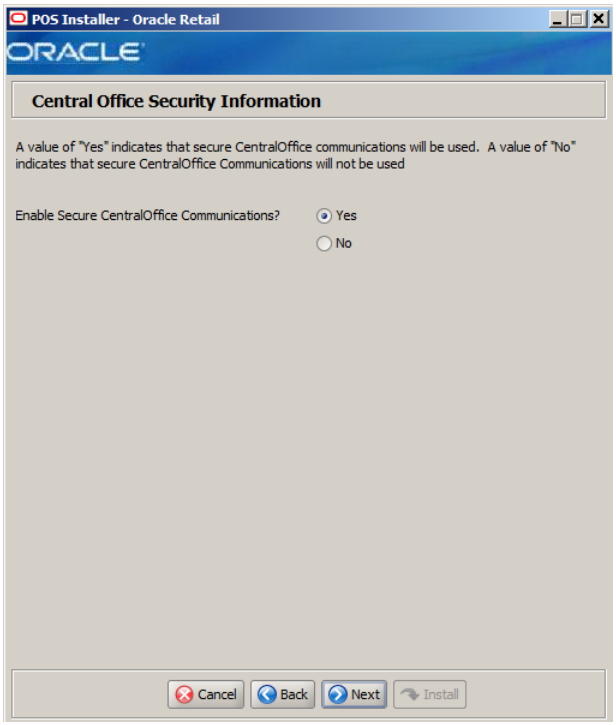


This window is only displayed if **Central Office/Back Office** is selected in the Integrate Applications window.

The field in this window 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–74 Central Office Security Information

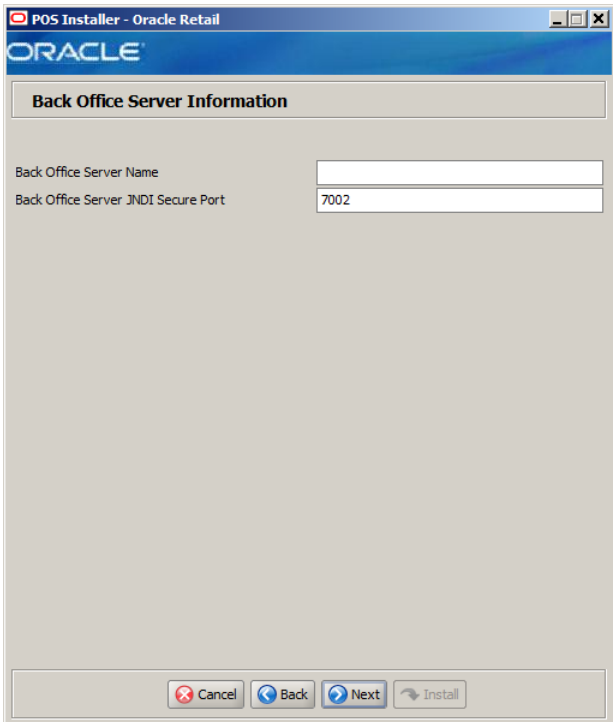


This window is only displayed if **Central Office/Back Office** is selected in the Integrate Applications window.

The field in this window 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–75 Back Office Server Information



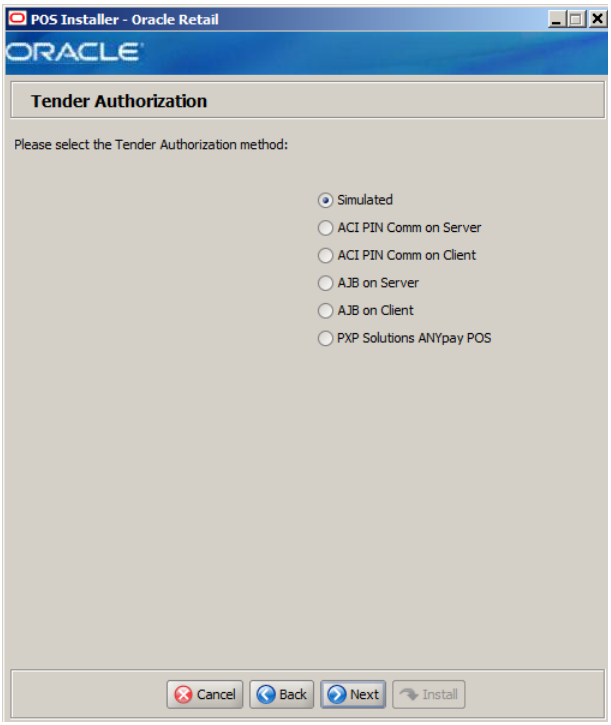
This window is only displayed if **Central Office/Back Office** is selected in the Integrate Applications window.

The fields in this window 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

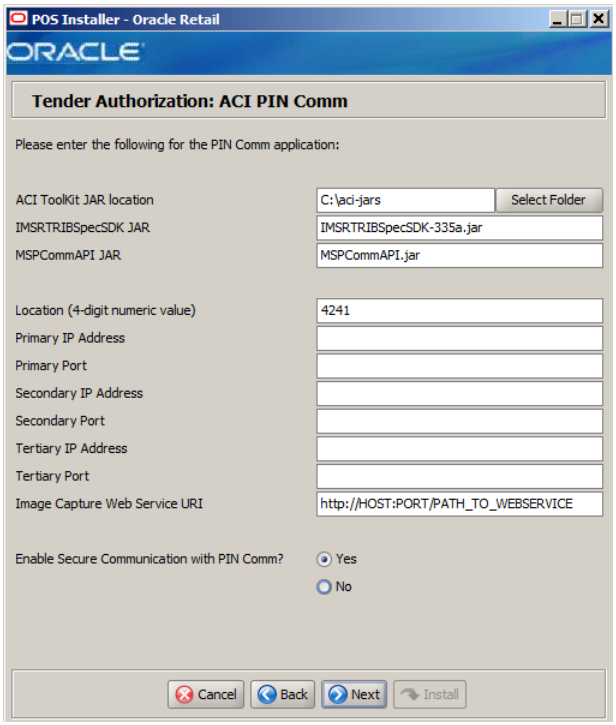
Figure A–76 Tender Authorization



The field in this window 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 by the store server to a third-party system to approve the authorizations, choose **ACI PIN Comm on Server**, **AJB on Server**, or **PXP Solutions ANYpay POS**. ▪ If approvals are handled by the client, select **ACI PIN Comm on Client** or **AJB on Client**. **Note:** If the store server is located at a remote location, it is highly recommended to configure ACI PINComm or AJB at each client in order to help minimize network delay. **Note:** Demo installations should use the Simulated option.
Example	Simulated

Figure A–77 Tender Authorization: ACI PIN Comm



This window is only displayed if **ACI PIN Comm on Server** is selected in the Tender Authorization window.

The fields in this window are described in the following tables:

Details	Content
Field Title	ACI ToolKit JAR Location
Field Description	Enter the path to the ACI ToolKit JAR file.
Example	▪ Microsoft Windows: C:\aci-jars ▪ Novell SLEPOS: /opt/aci-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	MSPCommAPI JAR
Field Description	Enter the name of the MSPCommAPI JAR file.
Example	MSPCommAPI.jar

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

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

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

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

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

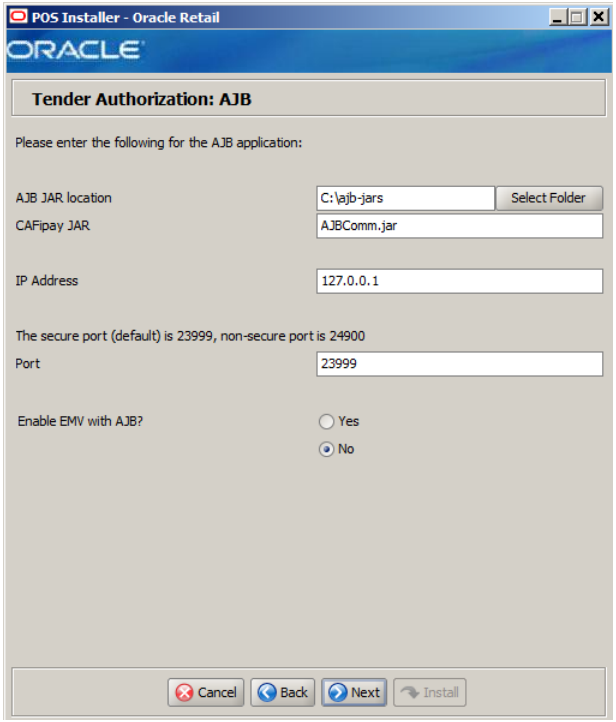
Details	Content
Field Title	Tertiary IP Address
Field Description	Enter the tertiary IP address used for the communication between the store server and the tender authorizer.

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

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

Details	Content
Field Title	Enable Secure Communication with PIN Comm?
Field Description	Select **Yes** for communication with ACI PINComm using HTTPS.
Example	Yes

Figure A–78 Tender Authorization: AJB



This window is only displayed if **AJB on Server** is selected in the Tender Authorization window.

The fields in this window are described in the following tables:

Details	Content
Field Title	AJB JAR Location
Field Description	Enter the path to the AJB JAR file.
Example	▪ Microsoft Windows: C:\ajb-jars ▪ Novell SLEPOS: /opt/ajb-jars

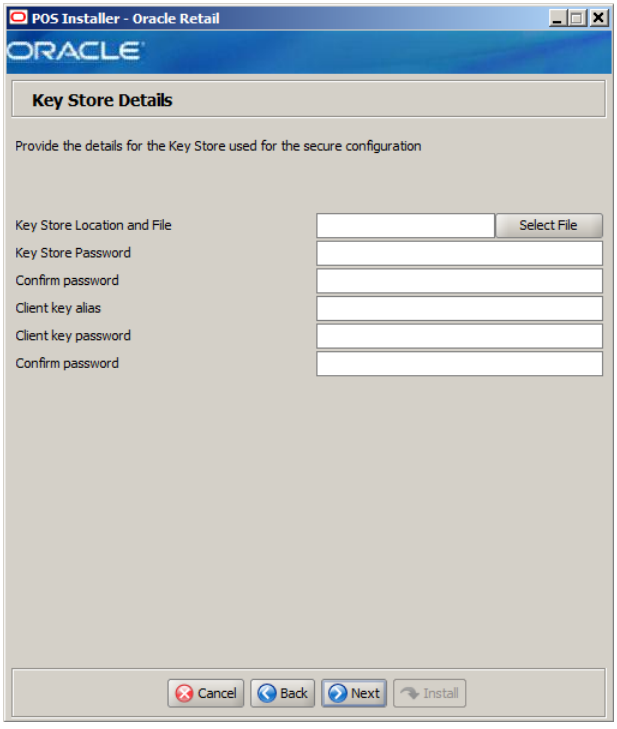
Details	Content
Field Title	CAFipay JAR
Field Description	Enter the name of the CAFipay JAR file.
Example	AJBComm.jar

Details	Content
Field Title	IP Address
Field Description	Enter the IP address used for the communication between the store server and the tender authorizer.
Example	127.0.0.1

Details	Content
Field Title	Port
Field Description	Enter the port number used for the communication between the store server and the tender authorizer.
Example	23999

Details	Content
Field Title	Enable EMV with AJB?
Field Description	Select whether Europay, MasterCard, and Visa (EMV) is enabled with AJB: ■ To enable EMV, select **Yes**. ■ To not enable EMV, select **No**.
Example	No

Figure A–79 Key Store Details



This window is displayed if **Policy B** is selected in the Configure Commerce Anywhere Web Services - Security Policy window.

The fields in this window are described in the following tables:

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

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

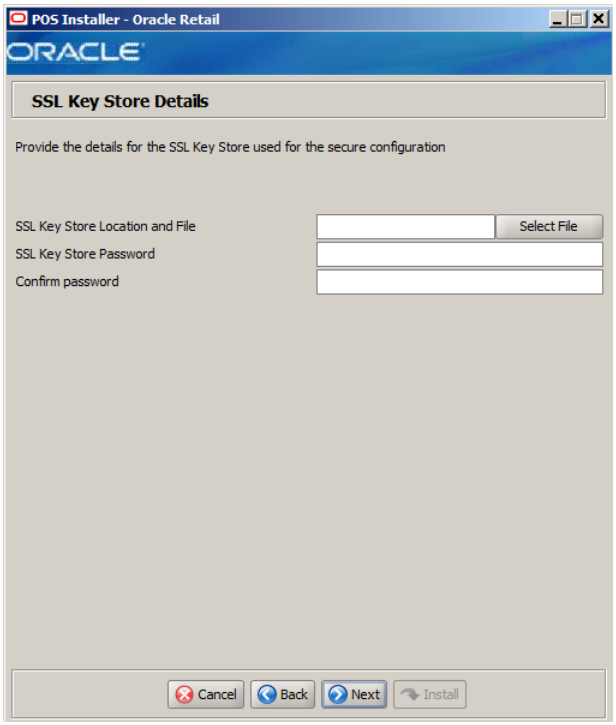
Details	Content
Field Title	Confirm Password
Field Description	Reentered Key Store Password used to confirm the password. **Note:** The passwords in the Key Store Password and Confirm Password fields must match.

Details	Content
Field Title	Client Key Alias
Field Description	Enter the alias for the client key.

Details	Content
Field Title	Client Key Password
Field Description	Enter the password for the client key.

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

Figure A–80 SSL Key Store Details



This window is displayed depending on the security options selected.

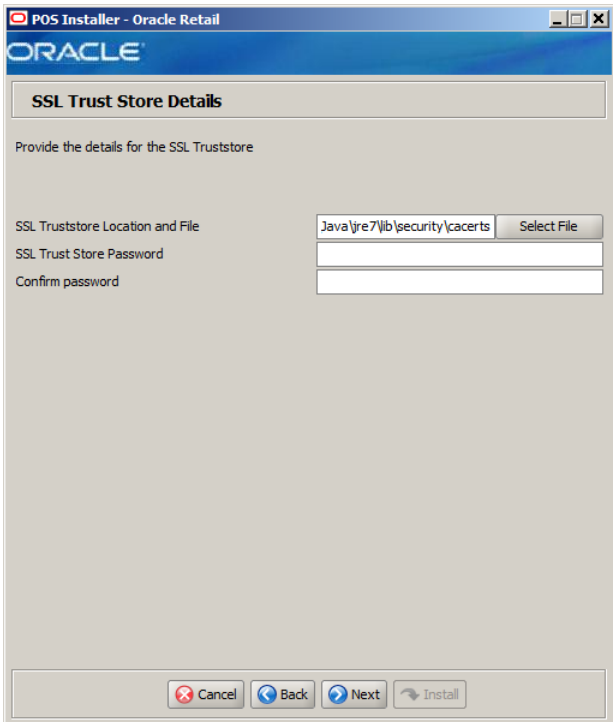
The fields in this window are described in the following tables:

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–81 SSL Trust Store Details



The fields in this window 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	▪ Microsoft Windows: C:\Program Files\Java\jre7\lib\security\cacerts ▪ Novell SLEPOS: /opt/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–82 Installation Progress

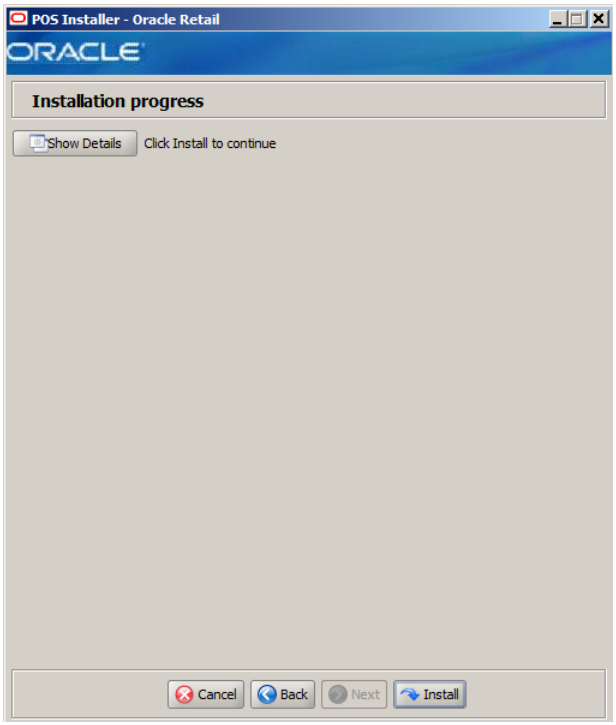
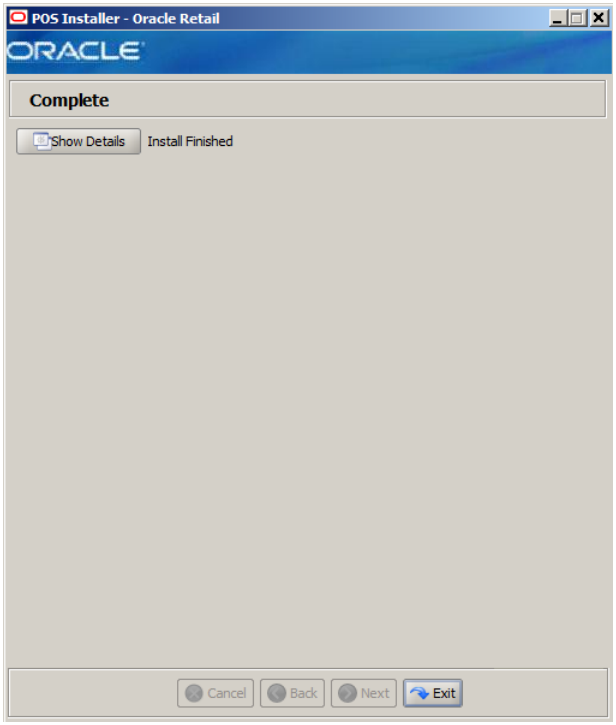


Figure A–83 Install Complete



B

Appendix: Installer Windows for Client Installation

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

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

For the installer windows for a server installation, see Appendix A.

> **Note:** The paths shown in the window examples in this appendix use the path format for Microsoft Windows. In the table describing those fields, example paths for both Microsoft Windows and Novell SLEPOS are shown.

Figure B–1 Introduction

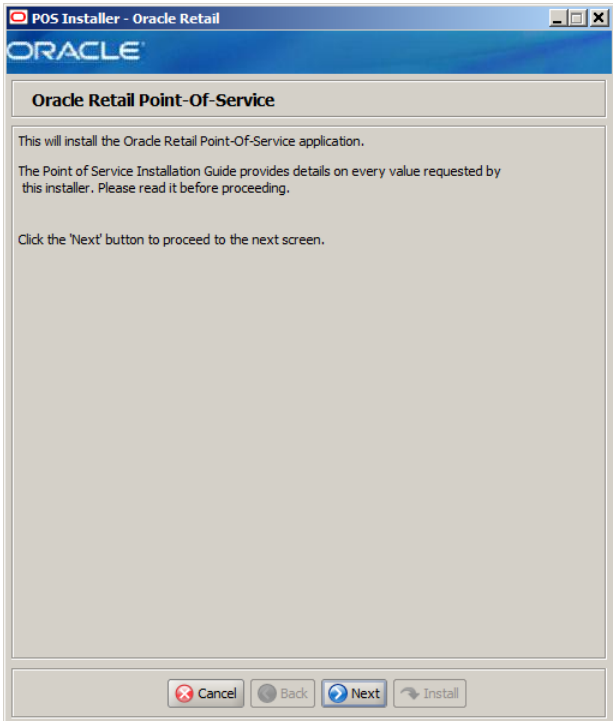


Figure B–2 Previous POS Install

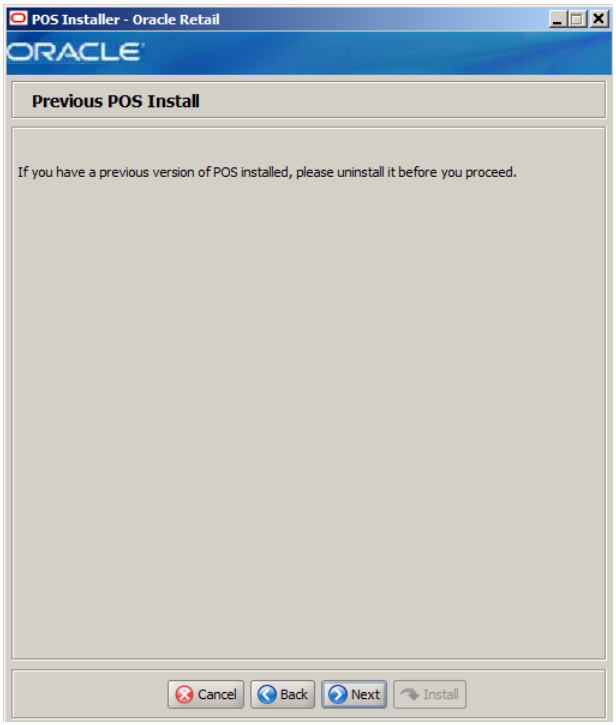
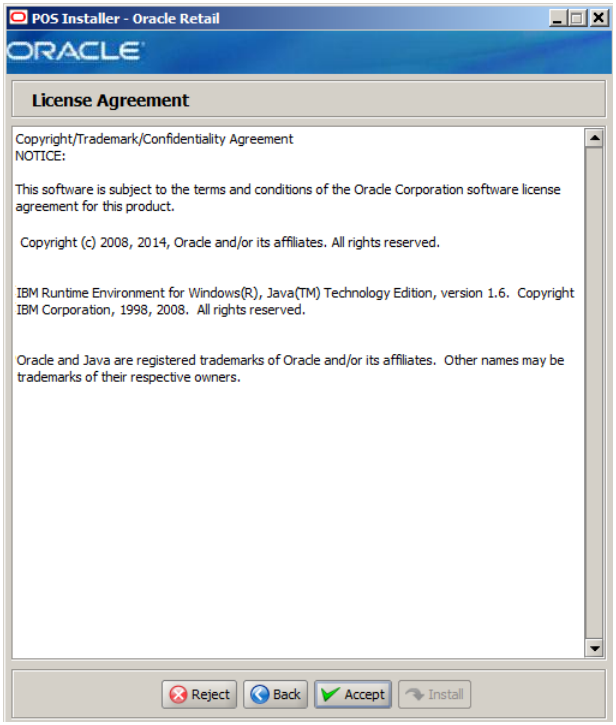
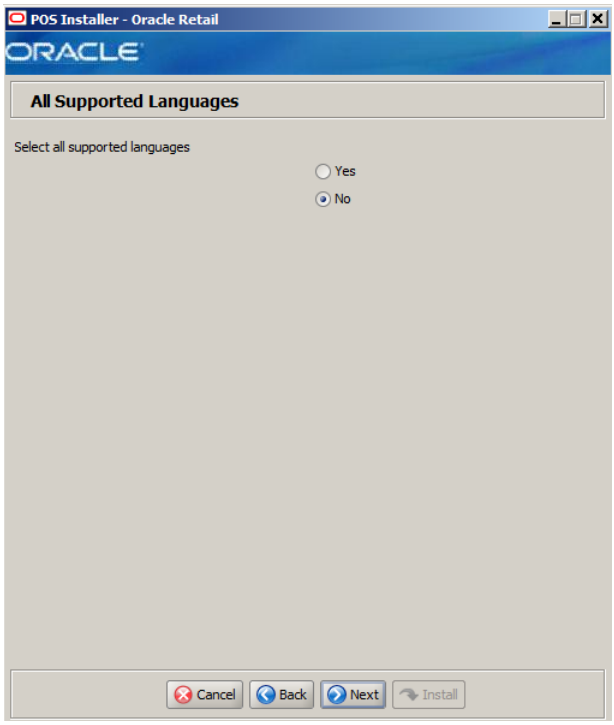


Figure B–3 License Agreement



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

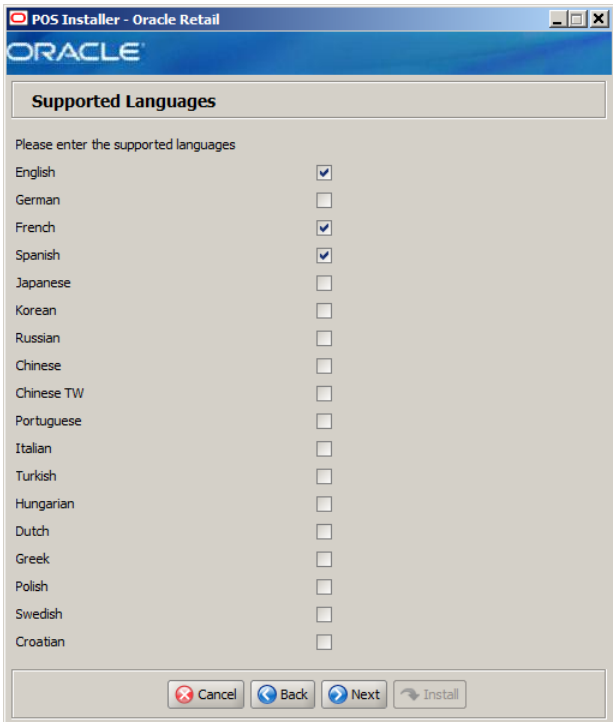
Figure B–4 All Supported Languages



The field in this window is described in the following table:

Details	Content
Field Title	Select all supported languages
Field Description	Choose whether all languages are initially selected on the Supported Languages screen: ▪ To have all available languages initially selected, select **Yes**. ▪ To have only English initially selected, select **No**.
Example	No

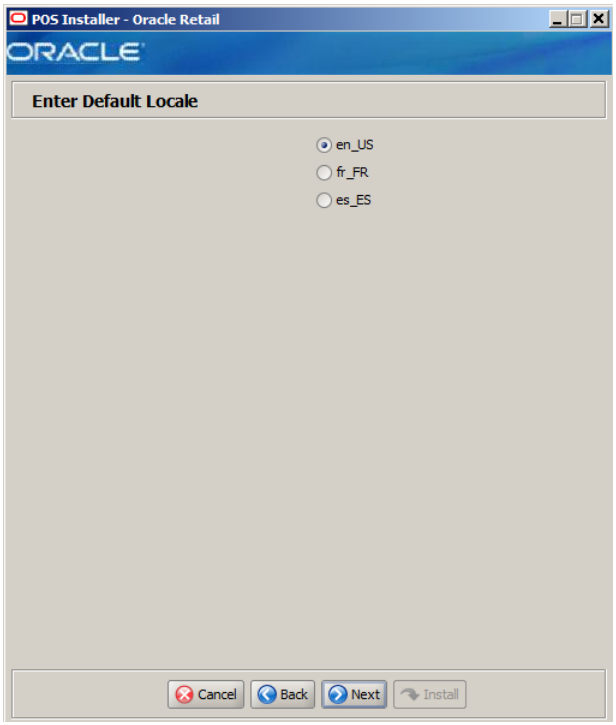
Figure B–5 Supported Languages



The field in this window 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 in this window determine the available choices in the Enter Default Locale window.
Example	English, French, and Spanish

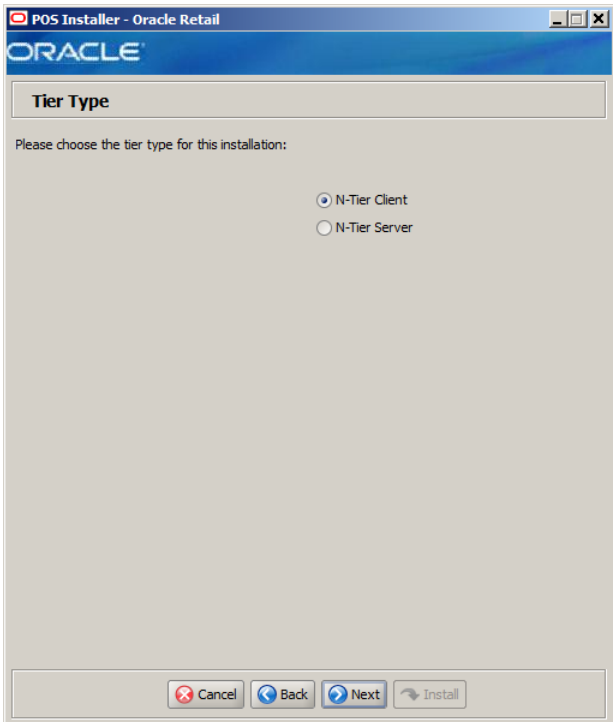
Figure B–6 Enter Default Locale



The field in this window 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 in the Supported Languages window. For each selected language, the default locale for that language is displayed in the Enter Default Locale window. For example, if English, French, and Italian are selected in the Supported Languages window, en_US, fr_FR, and it_IT are the available choices for the default locale.
Example	en_US

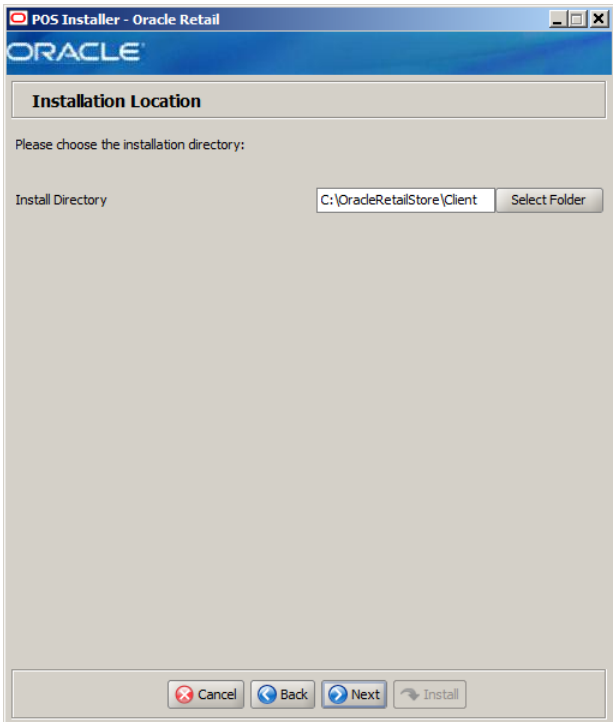
Figure B–7 Tier Type



The field in this window 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

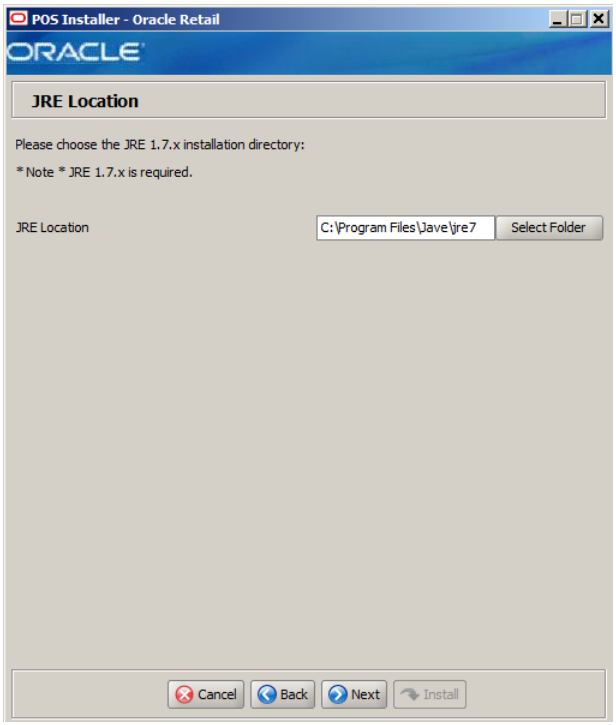
Figure B–8 Installation Location



The field in this window 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. **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	■ Microsoft Windows: C:\OracleRetailStore\Client ■ Novell SLEPOS: /OracleRetailStore/Client

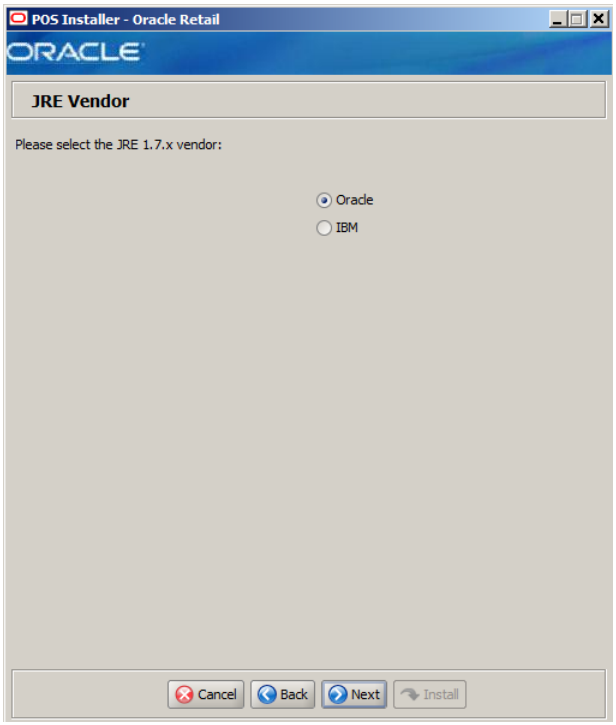
Figure B–9 JRE Location



The field in this window is described in the following table:

Details	Content
Field Title	JRE Location
Field Description	Enter the location where the JRE is installed.
Example	▪ Microsoft Windows: C:\Program Files\Java\jre7 ▪ Novell SLEPOS: /opt/Java/jre7

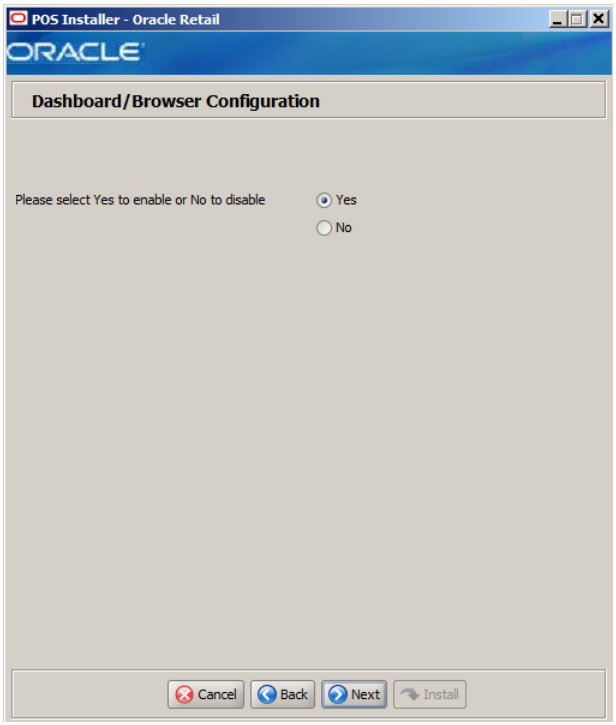
Figure B–10 JRE Vendor



The field in this window 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 in the JRE Location window: ▪ Oracle ▪ IBM
Example	Oracle

Figure B–11 Dashboard/Browser Configuration

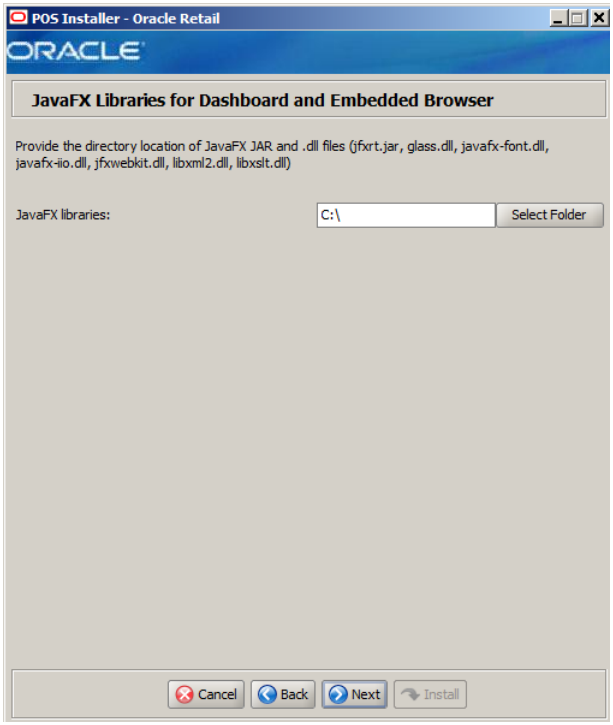


This window is only displayed if **IBM** is selected in the JRE Vendor window.

The field in this window is described in the following table:

Details	Content
Field Title	Please select Yes to enable or No to disable
Field Description	Select whether the dashboard and web browser are configured: ▪ To configure the dashboard and web browser, choose **Yes**. ▪ To not configure the dashboard and web browser, choose **No**.

Figure B–12 JavaFX and Shared Objects Lib for Microsoft Windows Embedded POSReady

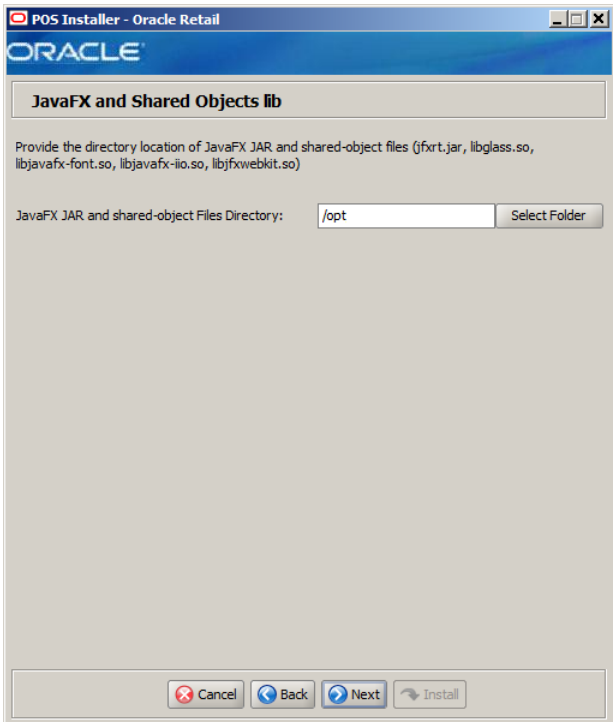


This window is only displayed on Microsoft Windows Embedded POSReady if **IBM** is selected in the JRE Vendor window and **Yes** is selected in the Dashboard/Browser Configuration window.

The field in this window is described in the following table:

Details	Content
Field Title	JavaFX libraries
Field Description	Select the location of the directory with the required files: ▪ jfxrt.jar ▪ glass.dll ▪ javafx-font.dll ▪ javafx-iio.dll ▪ jfxwebkit.dll ▪ libxml2.dll ▪ libxslt.dll
Example	C:\

Figure B–13 JavaFX and Shared Objects Lib for Novell SLEPOS

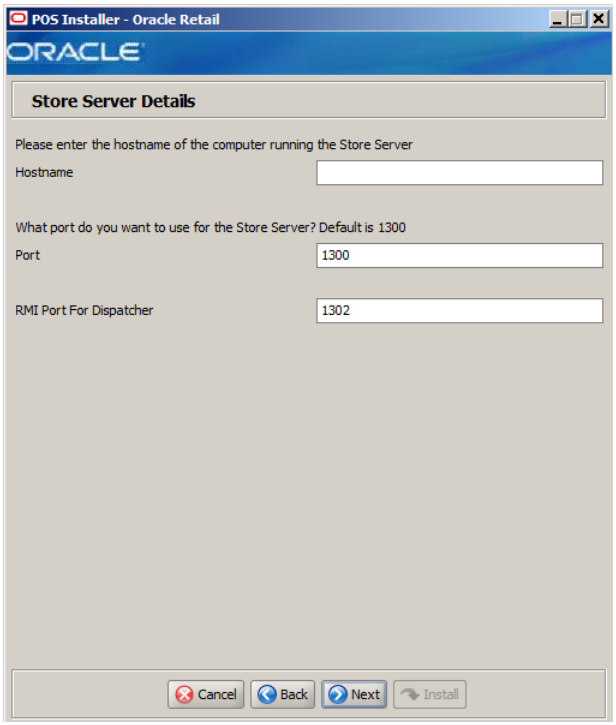


This window is only displayed on Novell SLEPOS if **IBM** is selected in the JRE Vendor window and **Yes** is selected in the Dashboard/Browser Configuration window.

The field in this window is described in the following table:

Details	Content
Field Title	JavaFX JAR and shared-object Files Directory
Field Description	Select the location of the directory with the required files: ▪ jfxrt.jar ▪ libglass.so ▪ libjavafx-font.so ▪ libjfxwebkit.so ▪ libjavafx-iio.so
Example	/opt/

Figure B–14 Store Server Details



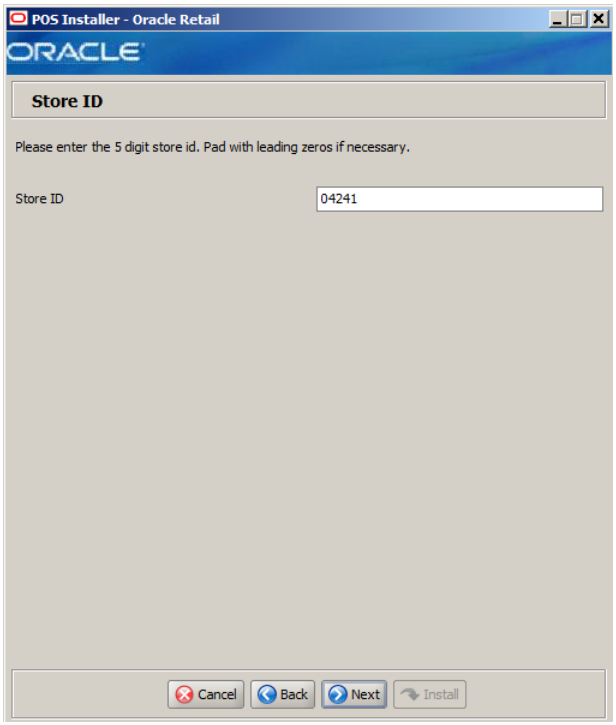
The fields in this window are described in the following tables:

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 JNDI lookups by this installation.
Example	1300

Details	Content
Field Title	RMI Port For Dispatcher
Field Description	Enter the port number of this host computer used for RMI communication to this installation's Point-of-Service dispatcher.
Example	1302

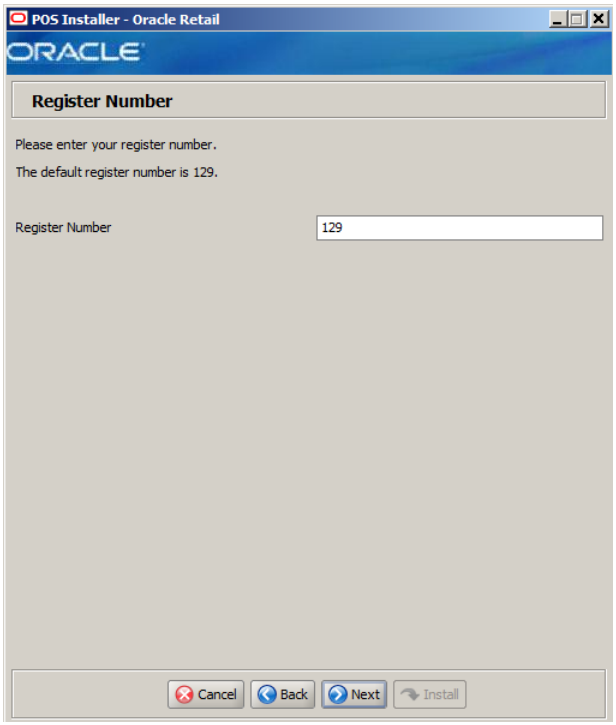
Figure B–15 Store ID



The field in this window 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

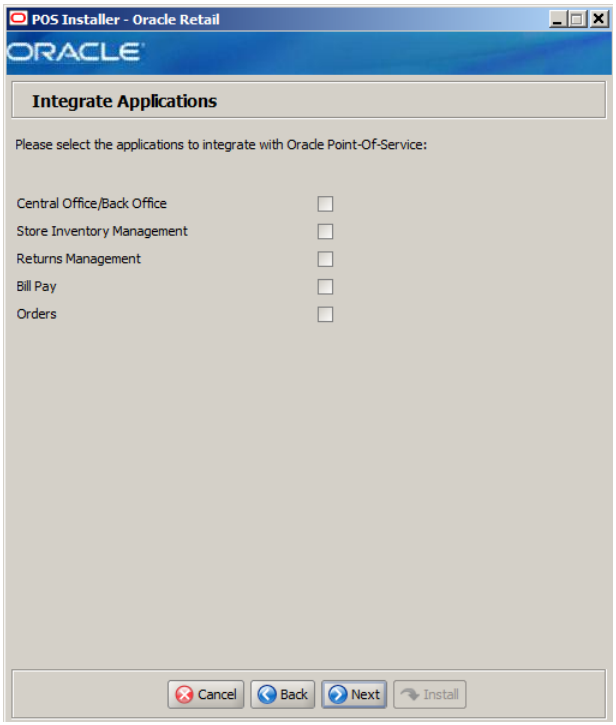
Figure B–16 Register Number



The field in this window 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 999 is supported for the register number. Do not install more than one client with the same register number at a store.

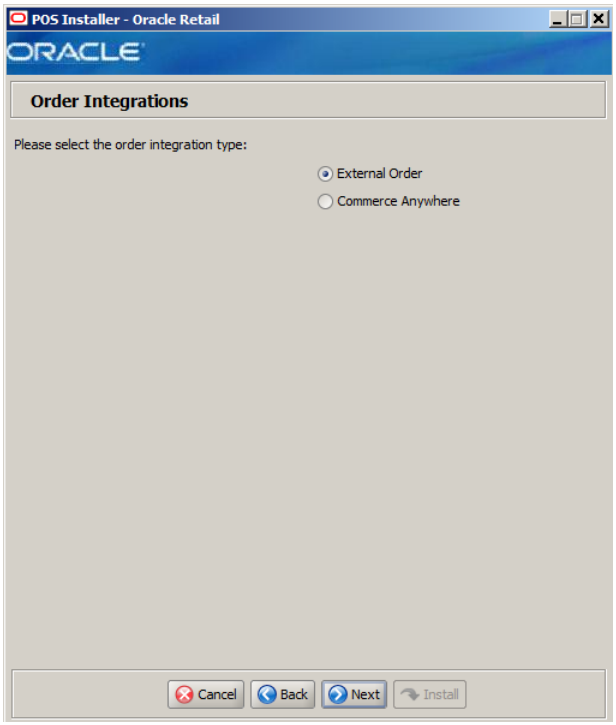
Figure B–17 Integrate Applications



The field in this window 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 ▪ Returns Management ▪ Bill Pay ▪ Orders

Figure B–18 Order Integrations

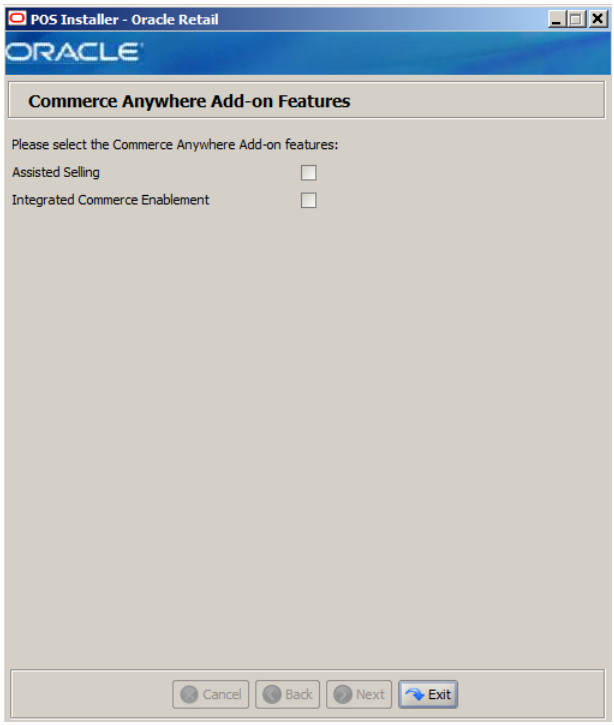


This window is only displayed if **Orders** is selected in the Integrate Applications window.

The field in this window is described in the following table:

Details	Content
Field Title	Please select the order type
Field Description	Select the type of orders to be used: ■ External Order ■ Commerce Anywhere
Example	External Order

Figure B–19 Commerce Anywhere Add-on Features

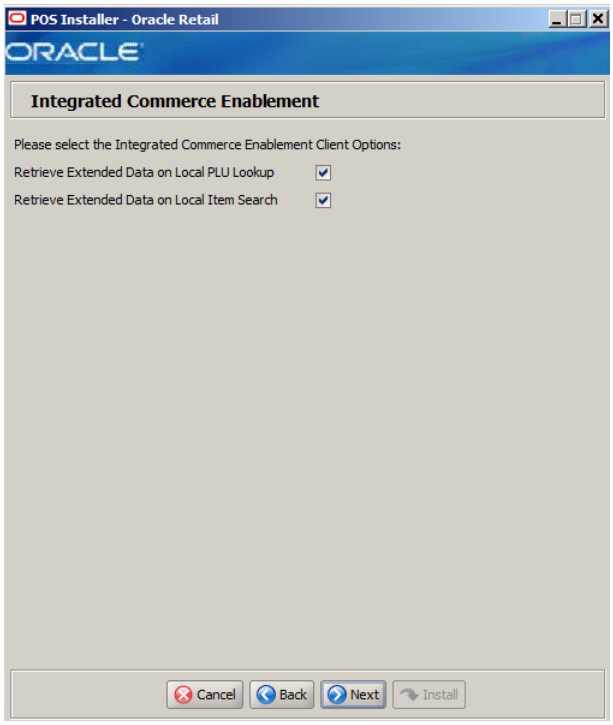


This window is only displayed if **Commerce Anywhere** is selected in the Order Integrations window.

The field in this window is described in the following table:

Details	Content
Field Title	Please select the Commerce Anywhere Add-on features
Field Description	Select the Commerce Anywhere features that will be used in Mobile Point-of-Service: ▪ To use the Assisted Selling Application (ASA), select **Assisted Selling**. **Note:** This feature is not tested in Release 14.1. ▪ To use integrated commerce, select **Integrated Commerce Enablement**.

Figure B–20 Integrated Commerce Enablement

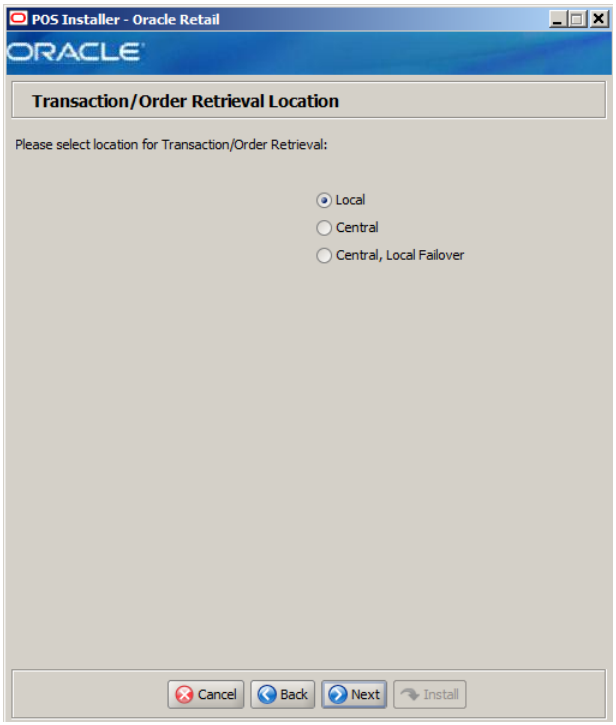


This window is only displayed if **Integrated Commerce Enablement** is selected in the Commerce Anywhere Add-on Features window.

The field in this window is described in the following table:

Details	Content
Field Title	Please select the Integrated Commerce Enablement Client features
Field Description	Select the Commerce Anywhere client features that will be used in Mobile Point-of-Service: ■ To retrieve extended data on local PLU lookup, select **Retrieve Extended Data on Local PLU lookup**. ■ To retrieve extended data on local item search, select **Retrieve Extended Data on Local Item Search**.

Figure B–21 Transaction Retrieval Location

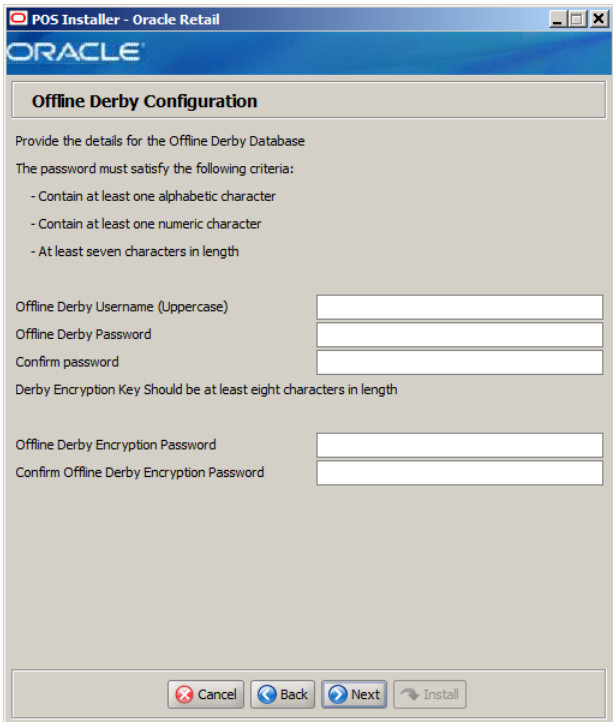


This window is only displayed if **Central Office/Back Office** is selected in the Integrate Applications window.

The field in this window 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–22 Offline Derby Configuration



The fields in this window are described in the following tables:

Details	Content
Field Title	Offline Derby Username (Uppercase)
Field Description	Enter the user name used for offline Derby processing. The user name must be in uppercase characters.

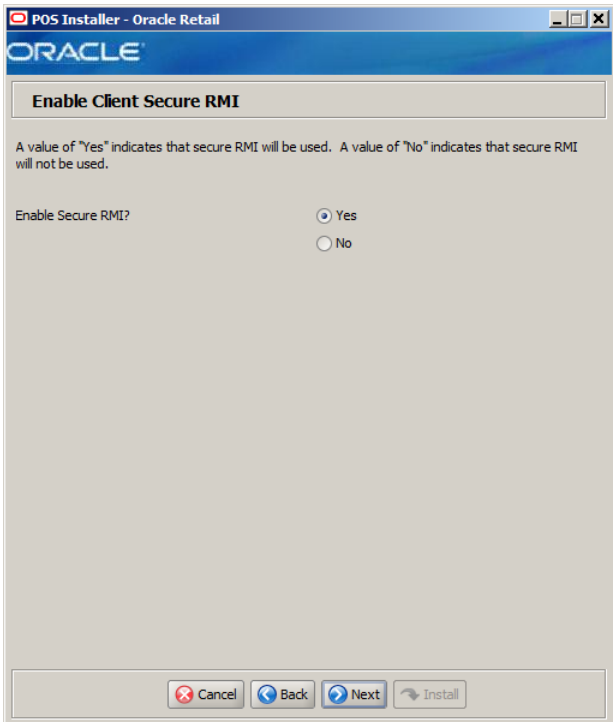
Details	Content
Field Title	Offline Derby Password
Field Description	Enter the password for the offline Derby user.

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

Details	Content
Field Title	Offline Derby Encryption Password
Field Description	Enter the encryption password for the offline Derby user.

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

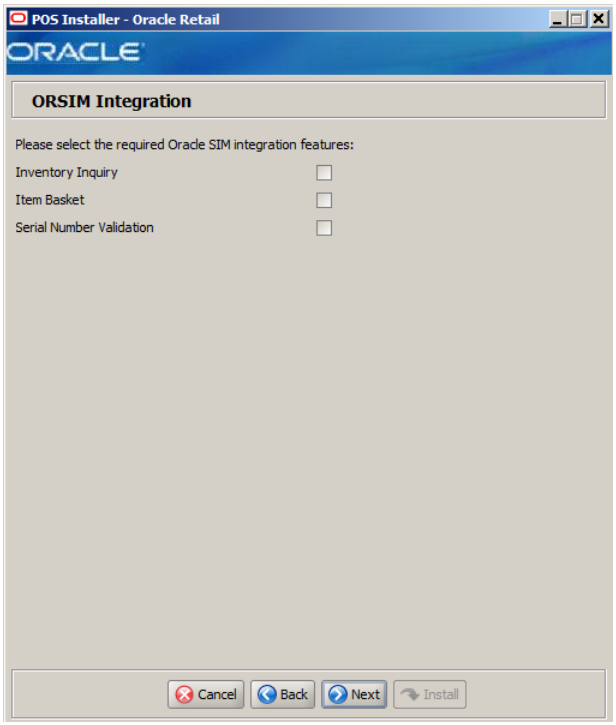
Figure B–23 Enable Client Secure RMI



The field in this window 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 registers. **Note:** If **Yes** is selected, secure RMI must also have been configured for the store server.
Example	Yes

Figure B–24 ORSIM Integration

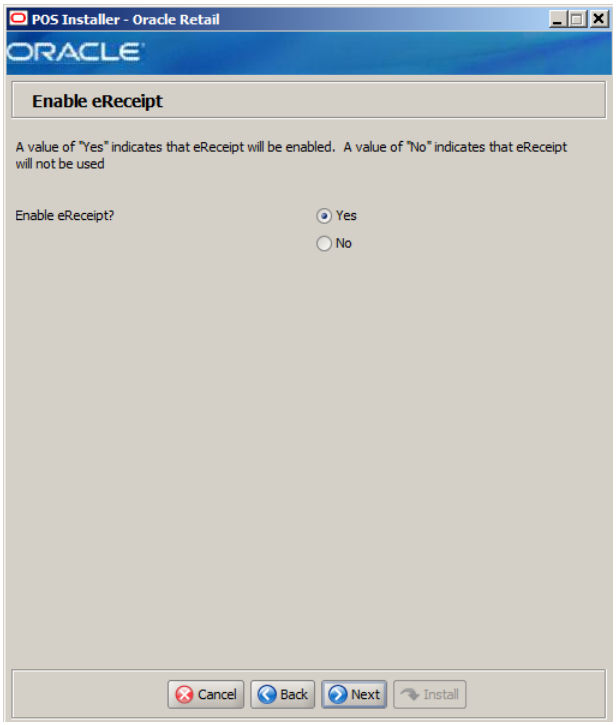


This window is only displayed if **Store Inventory Management** is selected in the Integrate Applications window.

The field in this window 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 serial number validation using SIM, select **Serial Number Validation**.

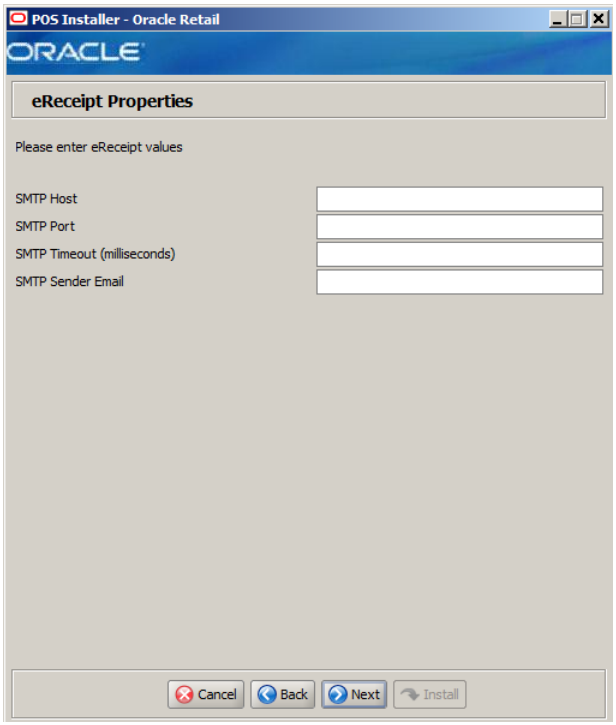
Figure B–25 Enable eReceipt



The field in this window 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–26 eReceipt Properties



This window is only displayed if **Yes** is selected in the Enable eReceipt window.

The fields in this window are described in the following tables:

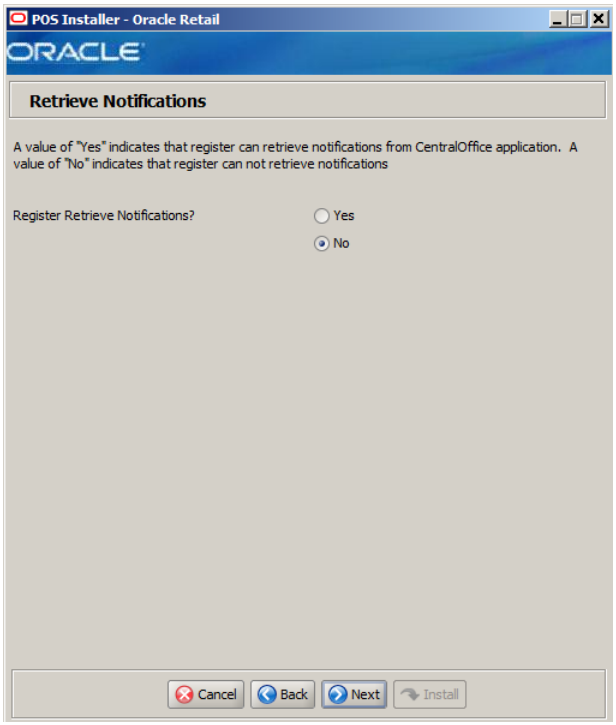
Details	Content
Field Title	SMTP Host
Field Description	Enter the host name for the SMTP server.

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–27 Retrieve Notifications

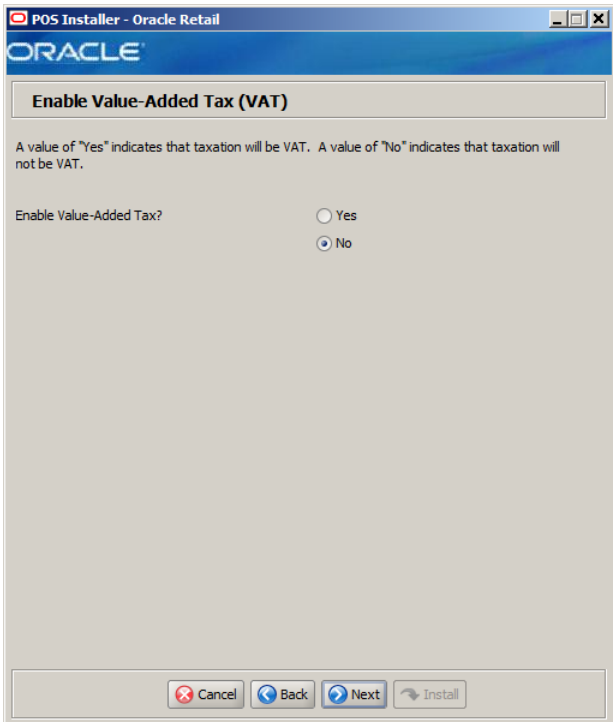


This window is only displayed if **Central Office/Back Office** is selected in the Integrate Applications window.

The field in this window is described in the following table:

Details	Content
Field Title	Register Retrieve Notifications?
Field Description	Select Yes if registers can retrieve notifications from Central Office.
Example	No

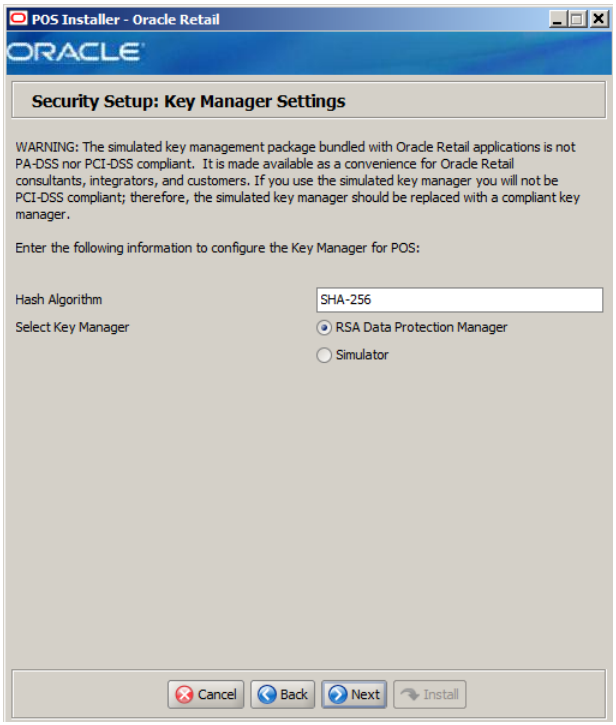
Figure B–28 Value-Added Tax (VAT)



The field in this window 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–29 Security Setup: Key Manager Settings



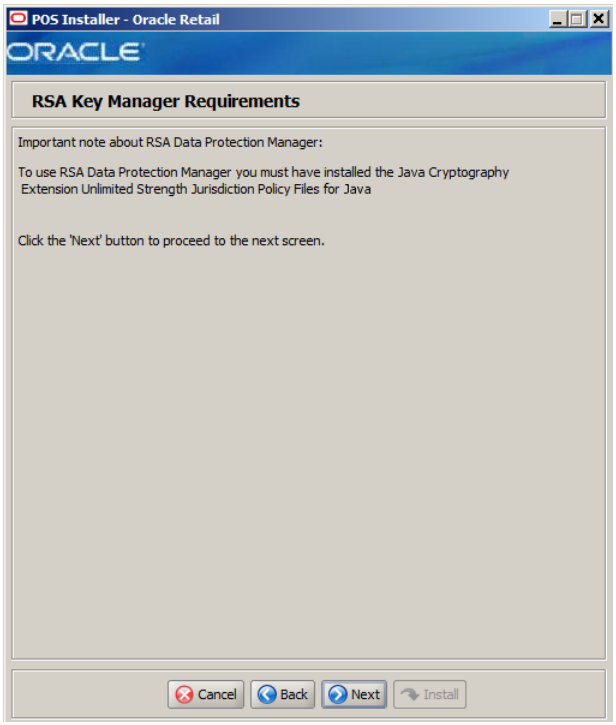
This window is used to configure the Encryption Key Store provider.

The fields in this window 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

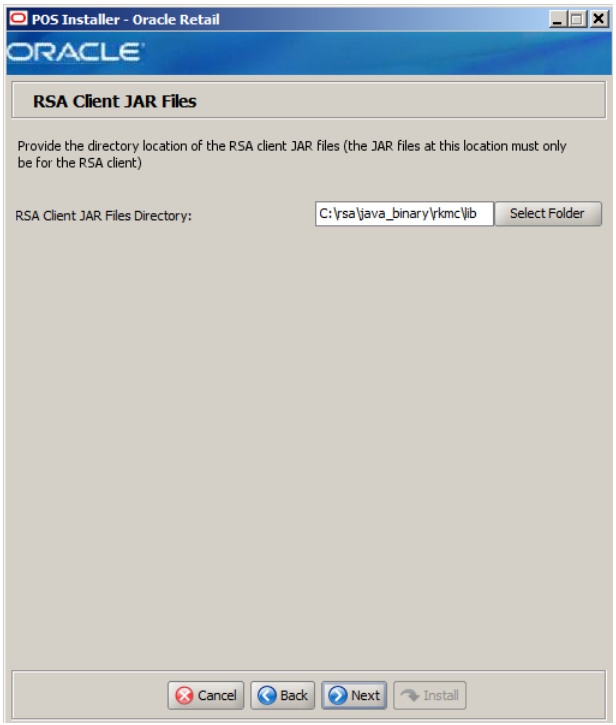
Details	Content
Field Title	Select Key Manager
Field Description	Provider for Key Store management. ▪ To use the RSA key management package, select **RSA Data Protection Manager**. The next window displayed is Figure B–30. ▪ To use the simulated key management package, select **Simulator**. The next window displayed is Figure B–33.
Example	RSA Data Protection Manager

Figure B–30 RSA Key Manager Requirements



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

Figure B–31 RSA Client JAR Files

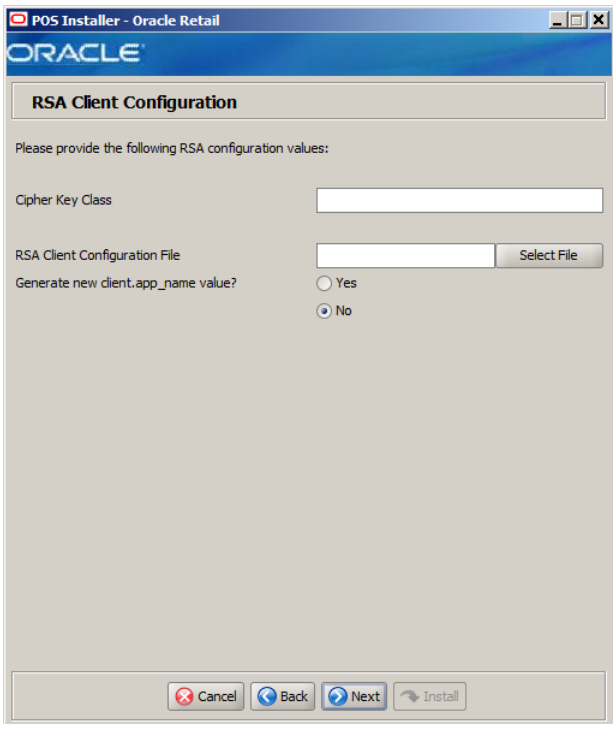


This window is only displayed if **RSA Data Protection Manager** is selected in the Security Setup: Key Manager window.

The field in this window is described in the following table:

Details	Content
Field Title	RSA Client JAR Files Directory
Field Description	Choose the directory where the following RSA client jar files are located: ▪ cryptojce.jar ▪ cryptojcommon.jar ▪ jcm.jar ▪ jcmFIPS.jar ▪ kmsclient.jar ▪ LB.jar ▪ LBJNI.jar ▪ sslj.jar
Example	▪ Microsoft Windows: C:\rsa\java_binary\rlmc\lib ▪ Novell SLEPOS: /opt/rsa/java_binary/rlmc/lib

Figure B–32 RSA Client Configuration



This window is only displayed if **RSA Data Protection Manager** is selected in the Security Setup: Key Manager window.

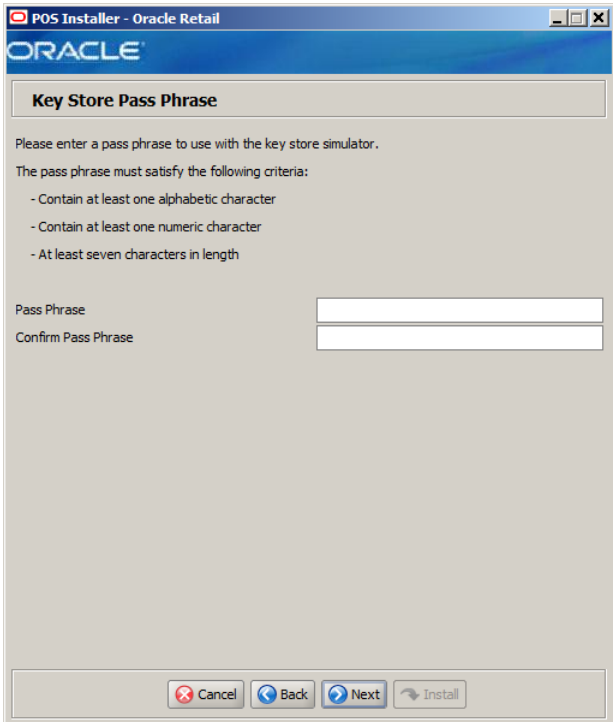
The fields in this window are described in the following tables:

Details	Content
Field Title	Cipher Key Class
Field Description	Enter the name of the cipher suite that define 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–33 Key Store Pass Phrase



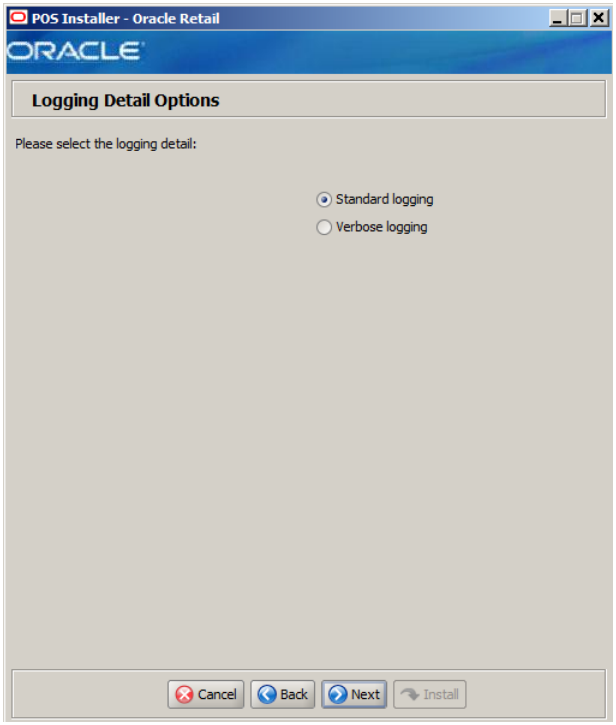
This window is only displayed if **Simulator** is selected in the Security Setup: Key Manager window.

The field in this window 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.

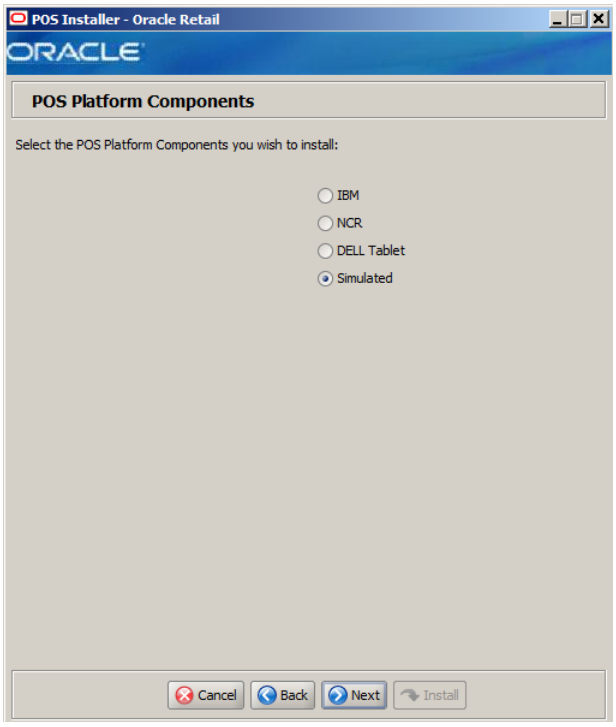
Figure B–34 Logging Detail Options



The field in this window 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	Standard logging

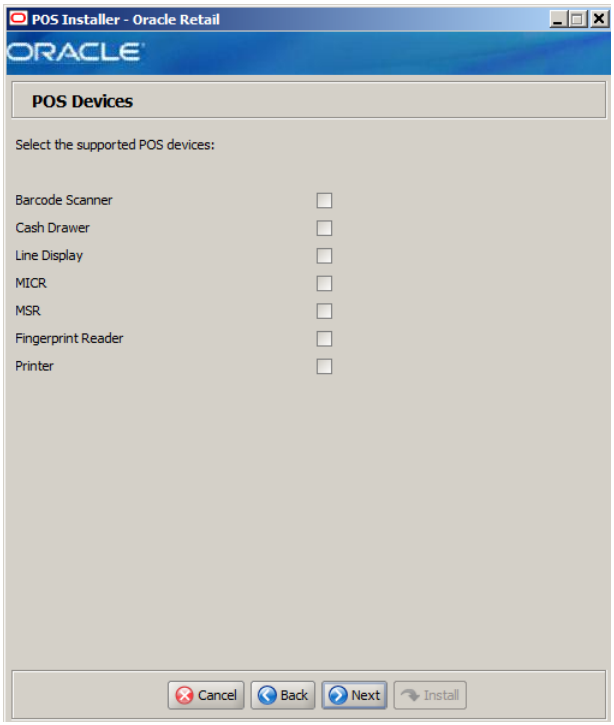
Figure B–35 POS Platform Components



The field in this window 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: ■ To use an IBM register, select **IBM**. ■ To use an NCR register, select **NCR**. ■ To use a Dell tablet, select **Dell Tablet**. ■ To use a register with no devices, select **Simulated**. This should only be selected for a development environment. A network printer may be used.
Example	Simulated

Figure B–36 POS Devices

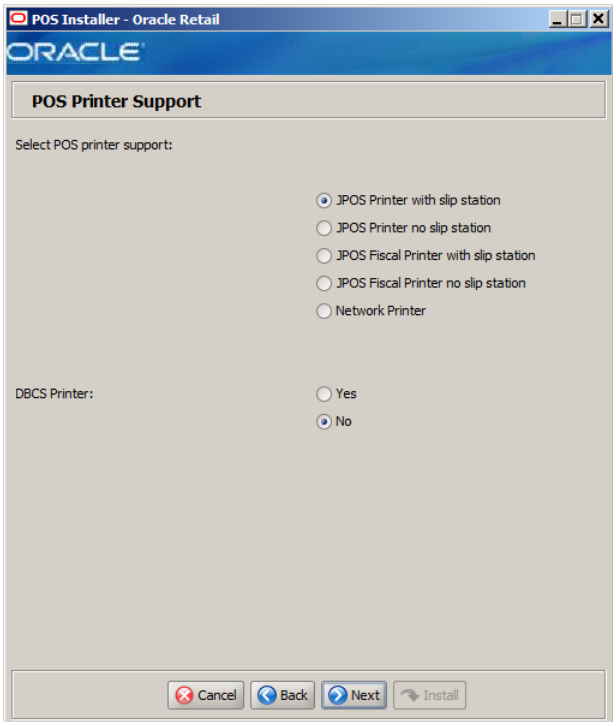


This window is only displayed if any component other than **Simulated** is selected in the POS Platform Components window.

The field in this window 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–37 POS Printer Support



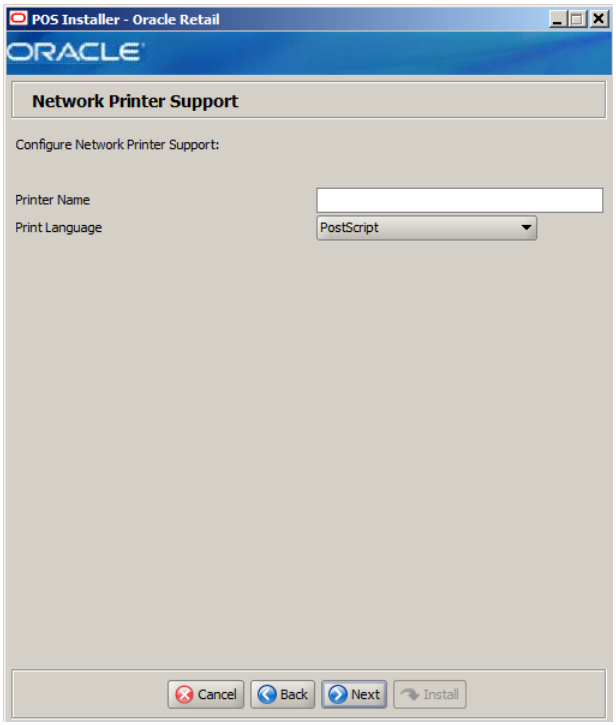
This window is only displayed if **Printer** is selected in the POS Devices window.

The fields in this window are described in the following tables:

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. For information on printing barcodes with JPOS fiscal printers, see the following sections: ■ Microsoft Windows: "Configure Devices for Fiscal Printing" in Chapter 3 ■ Novell SLEPOS: "Configure Devices for Fiscal Printing" in Chapter 4
Example	JPOS Printer with slip station

Details	Content
Field Title	DBCS Printer
Field Description	If the printer supports the double-byte character set (DBCS), select **Yes**.
Example	No

Figure B–38 Network Printer Support



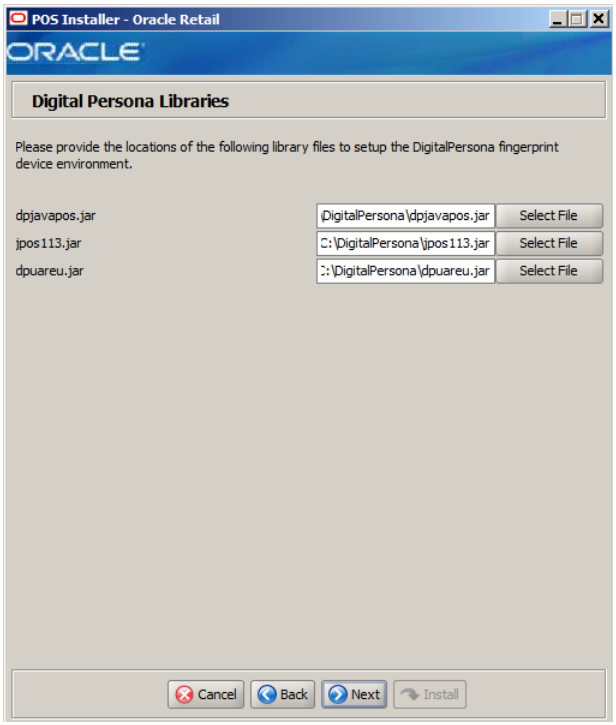
This window is only displayed if **Network Printer** is selected in the POS Printer Support window.

The fields in this window 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–39 Digital Persona Libraries



This window is only displayed if **Fingerprint Reader** is selected in the POS Devices window.

The fields in this window are described in the following tables:

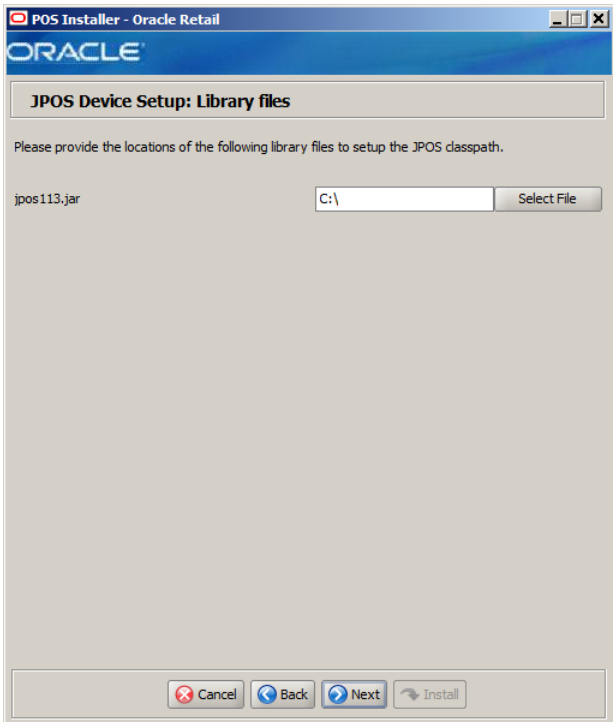
Details	Content
Field Title	dpjavapos.jar
Field Description	Enter the location of the jar file.
Example	▪ Microsoft Windows: C:\DigitalPersona\dpjavapos.jar ▪ Novell SLEPOS: /opt/pos/jars/dpjavapos.jar

Details	Content
Field Title	jpos113.jar
Field Description	Enter the location of the jar file.
Example	▪ Microsoft Windows: C:\DigitalPersona\jpos113.jar ▪ Novell SLEPOS: /opt/pos/jars/jpos113.jar

Details	Content
Field Title	dpuareu.jar

Details	Content
Field Description	Enter the location of the jar file.
Example	■ Microsoft Windows: C:\DigitalPersona\dpuareu.jar ■ Novell SLEPOS: /opt/pos/jars/dpuareu.jar

Figure B–40 JPOS Device Setup: Library Files

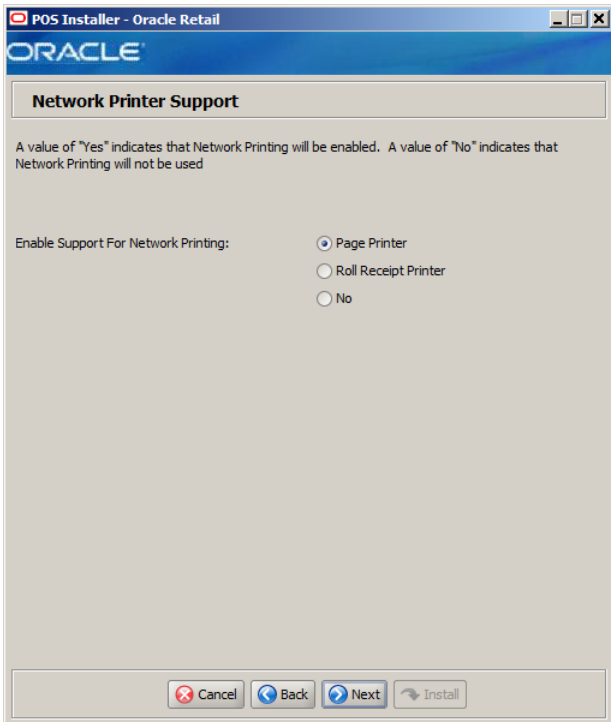


This window is only displayed if **Simulated** is selected in the POS Platform Components window.

The field in this window is described in the following table:

Details	Content
Field Title	jpos113.jar
Field Description	Enter the location of the directory. **Note:** The jar file is available from the manufacturer of the register.
Example	■ Microsoft Windows: C:\ ■ Novell SLEPOS: /opt/

Figure B–41 Network Printer Support for Simulated Platform

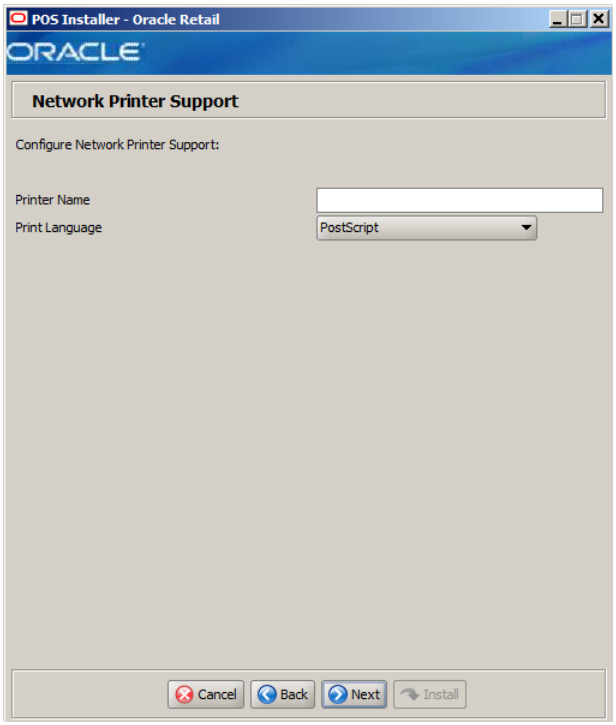


This window is only displayed if **Simulated** is selected in the POS Platform Components window.

The field in this window 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 B–42 Network Printer Support Configuration for Simulated Platform



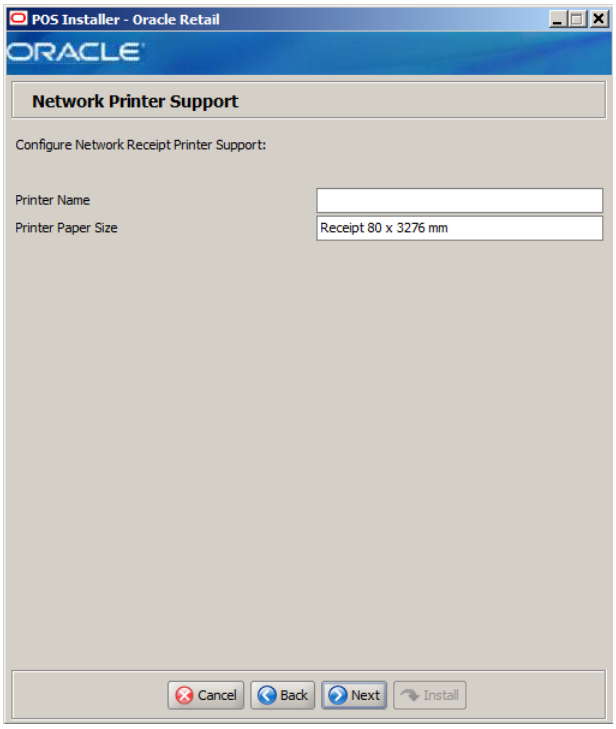
This window is only displayed if **Simulated** is selected in the POS Platform Components window and **Page Printer** is selected in the Network Printer Support window.

The fields in this window are described in the following tables:

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

Details	Content
Field Title	Print Language
Field Description	Select the language for the network printer.

Figure B–43 Network Printer Support Configuration for Simulated Platform



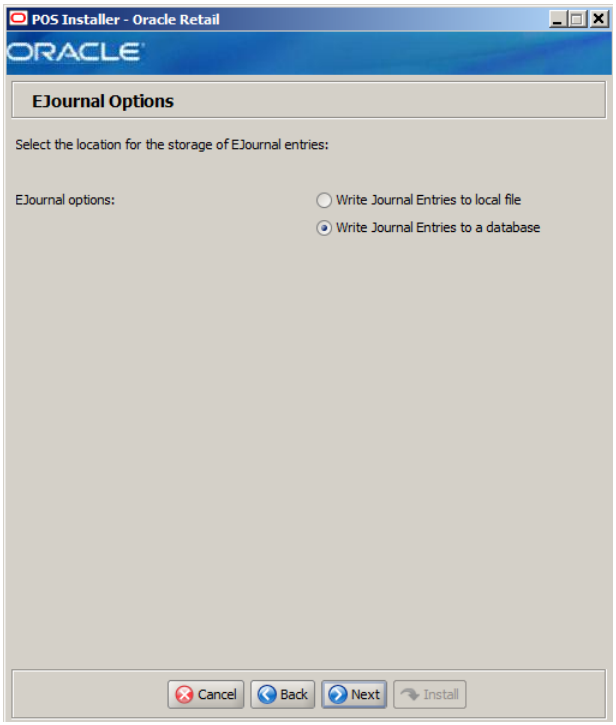
This window is only displayed if **Simulated** is selected in the POS Platform Components window and **Roll Receipt Printer** is selected in the Network Printer Support window.

The fields in this window are described in the following tables:

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

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

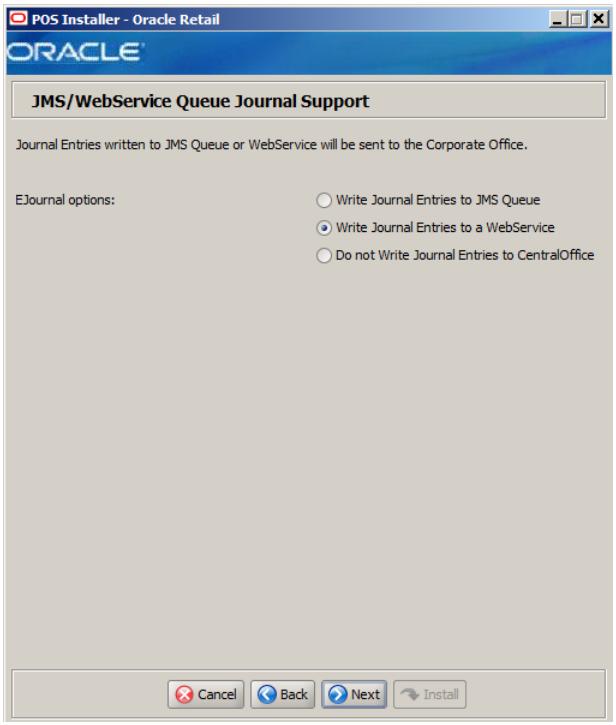
Figure B–44 EJournal Options



The field in this window 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–45 JMS /Webservice Queue Journal Support

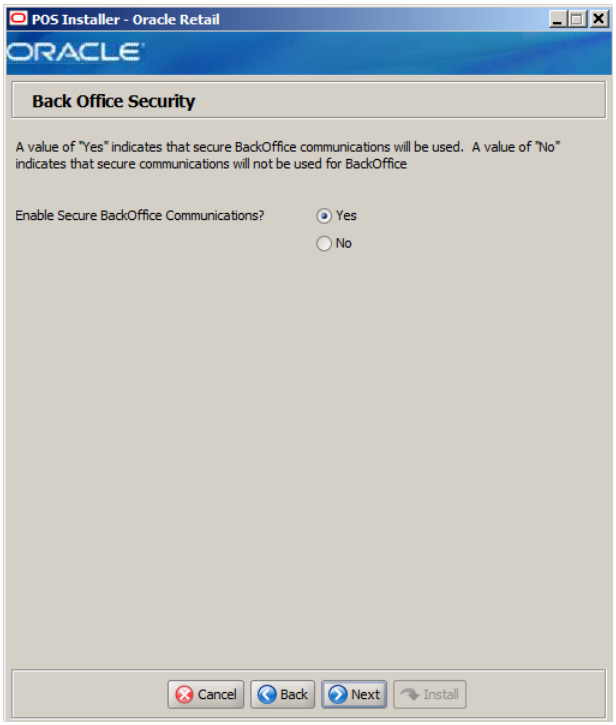


This window is only displayed if **Central Office/Back Office** is selected in the Integrate Applications window.

The field in this window 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–46 Back Office Security

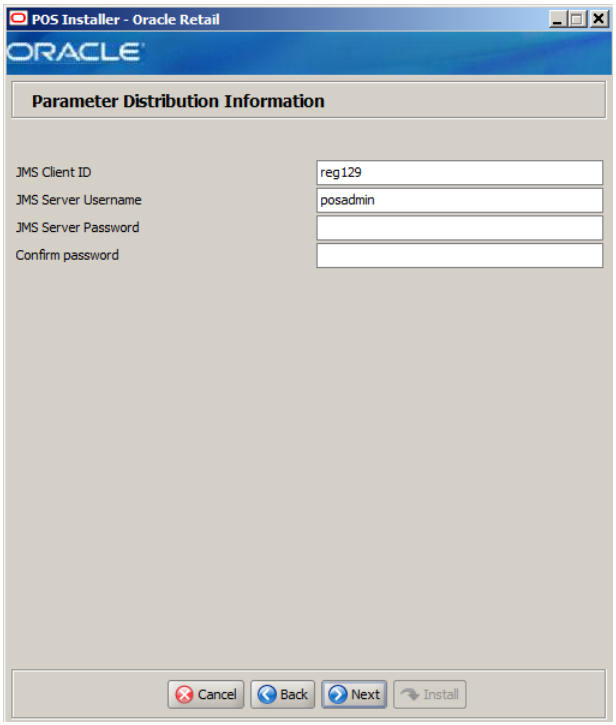


This window is only displayed if **Central Office/Back Office** is selected in the Integrate Applications window.

The field in this window 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–47 Parameter Distribution Information



This window is only displayed if **Central Office/Back Office** is selected in the Integrate Applications window.

The fields in this window 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

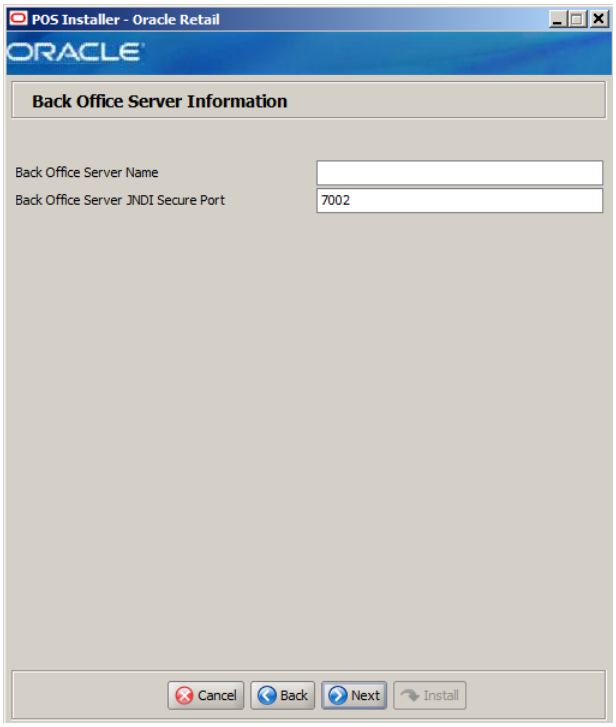
Details	Content
Field Title	JMS Username
Field Description	Identifier of the JMS user for receiving parameter updates.
Example	posadmin

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–48 Back Office Server Information



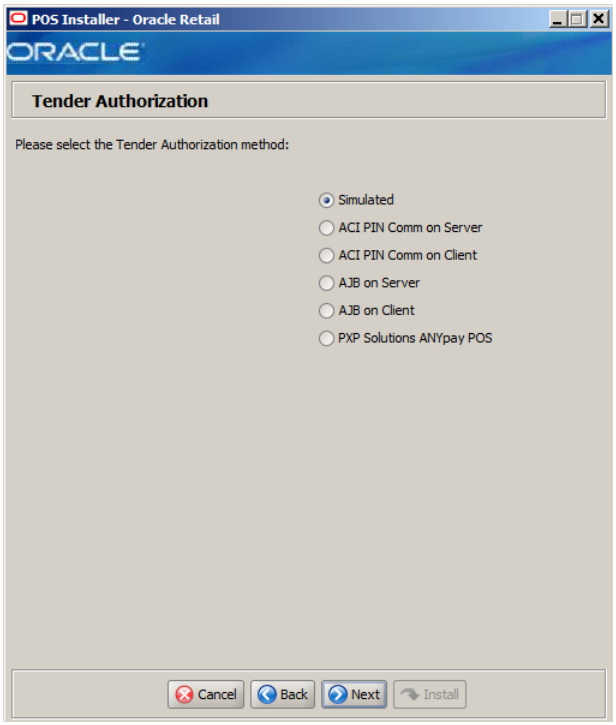
This window is only displayed if **Central Office/Back Office** is selected in the Integrate Applications window.

The fields in this window 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

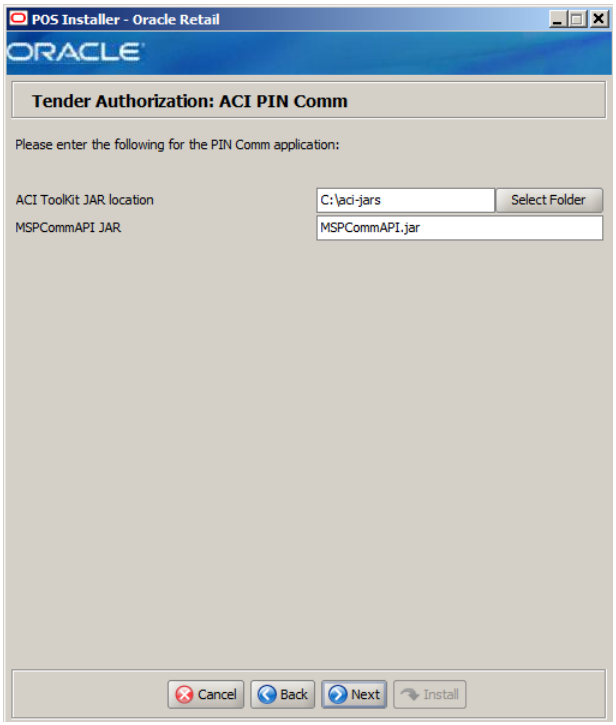
Figure B–49 Tender Authorization



The field in this window 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 by the store server to a third-party system to approve the authorizations, choose **ACI PIN Comm on Server**, **AJB on Server**, or **PXP Solutions ANYpay POS**. ▪ If approvals are handled by the client, select **ACI PIN Comm on Client** or **AJB on Client**. **Note:** If the store server is located at a remote location, it is highly recommended to configure ACI PINComm or AJB at each client in order to help minimize network delay. **Note:** Demo installations should use the Simulated option.
Example	Simulated

Figure B–50 Tender Authorization: ACI PIN Comm



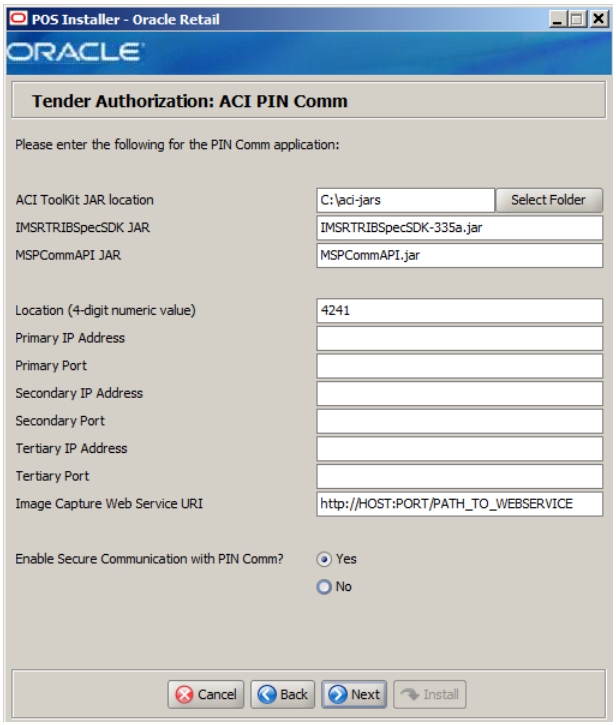
This window is only displayed if **ACI PIN Comm on Server** is selected in the Tender Authorization window.

The fields in this window are described in the following tables:

Details	Content
Field Title	ACI ToolKit JAR Location
Field Description	Enter the path to the ACI ToolKit JAR file.
Example	▪ Microsoft Windows: C:\aci-jars ▪ Novell SLEPOS: /opt/aci-jars

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

Figure B–51 Tender Authorization: ACI PIN Comm



This window is only displayed if **ACI PIN Comm on Client** is selected in the Tender Authorization window.

The fields in this window are described in the following tables:

Details	Content
Field Title	ACI ToolKit JAR Location
Field Description	Enter the path to the ACI ToolKit JAR file.
Example	▪ Microsoft Windows: C:\aci-jars ▪ Novell SLEPOS: /opt/aci-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	MSPCommAPI JAR
Field Description	Enter the name of the MSPCommAPI JAR file.
Example	MSPCommAPI.jar

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

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

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

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

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

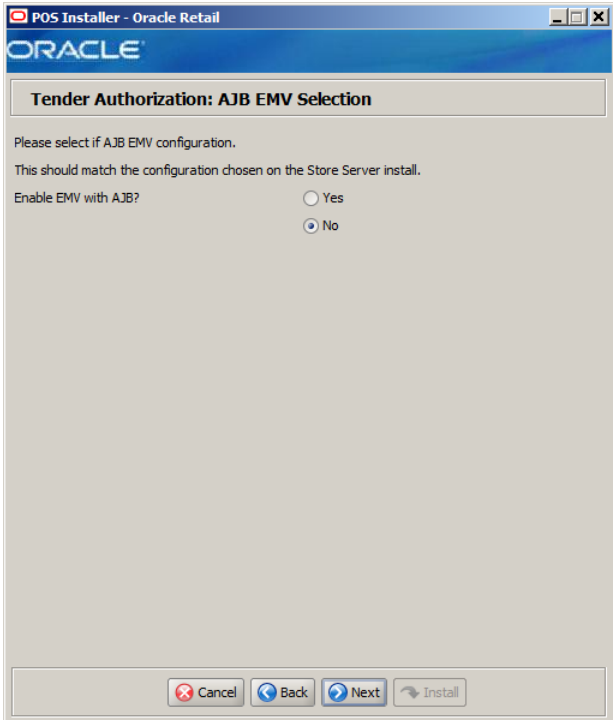
Details	Content
Field Title	Tertiary IP Address
Field Description	Enter the tertiary IP address used for the communication between the store server and the tender authorizer.

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

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

Details	Content
Field Title	Enable Secure Communication with PIN Comm?
Field Description	Select **Yes** for communication with ACI PINComm using HTTPS.
Example	Yes

Figure B–52 Tender Authorization: AJB

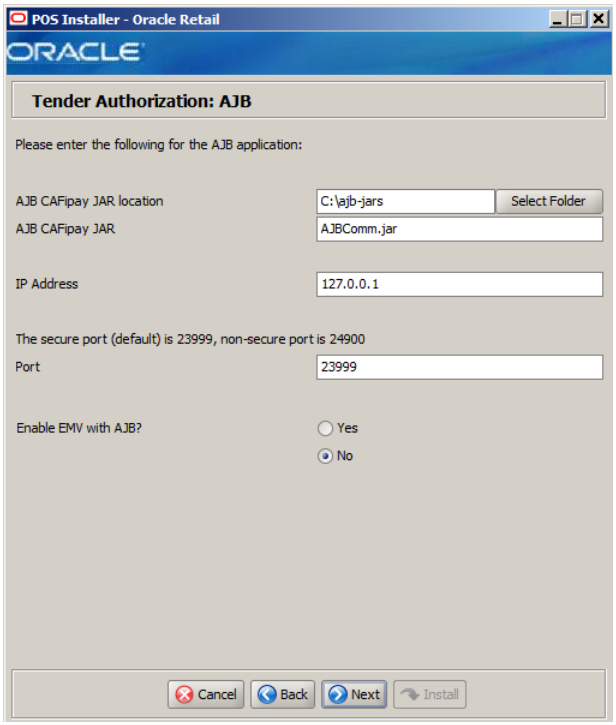


This window is only displayed if **AJB on Server** is selected in the Tender Authorization window.

The field in this window is described in the following table:

Details	Content
Field Title	Enable EMV with AJB?
Field Description	Select whether Europay, MasterCard, and Visa (EMV) is enabled with AJB: ■ To enable EMV, select **Yes**. ■ To not enable EMV, select **No**.
Example	No

Figure B–53 Tender Authorization: AJB



This window is only displayed if **AJB on Client** is selected in the Tender Authorization window.

The fields in this window are described in the following tables:

Details	Content
Field Title	AJB CAFipay JAR Location
Field Description	Enter the path to the AJB CAFipay JAR file.
Example	▪ Microsoft Windows: C:\ajb-jars ▪ Novell SLEPOS: /opt/ajb-jars

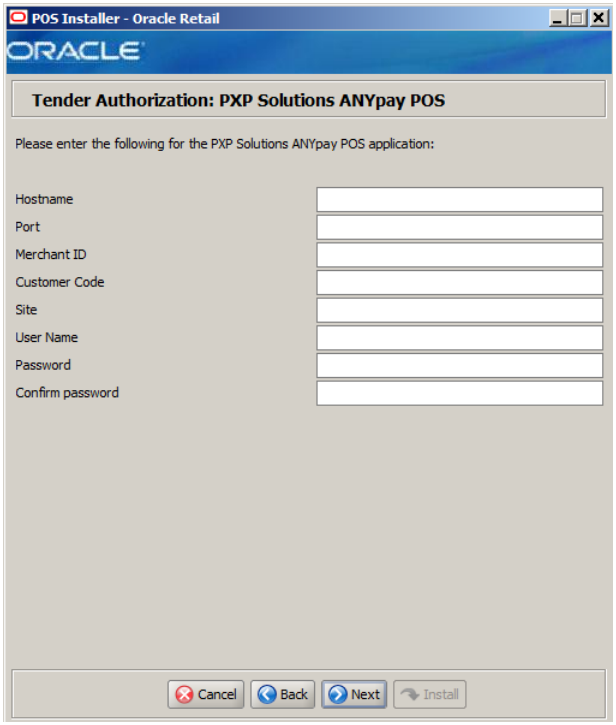
Details	Content
Field Title	AJB CAFipay JAR
Field Description	Enter the name of the CAFipay JAR file.
Example	AJBComm.jar

Details	Content
Field Title	IP Address
Field Description	Enter the IP address used for the communication between the store server and the tender authorizer.
Example	127.0.0.1

Details	Content
Field Title	Port
Field Description	Enter the port number used for the communication between the store server and the tender authorizer.
Example	23999

Details	Content
Field Title	Enable EMV with AJB?
Field Description	Select whether Europay, MasterCard, and Visa (EMV) is enabled with AJB: ■ To enable EMV, select **Yes**. ■ To not enable EMV, select **No**.
Example	No

Figure B–54 Tender Authorization: PXP Solutions ANYpay POS



This window is only displayed if **PXP Solutions ANYpay POS** is selected for the Tender Authorization.

The fields in this window 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.

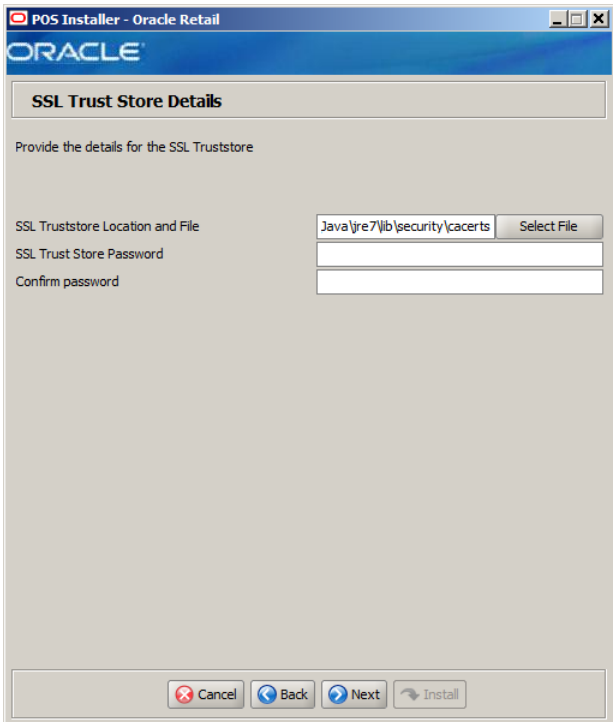
Details	Content
Field Title	Site
Field Description	Enter the site to access the PXP Solutions application.

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–55 SSL Trust Store Details



The fields in this window 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	▪ Microsoft Windows: C:\Program Files\Java\jre7\lib\security\cacerts ▪ Novell SLEPOS: /opt/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–56 Installation Progress

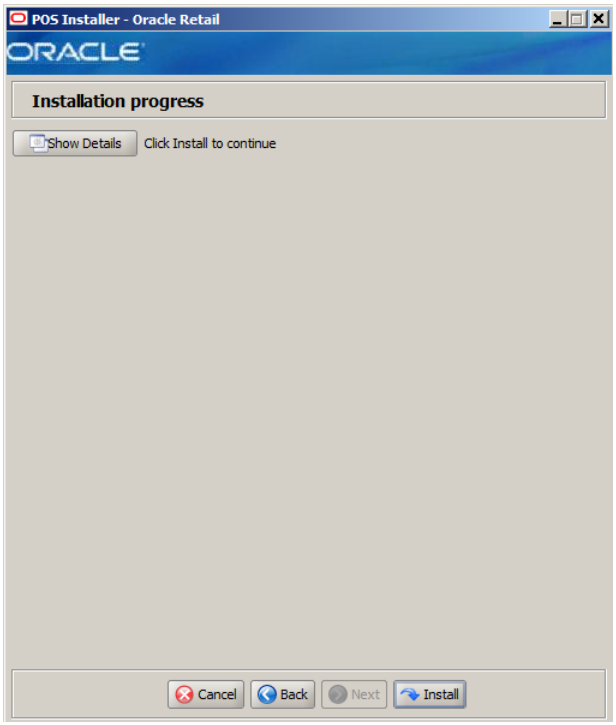
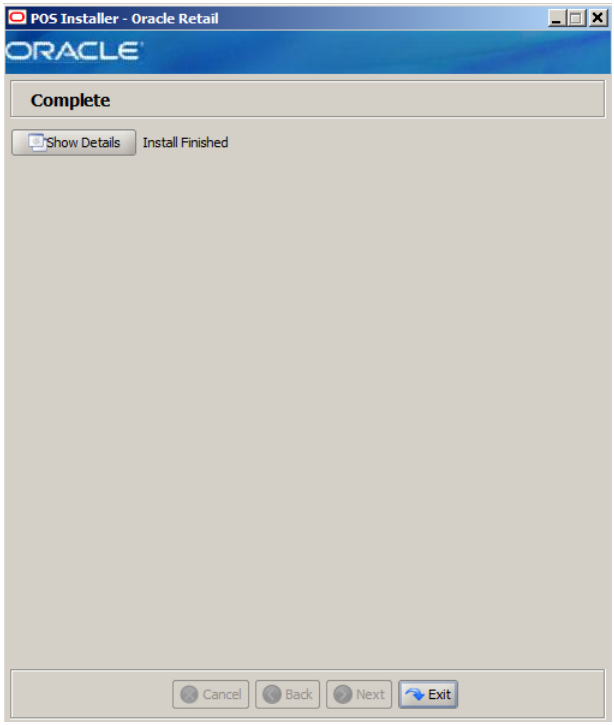


Figure B–57 Install Complete



C

Appendix: Installer Windows 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 windows that are displayed during the installation. Depending on the options you select, you may not see some windows or fields.

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

> **Note:** The paths shown in the window examples in this appendix use the path format for Microsoft Windows. In the table describing those fields, example paths for both Microsoft Windows and Novell SLEPOS are shown.

Figure C–1 Introduction

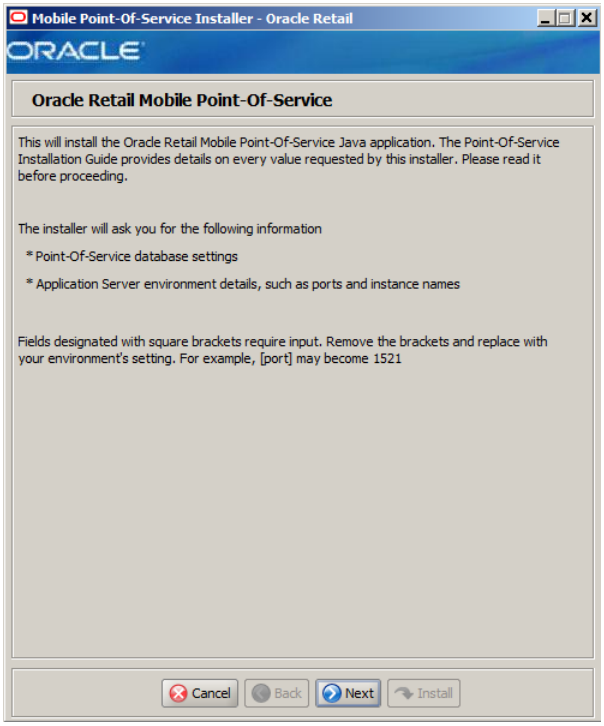


Figure C–2 Requirements

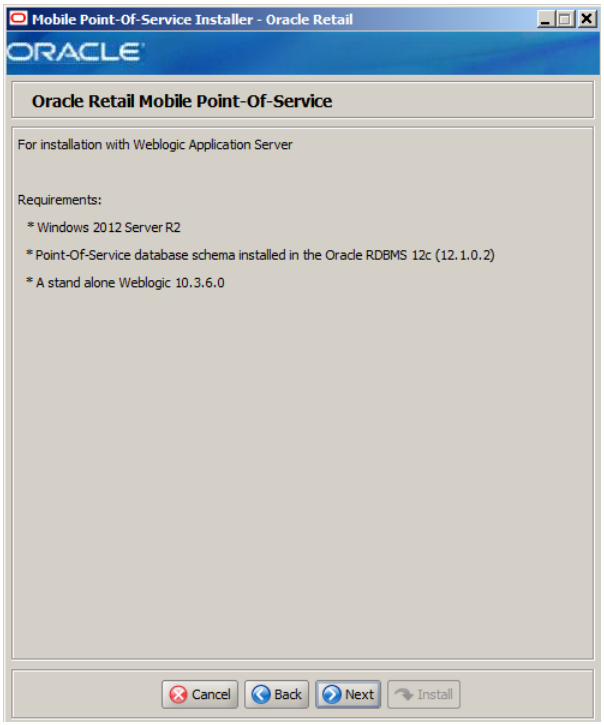
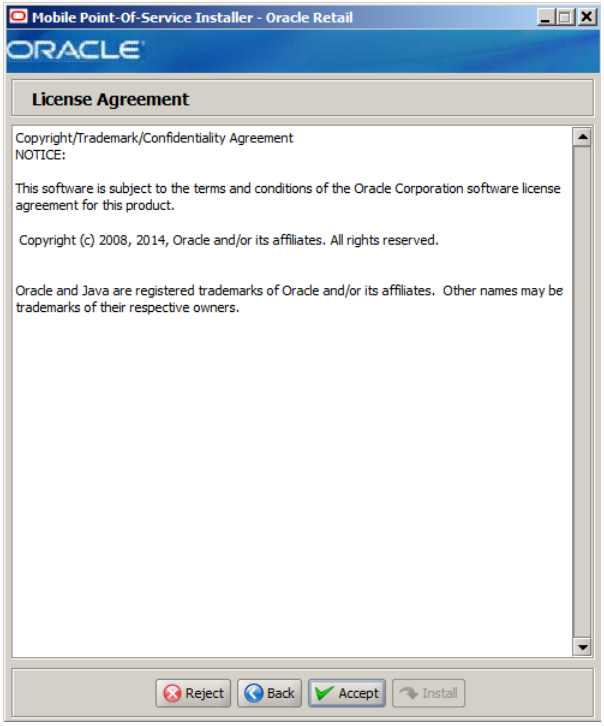
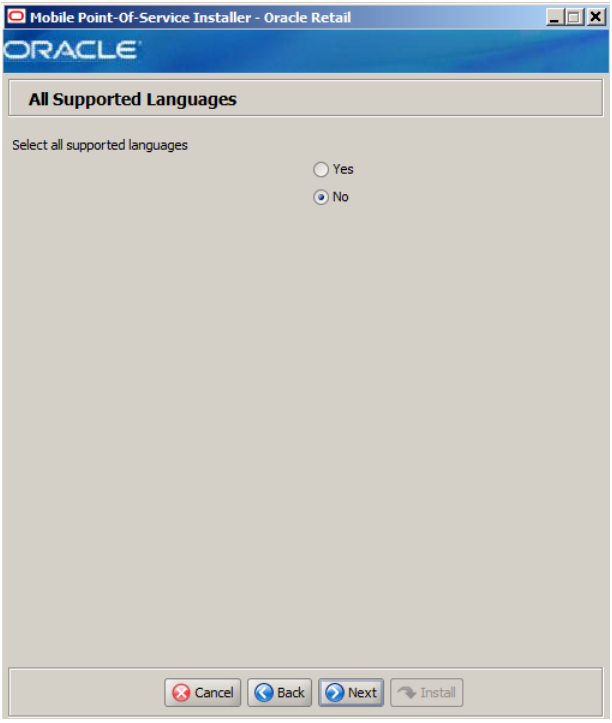


Figure C–3 License Agreement



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

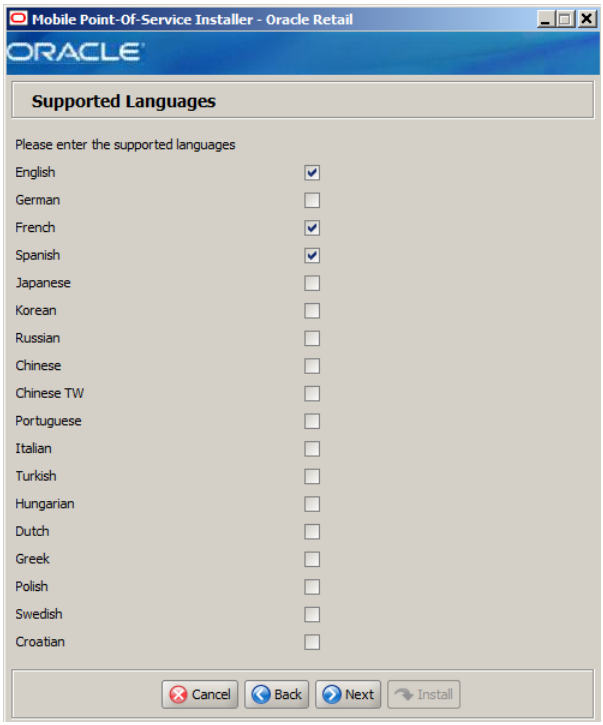
Figure C–4 All Supported Languages



The field in this window is described in the following table:

Details	Content
Field Title	Select all supported languages
Field Description	Choose whether all languages are initially selected on the Supported Languages screen: ▪ To have all available languages initially selected, select **Yes**. ▪ To have only English initially selected, select **No**.
Example	No

Figure C–5 Supported Languages



The field in this window is described in the following table:

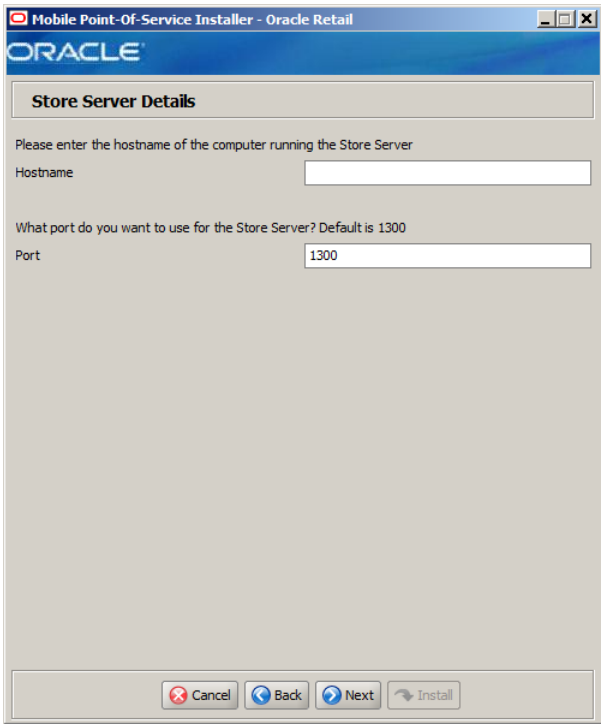
Details	Content
Field Title	Please enter the supported languages
Field Description	Select the languages that will be available for the Mobile Point-of-Service application. The languages selected in this window determine the available choices in the Enter Default Locale window.
Example	English, French,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

Figure C–6 Enter Default Locale

The field in this window 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 in the Supported Languages window. For each selected language, the default locale for that language is displayed in the Enter Default Locale window. For example, if English, French, and Italian are selected in the Supported Languages window, en_US, fr_FR, and it_IT are the available choices for the default locale.
Example	en_US

Figure C–7 Store Server Details

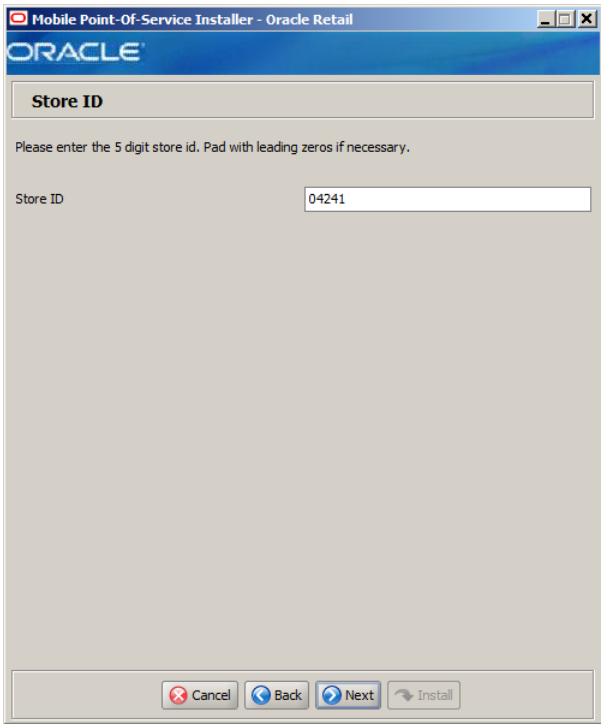


The fields in this window are described in the following tables:

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

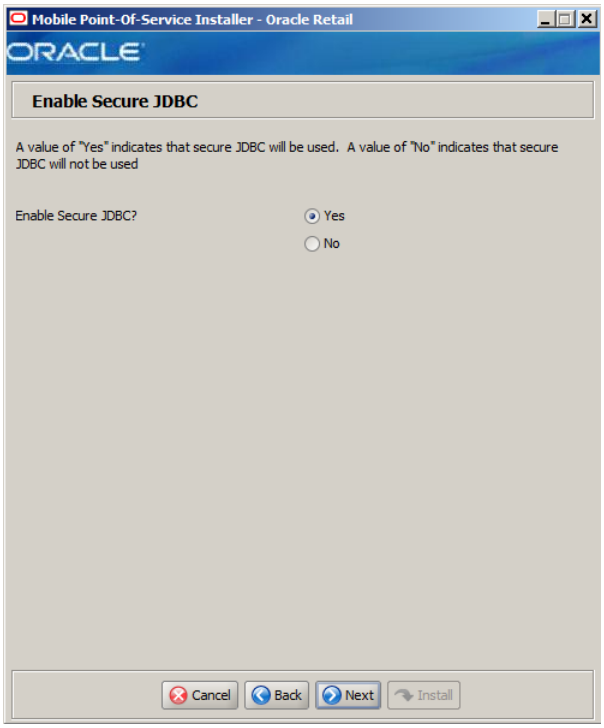
Figure C–8 Store ID



The field in this window 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

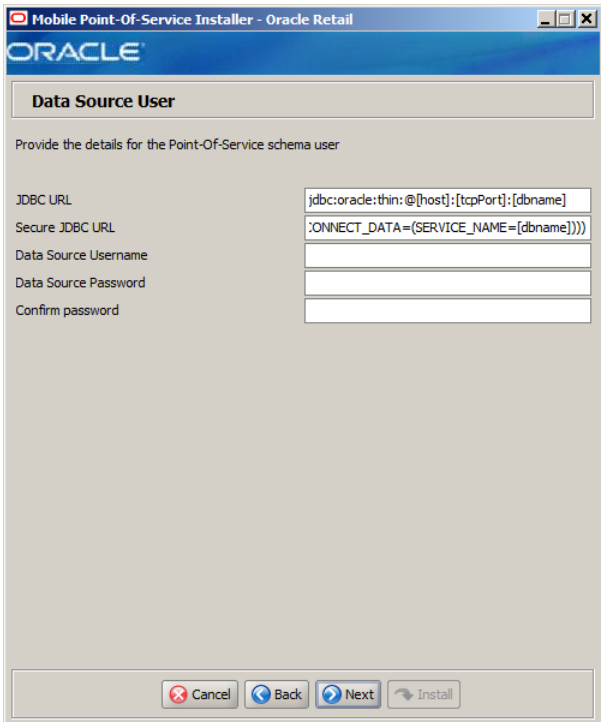
Figure C–9 Enable Secure JDBC



The field in this window 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 Database Source User



The fields in this window are described in the following tables:

Details	Content
Field Title	JDBC URL
Field Description	URL used by Mobile Point-of-Service to access the database schema. For the expected syntax, see Appendix E. **Note:** If Enable Secure JDBC is selected in the Secure Options window, this URL is only used by the installer.
Example	jdbc:oracle:thin:@DB_HOST_NAME:1521:DB_NAME

Details	Content
Field Title	Secure JDBC URL
Field Description	Secure URL containing the specific parameters used by Mobile Point-of-Service to access the database schema. See Appendix E for the expected syntax. This field is only displayed if Enable Secure JDBC is selected in the Secure Options window.
Example	jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=[host])(PORT=[tcpsPort]))(CONNECT_DATA=(SERVICE_NAME=[dbname])))

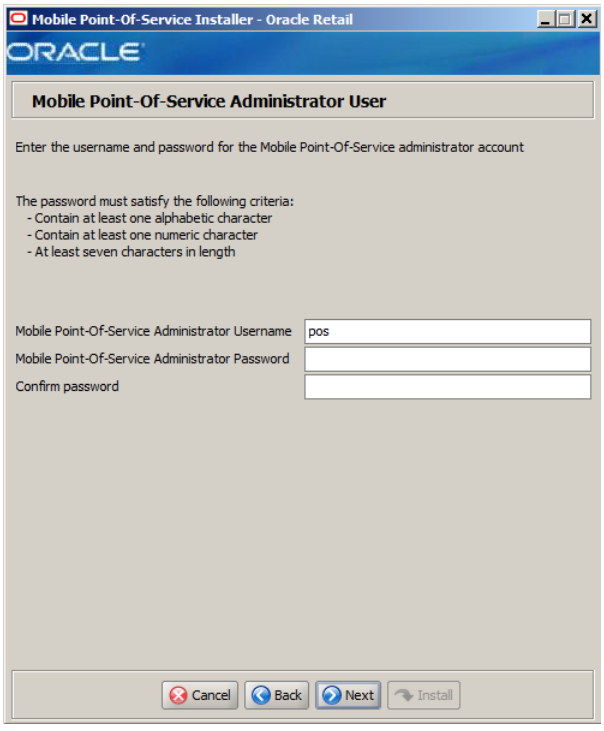
Details	Content
Field Title	Data Source Username

Details	Content
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–11 Mobile Point-of-Service Administrator User



The fields in this window are described in the following tables:

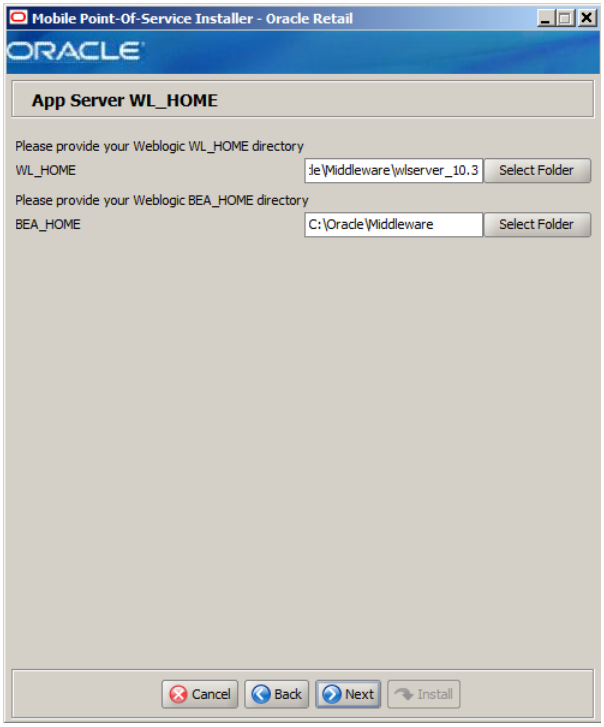
Details	Content
Field Title	Mobile Point-of-Service Administrator Username

Details	Content
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



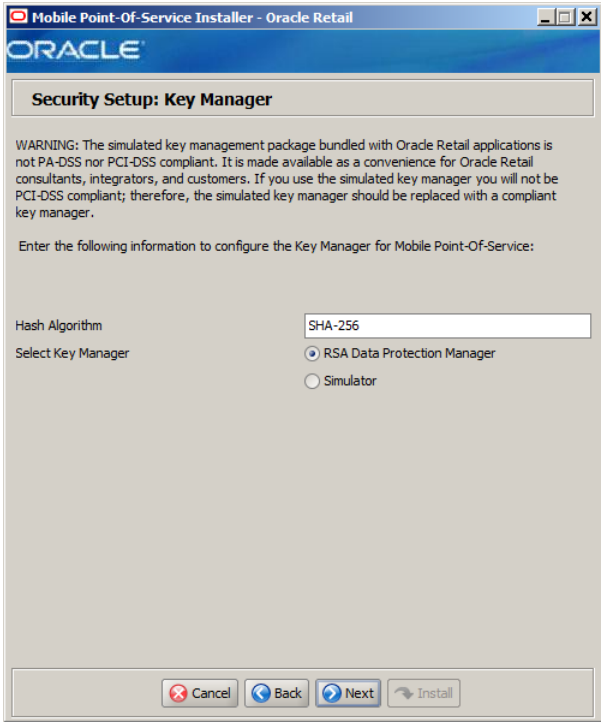
The fields in this window are described in the following tables:

Details	Content
Field Title	WL_HOME
Field Description	Home directory for the Oracle WebLogic Server installation.

Details	Content
Example	▪ Microsoft Windows: D:\Oracle\Middleware\wlserver_10.3 ▪ Novell SLEPOS: /opt/Oracle/Middleware/wlserver_10.3

Details	Content
Field Title	BEA_HOME
Field Description	Home directory for the Oracle BEA installation.
Example	▪ Microsoft Windows: D:\Oracle\Middleware ▪ Novell SLEPOS: /opt/Oracle/Middleware

Figure C–13 Security Setup: Key Manager



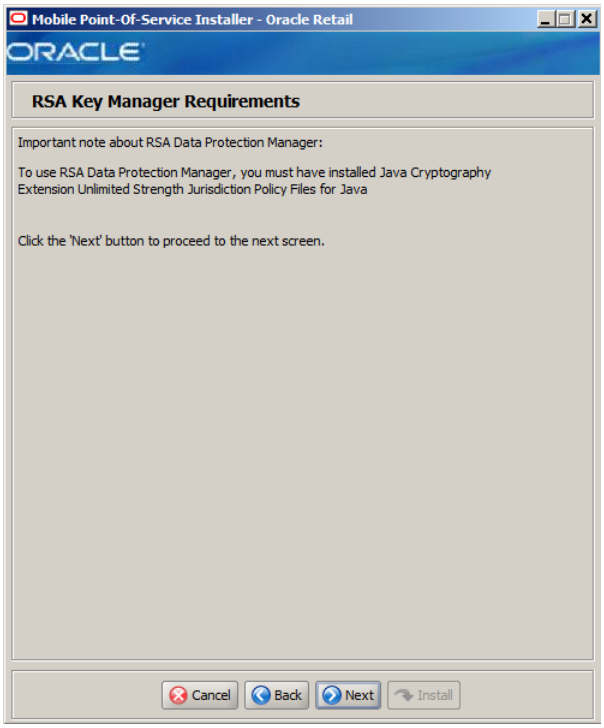
This window is used to configure the Encryption Key Manager.

The fields in this window 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

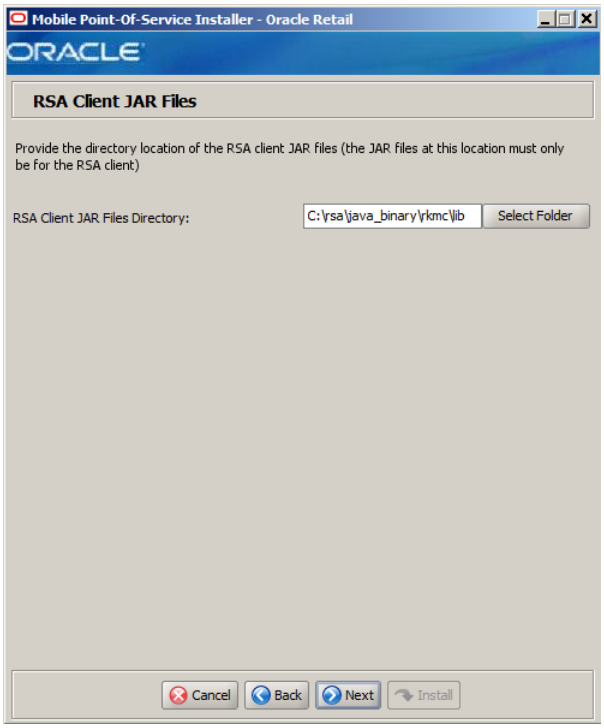
Details	Content
Field Title	Select Key Manager
Field Description	Provider for Key Store management. ▪ RSA Data Protection Manager package, select **RSA Data Protection Manager**. The next window displayed is Figure C–14. ▪ To use the simulated key management package, select **Simulator**. The next window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

Figure C–14 RSA Key Manager Requirements



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

Figure C–15 RSA Client JAR Files

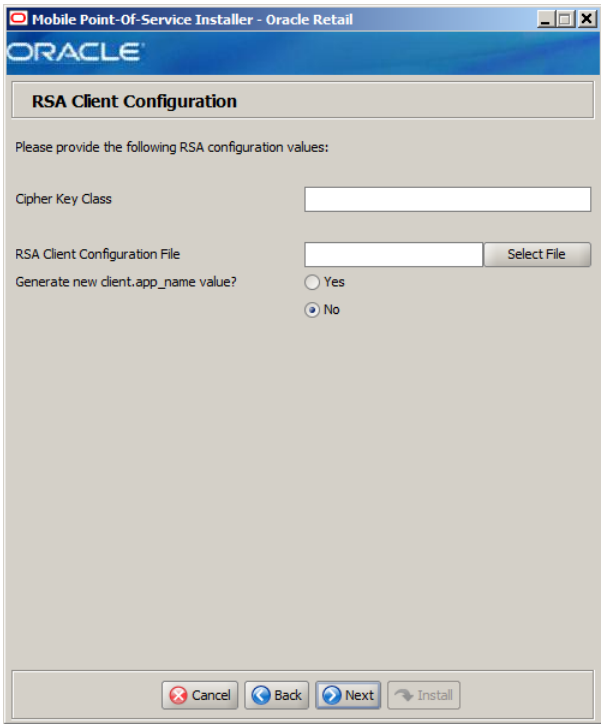


This window is only displayed if **RSA Data Protection Manager** is selected in the Security Setup: Key Manager window.

The field in this window is described in the following table:

Details	Content
Field Title	RSA Client JAR Files Directory
Field Description	Choose the directory where the following jar files are located: ▪ cryptojce.jar ▪ cryptojcommon.jar ▪ jcm.jar ▪ jcmFIPS.jar ▪ kmsclient.jar ▪ LB.jar ▪ LBJNI.jar ▪ sslj.jar
Example	▪ Microsoft Windows: C:\rsa\java_binary\rlmc\lib ▪ Novell SLEPOS: /opt/rsa/java_binary/rlmc/lib

Figure C–16 RSA Client Configuration



This window is only displayed if **RSA Data Protection Manager** is selected in the Security Setup: Key Manager window.

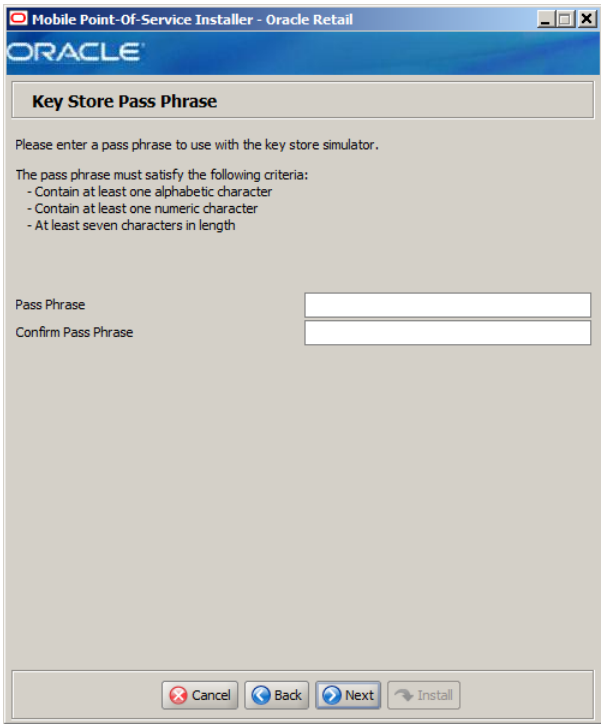
The fields in this window are described in the following tables:

Details	Content
Field Title	Cipher Key Class
Field Description	Enter the name of the cipher suite that define 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 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**.

Figure C–17 Key Store Pass Phrase



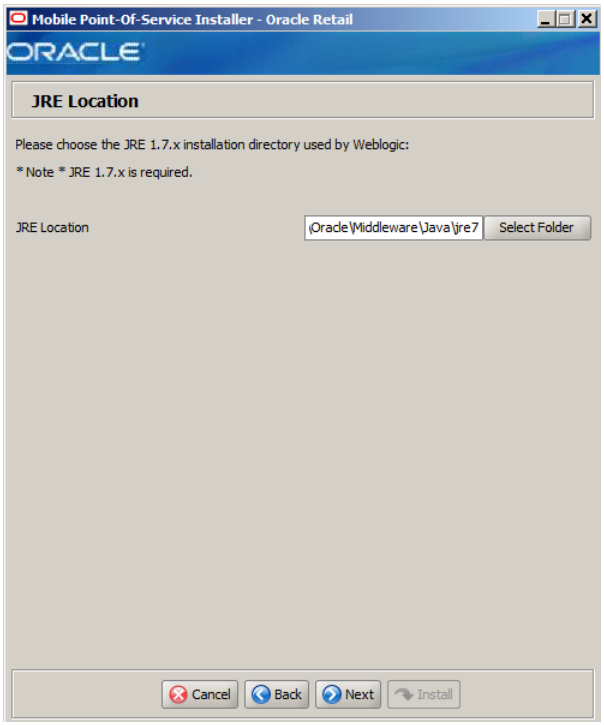
This window is only displayed if **Simulator** is selected in the Security Setup: Key Manager window.

The field in this window 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.

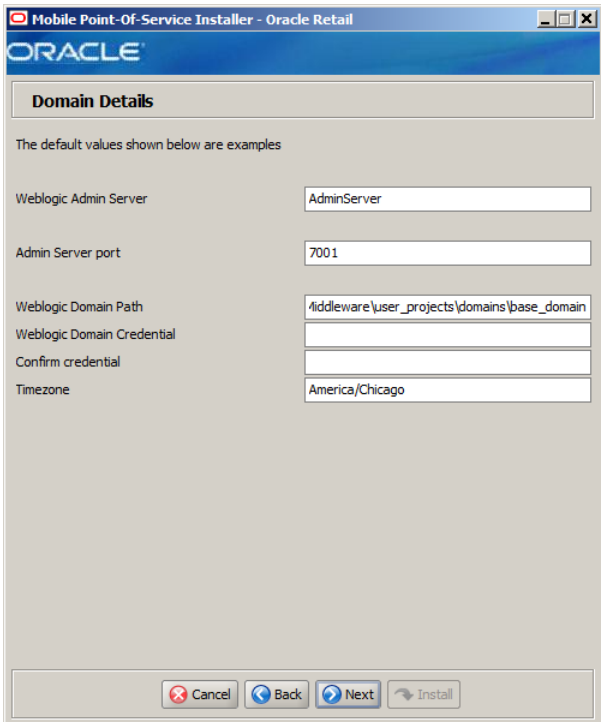
Figure C–18 JRE Location



The field in this window is described in the following table:

Details	Content
Field Title	JRE Location
Field Description	Enter the location where the JRE is installed.
Example	▪ Microsoft Windows: C:\Program Files\Java\jre7 ▪ Novell SLEPOS: /opt/Java/jre7

Figure C–19 Domain Details



The fields in this window 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

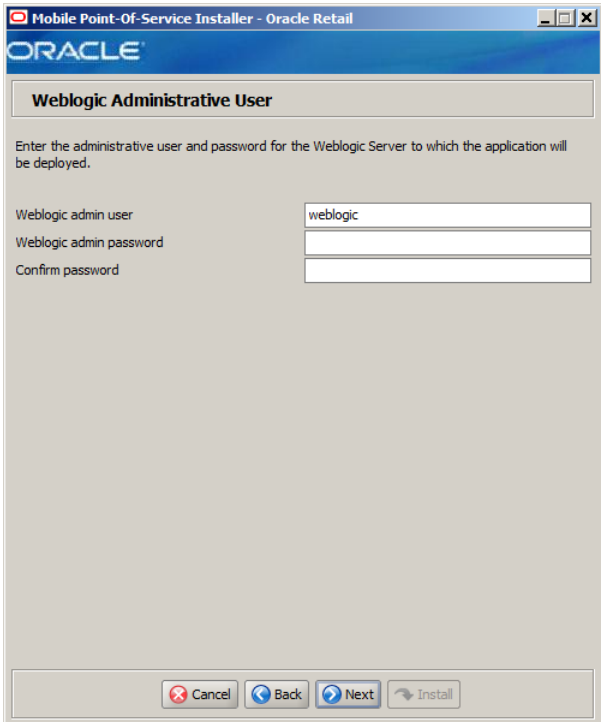
Details	Content
Field Title	Weblogic Domain Credential

Details	Content
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.

Details	Content
Field Title	Timezone
Field Description	Time zone for the Mobile Point-of-Service domain.
Example	America/Chicago

Figure C–20 Weblogic Administrative User



The fields in this window are described in the following tables:

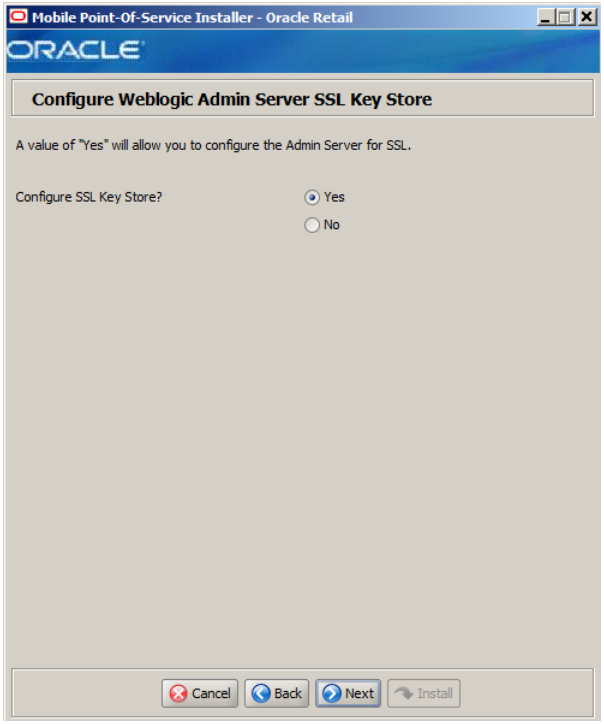
Details	Content
Field Title	Weblogic admin user
Field Description	User name of the administrative user for the WebLogic Server to which the Mobile Point-of-Service application is being deployed.

Details	Content
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.

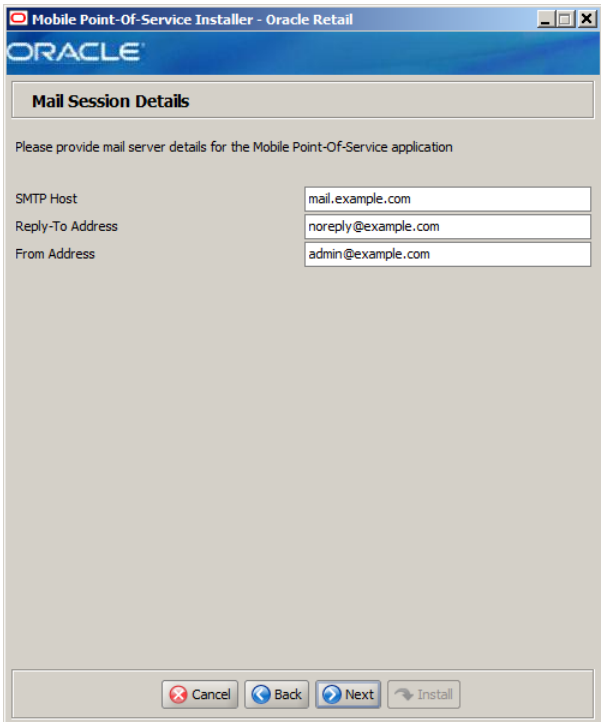
Figure C–21 Configure Weblogic Admin Server SSL Key Store



The field in this window 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 Mail Session Details



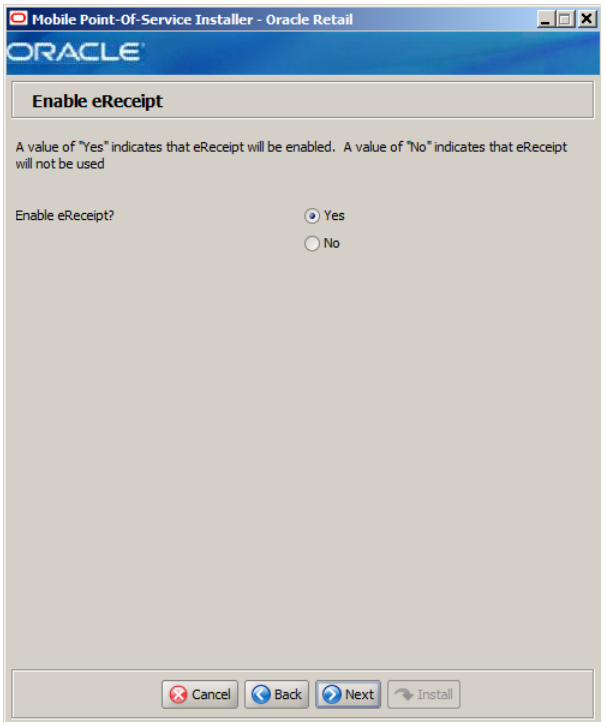
The fields in this window are described in the following tables:

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

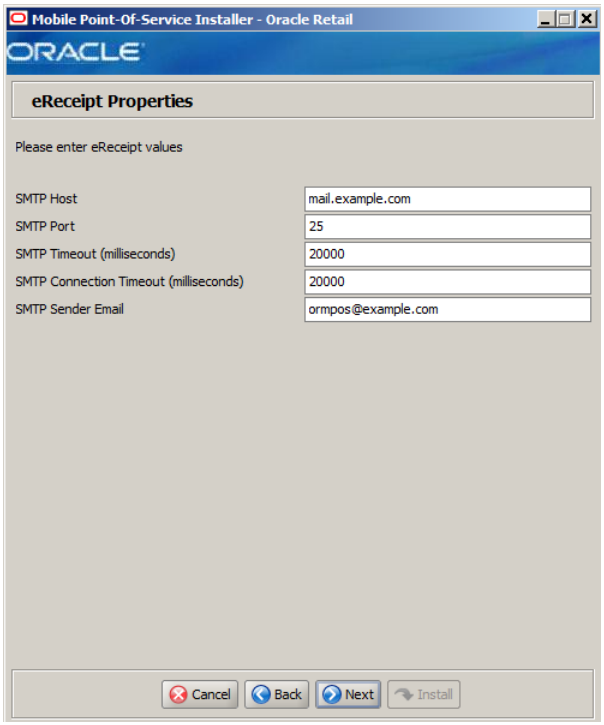
Figure C–23 Enable eReceipt



The field in this window 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–24 eReceipt Properties



This window is only displayed if **Yes** is selected in the Enable eReceipt window.

The fields in this window are described in the following tables:

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

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

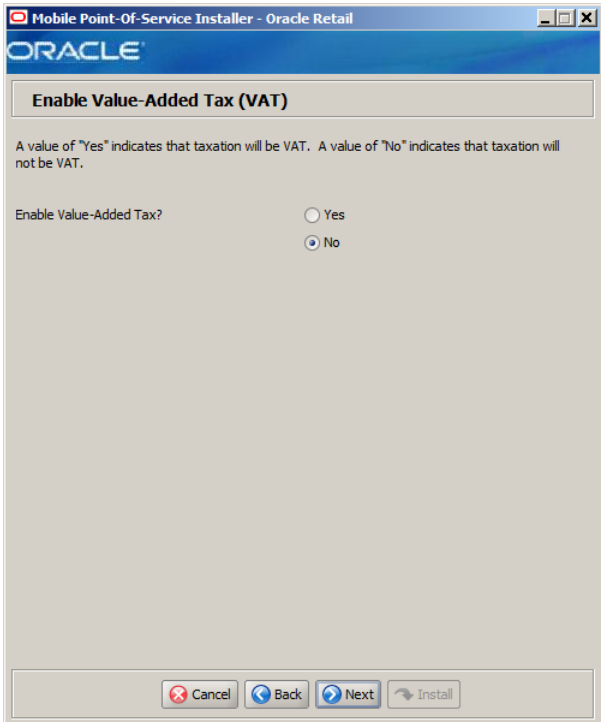
Details	Content
Field Title	SMTP Timeout (milliseconds)
Field Description	Enter the amount of time to wait for the SMTP server.
Example	20000

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

Details	Content
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

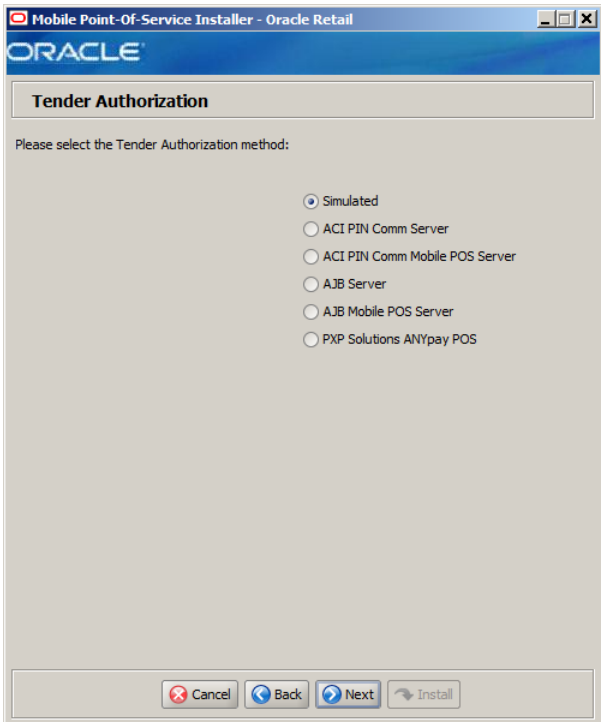
Figure C–25 Value-Added Tax (VAT)



The field in this window 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

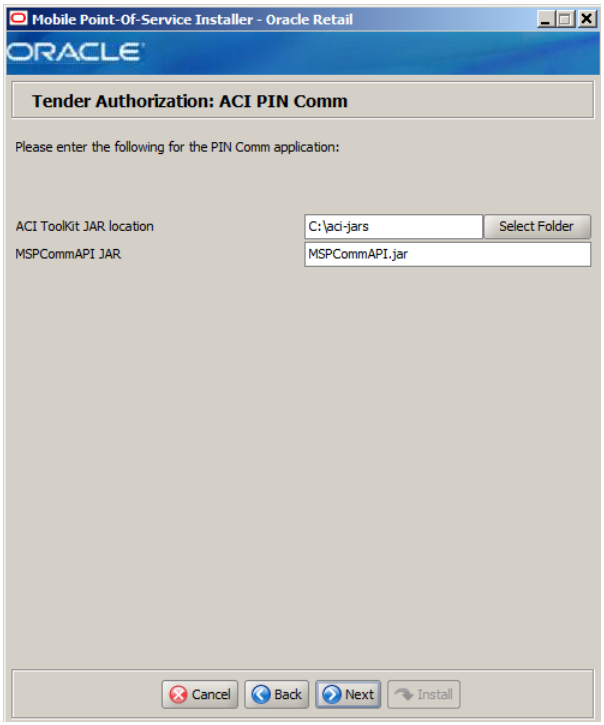
Figure C–26 Tender Authorization



The field in this window 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 by the store server to a third-party system to approve the authorizations, choose **ACI PIN Comm Server** or **AJB Server**. ▪ If approvals are handled by the Mobile Point-of-Service server, select **ACI PIN Comm Mobile POS Server**, **AJB Mobile POS Server**, or **PXP Solutions ANYpay POS**. **Note:** If the store server is located at a remote location, it is highly recommended to configure ACI PINComm at Mobile POS Server or AJB Mobile POS Server in order to help minimize network delay. **Note:** Demo installations should use the Simulated option.
Example	Simulated

Figure C–27 Tender Authorization: ACI PIN Comm



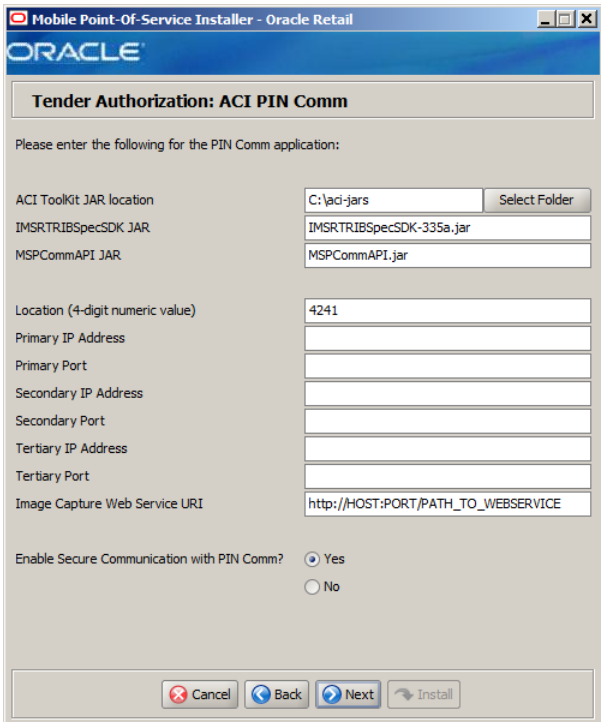
This window is only displayed if **ACI PIN Comm Server** is selected in the Tender Authorization window.

The fields in this window are described in the following tables:

Details	Content
Field Title	ACI ToolKit JAR Location
Field Description	Enter the path to the ACI ToolKit JAR file.
Example	▪ Microsoft Windows: C:\aci-jars ▪ Novell SLEPOS: /opt/aci-jars

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

Figure C–28 Tender Authorization: ACI PIN Comm



This window is only displayed if **ACI PIN Comm Mobile POS Server** is selected in the Tender Authorization window.

The fields in this window are described in the following tables:

Details	Content
Field Title	ACI ToolKit JAR Location
Field Description	Enter the path to the ACI ToolKit JAR file.
Example	▪ Microsoft Windows: C:\aci-jars ▪ Novell SLEPOS: /opt/aci-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	MSPCommAPI JAR
Field Description	Enter the name of the MSPCommAPI JAR file.
Example	MSPCommAPI.jar

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

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

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

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

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

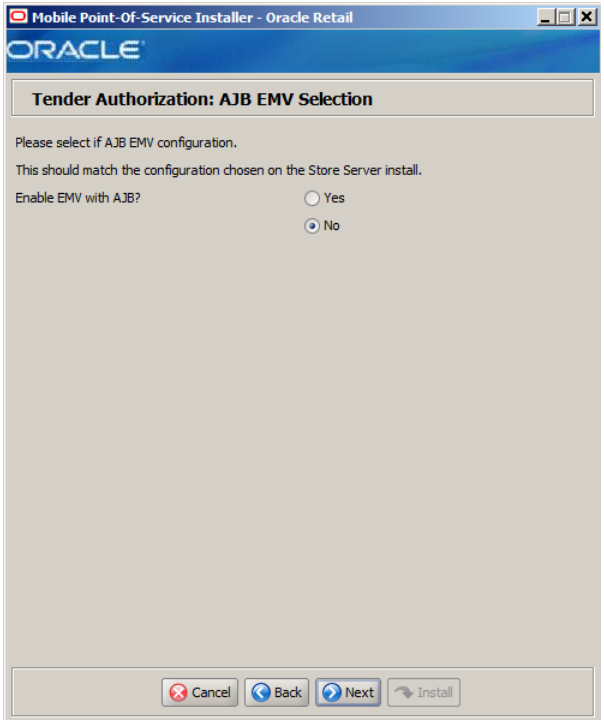
Details	Content
Field Title	Tertiary IP Address
Field Description	Enter the tertiary IP address used for the communication between the store server and the tender authorizer.

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

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

Details	Content
Field Title	Enable Secure Communication with PIN Comm?
Field Description	Select **Yes** for communication with ACI PIN Comm using HTTPS.
Example	Yes

Figure C–29 Tender Authorization: AJB

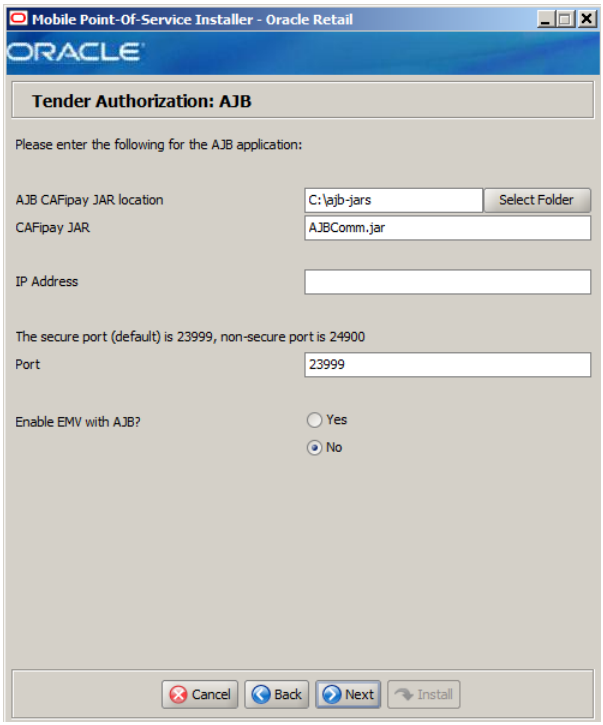


This window is only displayed if **AJB Server** is selected in the Tender Authorization window.

The field in this window is described in the following table:

Details	Content
Field Title	Enable EMV with AJB?
Field Description	Select whether Europay, MasterCard, and Visa (EMV) is enabled with AJB: ■ To enable EMV, select **Yes**. ■ To not enable EMV, select **No**.
Example	No

Figure C–30 Tender Authorization: AJB



This window is only displayed if **AJB Mobile POS Server** is selected in the Tender Authorization window.

The fields in this window are described in the following tables:

Details	Content
Field Title	AJB CAFipay JAR Location
Field Description	Enter the path to the AJB CAFipay JAR file.
Example	▪ Microsoft Windows: C:\ajb-jars ▪ Novell SLEPOS: /opt/ajb-jars

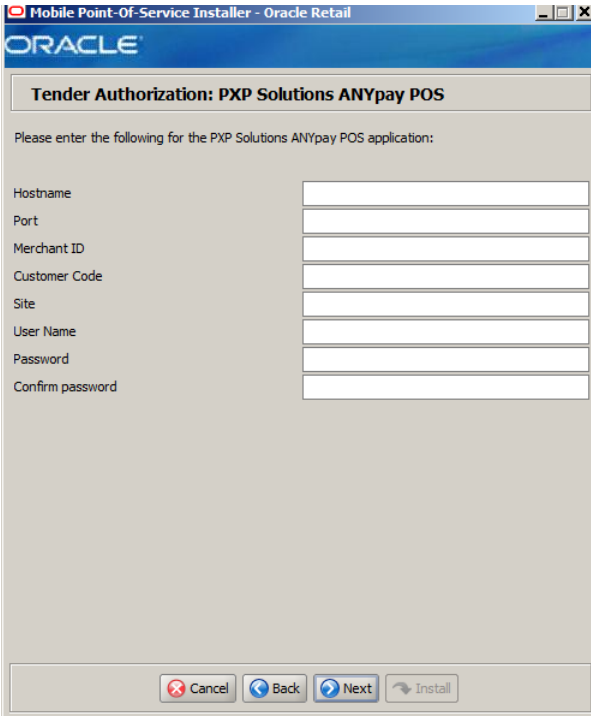
Details	Content
Field Title	CAFipay JAR
Field Description	Enter the name of the CAFipay JAR file.
Example	AJBComm.jar

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

Details	Content
Field Title	Port
Field Description	Enter the port number used for the communication between the store server and the tender authorizer.
Example	23999

Details	Content
Field Title	Enable EMV with AJB?
Field Description	Select whether Europay, MasterCard, and Visa (EMV) is enabled with AJB: ■ To enable EMV, select **Yes**. ■ To not enable EMV, select **No**.
Example	No

Figure C–31 Tender Authorization: PXP Solutions ANYpay POS



This window is only displayed if **PXP Solutions ANYpay POS** is selected for the Tender Authorization.

The fields in this window 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.

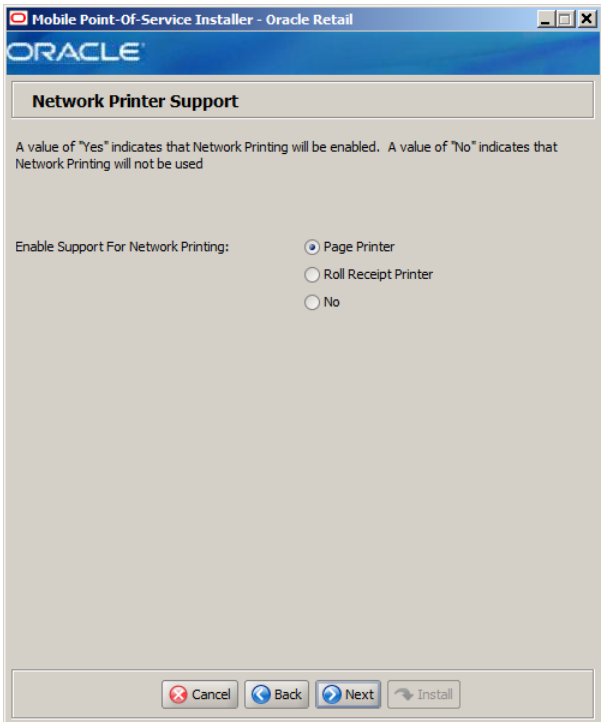
Details	Content
Field Title	Site
Field Description	Enter the site to access the PXP Solutions application.

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.

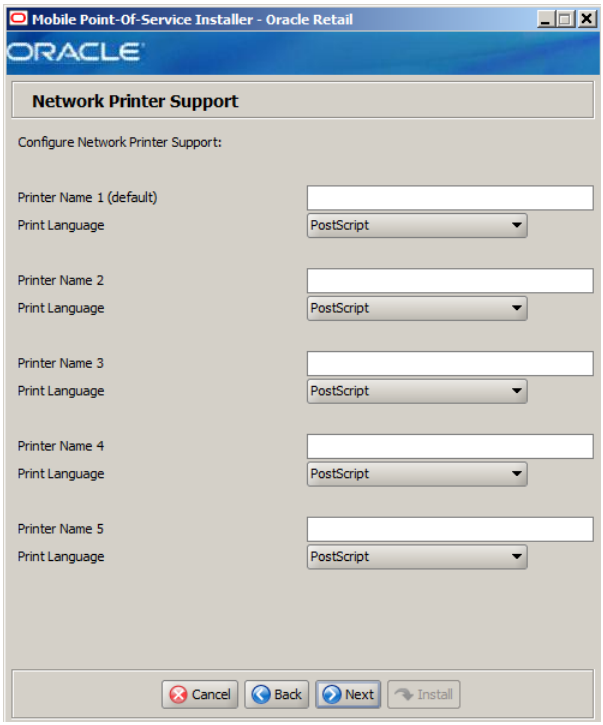
Figure C–32 Network Printer Support



The field in this window 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–33 Network Printer Support Configuration for Page Printers



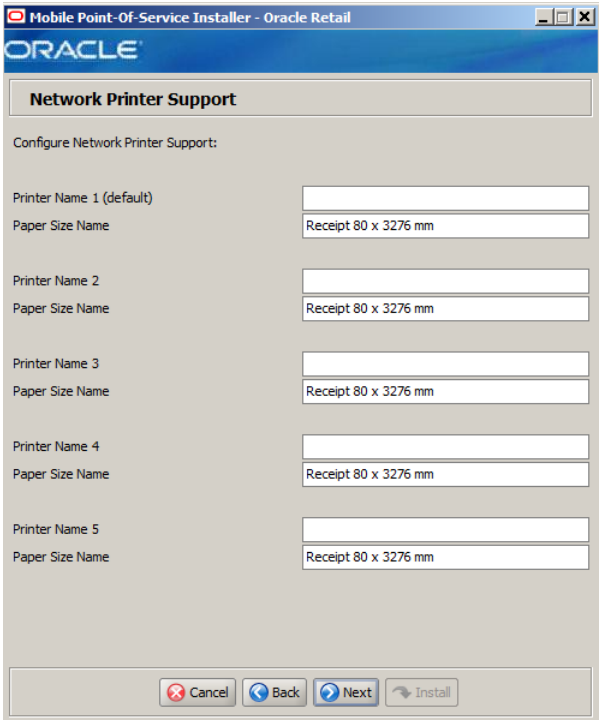
This window is only displayed if **Page Printer** is selected in the Network Printer Support window.

The fields in this window are described in the following tables. Enter the following information for each network printer:

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

Details	Content
Field Title	Print Language
Field Description	Select the language for the network printer.

Figure C–34 Network Printer Support Configuration for Roll Receipt Printers



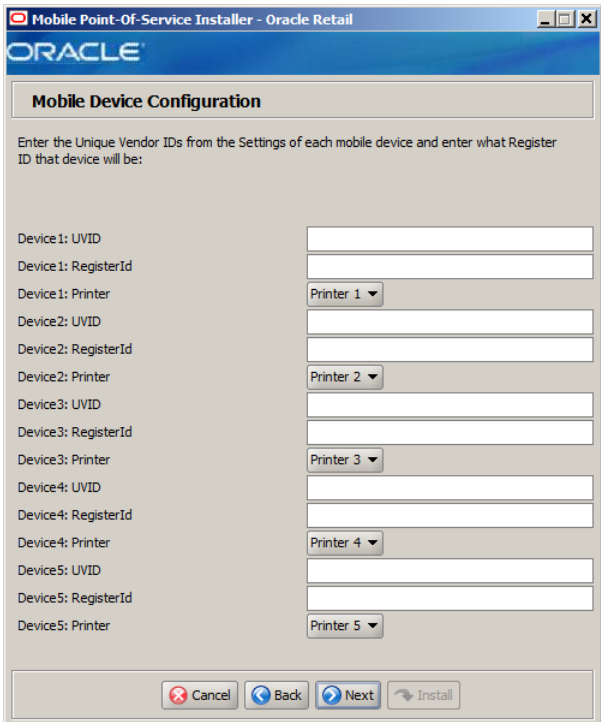
This window is only displayed if **Roll Receipt Printer** is selected in the Network Printer Support window.

The fields in this window are described in the following tables. Enter the following information for each roll receipt printer:

Details	Content
Field Title	Printer Name
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–35 Mobile Device Configuration



Each register associated with a mobile device must be configured to use register accountability. For more information, see "Register Accountability" in Chapter 5.

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

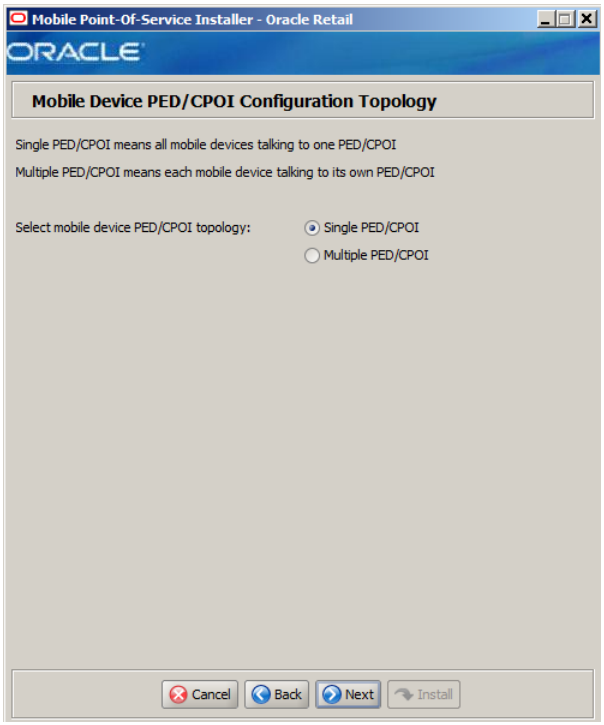
The fields in this window are described in the following tables. Enter the following information for each mobile device:

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

Details	Content
Field Title	RegisterId
Field Description	Enter the register ID to associate with the given vendor 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.

Details	Content
Field Title	Printer
Field Description	Select the printer for the device.

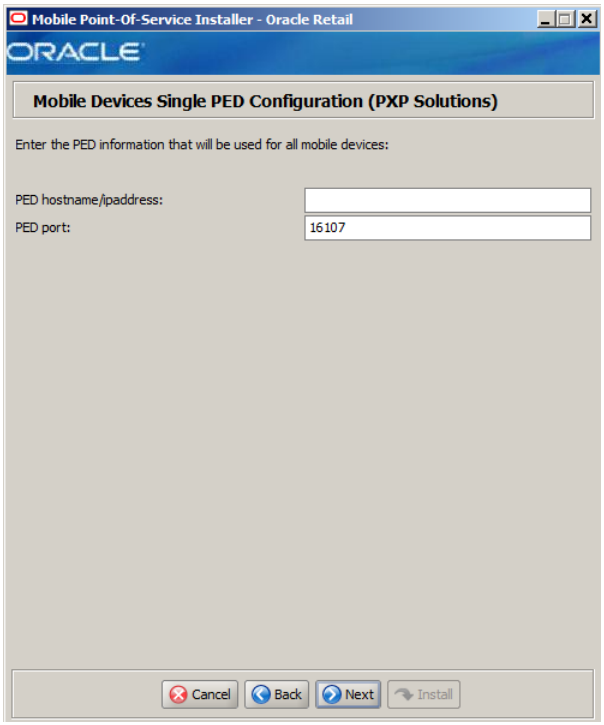
Figure C–36 Mobile Device PED/CPOI Configuration Topology



The field in this window is described in the following table:

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

Figure C–37 Mobile Devices Single PED Configuration (PXP Solutions)



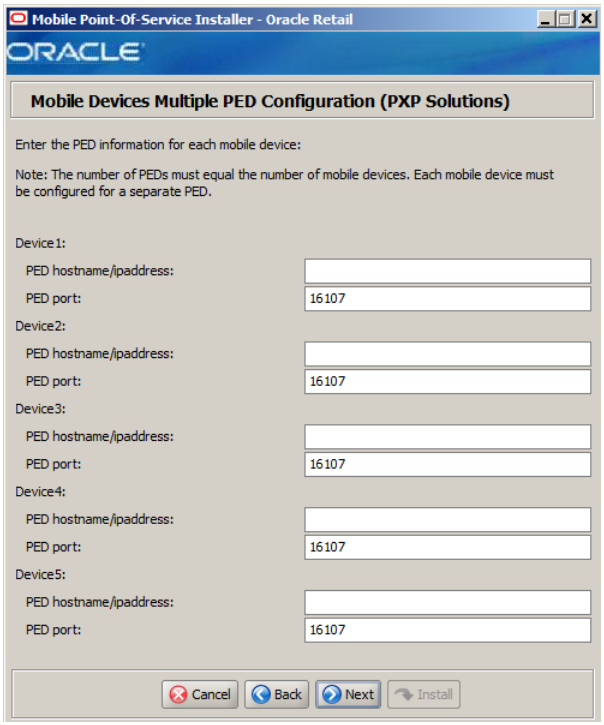
This window is only displayed if **PXP Solutions ANYpay POS** is selected in the Tender Authorization window and **Single PED/CPOI** in the Mobile Device PED/CPOI Configuration Topology window.

The fields in this window are described in the following tables:

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

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

Figure C–38 Mobile Devices Multiple PED Configuration (PXP Solutions)



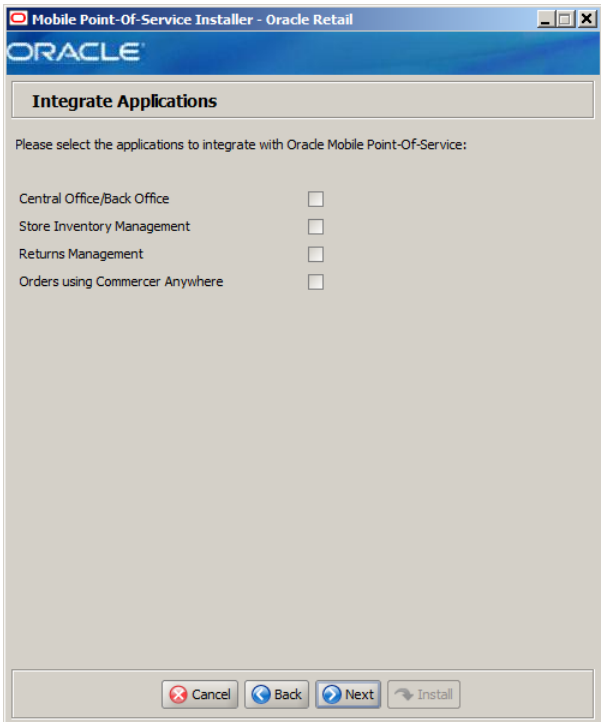
This window is only displayed if **PXP Solutions ANYpay POS** is selected in the Tender Authorization window and **Multiple PED/CPOI** is selected in the Mobile Device PED/CPOI Configuration Topology window.

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

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

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

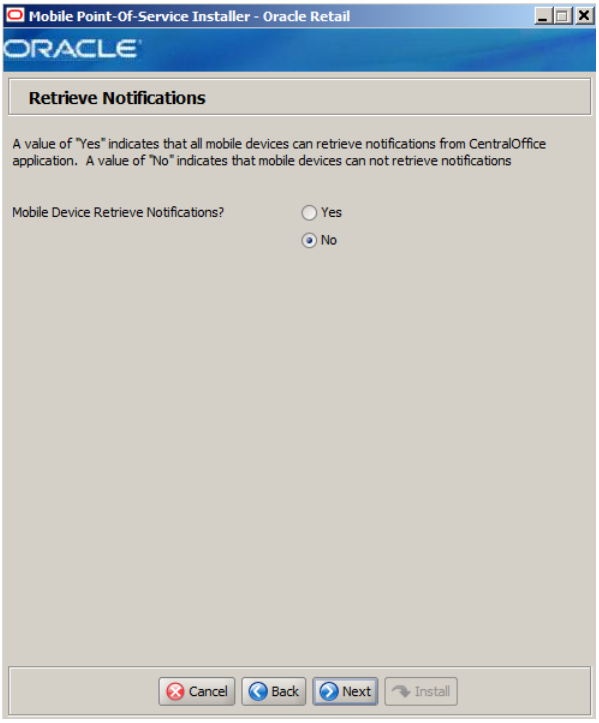
Figure C–39 Integrate Applications



The field in this window 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 ▪ Returns Management ▪ Orders using Commerce Anywhere

Figure C–40 Retrieve Notifications

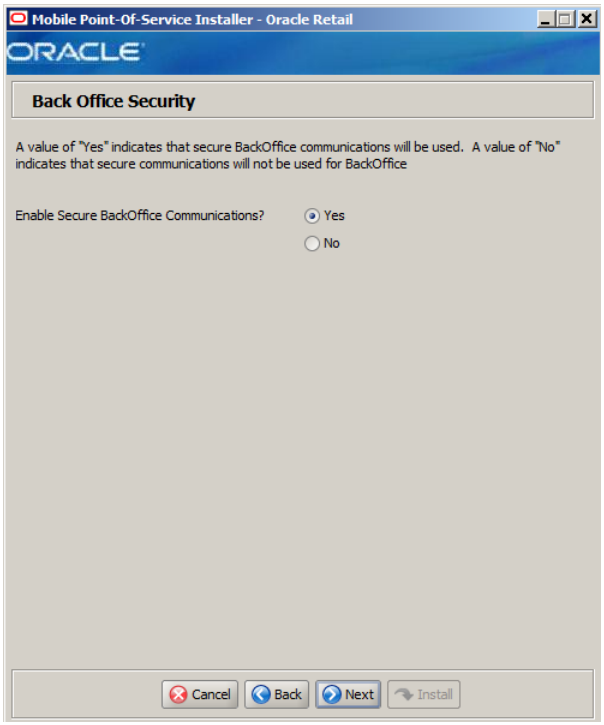


This window is only displayed if **Central Office/Back Office** is selected in the Integrate Applications window.

The field in this window is described in the following table:

Details	Content
Field Title	Mobile Device Retrieve Notifications?
Field Description	Select Yes if mobile devices can retrieve notifications from Central Office.
Example	No

Figure C–41 Back Office Security

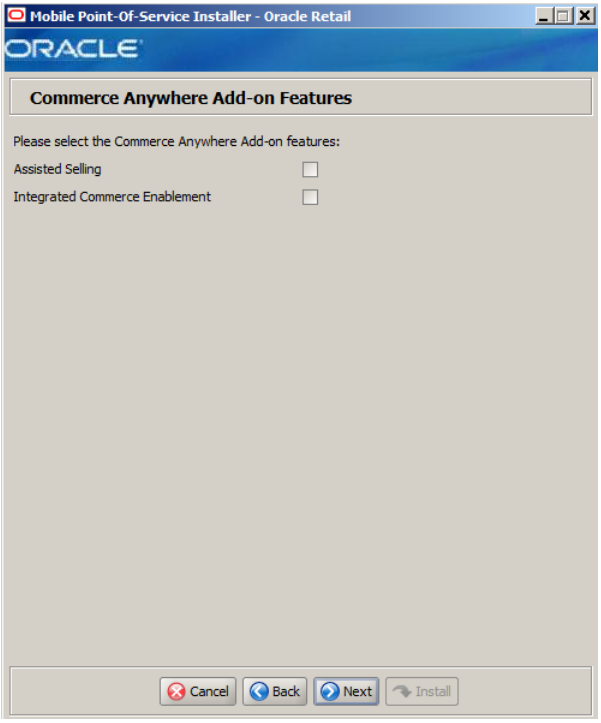


This window is only displayed if **Central Office/Back Office** is selected in the Integrate Applications window.

The field in this window 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–42 Commerce Anywhere Add-on Features

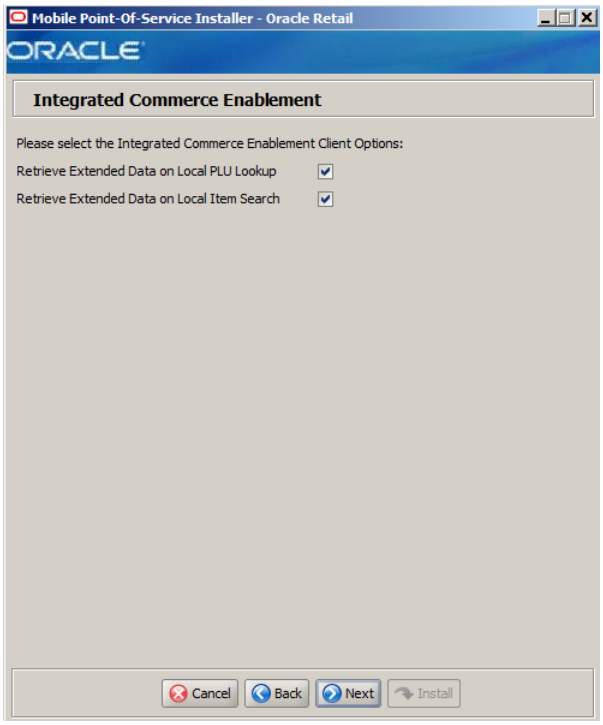


This window is only displayed if **Orders using Commerce Anywhere** is selected in the Integrate Applications window.

The field in this window is described in the following table:

Details	Content
Field Title	Please select the Commerce Anywhere Add-on features
Field Description	Select the Commerce Anywhere features that will be used in Mobile Point-of-Service: ▪ To use the Assisted Selling Application (ASA), select **Assisted Selling**. **Note:** This feature is not tested in Release 14.1. ▪ To enable integrated commerce, select **Integrated Commerce Enablement**.

Figure C–43 Integrated Commerce Enablement

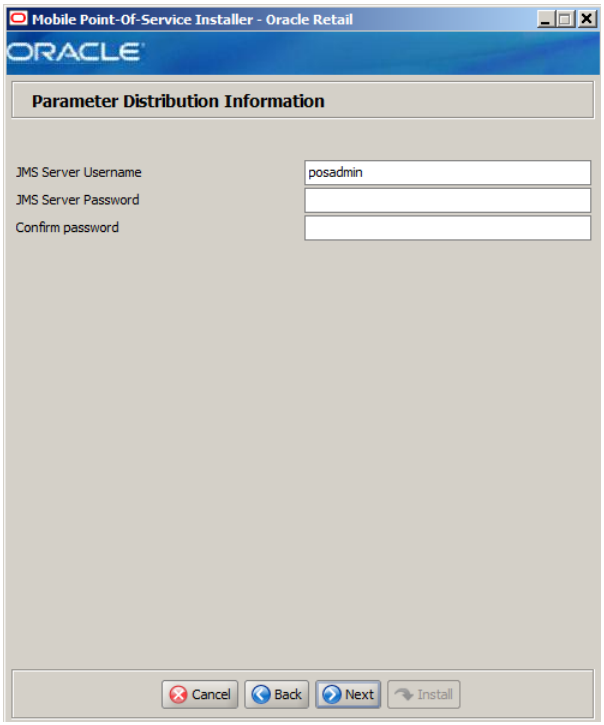


This window is only displayed if **Integrated Commerce Enablement** is selected in the Commerce Anywhere Add-on Features window.

The field in this window is described in the following table:

Details	Content
Field Title	Please select the Integrated Commerce Enablement Client features
Field Description	Select the Commerce Anywhere client features that will be used in Mobile Point-of-Service: ▪ To retrieve extended data on local PLU lookup, select **Retrieve Extended Data on Local PLU lookup**. ▪ To retrieve extended data on local item search, select **Retrieve Extended Data on Local Item Search**.

Figure C–44 Parameter Distribution Information



This window is only displayed if **Central Office/Back Office** is selected in the Integrate Applications window.

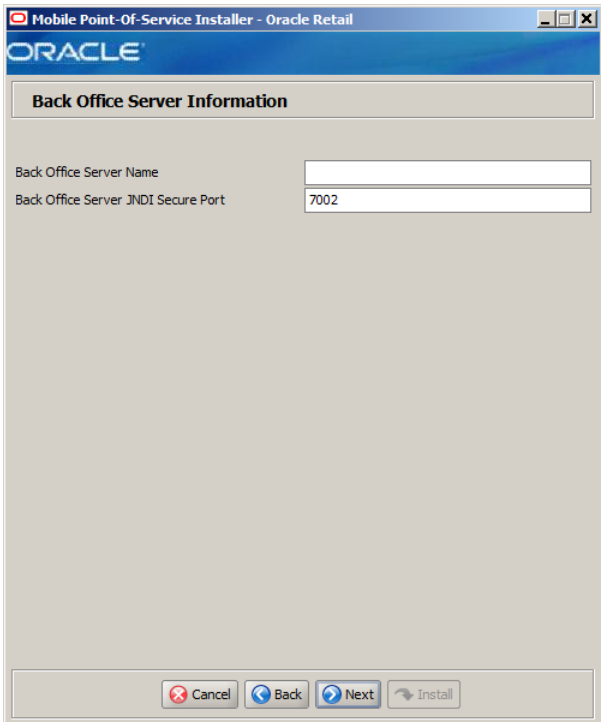
The fields in this window are described in the following tables:

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–45 Back Office Server Information



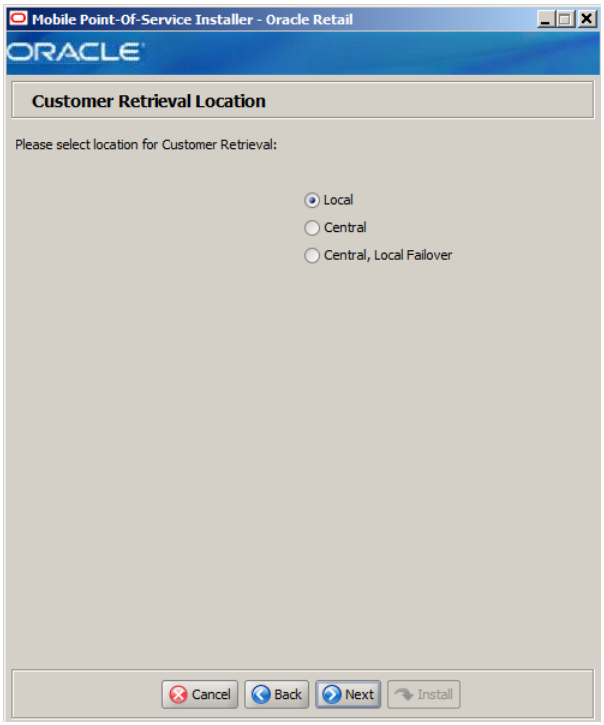
This window is only displayed if **Central Office/Back Office** is selected in the Integrate Applications window.

The fields in this window 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–46 Transaction Retrieval Location

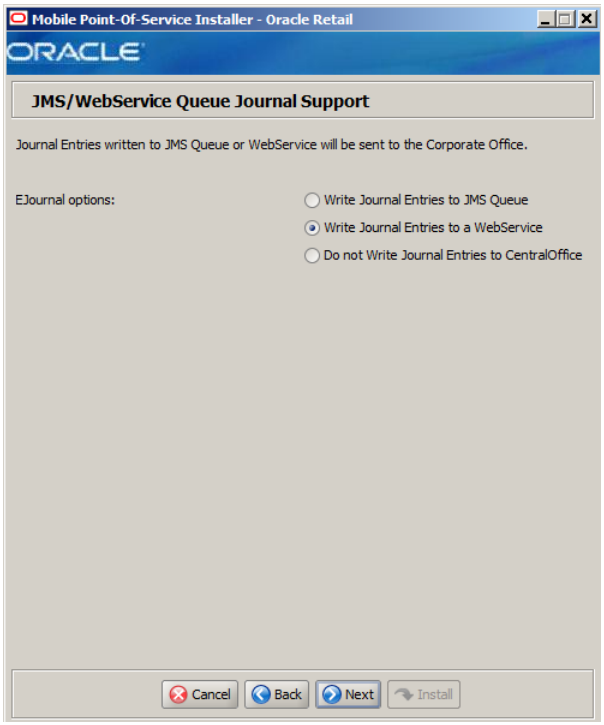


This window is only displayed if **Central Office/Back Office** is selected in the Integrate Applications window.

The field in this window 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 C–47 JMS /Webservice Queue Journal Support

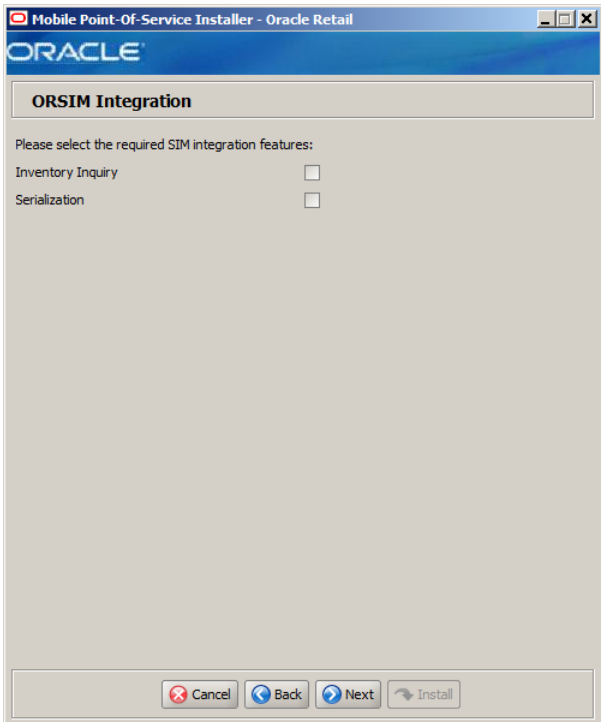


This window is only displayed if **Central Office/Back Office** is selected in the Integrate Applications window.

The field in this window 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 C–48 ORSIM Integration

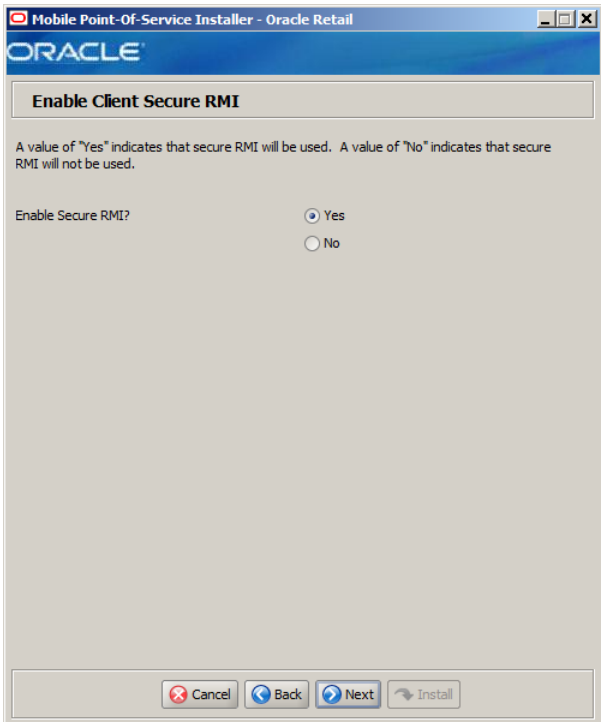


This window is only displayed if **Store Inventory Management** is selected in the Integrate Applications window.

The field in this window 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**.

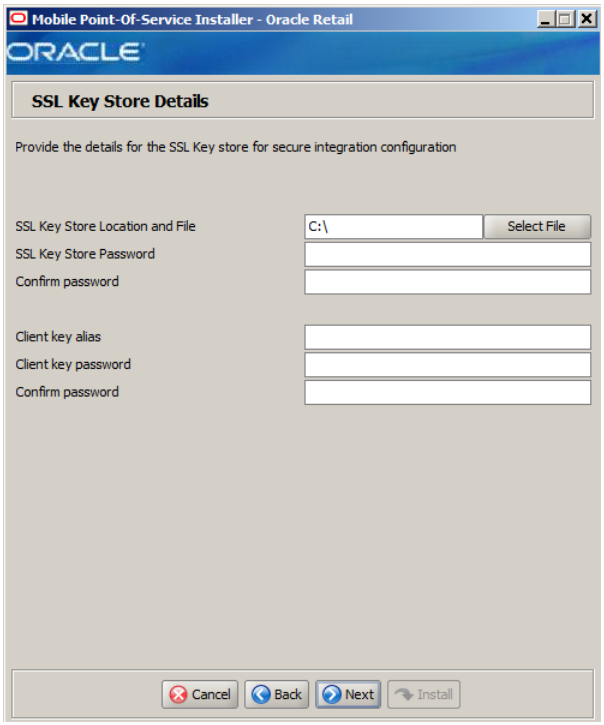
Figure C–49 Enable Client Secure RMI



The field in this window 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–50 SSL Key Store Details



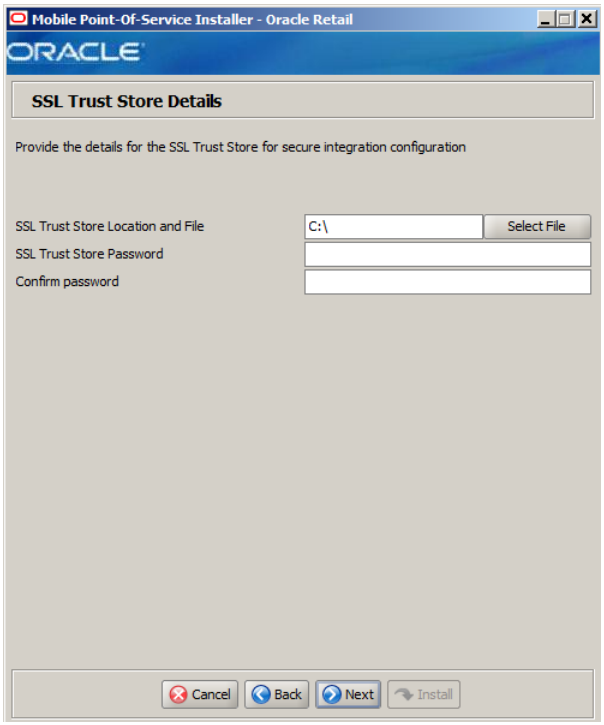
The fields in this window are described in the following tables:

Details	Content
Field Title	SSL Key Store Location and File
Field Description	Enter the location and name of the SSL key store file.
Example	▪ Microsoft Windows: C:\ ▪ Novell SLEPOS: /opt/

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

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

Figure C–51 SSL Trust Store Details



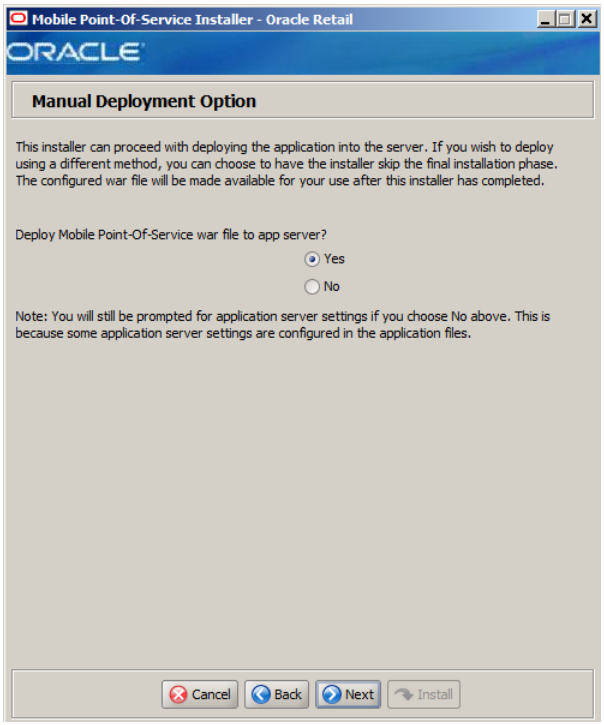
The fields in this window are described in the following tables:

Details	Content
Field Title	SSL Truststore Location and File
Field Description	Enter the location and name of the truststore file.
Example	▪ Microsoft Windows: C:\ ▪ Novell SLEPOS: /opt/

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.

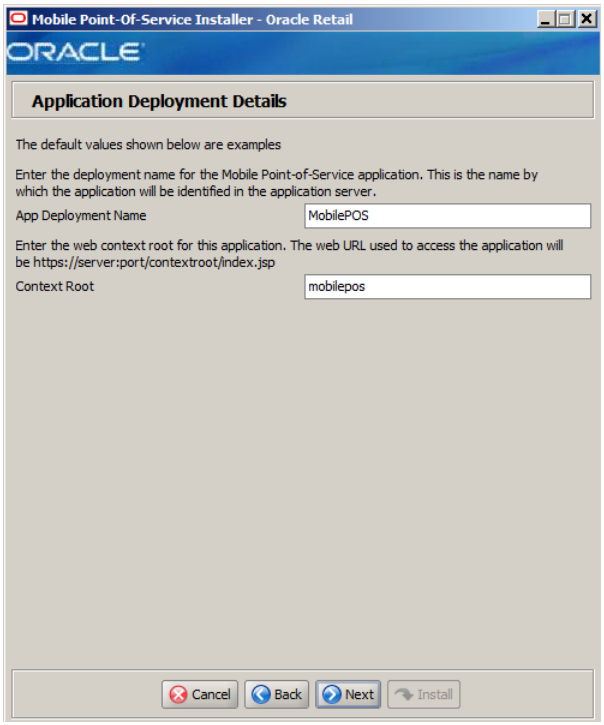
Figure C–52 Manual Deployment Option



The field in this window 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 window 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 5 for the manual steps you need to perform after the installer completes.
Example	Yes

Figure C–53 Application Deployment Details

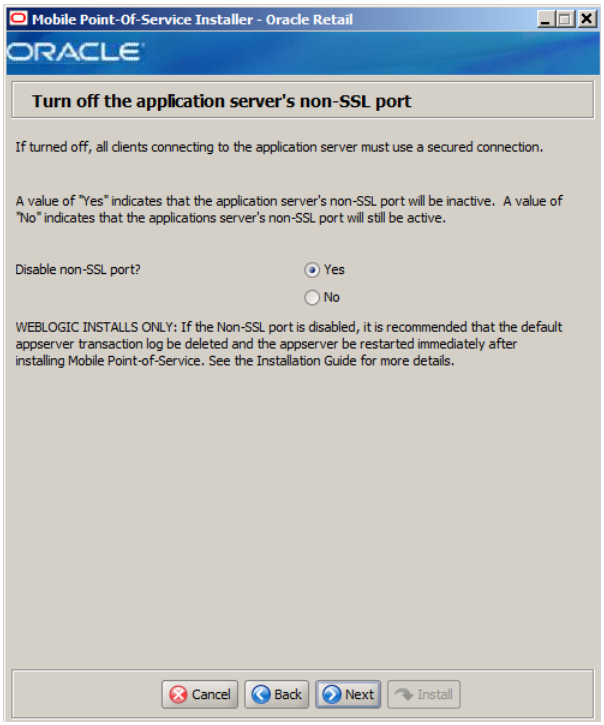


The fields in this window are described in the following tables:

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.
Example	mobilepos

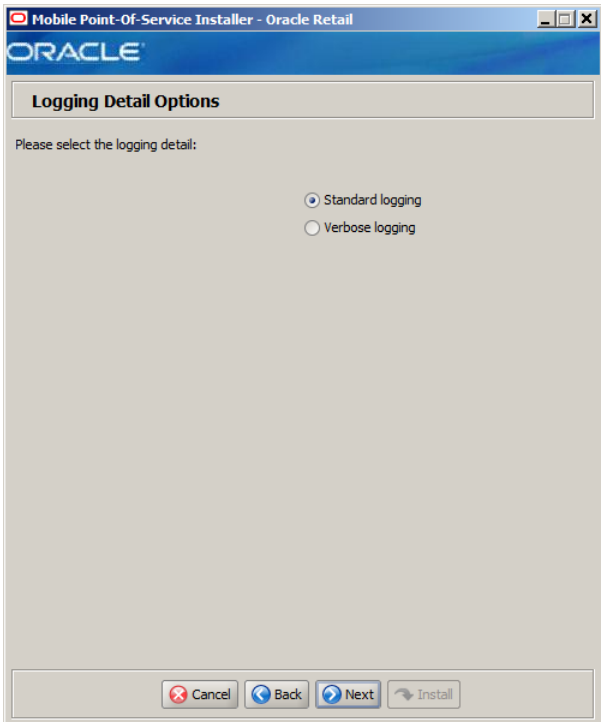
Figure C–54 Turn Off the Application Server's Non-SSL Port



The field in this window 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 "Disable Non-SSL Port" in Chapter 5.
Example	Yes

Figure C–55 Logging Detail Options



The field in this window 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–56 Installation Progress

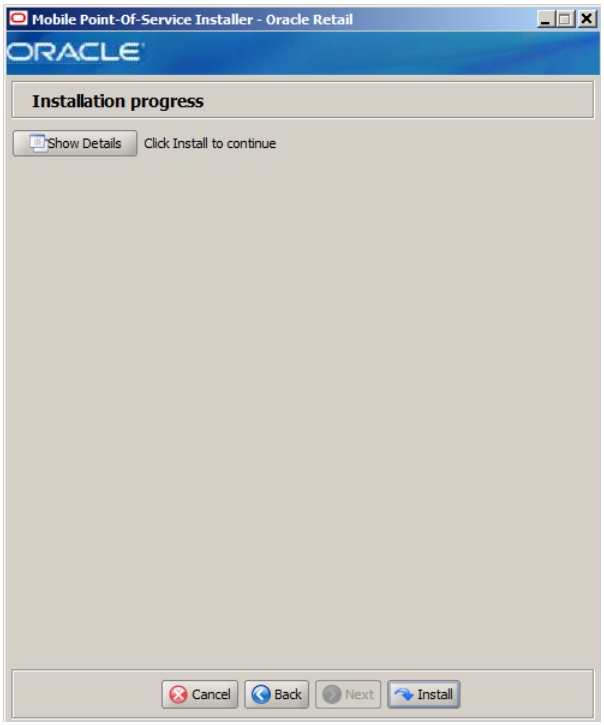
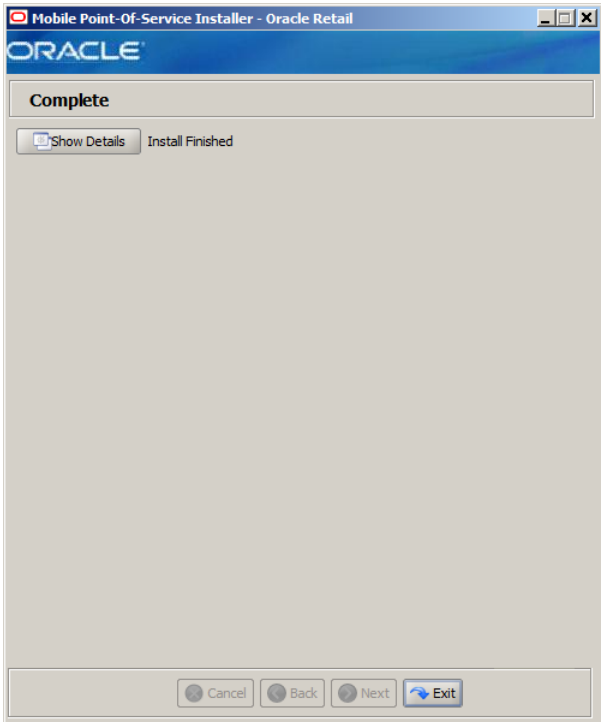


Figure C–57 Install Complete



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 DigitalPersona fingerprint device, make sure the following properties in the `ant.install.properties` file are correct:
   - Microsoft POSReady:

     ```
     ## 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\\jpos113.jar
     input.dpfingerprint.dpotjni = C:\\DigitalPersona\\Bin\\Java\\dpuareu.jar
     ```

   - Novell SLEPOS:

     ```
     ## Properties from Page:fingerPrintDevice
     input.client.device.dpfingerprint = true
     ## Properties from Page:DPEnvironmentClasspath
     ```

```
input.dpfingerprint.dpjavapos =
//opt//DigitalPersona//Bin//JavaPOS//dpjavapos.jar
input.dpfingerprint.jpos = //opt//DigitalPersona//Bin//JavaPOS//jpos113.jar
input.dpfingerprint.dpotjni = //opt//DigitalPersona//Bin//Java//dpuareu.jar
```

4. Run the installer again with the silent argument:
   - Microsoft Windows:

     ```
     install.cmd silent
     ```

   - Novell SLEPOS:

     ```
     install.sh silent
     ```

5. If this is a server install, after the installation is successfully completed, the CREATE SYNONYM privilege must be revoked. In the installer console window, it prompts for a database administrator to run the revokesyn SQL script to revoke the privilege. The script is found in the *<INSTALL_DIR>* directory.

Figure D–1 Installer Prompt to Run revokesyn

For information on granting this privilege on Microsoft Windows, see "Create the Database Schema Owner and Data Source Users" in Chapter 3. For information on granting this privilege on Novell SLEPOS, see "Create the Database Schema Owner and Data Source Users" in Chapter 4.

6. If this is a client install and you are using a fingerprint device, verify the following:
   - The fingerprint device properties from Step 3 are correct in the following file:

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

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

E

Appendix: URL Reference

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

JDBC URL for a Database

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

Using the SID

Syntax:

`jdbc:oracle:thin:@[host]:[tcpPort]:[SIDname]`

- *[host]*: host name of the database server
- *[tcpPort]*: database listener port
- *[SIDname]*: system identifier for the database

Example:

```
jdbc:oracle:thin:@myhost:1525:mySIDdatabase
```

Using the Service Name

Syntax:

`jdbc:oracle:thin:@//[host]:[tcpPort]/[service_name]`

- *[host]*: host name of the database server
- *[tcpPort]*: database listener port
- *[service_name]*: system identifier for the database

Example:

```
jdbc:oracle:thin:@//myhost:1525/myserviceDB
```

Using the Oracle Net Connection

Syntax:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=[host])
(PORT=[tcpPort]))(CONNECT_DATA=(SERVICE_NAME=[service_name])))
```

- *[host]*: host name of the database server
- *[tcpPort]*: database listener port
- *[service_name]*: system identifier for the database

Example:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=myhost1)
(PORT=1525))(CONNECT_DATA=(SERVICE_NAME=mydatabase1)))
```

Secure JDBC URL for a Database

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

Using the Secure Oracle Net Connection

Syntax:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=[host])
(PORT=[tcpsPort]))(CONNECT_DATA=(SERVICE_NAME=[service_name])))
```

- *[host]*: host name of the database server
- *[tcpsPort]*: database listener port
- *[service_name]*: system identifier for the database

Example:

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=myhost1)
(PORT=7004))(CONNECT_DATA=(SERVICE_NAME=mydatabase1)))
```

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 domain was created
- *<port>*: port number selected when the WebLogic domain was created

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 domain was created
- *<port>*: port number selected when the WebLogic domain was created

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 in the Database Configuration window 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

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

In the Central Office/Back Office Server Information window, 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. Example locations for this file are `C:\POS\IBMJPOS\jpos.xml` and `opt/POS/IBMJPOS/jpos.xml`.

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

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

- "Configuring Devices for an NCR Register"
- "Configuring Devices for an IBM SurePOS Register"
- "Configuring a Device for ACI PINComm"

Configuring Devices for an NCR Register

To configure an NCR device:

1. Install the JPOS drivers acquired from NCR and use the NCR Retail Systems Manager (RSM) to configure the JPOS devices. The JPOS configuration is saved by RSM as the config.xml file in the following directory:

   ```
   c:\Program Data\NCR\NCR JavaPOS\jpos\res
   ```

2. Create the device entries using the logical names shown in the following example config.xml entries. The logicalName of the device in the config.xml file must match the deviceName in the PosDevicesTechnician.xml file.

   Note that references to jpos.xml in the Point-of-Service documentation refer to config.xml for the NCR register. When the NCR JPOS drivers are installed the system, CLASSPATH and PATH are set for the NCR JPOS devices. The system CLASSPATH and PATH are used by Point-of-Service.

   If for some reason the NCR config.xml is edited manually, be sure that Point-of-Service is not active at the time of the modification. The config.xml file may be written back when Point-of-Service stops overlaying any modifications.

```
<JposEntry logicalName="defaultMSR">
        <creation factoryClass="com.ncr.retail.jpos.NCRJposServiceInstanceFactory"
  serviceClass="com.ncr.retail.jpos.services.msr.MSRService"/>
        <vendor name="NCR" url="http://www.ncr.com"/>
```

```
        <jpos category="MSR" version="1.7"/>
        <product description="NCR MSR Service" name="NCR MSR Service for
JavaPOS(TM) Standard" url="http://www.ncr.com"/>

        <!--Other non JavaPOS required property (mostly vendor properties and bus
specific properties i.e. RS232 )-->
        <prop name="IO.DevUsagePage" type="String" value="142"/>
        <prop name="IO.Reports" type="String" value="1"/>
        <prop name="sModelClassName" type="String" value="NCRIOChannelMSRModel"/>
        <prop name="Version" type="String" value="1.13.0"/>
        <prop name="IO.DevUsage" type="String" value="1"/>
        <prop name="IO.VendorID" type="String" value="1028"/>
        <prop name="IO.ProductID" type="String" value="0"/>
        <prop name="Type" type="String" value="ISO"/>
        <prop name="ModelDescription" type="String" value="NCR I/O Channel MSR"/>
        <prop name="ConnectionType" type="String" value="U"/>
        <prop name="ModelVersion" type="String" value="3.12.3.170"/>
        <prop name="IO.ClearAfterRead" type="String" value="true"/>
        <prop name="Description" type="String" value="NCR JavaPOS MSR Device
Service"/>
        <prop name="IO.DevPath" type="String" value=""/>
</JposEntry>

    <JposEntry logicalName="defaultFingerprintReader">
        <creation
factoryClass="com.digitalpersona.javapos.services.biometrics.ServiceInstanceFactor
y"
serviceClass="com.digitalpersona.javapos.services.biometrics.UAREU4000BReader"/>
        <vendor name="DigitalPersona" url="http://www.digitalpersona.com"/>
        <jpos category="Biometrics" version="1.11"/>
        <product description="Finger Printing Device" name="U.are.U 4000B Reader"
url="http://www.digitalpersona.com"/>

        <!--Other non JavaPOS required property (mostly vendor properties and bus
specific properties i.e. RS232 )-->
</JposEntry>

    <JposEntry logicalName="defaultCashDrawer">
        <creation factoryClass="com.ncr.retail.jpos.NCRJposServiceInstanceFactory"
serviceClass="com.ncr.retail.jpos.services.cashdrawer.CashDrawerService"/>
        <vendor name="NCR" url="http://www.ncr.com"/>
        <jpos category="CashDrawer" version="1.7"/>
        <product description="NCR CashDrawer Service" name="NCR CashDrawer Service
for JavaPOS(TM) Standard" url="http://www.ncr.com"/>

        <!--Other non JavaPOS required property (mostly vendor properties and bus
specific properties i.e. RS232 )-->
        <prop name="nDeviceNumber" type="String" value="0"/>
        <prop name="sModelClassName" type="String"
value="NCRCashDrawerProcessor"/>
        <prop name="Version" type="String" value="1.10.0"/>
        <prop name="Model.Model" type="String" value="INTEGRATED"/>
        <prop name="ModelDescription" type="String" value="NCR Cash Drawer
Kickout"/>
        <prop name="Model.OpenDrawerSUE" type="String" value="0"/>
        <prop name="ConnectionType" type="String" value="M"/>
        <prop name="ModelVersion" type="String" value="3.12.1.123"/>
        <prop name="Description" type="String" value="NCR JavaPOS CashDrawer
Device Service"/>
        <prop name="YCableStatus" type="String" value="1"/>
```

```
</JposEntry>

    <JposEntry logicalName="defaultScanner">
        <creation factoryClass="com.ncr.retail.jpos.NCRJposServiceInstanceFactory"
serviceClass="com.ncr.retail.jpos.services.scanner.ScannerService"/>
        <vendor name="NCR" url="http://www.ncr.com"/>
        <jpos category="Scanner" version="1.7"/>
        <product description="NCR Scanner Service" name="NCR Scanner Service for
JavaPOS(TM) Standard" url="http://www.ncr.com"/>

        <!--Other non JavaPOS required property (mostly vendor properties and bus
specific properties i.e. RS232 )-->
        <prop name="Model.Model" type="String" value="3207"/>
        <prop name="ModelVersion" type="String" value="3.12.6.195"/>
        <prop name="Model.AutoCD" type="String" value="0"/>
        <prop name="Model.NoDSRCable" type="String" value="0"/>
        <prop name="IO.DevPath" type="String" value=""/>
        <prop name="Model.AuxLED" type="String" value="??"/>
        <prop name="IO.CTSFlowControl" type="String" value="0"/>
        <prop name="Model.TriggerMode" type="String" value="0"/>
        <prop name="ModelDescription" type="String" value="NCR78xx Scanner"/>
        <prop name="IO.VendorID" type="String" value="1504"/>
        <prop name="IO.dataBits" type="String" value="3"/>
        <prop name="IO.portName" type="String" value="COM1"/>
        <prop name="Config" type="String" value=""/>
        <prop name="IO.parity" type="String" value="0"/>
        <prop name="Model.Bcc" type="String" value="0"/>
        <prop name="Model.AllSymbologies" type="String" value="0"/>
        <prop name="Model.ProgSeq" type="String" value=""/>
        <prop name="Model.ScannerScaleFormat" type="String" value="0"/>
        <prop name="Description" type="String" value="NCR JavaPOS Scanner Device
Service"/>
        <prop name="IO.baudRate" type="String" value="9600"/>
        <prop name="Model.ReadTimeout" type="String" value="??"/>
        <prop name="IO.DevUsage" type="String" value="19200"/>
        <prop name="IO.Reports" type="String" value="2"/>
        <prop name="Model.EnableIfOff" type="String" value="0"/>
        <prop name="Model.LightLED" type="String" value="??"/>
        <prop name="Model.Config" type="String" value=""/>
        <prop name="ConnectionType" type="String" value="U"/>
        <prop name="Model.Prefix" type="String" value=""/>
        <prop name="IO.DSRFlowControl" type="String" value="0"/>
        <prop name="IO.stopBits" type="String" value="0"/>
        <prop name="Model.Suffix" type="String" value="0x0D"/>
        <prop name="IO.DevUsagePage" type="String" value="65349"/>
        <prop name="Model.AimerLED" type="String" value="??"/>
        <prop name="Model.RSS" type="String" value="0"/>
        <prop name="IO.ClearAfterRead" type="String" value="true"/>
        <prop name="Version" type="String" value="1.13.0"/>
        <prop name="Model.LabelID" type="String" value="1"/>
        <prop name="IO.ProductID" type="String" value="0"/>
        <prop name="sModelClassName" type="String" value="NCR78xxScannerScale"/>
</JposEntry>

    <JposEntry logicalName="defaultPrinter">
        <creation factoryClass="com.ncr.retail.jpos.NCRJposServiceInstanceFactory"
serviceClass="com.ncr.retail.jpos.services.posprinter.POSPrinterService"/>
        <vendor name="NCR" url="http://www.ncr.com"/>
        <jpos category="POSPrinter" version="1.7"/>
        <product description="NCR POSPrinter Service" name="NCR POSPrinter Service
```

```
for JavaPOS(TM) Standard" url="http://www.ncr.com"/>

        <!--Other non JavaPOS required property (mostly vendor properties and bus
specific properties i.e. RS232 )-->
        <prop name="TSTPreDefinedImage3" type="String" value=""/>
        <prop name="Model.Model" type="String" value="7168"/>
        <prop name="TST2SideMode" type="String" value="0"/>
        <prop name="TSTPreDefinedImage2" type="String" value=""/>
        <prop name="ModelVersion" type="String" value="3.12.0.206"/>
        <prop name="TSTPreDefinedImage1" type="String" value=""/>
        <prop name="TSTReprintOnError" type="String" value="0"/>
        <prop name="ModelDescription" type="String" value="NCR 71xx POS Printer"/>
        <prop name="IO.dataBits" type="String" value="3"/>
        <prop name="TSTFrontLine1Attributes" type="String" value="0"/>
        <prop name="IO.portName" type="String" value="COM5"/>
        <prop name="IO.parity" type="String" value="0"/>
        <prop name="TSTOrientation" type="String" value="0"/>
        <prop name="TSTReprintAttrib2" type="String" value="0"/>
        <prop name="TSTFrontLine1Text" type="String" value="-1"/>
        <prop name="TSTReprintAttrib1" type="String" value="0"/>
        <prop name="TSTPreDefinedTextFront" type="String" value="0"/>
        <prop name="TSTBackLine1Attributes" type="String" value="0"/>
        <prop name="Description" type="String" value="NCR JavaPOS POSPrinter
Device Service"/>
        <prop name="sEncoding" type="String" value=""/>
        <prop name="IO.baudRate" type="String" value="115200"/>
        <prop name="SlipToTopOfForm" type="String" value="T"/>
        <prop name="TSTReprintLine2" type="String" value="-1"/>
        <prop name="TSTReprintLine1" type="String" value="-1"/>
        <prop name="LineSize" type="String" value="80"/>
        <prop name="TSTBackLine2Text" type="String" value="-1"/>
        <prop name="HeartbeatPollTime" type="String" value="1000"/>
        <prop name="TSTPrintSides" type="String" value="0"/>
        <prop name="AsyncBlockStatusTimeout" type="String" value="200"/>
        <prop name="AsyncBlockSize" type="String" value="10"/>
        <prop name="CharacterByteSize" type="String" value="1"/>
        <prop name="ConnectionType" type="String" value="S"/>
        <prop name="ColorPaper" type="String" value="1"/>
        <prop name="TSTFrontLine2Attributes" type="String" value="0"/>
        <prop name="EscapeSequenceModule" type="String"
value="NCRUPOSPrinterParsers"/>
        <prop name="PrintIntegrityMode" type="String" value="1"/>
        <prop name="SlipOutSettleTime" type="String" value=""/>
        <prop name="TSTMinRecLen" type="String" value="0"/>
        <prop name="IO.stopBits" type="String" value="0"/>
        <prop name="TSTPreDefReprint" type="String" value="0"/>
        <prop name="SlipInSettleTime" type="String" value=""/>
        <prop name="TSTBackLine1Text" type="String" value="-1"/>
        <prop name="TSTBackLine2Attributes" type="String" value="0"/>
        <prop name="PrintStatusWaitTime" type="String" value="30000"/>
        <prop name="TST2SidePaperDetect" type="String" value="0"/>
        <prop name="Version" type="String" value="1.13.0"/>
        <prop name="TSTPreDefinedTextBack" type="String" value="0"/>
        <prop name="AutoLineFeed" type="String" value="F"/>
        <prop name="EjectSlipFeed" type="String" value=""/>
        <prop name="TwoByteCodePage" type="String" value="932"/>
        <prop name="TSTEndTransactionAutoKnife" type="String" value="1"/>
        <prop name="sModelClassName" type="String"
value="NCR71xxPrinterCDMICRModel"/>
        <prop name="TSTFrontLine2Text" type="String" value="-1"/>
```

```
</JposEntry>

    <JposEntry logicalName="defaultLineDisplay">
        <creation factoryClass="com.ncr.retail.jpos.NCRJposServiceInstanceFactory"
serviceClass="com.ncr.retail.jpos.services.linedisplay.LineDisplayService"/>
        <vendor name="NCR" url="http://www.ncr.com"/>
        <jpos category="LineDisplay" version="1.7"/>
        <product description="NCR LineDisplay Service" name="NCR LineDisplay
Service for JavaPOS(TM) Standard" url="http://www.ncr.com"/>

        <!--Other non JavaPOS required property (mostly vendor properties and bus
specific properties i.e. RS232 )-->
        <prop name="IO.DevUsagePage" type="String" value="0xFF7F"/>
        <prop name="IO.Reports" type="String" value="2"/>
        <prop name="sModelClassName" type="String"
value="NCR59752x20LineDisplay"/>
        <prop name="Version" type="String" value="1.10.0"/>
        <prop name="ScreenSaver" type="String" value="0"/>
        <prop name="IO.DevUsage" type="String" value="6"/>
        <prop name="IO.VendorID" type="String" value="1028"/>
        <prop name="IO.ProductID" type="String" value="824"/>
        <prop name="ModelDescription" type="String" value="NCR 5975 2x20 Line
Display"/>
        <prop name="DeviceWindows" type="String" value="5"/>
        <prop name="ConnectionType" type="String" value="U"/>
        <prop name="CodePage" type="String" value="858"/>
        <prop name="ModelVersion" type="String" value="3.12.1.107"/>
        <prop name="IO.ClearAfterRead" type="String" value="true"/>
        <prop name="Description" type="String" value="NCR JavaPOS LineDisplay
Device Service"/>
        <prop name="IO.DevPath" type="String" value=""/>
        <prop name="sEncoding" type="String" value=""/>
</JposEntry>
```

Configuring Devices for an IBM SurePOS Register

To configure the devices for an IBM SurePOS register:

1. Install the JPOS drivers acquired from IBM and use the IBM Pos Control Center to configure the JPOS devices. The JPOS configuration file, jpos.xml, is saved by default in `C:\POS\IBMJPOS`.
2. Create the device entries using the logical names shown in the following example jpos.xml entries. The logicalName of the device in the jpos.xml file must match the deviceName in the PosDevicesTechnician.xml file.

```
    <JposEntry logicalName="defaultCashDrawer">
        <creation
factoryClass="com.ibm.jpos.services.IBMJposServiceInstanceFactory"
serviceClass="com.ibm.jpos.services.IBMCashDrawer"/>
        <vendor name="IBM" url="http://www.ibm.com"/>
        <jpos category="CashDrawer" version="1.13.4"/>
        <product description="IBM JavaPOS(TM) CashDrawer Service for
SureOne/SurePOS 100/300/72x/74x/78x-A" name="IBM JavaPOS for Linux/Windows Version
1.13.4" url="http://www.pc.ibm.com/store/"/>

        <prop name="deviceBus" type="String" value="Proprietary"/>
        <prop name="com.ibm.posj.bus.ProprietaryBusSubType" type="String"
value="Embedded"/>
        <prop name="abstractionClass" type="String"
```

```
value="com.ibm.jpos.services.IBMCashDrawer"/>
        <prop name="impClass" type="String"
value="com.ibm.jpos.services.sdi.CashDrawerServiceImp"/>
        <prop name="com.ibm.posj.bus.deviceNumber" type="String" value="0"/>
        <prop name="com.ibm.jpos.sdi.config.CashDrawer.OpenDrawerRetries"
type="String" value="0"/>
</JposEntry>

    <JposEntry logicalName="defaultLineDisplay">
        <creation
factoryClass="com.ibm.jpos.services.IBMJposServiceInstanceFactory"
serviceClass="com.ibm.jpos.services.LineDisplayAnop0"/>
        <vendor name="IBM" url="http://www.ibm.com"/>
        <jpos category="LineDisplay" version="1.13.4"/>
        <product description="IBM JavaPOS(TM) LineDisplay USB Service for IBM
Liquid Crystal Display (LCD)" name="IBM JavaPOS for Linux/Windows Version 1.13.4"
url="http://www.pc.ibm.com/store/"/>
        <prop name="com.ibm.posj.bus.hid.usageId" type="String" value="0x2600"/>
        <prop name="deviceBus" type="String" value="HID"/>
        <prop name="abstractionClass" type="String"
value="com.ibm.jpos.services.LineDisplayAnop0"/>
        <prop name="impClass" type="String"
value="com.ibm.jpos.services.sdi.LineDisplayServiceImp"/>
        <prop name="com.ibm.posj.bus.hid.usagePage" type="String" value="0xFF45"/>
        <prop name="com.ibm.posj.bus.deviceNumber" type="String" value="0"/>
        <prop
name="com.ibm.jpos.services.sdi.config.LineDisplay.CharacterSetASCIIBehavior"
type="String" value="858"/>
</JposEntry>

    <JposEntry logicalName="defaultMICR">
        <creation
factoryClass="com.ibm.jpos.services.IBMJposServiceInstanceFactory"
serviceClass="com.ibm.jpos.services.IBM4610MICR"/>
        <vendor name="IBM" url="http://www.ibm.com"/>
        <jpos category="MICR" version="1.13.4"/>
        <product description="IBM JavaPOS(TM) MICR USB Service for IBM 4610
TI2/4/8/9 2CR Printer" name="IBM JavaPOS for Linux/Windows Version 1.13.4"
url="http://www.pc.ibm.com/store/"/>

        <prop name="com.ibm.posj.bus.hid.usageId" type="String" value="0x3500"/>
        <prop name="deviceBus" type="String" value="HID"/>
        <prop name="abstractionClass" type="String"
value="com.ibm.jpos.services.IBM4610MICR"/>
        <prop name="impClass" type="String"
value="com.ibm.jpos.services.sdi.MICRServiceImp"/>
        <prop name="com.ibm.posj.bus.hid.usagePage" type="String" value="0xFF45"/>
        <prop name="com.ibm.posj.bus.deviceNumber" type="String" value="0"/>
        <prop name="com.ibm.jpos.sdi.config.MICR.exceptionTableFile" type="String"
value="[file-path-goes-here]"/>
        <prop name="com.ibm.jpos.sdi.config.MICR.exceptionTable4" type="String"
value="B778899001D154R"/>
        <prop name="com.ibm.jpos.sdi.config.MICR.exceptionTable3" type="String"
value="B667788990D153R"/>
        <prop name="com.ibm.jpos.sdi.config.MICR.exceptionTable2" type="String"
value="P123456780AAAAAXSSS"/>
        <prop name="com.ibm.jpos.sdi.config.MICR.exceptionTable1" type="String"
value="B445566778D151R"/>
        <prop name="com.ibm.jpos.sdi.config.MICR.exceptionTable0" type="String"
value="B334455667D150R"/>
```

```
        <prop name="com.ibm.jpos.sdi.config.MICR.stripAccountDashes" type="String"
value="false"/>
        <prop name="com.ibm.jpos.sdi.config.MICR.stripTransitDashes" type="String"
value="false"/>
        <prop name="com.ibm.jpos.sdi.config.MICR.switchTransitDashToSpace"
type="String" value="false"/>
</JposEntry>

    <JposEntry logicalName="defaultMSR">
        <creation
factoryClass="com.ibm.jpos.services.IBMJposServiceInstanceFactory"
serviceClass="com.ibm.jpos.services.IBMMSR"/>
        <vendor name="IBM" url="http://www.ibm.com"/>
        <jpos category="MSR" version="1.13.4"/>
        <product description="IBM JavaPOS(TM) MSR USB Service for IBM
ANKPOS/Keyboard V/Modular/NANPOS/133 key/4685/4820/50key Keyboard" name="IBM
JavaPOS for Linux/Windows Version 1.13.4" url="http://www.pc.ibm.com/store/"/>

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

    <JposEntry logicalName="defaultPrinter">
        <creation
factoryClass="com.ibm.jpos.services.IBMJposServiceInstanceFactory"
serviceClass="com.ibm.jpos.services.SdiIBM4610EPOSPrinter"/>
        <vendor name="IBM" url="http://www.ibm.com"/>
        <jpos category="POSPrinter" version="1.13.4"/>
        <product description="IBM JavaPOS(TM) POSPrinter USB Service for IBM 4610
TI3/4/5/8/9 TM/F 6/7 2xR/1NR Printer" name="IBM JavaPOS for Linux/Windows Version
1.13.4" url="http://www.pc.ibm.com/store/"/>

        <prop name="com.ibm.posj.bus.hid.usageId" type="String" value="0x3500"/>
        <prop name="deviceBus" type="String" value="HID"/>
        <prop name="abstractionClass" type="String"
value="com.ibm.jpos.services.SdiIBM4610EPOSPrinter"/>
        <prop name="impClass" type="String"
value="com.ibm.jpos.services.sdi.IBM4610PrinterServiceImp"/>
        <prop name="com.ibm.posj.bus.hid.usagePage" type="String" value="0xFF45"/>
        <prop name="com.ibm.posj.bus.deviceNumber" type="String" value="0"/>
</JposEntry>

    <JposEntry logicalName="defaultScanner">
        <creation
factoryClass="com.ibm.jpos.services.IBMJposServiceInstanceFactory"
serviceClass="com.ibm.jpos.services.ScannerUSBOEM"/>
        <vendor name="IBM" url="http://www.ibm.com"/>
        <jpos category="Scanner" version="1.13.4"/>
        <product description="IBM JavaPOS(TM) Scanner USB Service for OEM Hand
Held Scanner" name="IBM JavaPOS for Linux/Windows Version 1.13.4"
url="http://www.pc.ibm.com/store/"/>

        <prop name="setEnableCODE39" type="Boolean" value="true"/>
        <prop name="setEnableCode128" type="Boolean" value="true"/>
```

```
        <prop name="setEnableInterleaved2of5" type="Boolean" value="true"/>
        <prop name="com.ibm.posj.bus.hid.usagePage" type="String" value="0xFF45"/>
        <prop name="abstractionClass" type="String"
value="com.ibm.jpos.services.ScannerUSBOEM"/>
        <prop name="setEnableUCC_EAN128" type="Boolean" value="true"/>
        <prop name="setEnableCodabar" type="Boolean" value="true"/>
        <prop name="impClass" type="String"
value="com.ibm.jpos.services.sdi.ScannerServiceImp"/>
        <prop name="setEnableUPCD1D5" type="Boolean" value="true"/>
        <prop name="setEnableCode93" type="Boolean" value="true"/>
        <prop name="setEnableUPCAE_EANJAN813" type="Boolean" value="true"/>
        <prop name="deviceBus" type="String" value="HID"/>
        <prop name="com.ibm.posj.bus.hid.usageId" type="String" value="0x4B00"/>
        <prop name="setEnable_5_DigitSupplementals" type="Boolean" value="true"/>
        <prop name="setEnable_2_DigitSupplementals" type="Boolean" value="true"/>
            <prop name="setITFLengthSpecifiedTwo" type="Boolean" value="true"/>
        <prop name="setITFLength1" type="Byte" value="12"/>
            <prop name="setITFLength2" type="Byte" value="16"/>
        <prop name="com.ibm.posj.bus.deviceNumber" type="String" value="0"/>
        <prop name="setEnableUPC_A_CheckDigit" type="Boolean" value="true"/>
        <prop name="setEnableUPC_E_CheckDigit" type="Boolean" value="true"/>

</JposEntry>
```

Configuring a Device for ACI PINComm

To configure an ACI PINComm 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 PINComm 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)
2. Oracle Retail Sales Audit (ReSA)
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 Optimization (RPO)
19. Oracle Retail Merchandise Financial Planning (MFP)
20. Oracle Retail Size Profile Optimization (SPO)
21. Oracle Retail Assortment Planning (AP)
22. Oracle Retail Item Planning (IP)
23. Oracle Retail Item Planning Configured for COE (IP COE)
24. Oracle Retail Advanced Inventory Planning (AIP)
25. Oracle Retail Analytics
26. Oracle Retail Advanced Science Engine (ORASE)
27. Oracle Retail Integration Bus (RIB)
28. Oracle Retail Service Backbone (RSB)
29. Oracle Retail Financial Integration (ORFI)
30. Oracle Retail Point-of-Service (ORPOS)
    - Oracle Retail Mobile Point-of-Service (ORMPOS) (requires ORPOS)
31. Oracle Retail Markdown Optimization (MDO)
32. Oracle Retail Clearance Optimization Engine (COE)
33. Oracle Retail Analytic Parameter Calculator for Markdown Optimization (APC-MDO)
34. Oracle Retail Analytic Parameter Calculator for Regular Price Optimization (APC-RPO)
35. Oracle Retail Macro Space Planning (MSP)

    The Oracle Retail Enterprise suite includes Macro Space Planning. This can be installed independently of and does not affect the installation order of the other applications in the suite. If Macro Space Planning is installed, the installation order for its component parts is:

    - Oracle Retail Macro Space Management (MSM)
    - Oracle Retail In-Store Space Collaboration (ISSC) (requires MSM)

- Oracle Retail Mobile In-Store Space Collaboration (requires MSM and ISSC)