

## **Oracle® Retail Returns Management**

Installation Guide, Volume 2 - IBM Stack

Release 2.3.3

October 2011

Copyright © 2011, Oracle and/or its affiliates. All rights reserved.

Primary Author: Bernadette Goodman

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

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

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

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

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

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

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

## Value-Added Reseller (VAR) Language

### Oracle Retail VAR Applications

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

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

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

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

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

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

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



---

---

# Contents

|   |             |
|---|-------------|
| <b>Send Us Your Comments .....</b>                                    | <b>xi</b>   |
| <b>Preface .....</b>  | <b>xiii</b> |
| Audience.....   | xiii        |
| Documentation Accessibility .....                                     | xiii        |
| Related Documents .....   | xiv         |
| Customer Support .....  | xiv         |
| Review Patch Documentation .....                                      | xiv         |
| Oracle Retail Documentation on the Oracle Technology Network .....    | xiv         |
| Conventions .....   | xv          |
| <br><b>1 Preinstallation Tasks</b>                                    |             |
| Patch Contents .....  | 1-1         |
| Check for the Current Version of the Installation Guide.....          | 1-1         |
| Check Supported Database Server Requirements.....                     | 1-2         |
| Required Settings for Database Installation.....                      | 1-2         |
| Check Supported Application Server Requirements.....                  | 1-2         |
| Check for SSL Certificate.....  | 1-2         |
| Check Oracle Retail Software Dependencies .....                       | 1-2         |
| Check Third-Party Software Dependencies.....                          | 1-2         |
| Check Supported Client PC and Web Browser Requirements .....          | 1-3         |
| Hardware Requirements .....   | 1-3         |
| Implementation Guidelines for Security .....                          | 1-3         |
| <br><b>2 Installation of the IBM Stack</b>                            |             |
| Check the WebSphere Application Server Settings .....                 | 2-1         |
| Authentication Cache Timeout .....                                    | 2-1         |
| Secure Configuration.....   | 2-1         |
| Create the Database Schema Owner and Data Source Users .....          | 2-1         |
| Expand the Returns Management Distribution.....                       | 2-2         |
| Obtain Third-Party Library Files Required by Returns Management ..... | 2-3         |
| Securing the JDBC for the IBM DB2 Database .....                      | 2-4         |
| Set up the JMS SSL Key Store .....                                    | 2-4         |
| Enable Data Import.....   | 2-5         |

|   |      |
|---|------|
| Oracle Configuration Manager.....                                   | 2-5  |
| Installation Options.....   | 2-5  |
| Database Install Options .....                                      | 2-5  |
| Manually Creating the Database Schema.....                          | 2-6  |
| Run the Returns Management Application Installer.....               | 2-7  |
| Resolving Errors Encountered During Application Installation.....   | 2-8  |
| Configure IBM WebSphere MQ.....                                     | 2-8  |
| Update JMS Configuration for Integration with Point-of-Service..... | 2-9  |
| Manual Deployment of the Returns Management Application .....       | 2-9  |
| Install Parameters.....   | 2-10 |
| Import Initial Parameters.....                                      | 2-10 |
| Importing Parameters Through the User Interface.....                | 2-11 |
| Importing Parameters by using an Ant Target.....                    | 2-11 |
| Load Optional Purge Procedures .....                                | 2-11 |
| Using the Returns Management Application .....                      | 2-12 |
| <br><b>A Appendix: Installer Screens for the IBM Stack</b>          |      |
| <br><b>B Appendix: Installer Silent Mode</b>                        |      |
| <br><b>C Appendix: Reinstalling Returns Management</b>              |      |
| Reinstalling Returns Management on the IBM Stack .....              | C-1  |
| <br><b>D Appendix: URL Reference</b>                                |      |
| URLs for the IBM Stack .....  | D-1  |
| JDBC URL for a Database .....                                       | D-1  |
| JNDI Provider URL for an Application .....                          | D-1  |
| <br><b>E Appendix: Common Installation Errors</b>                   |      |
| Unreadable Buttons in the Installer .....                           | E-1  |
| <br><b>F Appendix: Returns Data Loader</b>                          |      |
| Using the Returns Data Loader .....                                 | F-1  |
| <br><b>G Appendix: Best Practices for Passwords</b>                 |      |
| Password Guidelines.....  | G-1  |
| Special Security Options for IBM DB2 Databases .....                | G-2  |
| <br><b>H Appendix: Secure JDBC with IBM DB2</b>                     |      |
| Summary.....  | H-1  |
| Prerequisites.....  | H-1  |
| Setting up the Key Store.....                                       | H-2  |
| Creating a Self-signed Digital Certificate for Testing.....         | H-2  |
| Configuring the IBM DB2 Server .....                                | H-2  |
| Exporting a Certificate from iKeyman .....                          | H-4  |

|  |     |
|--|-----|
| Configuring the IBM FIPS-compliant Provider for SSL (optional) ..... | H-4 |
| Configuring Returns Management on IBM WebSphere.....                 | H-5 |
| Useful Links .....   | H-6 |
| <br><b>I Appendix: Troubleshooting</b>                               |     |
| Apache Axis2 Servlet Not Accessible.....                             | I-1 |
| <br><b>J Appendix: Installation Order</b>                            |     |
| Enterprise Installation Order .....                                  | J-1 |

## List of Figures

|      |  |      |
|------|--|------|
| A-1  | Introduction .....                         | A-1  |
| A-2  | Oracle Customer Information .....          | A-2  |
| A-3  | Requirements.....                          | A-3  |
| A-4  | License Agreement .....                    | A-3  |
| A-5  | Database Owner.....                        | A-4  |
| A-6  | Data Source User .....                     | A-5  |
| A-7  | Enable Secure JDBC .....                   | A-6  |
| A-8  | Data Source SSL Configuration .....        | A-7  |
| A-9  | Enable DIMP .....                          | A-8  |
| A-10 | DIMP Configuration.....                    | A-9  |
| A-11 | Install Database Option.....               | A-10 |
| A-12 | Default Locale.....                        | A-11 |
| A-13 | Returns Management Administrator User..... | A-12 |
| A-14 | Key Store Pass Phrase.....                 | A-13 |
| A-15 | App Server WAS_HOME .....                  | A-14 |
| A-16 | Mail Session Details .....                 | A-15 |
| A-17 | Application Server Details.....            | A-16 |
| A-18 | JMS Server Details.....                    | A-17 |
| A-19 | Select JMS SSL Level.....                  | A-18 |
| A-20 | JMS SSL Keystore Details.....              | A-19 |
| A-21 | Filter Based on Distinguished Name .....   | A-20 |
| A-22 | Distinguished Name Filter .....            | A-21 |
| A-23 | Configure WebSphere MQ Option.....         | A-22 |
| A-24 | WebSphere MQ Directory .....               | A-23 |
| A-25 | Manual Deployment Option .....             | A-24 |
| A-26 | Application Deployment Details .....       | A-25 |
| A-27 | Install Parameters Option.....             | A-26 |
| A-28 | Installation Progress .....                | A-27 |
| A-29 | Installation Complete .....                | A-27 |



**List of Tables**

|     |  |     |
|-----|--|-----|
| 1-1 | Database Server Requirements .....     | 1-2 |
| 1-2 | Application Server Requirements .....  | 1-2 |
| 1-3 | Supported Oracle Retail Products ..... | 1-2 |



---

---

## Send Us Your Comments

Oracle Retail Returns Management Installation Guide, Volume 2 - IBM Stack, Release 2.3.3

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

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

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

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

---

---

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

---

---

Send your comments to us using the electronic mail address: [retail-doc\\_us@oracle.com](mailto:retail-doc_us@oracle.com)

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

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

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



---

---

# Preface

This Installation Guide describes the requirements and procedures to install this Oracle Retail Returns Management release.

## Audience

This Installation Guide is written for the following audiences:

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

## Documentation Accessibility

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

### Accessibility of Code Examples in Documentation

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

### Accessibility of Links to External Web Sites in Documentation

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

### Access to Oracle Support

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

## Related Documents

For more information, see the following document in the Oracle Retail Returns Management Release 2.3.3 documentation set:

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

## Customer Support

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

<https://support.oracle.com>

When contacting Customer Support, please provide the following:

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

## Review Patch Documentation

When you install the application for the first time, you install either a base release (for example, 2.3) or a later patch release (for example, 2.3.3). If you are installing the base release, additional patch, and bundled hot fix releases, read the documentation for all releases that have occurred since the base release before you begin installation. Documentation for patch and bundled hot fix releases can contain critical information related to the base release, as well as information about code changes since the base release.

## Oracle Retail Documentation on the Oracle Technology Network

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

[http://www.oracle.com/technology/documentation/oracle\\_retail.html](http://www.oracle.com/technology/documentation/oracle_retail.html)

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

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

# Conventions

The following text conventions are used in this document:

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





---

# Preinstallation Tasks

This chapter describes the requirements for the IBM stack that must be met before Oracle Retail Returns Management can be installed.

---

**Note:** This is the IBM stack configuration that was tested for this release. While Returns Management may work in other configurations, this configuration was tested.

---

If you will be installing multiple Oracle Retail applications, see [Appendix J](#) for a guideline for the order in which the applications should be installed.

## Patch Contents

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

- Oracle Retail Returns Management 2.3.0.1

## Check for the Current Version of the Installation Guide

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

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

[http://www.oracle.com/technology/documentation/oracle\\_retail.html](http://www.oracle.com/technology/documentation/oracle_retail.html)

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

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

## Check Supported Database Server Requirements

[Table 1–1](#) lists the general requirements for a database server running Oracle Retail Returns Management and the versions supported for this release.

**Table 1–1 Database Server Requirements**

| Supported on     | Versions Supported   |
|------------------|--|
| Operating System | IBM SLES 11 SP 1   |
| Database         | IBM DB2 version 9.7 (64-bit) from WRS 7.1 Standard Edition |

## Required Settings for Database Installation

During database creation, the database must be set to store data in UTF-8 encoding.

## Check Supported Application Server Requirements

[Table 1–2](#) lists the general requirements for an application server capable of running Back Office and the versions supported for this release.

**Table 1–2 Application Server Requirements**

| Component                   | Version Tested  |
|-----------------------------|---|
| Operating System            | IBM SLES 11 SP 1  |
| J2EE Application Server     | IBM WebSphere ND 7.0.0.11 from WRS 7.1 Standard Edition |
| J2EE Application Server JVM | IBM JRE 1.6.0   |
| Messaging Provider          | IBM WebSphere MQ 7.0.1.3 from WRS 7.1 Standard Edition  |

## Check for SSL Certificate

Oracle Retail Returns Management is accessed through a secure HTTP connection. The installation of an SSL Certificate is required on your application server. If the certificate is not installed, warnings are displayed when trying to access Oracle Retail Returns Management.

For information on installing the SSL Certificate, refer to your application server documentation.

## Check Oracle Retail Software Dependencies

[Table 1–3](#) lists the Oracle Retail products that Oracle Retail Returns Management is integrated with and the required versions.

**Table 1–3 Supported Oracle Retail Products**

| Integrates with                | Version |
|--------------------------------|---------|
| Oracle Retail Point-of-Service | 13.3.3  |

## Check Third-Party Software Dependencies

The following third-party software must be obtained:

- The Pager Tag library must be downloaded and the `pager-taglib.jar` file must be extracted.

- The `db2jcc.jar` and `db2jcc_license_cu.jar` files must be obtained from your IBM DB2 database server.

For more information, see "Obtain Third-Party Library Files Required by Returns Management" in Chapter 2.

## Check Supported Client PC and Web Browser Requirements

The general requirements for the client system include the following:

- Adobe Acrobat Reader or another application capable of rendering Portable Data Format (PDF) files

The following web browsers are supported on Microsoft Windows XP SP2:

- Microsoft Internet Explorer 7
- Mozilla Firefox 3.6

## Hardware Requirements

Specific hardware requirements for the machines running Oracle Retail Returns Management depend on variables including the number of users, number of stores and registers, transaction volume, returns data retention period, and other applications running on the same machine.

Please note the following about the hardware requirements:

- The CPU requirement depends on variables including the operating system and middleware selected.
- The memory requirements and performance depend on variables including the operating system and middleware selected.
- 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 data retention period and so on.

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

## 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.

---

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

<https://support.oracle.com>

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

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



---

## Installation of the IBM Stack

Before proceeding, you must install the database and application server software. For a list of supported versions, see [Chapter 1](#).

During installation, the Returns Management database schema will be created and the Returns Management application will be deployed. The Java JDK that is included with the IBM WebSphere Application Server will be used to run the application.

### Check the WebSphere Application Server Settings

Some application server settings affect Returns Management processing and deployment. Verify that these settings are set correctly for your installation.

#### Authentication Cache Timeout

The Authentication Cache Timeout setting for the IBM WebSphere application server must be set correctly for Returns Management password processing. For information on how to determine the value you should use for this setting and how to set the value for the application server, refer to your IBM WebSphere documentation.

### Secure Configuration

For a secure configuration, SSL is required for login. The **Requires SSL** flag must be set in the IBM WebSphere master configuration. To set the flag:

1. From the WebSphere Administration Console, under **Security**, select **Global Security**.
2. Select Web and SIP security.
3. Select **Single Sign-on (SSO)**.
4. Select the **Requires SSL** check box.
5. To save the change to the master configuration, select **Save**.

### Create the Database Schema Owner and Data Source Users

The following recommendations should be considered for schema owners:

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

For information on best practices for passwords, see [Appendix G](#).

To create the database schema owner and data source users:

1. Log in using the database administrator user ID.

2. Create the schema owner user.

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

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

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

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

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

5. Create the data source user.

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

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

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

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

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

The installer grants the data source user access to the application database objects. If you choose **No** on the Manual Deployment Option screen, you need to grant the access after the installer completes. For more information, see "[Manual Deployment of the Returns Management Application](#)".

## Expand the Returns Management Distribution

To extract the Returns Management files:

1. Extract the ORRM-2.3.3.zip file from the Returns Management 2.3.3 distribution.
2. Log in to the UNIX server as the user who owns the WebSphere AS installation. Create a new staging directory for the Returns Management application distribution (ORRM-2.3.3.zip), for example, /tmp/orrm-staging.

---

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

---

3. Copy or upload ORRM-2.3.3.zip to the staging directory and extract its contents. The following files and directories should be created under <staging\_directory>/ORRM-2.3.3:

```
ant/  
ant-ext/  
antinstall/  
connectors/  
external-lib/
```

```
installer-resources/  
ocm-integration/  
returnsmgmt/  
.postinstall.cmd  
.postinstall.sh  
.preinstall.cmd  
.preinstall.sh  
.preinstall-oas.cmd  
.preinstall-oas.sh  
.preinstall-was.cmd  
.preinstall-was.sh  
.preinstall-wl.cmd  
.preinstall-wl.sh  
antinstall-config.xml  
build.xml  
build-common.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  
jmsconfiguration.dat  
prepare.xml  
retail-OCM-stores.zip  
wallet.xml
```

For the remainder of this chapter, *<staging\_directory>/ORRM-2.3.3* is referred to as *<INSTALL\_DIR>*.

## Obtain Third-Party Library Files Required by Returns Management

The Returns Management application uses the Pager Tag Library from JSPTags and the DB2 drivers from IBM. Before running the Returns Management application installer, you must download the necessary files from the JSPTags Web site and obtain the DB2 files from your database server.

To get the Pager Tag library:

1. Download the `pager-taglib-2.0.war` file from the JSPTags Web site:  
<http://jsptags.com/tags/navigation/pager/download.jsp>
2. Extract the `pager-taglib.jar` file from the `WEB-INF/lib` subdirectory in the `pager-taglib-2.0.war` file.
3. Copy `pager-taglib.jar` into *<INSTALL\_DIR>/external-lib/*.

To get the DB2 files:

1. Obtain the `db2jcc.jar` and `db2jcc_license_cu.jar` files from your database server at *<IBM\_DB2\_INSTALL\_DIR>*.

---

**Note:** The `db2jcc_license_cu.jar` file is needed to permit JDBC/SQLJ connectivity to the IBM DB2 database. The file is the standard license included with all editions of the IBM DB2 database.

---

2. Copy the jar files into `<INSTALL_DIR>/external-lib/`.

## Securing the JDBC for the IBM DB2 Database

On the Enable Secure JDBC screen, you select whether secure JDBC will be used for communication with the database. See [Figure A-7](#).

- If **Yes** is selected, you must install the database digital certificate into the application server truststore.
  1. Log in to the WebSphere Integrated Solutions Console (Admin Console).
  2. Expand the Security menu.
  3. Click the **SSL certificate and key management** option.
  4. In the Related Items list, click **Key stores and certificates**.
  5. Click the **NodeDefaultTrustStore** link in the list.
  6. In the Additional Properties list, click the **Signer certificates** link.
  7. Click the **Add** button.
  8. Enter a distinct alias and the full path to the certificate file on the server in the File name field. Make sure the Data type corresponds to the type in the file. The certificate should appear in the list of Signer certificates.
- If **No** is selected and you want to manually set up the secure JDBC after the installer completes, see [Appendix H](#).

## Set up the JMS SSL Key Store

Selecting US Strength or Export Strength on the Select JMS SSL Level screen requires that a CA certificate and Key Store are used for IBM WebSphere Application Server and WebSphere MQ. You can manually deploy the CA certificate and Key Store for IBM WebSphere Application Server and WebSphere MQ or you can have the installer perform the deployment.

The Key Store entry alias and the Key Store type that the installer uses are contained in the following script:

```
<INSTALL_DIR>/returnsmgmt/appservers/was/cert-env.sh
```

The default alias is `myalias`. The default type of the source Key Store is `jks`. These values can be changed in the script. The type has to be a type supported by the IBM `ikeycmd` utility.

To have the installer do the deployment, enter the details on the JMS SSL Keystore Details screen. See [Figure A-20](#).

If **Yes** is selected on the Filter Based on Distinguished Name screen, you enter the filter name on the Distinguished Name Filter screen. See [Figure A-21](#) and [Figure A-22](#). It is recommended that SSL certificates contain a distinguished name which follows the retailer's naming convention.



## Enable Data Import

Data Import (DIMP) is used by external systems to send data bundles to Returns Management for routine data loading of certain types of data. To use DIMP, you need to create a directory for the incoming bundles and a directory where the bundles are archived after being processed.

On the Enable DIMP installer screen, you select whether DIMP will be used. See [Figure A-9](#). If **Yes** is selected on the screen, you then provide the paths to the directories on the DIMP Configuration installer screen. See [Figure A-10](#).

For detailed information on DIMP, see the *Oracle Retail POS Suite 13.3.3/Merchandising Operations Management 13.2.3 Implementation Guide*.

## Oracle Configuration Manager

The Oracle Retail OCM Installer packaged with this release installs the latest version of OCM.

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

<https://support.oracle.com>

### *Oracle Configuration Manager Installer Guide (Doc ID: 1071030.1)*

This guide describes the procedures and interface of the Oracle Retail Oracle Configuration Manager Installer that a retailer runs near the completion of its installation process.

### OCM Documentation Link

[http://www.oracle.com/technology/documentation/oracle\\_retail.html](http://www.oracle.com/technology/documentation/oracle_retail.html)

## Installation Options

During installation, there are options that enable you to select whether the installer completes parts of the installation or if you want to complete those parts manually. For information on the available options, see the following sections:

- ["Database Install Options"](#)
- ["Configure IBM WebSphere MQ"](#)
- ["Manual Deployment of the Returns Management Application"](#)
- ["Install Parameters"](#)

## Database Install Options

The database schema must be created and populated before configuring the application server. On the Install Database Option screen, you select whether the installer creates and populates the database schema or if you want to do this manually.

- If you choose **Create schema with sample dataset**, the installer creates and populates the database with sample data, such as item data. This is the default selection on the screen. The sample dataset includes the minimum dataset. If you want data available to use for demonstrating Returns Management functionality after installation, you can select this option.

- If you choose **Create schema with minimum dataset**, the installer creates and populates the database with the minimum amount of data needed to launch and run Returns Management. 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. You choose this option if you want to create and populate the database schema manually. For information on manually creating and populating the database schema, see ["Manually Creating the Database Schema"](#).

---

---

**Note:** You must populate the database schema before running the installer. Otherwise, the installer will fail when configuring security.

---

---

## Manually Creating the Database Schema

To create and populate the database schema:

1. Change to the `<INSTALL_DIR>/returnsmgmt/db` directory.
2. Set the `JAVA_HOME` and `ANT_HOME` environment variables. You can use the JDK and Ant that are installed with the IBM WebSphere Application Server.

```
JAVA_HOME=<WAS_INSTALL_DIR>/Java; ANT_HOME=<INSTALL_DIR>/ant;
export JAVA_HOME ANT_HOME
```
3. Add `$JAVA_HOME/bin` and `$ANT_HOME/bin` to the front of the `PATH` environment variable.

```
PATH=$JAVA_HOME/bin:$ANT_HOME/bin:$PATH; export PATH
```
4. Expand the `returnsmgmtDBInstall.jar` file.

```
jar -xvf returnsmgmtDBInstall.jar
```
5. Modify `db.properties`.
  - a. Uncomment the DB2 properties and comment out the properties for the other vendors such as Oracle and MS-SqlServer.
  - b. Set the following properties with your database settings. The values to be set are shown in bold in the examples.

Set the hash algorithm, for example, to SHA-256.

```
# Hash Algorithm
inst.hash.algorithm=HASH_ALGORITHM
```

Enter the values for the users shown in bold in the following example:

```
inst.app.admin.user=my-pos-admin-user
inst.app.admin.password-encrypted=my-encrypted-pos-admin-password
```

```
db.user=DB_USER_ID
db.password-encrypted=**DB_PASSWORD_ENCRYPTED**
```

```
db.owner.user=DB_OWNER_USER_ID
db.owner.password-encrypted=**DB_OWNER_PASSWORD_ENCRYPTED**
```

The ant target will prompt for the passwords. Run the following ant target to encrypt the passwords:

```
ant -f db.xml encrypt-webapp-passwords
```

Enter the values for the URL used by the Returns Management application to access the database schema. See [Appendix D](#) for the expected syntax:

```
db.jdbc-url=jdbc:db2://DB_HOST_NAME:50001/DB_NAME
```

Enter the value for the store ID shown in the following example:

```
configured.store.id=04241
```

Enter the value for the supported locales shown in the following example:

```
gen.locales=
```

- c. Set the host name and port number for the `parameters.apphost` property to point to your Returns Management installation.

```
parameters.apphost=t3://localhost:<rm_i_port_number>
```

- d. In the `parameters.classpath` property, replace the semicolons used as separators with colons. This is needed to run with UNIX systems.

- 6. Uncomment the following properties in `jndi.properties`. This file is in the `jndi` directory.

```
java.naming.factory.initial=com.evermind.server.rmi.RMIInitialContextFactory
java.naming.security.principal=<user>
java.naming.security.credentials=<user>
```

- 7. Run one of the available Ant targets to create the database schema and load data:

- `load_sample`: creates the database schema containing the sample dataset. The sample dataset includes the minimum dataset.
- `load_minimum`: creates the database schema containing the minimum dataset.

For example: `ws_ant load_sample`

## Run the Returns Management Application Installer

The installer will configure and deploy the Returns Management application. Before running the installer, verify that a profile has been created and the IBM WebSphere application server is running.

---

**Note:** To see details on every screen and field in the application installer, see [Appendix A](#).

---

1. Change to the `<INSTALL_DIR>` directory.
2. Set the `JAVA_HOME` environment variable to point to the Java in the IBM WebSphere application server, that is, `<WAS_INSTALL_DIR>/Java`.

---

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

---

3. If you are using an X server such as Xceed, set the DISPLAY environment variable so that you can run the installer in GUI mode (recommended). If you are not using an X server, or the GUI is too slow over your network, unset DISPLAY for text mode or use the `install.sh` script.

---

**Caution:** Password fields are masked in GUI mode, but in text mode your input is shown in plain text in the console window.

---

4. Run the installer.
  - a. Log into the UNIX server as a user who is authorized to install software.
  - b. Change the mode of all `.sh` files to executable.
  - c. Run the `install.sh` script. This will launch the installer.

---

**Note:** The usage details for `install.sh` are shown below. The typical usage for GUI mode does not use arguments.

```
install.sh [text | silent webspHERE]
```

---

After installation is complete, a detailed installation log file is created:  
`orrm-install-app.<timestamp>.log`

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

## Resolving Errors Encountered During Application Installation

If the application installer encounters any errors, it will halt execution immediately. You can run the installer in silent mode so that you do not have to reenter the settings for your environment. For instructions on silent mode, see [Appendix B](#).

For a list of common installation errors, see [Appendix E](#).

Since the application installation is a full reinstall every time, any previous partial installs will be overwritten by the successful installation.

## Configure IBM WebSphere MQ

IBM WebSphere MQ must be configured with a queue manager and the JMS queues and topics required by Returns Management, before Returns Management can be deployed. On the Configure MQ Series Option screen, you select whether the installer configures IBM WebSphere MQ or if you manually configure it.

---

**Note:** If IBM WebSphere MQ is installed on a different machine than IBM WebSphere Application Server, you must manually configure it.

---

Typically, when IBM WebSphere MQ is installed, a special user ID (usually `mqm`), and a user group (also `mqm`) are created in the operating system. The MQ installation files and directories have their owner and group set to the IBM WebSphere MQ user ID and group ID.

The user ID used for the Returns Management installation, must be made a member of IBM WebSphere MQ's user group, before attempting to create the Returns Management queue manager, queues, and topics. For example, if Returns Management is installed as user `root`, then `root` must be made a member of the `mqm` group.

Use the following commands to configure IBM WebSphere MQ. `MQ_Install_Dir` is the directory where IBM WebSphere MQ was installed. The values for `<input.jms.server.queue>` and `<input.jms.server.port>` come from the `ant.install.properties` file.

```
<MQ_Install_Dir>/bin/crtmqm    -q <input.jms.server.queue>
<MQ_Install_Dir>/bin/strmqm    <input.jms.server.queue>
<MQ_Install_Dir>/bin/runmqslr -m <input.jms.server.queue> -p
    <input.jms.server.port> -t tcp &
<MQ_Install_Dir>/bin/runmqsc    <input.jms.server.queue> <
    <INSTALL_DIR>/returnsmgmt/appserver/was/createq.dat

<MQ_Install_Dir>/bin/runmqsc    <input.jms.server.queue> <
    <MQ_Install_Dir>/java/bin/MQJMS_PSQ.mqsc
<MQ_Install_Dir>/bin/strmqbrk  -m <input.jms.server.queue>
```

## Update JMS Configuration for Integration with Point-of-Service

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

---

**Note:** To use the remote queue, updates are also needed to the JMS configuration for Back Office and Point-of-Service. For more information, see the following guides:

- *Oracle Retail Back Office Installation Guide, Volume 2 - IBM Stack*
  - *Oracle Retail Point-of-Service Installation Guide, Volume 2 - IBM Stack*
- 

To update the Returns Management JMS configuration:

```
DEFINE CHANNEL ('BO.TO.RM') CHLTYPE(RCVR) TRPTYPE(tcp)
```

## Manual Deployment of the Returns Management Application

Skip this section if you chose the default option of allowing the installer to complete installation to the application server.

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>/returnsmgmt/configured-output/`.

If you chose this installer option, you can deploy the Returns Management ear file by following these steps:

- To deploy using the ant target:
  1. Check that the Key Store connector JNDI name in the `<WAS_PROFILE_DIR>/installedApps/<hostnameNodeNNCell>/applib/spring.properties` file matches the JNDI name of the Key Store connector deployed on the application server.
  2. Update the following property in the `ant.install.properties` file.  

```
input.install.to.appserver = true
```
  3. Run the following ant target:  

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

- To deploy from the application server console:

---

**Note:** When deploying the ear 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.

---

1. Move your ear file to `<INSTALL_DIR>/returnsmgmt/ear`.
2. Change to the `<INSTALL_DIR>` directory.
3. Configure the ear file.  

```
./install.cmd ant init configure
```
4. Manually deploy the ear file from the following location:  
`<INSTALL_DIR>/returnsmgmt/returnsmgmt.ear`

## Install Parameters

The application parameters must be installed before the Returns Management application is fully operational. On the Install Parameters screen, you select whether the installer completes installation of the parameters or if you want to do this manually.

- If you chose Yes, you do not need to perform any further steps to install the parameters. This is the default selection on the screen.
- If you chose No, the installer did not install the parameters. For information on installing the parameters, see ["Import Initial Parameters"](#).

## Import Initial Parameters

---

**Note:** If you did not choose to have the installer set the initial parameters, you must import an initial set of parameters before you can use Returns Management. For more information on parameters, see the *Oracle Retail POS Suite Configuration Guide*.

---

This section provides an overview of the procedures for importing an initial set of parameters. You can import the parameters through the Returns Management user interface or by using an Ant target. You only need to use one of the procedures. The procedure for importing parameters through the application user interface is described in more detail in the *Oracle Retail Returns Management User Guide*.

These instructions assume you have already expanded the `centralofficeDBInstall.jar` file under the `<INSTALL_DIR>` directory as part of the database schema installation earlier in this chapter.

## Importing Parameters Through the User Interface

To import the initial parameters through the user interface:

1. Open the Returns Management application in a web browser. The address is provided at the end of the installer output and in the log file.  
`http://<your host name>:<your port number>/<context root>`
2. Log in to the application with a user ID that has full administrative rights.
3. Click the **Data Management** tab. The Available Imports screen appears.
4. To import the master parameter set, click the **File** link in the Import Parameters for Distribution row. Follow the instructions to import `parameterset.xml` from the `<INSTALL_DIR>/returnsmgmt/configured-output/db` directory.
5. To import the initial set of Returns Management application parameters, click the **File** link in the Import Application Parameters row. Follow the instructions to import `returnsmgmt.xml` from the `<INSTALL_DIR>/returnsmgmt/configured-output/db` directory.

## Importing Parameters by using an Ant Target

To import parameters using an Ant target:

1. Change to the `<INSTALL_DIR>/returnsmgmt/configured-output/db` directory.
2. Execute the following command:  
`ws_ant load_parameters`

## Load Optional Purge Procedures

For information on how to invoke the procedures provided for purging aged data, see the *Oracle Retail Returns Management Operations Guide*.

To load the purge procedures:

1. Run the available Ant target to load the procedures.  
`ws_ant load_purge_procedures`
2. Log in as the database schema owner, `<schema_username>`.
3. Create a user for running the purge procedures. This user should only have the privileges required to run the purge procedures.

## Using the Returns Management Application

---

---

**Note:** When you are done installing Returns Management, log out and close the browser window. This ensures that your session information is cleared and prevents another user from accessing Returns Management with your login information.

---

---

After the application installer completes and you have run the initial parameter load, you should have a working Returns Management application installation. To launch the application, open a web browser and go to

`https://<servername>:<portnumber>/<context root>`

For example, `https://myhost:9443/returnsmanagement`

---

---

**Note:** The installer created and started the MQ queue manager. If you restart WebSphere, you must also restart the MQ queue manager.

---

---



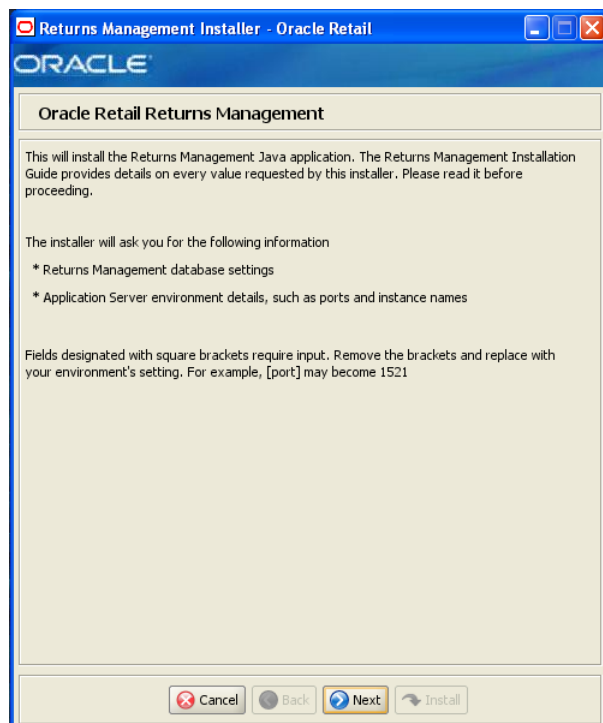
# A

## Appendix: Installer Screens for the IBM Stack

You need the following details about your environment for the installer to successfully deploy the Returns Management application on the IBM stack. Depending on the options you select, you may not see some screens or fields.

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

**Figure A-1** Introduction



**Figure A-2 Oracle Customer Information**

The screenshot shows a window titled "Returns Management Installer - Oracle Retail". Inside, there's a section titled "ORACLE" and "Oracle Customer Information". Below this, a message states: "Provide your email address to be informed of security issues, install the product and initiate configuration manager. See <http://www.oracle.com/support/policies.html> for details." There are three input fields: "Email:" with the placeholder "[username@oracle.com]", "I wish to receive security updates via My Oracle Support." with a checked checkbox, and "My Oracle Support Password:". At the bottom, there are four buttons: "Cancel", "Back", "Next", and "Install".

This screen is only displayed if Oracle Configuration Manager (OCM) is to be installed. The OCM collector must be registered with your My Oracle Support account so that the uploaded configuration information can be stored properly and be readily available during the resolution of a service request.

After the Returns Management installer completes, the OCM installer runs if OCM is not already installed. For information on OCM, see "[Oracle Configuration Manager](#)" in [Chapter 2](#).

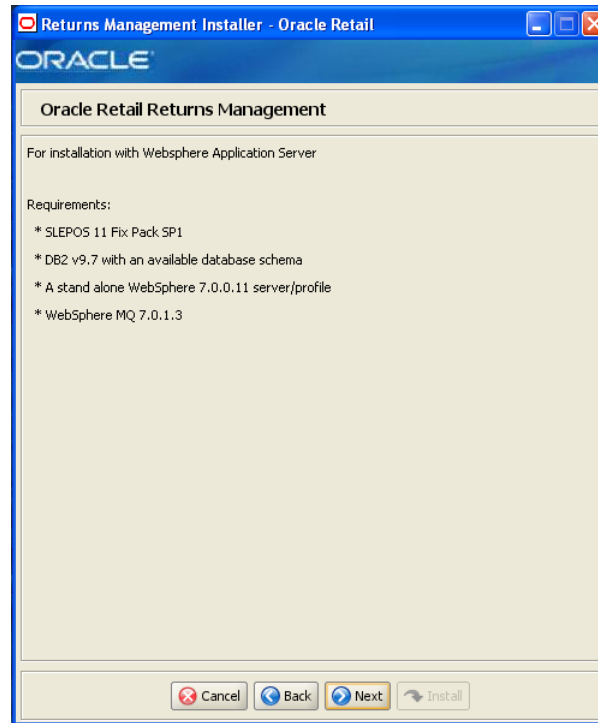
The fields on this screen are described in the following tables.

| Field Title       | Email                                      |
|-------------------|--|
| Field Description | Email address to use for OCM installation. |

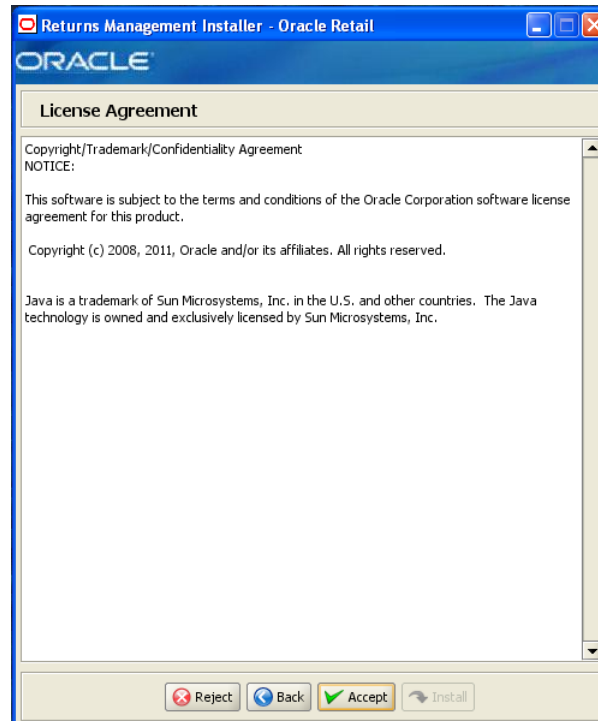
| Field Title       | I wish to receive security updates via My Oracle Support. |
|-------------------|---|
| Field Description | To receive security updates, check the box.               |

| Field Title       | My Oracle Support Password   |
|-------------------|--|
| Field Description | Password for the My Oracle Support user to receive security updates. |

**Figure A-3 Requirements**



**Figure A-4 License Agreement**



---

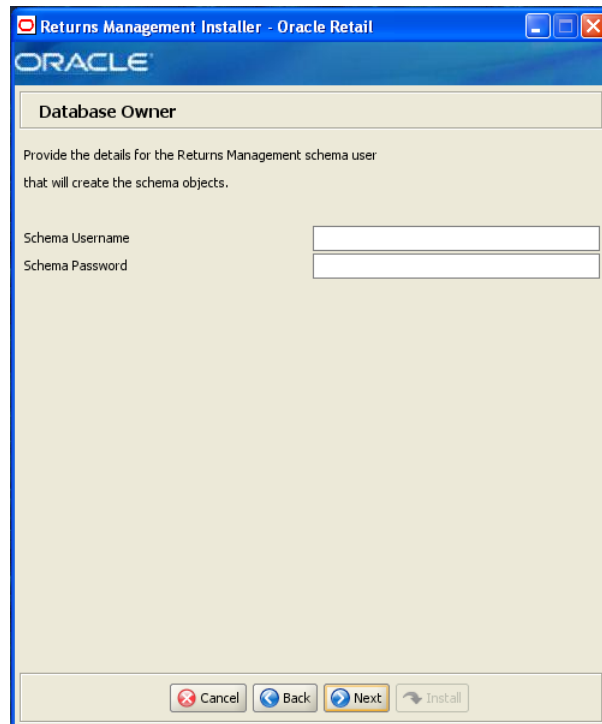
---

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

---

---

**Figure A–5 Database Owner**



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

| Field Title       | Schema Username  |
|-------------------|--|
| Field Description | Schema user name that manages the objects in the schema. This user has Create, Drop, and Alter privileges in the schema, that is, Data Definition Language (DDL) execution privileges. For information on creating this user, see <a href="#">"Create the Database Schema Owner and Data Source Users"</a> in <a href="#">Chapter 2</a> .<br><br><b>Note:</b> This user creates the database objects used by Returns Management. |
| Example           | DBOWNER  |

| Field Title       | Schema Password                  |
|-------------------|----------------------------------|
| Field Description | Password for the database owner. |

Figure A-6 Data Source User

Returns Management Installer - Oracle Retail

ORACLE

**Data Source User**

Provide the details for the Returns Management schema user

JDBC URL

Data Source Username

Data Source Password

Cancel Back Next Install

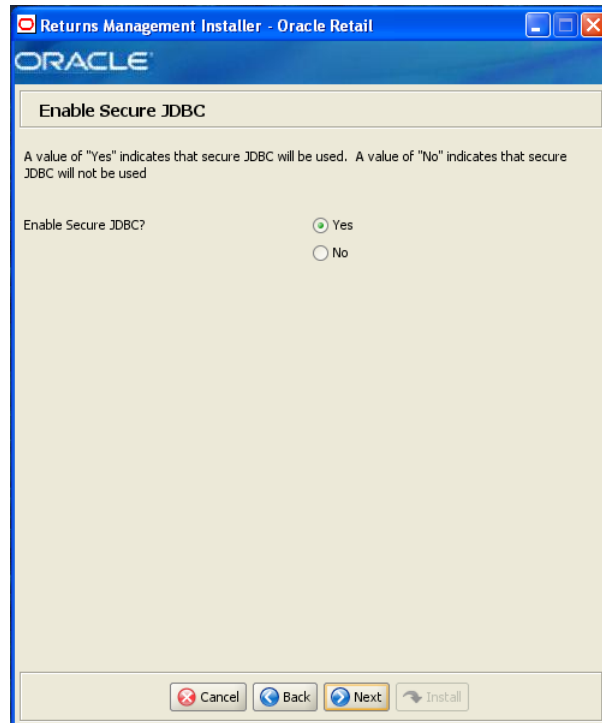
The fields on this screen are described in the following tables.

| Field Title       | JDBC URL  |
|-------------------|---|
| Field Description | URL used by the Returns Management application to access the database schema. See <a href="#">Appendix D</a> for the expected syntax. |
| Example           | jdbc:db2://[host]:[tcpPort]/[dbname]  |

| 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 " <a href="#">Create the Database Schema Owner and Data Source Users</a> " in <a href="#">Chapter 2</a> . |
|                   | <b>Note:</b> This schema user is used by Returns Management to access the database.  |
| Example           | DBUSER   |

| Field Title       | Data Source Password               |
|-------------------|------------------------------------|
| Field Description | Password for the data source user. |

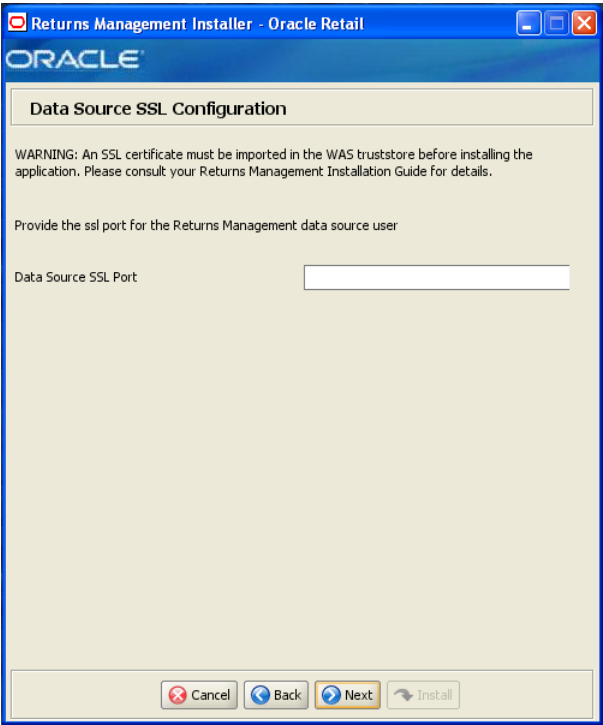
**Figure A-7 Enable Secure JDBC**



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

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

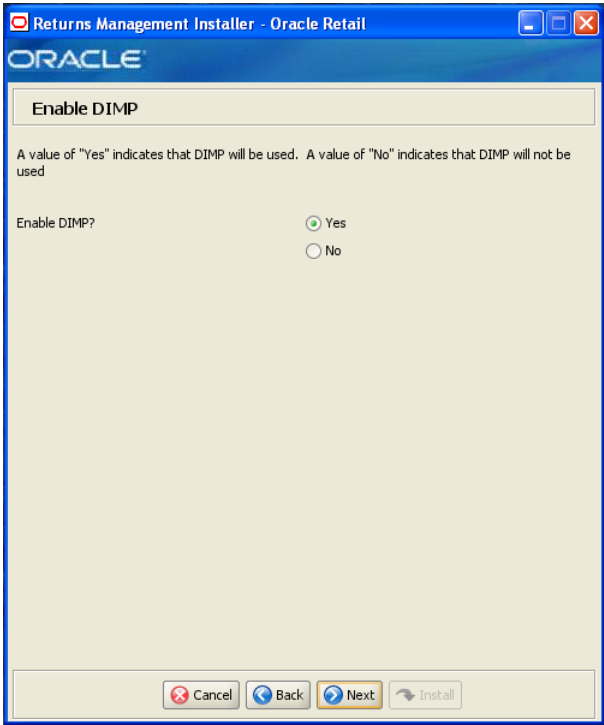
**Figure A–8 Data Source SSL Configuration**



This screen is only displayed if **Yes** is selected on the Enable Secure JDBC screen. The field on this screen is described in the following table.

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

Figure A-9 Enable DIMP

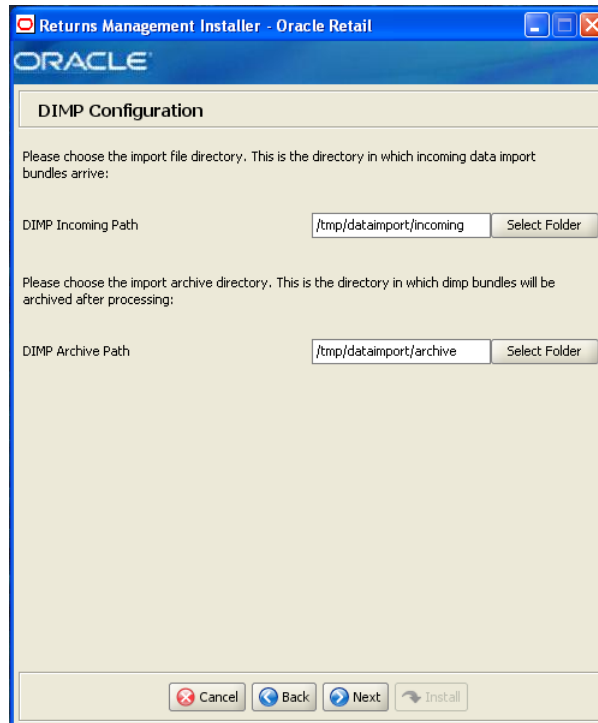


The field on this screen is described in the following table.

| Field Title       | Enable DIMP?   |
|-------------------|--|
| Field Description | Select whether DIMP will be used. For information on DIMP, see <a href="#">"Enable Data Import"</a> in <a href="#">Chapter 2</a> . |
| Example           | Yes  |



**Figure A–10 DIMP Configuration**



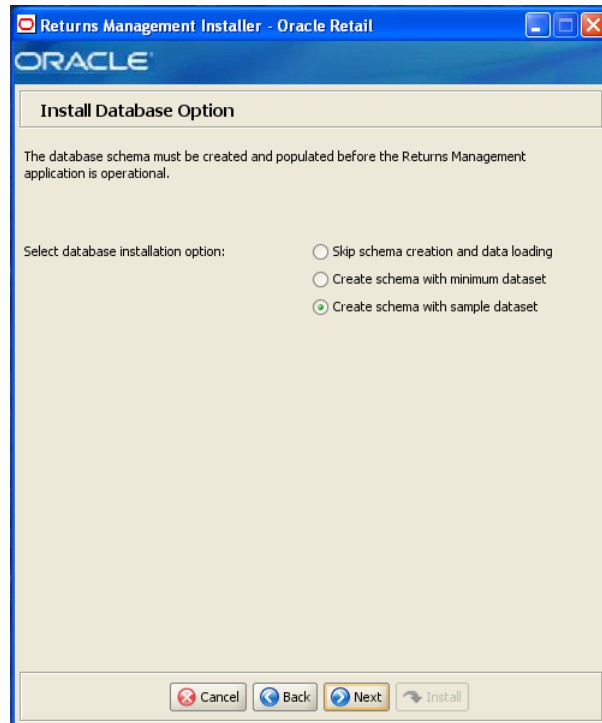
This screen is only displayed if **Yes** is selected on the Enable DIMP screen.

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

| Field Title       | DIMP Incoming Path                                       |
|-------------------|--|
| Field Description | Directory where the incoming data import bundles arrive. |
| Example           | /tmp/dataimport/incoming                                 |

| Field Title       | DIMP Archive Path   |
|-------------------|---|
| Field Description | Directory where the incoming data import bundles are archived after processing. |
| Example           | /tmp/dataimport/archive   |

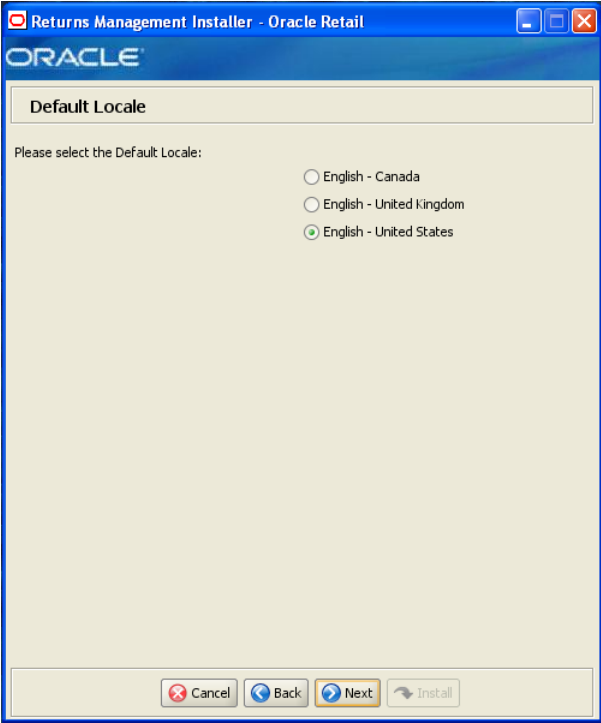
**Figure A–11 Install Database Option**



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

| Field Title       | Select database installation option  |
|-------------------|--|
| Field Description | <p>The database schema must be created and populated before starting Returns Management. This screen gives you the option to have the installer create and populate the database schema or leave the database schema unmodified.</p> <ul style="list-style-type: none"><li>■ To have the installer leave the database schema unchanged, select <b>Skip schema creation and data loading</b>.</li><li>■ To have the installer create and populate the database schema with the minimum dataset, select <b>Create schema with minimum dataset</b>.</li><li>■ To have the installer create and populate the database schema with the sample dataset, select <b>Create schema with sample dataset</b>.</li></ul> <p>For more information, see "<a href="#">Database Install Options</a>" in <a href="#">Chapter 2</a>.</p> |
| Example           | Yes  |

Figure A-12 Default Locale



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

| Field Title       | Please select the Default Locale   |
|-------------------|--|
| Field Description | Limited locale support in Returns Management enables the date, time, currency, and calendar to be displayed in the format for the selected default locale.<br><br><b>Note:</b> The only language currently supported is United States English. |
| Example           | English - United States  |

**Figure A-13 Returns Management Administrator User**

Returns Management Installer - Oracle Retail

ORACLE

**Returns Management Administrator User**

Enter the username and password for the Returns Management administrator account

The password must satisfy the following criteria:

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

Returns Management Admin Username: pos

Returns Management Admin Password:

Cancel Back Next Install

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

| Field Title       | Returns Management AdminUsername   |
|-------------------|--|
| Field Description | User name used for performing Returns Management administrative functions. |
| Example           | pos  |

| Field Title       | Returns Management Admin Password    |
|-------------------|--------------------------------------|
| Field Description | Password for the administrator user. |

Figure A-14 Key Store Pass Phrase

Returns Management Installer - Oracle Retail

ORACLE

**Key Store Pass Phrase**

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

The pass phrase must satisfy the following criteria:

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

Hash Algorithm: SHA-256

Pass Phrase:

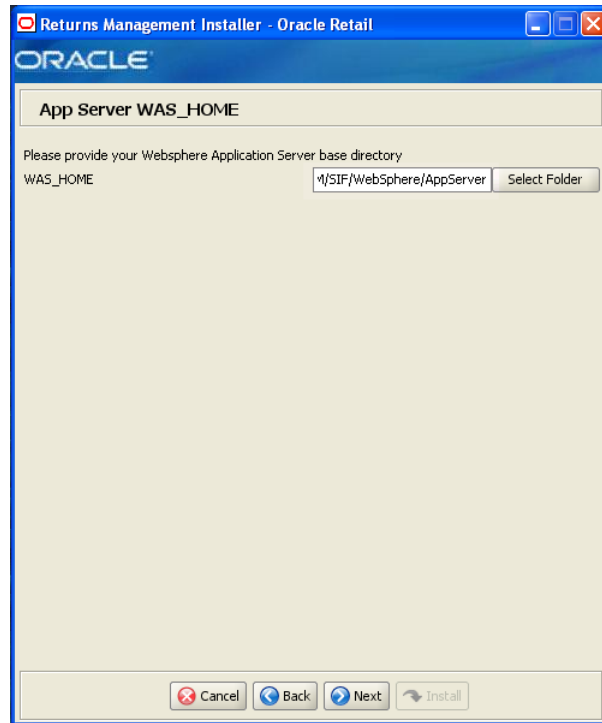
Cancel Back Next Install

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

| Field Title       | Hash Algorithm  |
|-------------------|---|
| Field Description | Enter the name of the algorithm used to hash passwords. |
| Example           | SHA-256   |

| Field Title       | Pass Phrase  |
|-------------------|--|
| Field Description | Enter the pass phrase used for the Key Store simulator.<br><b>Note:</b> Use the same pass phrase for all Oracle Retail POS Suite applications in your configuration. |

**Figure A-15 App Server WAS\_HOME**



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

| Field Title       | WAS_HOME  |
|-------------------|---|
| Field Description | Base directory for the IBM WebSphere Application Server installation. |
| Example           | /opt/IBM/SIF/WebSphere/AppServer                                      |

**Figure A-16 Mail Session Details**

Returns Management Installer - Oracle Retail

ORACLE

**Mail Session Details**

Please provide mail server details for the Returns Management application

SMTP host: mail.example.com

From Address: admin@example.com

Cancel Back Next Install

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

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

| Field Title       | From Address   |
|-------------------|--|
| Field Description | From address in e-mails generated by Returns Management. |
| Example           | admin@example.com  |

**Figure A-17 Application Server Details**

The screenshot shows a window titled "Returns Management Installer - Oracle Retail". Inside, there's a tab labeled "Application Server Details". Below the tab, there are several input fields with labels to their left: "Server Name" (containing "server1"), "Node Name" (empty), "Cell Name" (empty), "IIOP Port" (containing "2809"), "Server Profile" (empty), and "Timezone" (containing "America/Chicago"). At the bottom of the window, there are four buttons: "Cancel", "Back", "Next", and "Install".

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

| Field Title       | Server Name                       |
|-------------------|-----------------------------------|
| Field Description | Name of the IBM WebSphere server. |
| Example           | server1                           |

| Field Title       | Node Name                       |
|-------------------|---------------------------------|
| Field Description | Name of the IBM WebSphere node. |
| Example           | myhostNode01                    |

| Field Title       | Cell Name                       |
|-------------------|---------------------------------|
| Field Description | Name of the IBM WebSphere cell. |
| Example           | myhostNode01Cell                |

| Field Title       | IIOP port   |
|-------------------|---|
| Field Description | IIOP/BOOTSTRAP_ADDRESS port of the IBM WebSphere server. This port can be found in the following file:<br><WAS_PROFILE_DIR>/logs/AboutThisProfile.txt |
| Example           | 2809  |



| Field Title       | Server Profile                     |
|-------------------|------------------------------------|
| Field Description | Name of the IBM WebSphere profile. |
| Example           | AppSrv01                           |

| Field Title       | Timezone                                |
|-------------------|---|
| Field Description | Time zone where this server is running. |
| Example           | America/Chicago                         |

**Figure A-18 JMS Server Details**

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

| Field Title       | JMS Host Name   |
|-------------------|---|
| Field Description | Name of the JMS server.<br><br><b>Note:</b> Always use the actual host name and not the IP address or "localhost". There may be problems integrating with Point-of-Service if the actual host name is not used. |
| Example           | myhost  |

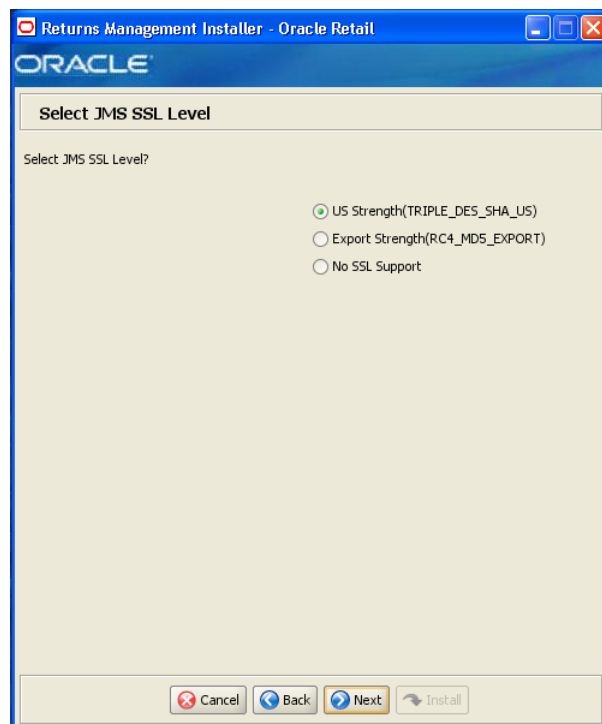
| Field Title       | JMS Port                            |
|-------------------|-------------------------------------|
| Field Description | Port number used by the JMS server. |
| Example           | 1415                                |

| Field Title       | JMS Username   |
|-------------------|--|
| Field Description | User name for the JMS server. This user must exist in the Returns Management schema. |
| Example           | myuser   |

| Field Title       | JMS Password                 |
|-------------------|------------------------------|
| Field Description | Password for the JMS server. |

| Field Title       | JMS Queue Manager              |
|-------------------|--------------------------------|
| Field Description | Name of the JMS queue manager. |
| Example           | rm.queue.manager               |

**Figure A–19** *Select JMS SSL Level*



The field on this screen is described in the following table. For more information, see ["Set up the JMS SSL Key Store" in Chapter 2](#).

| Field Title       | Select JMS SSL Level   |
|-------------------|--|
| Field Description | JMS SSL level to be used. <ul style="list-style-type: none"> <li>To use US strength, select <b>US Strength(TRIPLE_DES_SHA_US)</b>.</li> <li>To use export strength, select <b>Export Strength(RC4_MDS_EXPORT)</b>.</li> <li>To not use ssl support, select <b>No SSL Support</b>.</li> </ul> |
| Example           | US Strength(TRIPLE_DES_SHA_US)   |

**Figure A–20 JMS SSL Keystore Details**

Central Office Installer - Oracle Retail

ORACLE

**JMS SSL Keystore Details**

what are the passwords for the Keystore

Keystore Details

Corporate CA Certificate File

MQ Keystore Password

MQ Source Keystore

Password for MQ Source Keystore

WebSphere Keystore Password

WebSphere Source Keystore

Password for WebSphere Source Keystore

Note: The MQ source keystore must be in a directory accessible by the MQ user and the MQ user must have read permissions for the file.

This screen is only displayed if **US Strength(TRIPLE\_DES\_SHA\_US)** or **Export Strength(RC4\_MDS\_EXPORT)** is selected on the Select JMS SSL Level screen.

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

| Field Title       | Corporate CA Certificate File               |
|-------------------|---|
| Field Description | Location of the corporate certificate file. |
| Example           | /tmp/root-cert.pem                          |

| Field Title       | MQ Keystore Password                 |
|-------------------|--------------------------------------|
| Field Description | Key Store password for WebSphere MQ. |

| Field Title       | MQ Source Keystore                                 |
|-------------------|--|
| Field Description | Location of the source Key Store for WebSphere MQ. |
| Example           | /tmp/mq-keystore.jks                               |

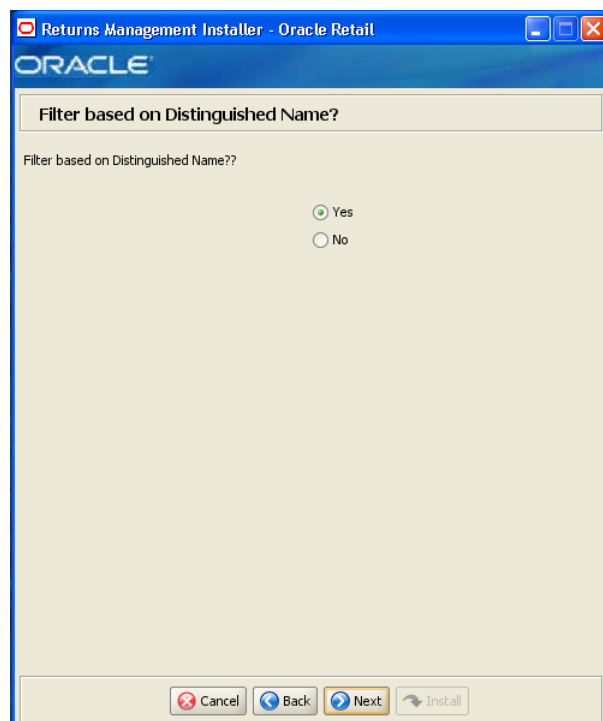
| Field Title       | Password for MQ Source Keystore   |
|-------------------|-----------------------------------|
| Field Description | Key Store password for MQ source. |

| Field Title       | WebSphere Keystore Password                              |
|-------------------|--|
| Field Description | Key Store password for the WebSphere Application Server. |

| Field Title       | WebSphere Source Keystore                       |
|-------------------|---|
| Field Description | Location of the source Key Store for WebSphere. |
| Example           | /tmp/was-keystore.jks                           |

| Field Title       | Password for WebSphere Source Keystore |
|-------------------|--|
| Field Description | Key Store password for WebSphere.      |

**Figure A-21 Filter Based on Distinguished Name**



This screen is only displayed if **US Strength(TRIPLE\_DES\_SHA\_US)** or **Export Strength(RC4\_MDS\_EXPORT)** is selected on the Select JMS SSL Level screen.

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

| Field Title       | Filter based on Distinguished Name?   |
|-------------------|---|
| Field Description | This screen gives you the option to filter based on the distinguished name. |
| Example           | Yes   |

**Figure A-22 Distinguished Name Filter**

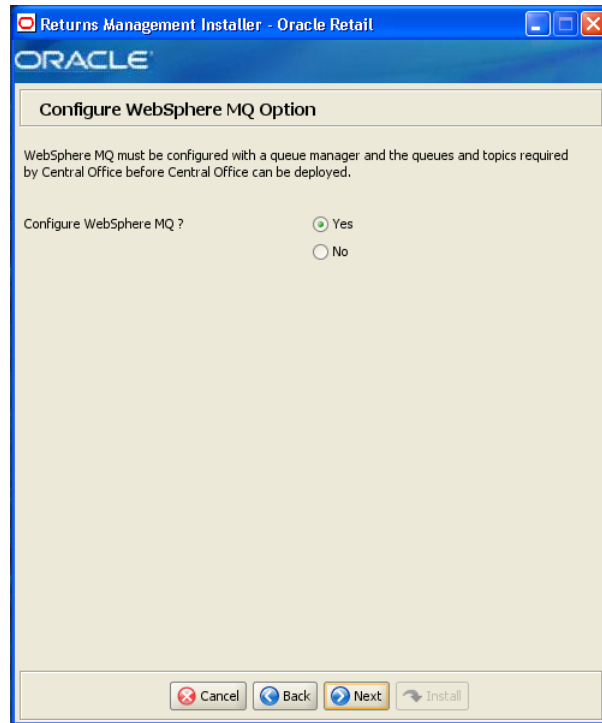


This screen is only displayed if **Yes** is selected on the Filter based on Distinguished Name screen.

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

| Field Title       | Filter Value                               |
|-------------------|--|
| Field Description | Distinguished name for the JMS SSL filter. |
| Example           | CN=rm.server.example.com                   |

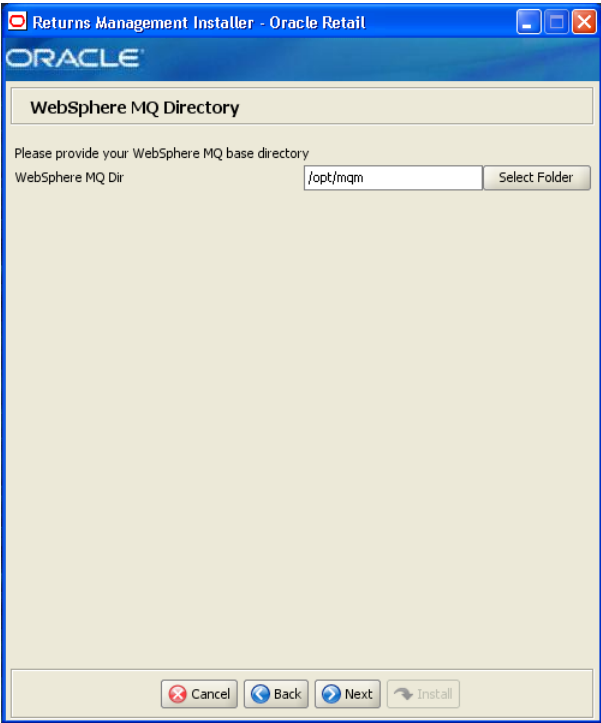
**Figure A-23 Configure WebSphere MQ Option**



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

| Field Title       | Configure WebSphere MQ?   |
|-------------------|---|
| Field Description | IBM WebSphere MQ must be configured with a queue manager and the queues and topics required by Returns Management before Returns Management can be deployed. This screen gives you the option to configure IBM WebSphere MQ manually. If you choose No, there are manual steps you need to perform after the installer completes. See <a href="#">"Configure IBM WebSphere MQ"</a> in <a href="#">Chapter 2</a> . |
| Example           | Yes   |

**Figure A–24    WebSphere MQ Directory**

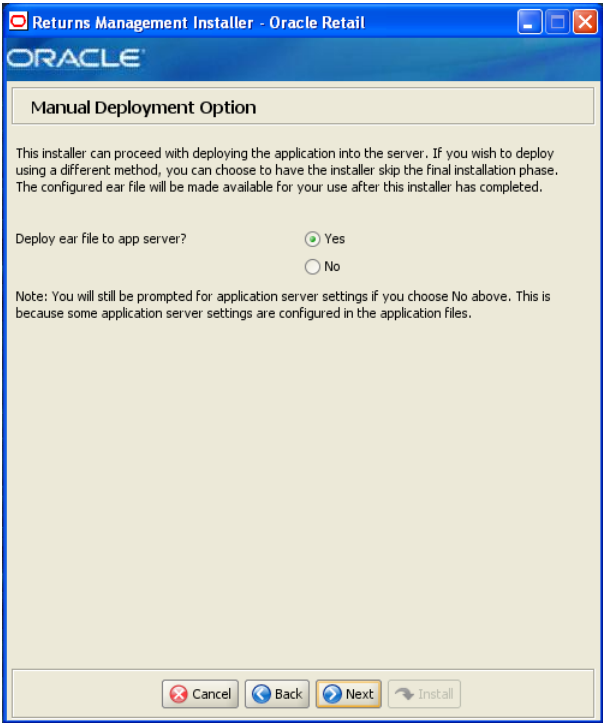


This screen is only displayed if **Yes** is selected on the Configure WebSphere MQ Option screen.

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

| Field Title       | WebSphere MQ Dir                     |
|-------------------|--------------------------------------|
| Field Description | Base directory for IBM WebSphere MQ. |
| Example           | /opt/mqm                             |

Figure A-25 Manual Deployment Option



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

| Field Title       | Install files to app server?   |
|-------------------|--|
| Field Description | <p>By default, the installer will deploy the ear file and copy files under the application server ORACLE_HOME. This screen gives you the option to leave ORACLE_HOME 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 ORACLE_HOME must be reviewed by another party before being applied.</p> <p>If you choose No, see <a href="#">"Manual Deployment of the Returns Management Application"</a> in <a href="#">Chapter 2</a> for the manual steps you need to perform after the installer completes.</p> |
| Example           | Yes  |



**Figure A–26 Application Deployment Details**

Central Office Installer - Oracle Retail

ORACLE

**Application Deployment Details**

The default values shown below are examples

Enter the deployment name for the Returns Management application. This is the name by which the application will be identified in the application server.

App Deployment Name

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

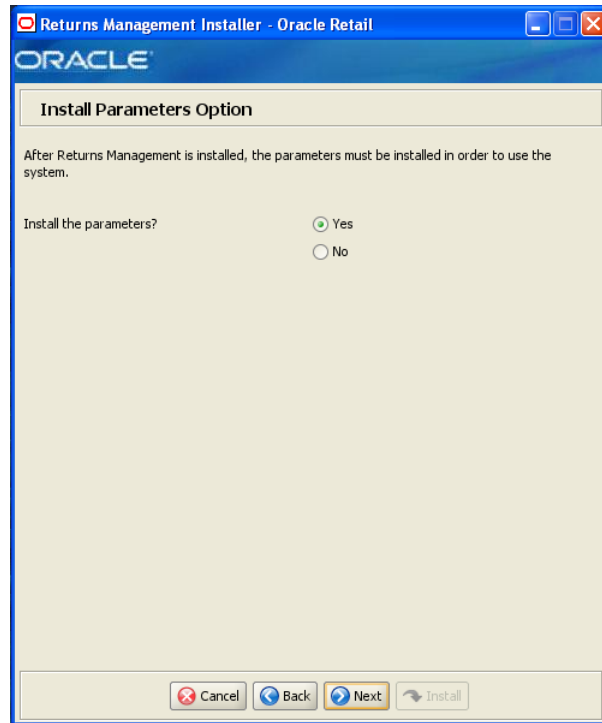
Context Root

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

| Field Title       | App Deployment Name   |
|-------------------|---|
| Field Description | Name by which this Returns Management application will be identified in the application server. |
| Example           | ReturnsManagement   |

| Field Title       | Context Root   |
|-------------------|--|
| Field Description | Path under the HTTP URL that will be used to access the Returns Management application. For example, a context root of 'returnsmanagement' will result in the application being accessed at https://<host>:<port>/returnsmanagement/index.jsp. |
| Example           | returnsmanagement  |

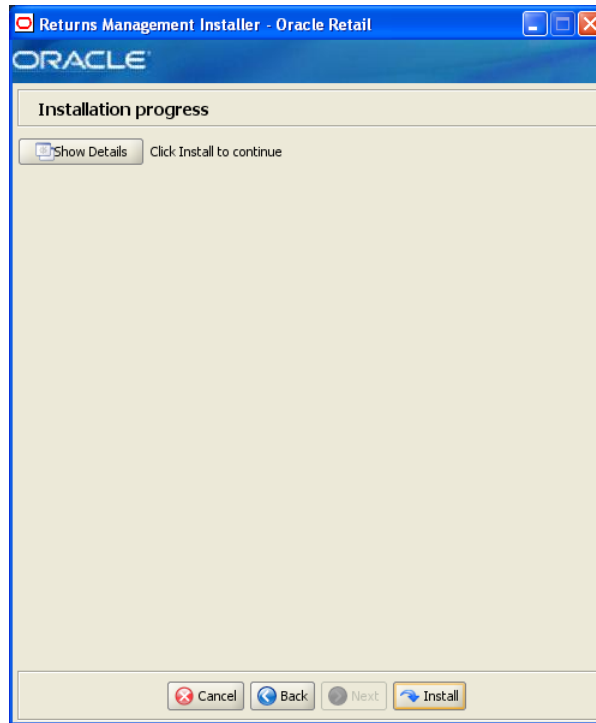
**Figure A-27** *Install Parameters Option*



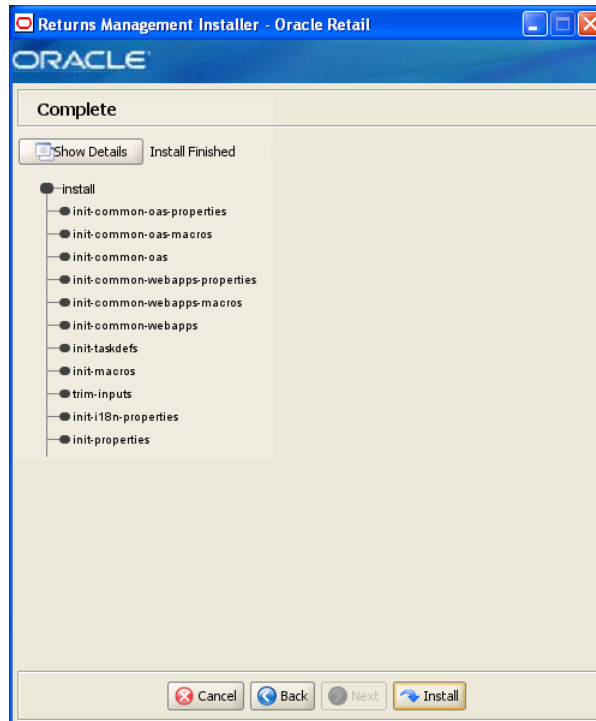
The field on this screen is described in the following table.

| Field Title       | Install the parameters?  |
|-------------------|--|
| Field Description | The application parameters must be set up before Returns Management can be used. This screen gives you the option to set up the parameters manually. If you choose No, see <a href="#">"Install Parameters"</a> in <a href="#">Chapter 2</a> for the manual steps you need to perform after the installer completes. |
| Example           | Yes  |

**Figure A–28 Installation Progress**



**Figure A–29 Installation Complete**



After the installer completes, the Oracle Configuration Manager (OCM) installer runs if OCM is not already installed. For information on OCM, see ["Oracle Configuration Manager"](#) in [Chapter 2](#).



---

## Appendix: Installer Silent Mode

In addition to the GUI and text interfaces of the Returns Management installer, there is a silent mode that can be run. This mode is useful if you wish to run a repeat installation without reentering the settings you provided in the 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. Edit the `ant.install.properties` file and correct any invalid settings that may have caused the installer to fail in its previous run.
2. If the previous install was successful, the `cwallet.sso` file is found in the installation directory for that install. Copy the `cwallet.sso` file to `<INSTALL_DIR>` for this silent install.
3. Run the installer again with the silent argument.

```
install.sh silent websphere
```



---

## Appendix: Reinstalling Returns Management

Returns Management does not provide the capability to uninstall and reinstall the application. If you need to run the Returns Management installer again, perform the following steps.

### Reinstalling Returns Management on the IBM Stack

To reinstall:

1. Stop the WebSphere application server in the profile that contains Returns Management.
2. Delete the profile.
3. Stop the WebSphere MQ queue manager (for example, `rm.queue.manager`) and listener.
4. Delete the queue manager.
5. Recreate the profile.
6. Start the WebSphere application server in the profile.
7. Run the Returns Management installer. For more information, see "[Run the Returns Management Application Installer](#)" in [Chapter 2](#).





---

## Appendix: URL Reference

Both the database schema and application installers for the Returns Management product will ask for several different URLs. These include the following.

### URLs for the IBM Stack

The following URLs are used for the IBM stack.

### JDBC URL for a Database

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

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

- `<dbhost>`: hostname of the database server
- `<dbport>`: database listener port
- `<dbname>`: system identifier for the database

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

### JNDI Provider URL for an Application

Used for server-to-server calls between applications.

Syntax: `corbaloc:iiop:<host>:<iiopport>`

- `<host>`: hostname of the WebSphere server
- `<iiopport>`: IIOP/BOOTSTRAP\_ADDRESS port of the WebSphere server. This can be found in the `<WAS_HOME>/profiles/<profile_name>/properties/portdef.props` file.

For example, `corbaloc:iiop:myhost:2809`



---

## Appendix: Common Installation Errors

This appendix describes some common errors encountered during installation of Returns Management.

### Unreadable Buttons in the Installer

If you are unable to read the text within the installer buttons, it probably means that your JAVA\_HOME needs to be set to a version 1.6 JDK. Set JAVA\_HOME to a Java development kit of version 1.6 or later and run the installer again.



## Appendix: Returns Data Loader

The Oracle Retail Returns Management installation includes return ticket data, in XML format, which you can optionally load into the Returns Management database. There are several reasons why you would want to load this data:

- Once return tickets are loaded into the database, you can use the data to get familiar with those parts of the user interface that deal with return tickets, such as, searching for return tickets.
- Loading the return tickets acts as an end-to-end test of the Oracle Retail Returns Management software installation, from the web services interface up to the back-end database.
- The return ticket data is good sample data that can be used as a starting point for customization and experimentation with data relevant to your organization.

### Using the Returns Data Loader

To use the returns data loader:

1. Change to the db directory. For Oracle Application Server, change to the `<INSTALL_DIR>/returnsmgmt/db` directory.
2. If the `returnsManagementDBInstall.jar` file was not expanded as part of the installation, that jar file must be expanded to access the files needed to run the loader.

```
jar xvf returnsmgmtDBInstall.jar
```

3. Edit the part of the `db.properties` file that deals with the returns data loader.

Set the values of the properties as needed. Replace the host name `My_RM_Server` shown in the following example.

```
#####
# Properties for Returns Seed Data Loading
#####

# the host name where the seed data should be loaded
dataLoader.host=My_RM_Server

# the port number where the seed data should be loaded
# WebSphere App Server 6.x normally uses 9080, JBoss is 8080
dataLoader.port=9080

# The URL shouldn't need to be modified unless the deployment location moves
dataLoader.url=http://${dataLoader.host}:${dataLoader.port}/retwebsvc/services/
ReturnsManager
```

4. Execute the following command:

```
ws_ant load_returns_data
```

About 100 sample return requests and final result messages are sent to the Returns Management server. This step may take several minutes to complete.

This command sends some output to `DataTools.log` in the current directory. Ignore the warning message about attachment support, as the DataLoader does not need it to operate properly.

You can view the contents of the submitted XML messages in the `returns-data/tickets` directory. You can also modify the messages and resubmit them by repeating this step.

---

## Appendix: Best Practices for Passwords

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

- ["Password Guidelines"](#)
- ["Special Security Options for IBM DB2 Databases"](#)

### Password Guidelines

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

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

## Special Security Options for IBM DB2 Databases

The security for DB2 is done at the operating system level. Consult your IBM DB2 documentation for information on creating a security profile that follows the password guidelines.



---

## Appendix: Secure JDBC with IBM DB2

This appendix has information on how to enable SSL for IBM DB2. Information from the DB2 V9 Information Center, *Global Security Kit Secure Sockets Layer Introduction*, and *iKeyman User's Guide* is included in this appendix.

IBM DB2 has supported SSL encryption since version 9.1 Fix Pack 3. Information on how to configure SSL on the server and client can be found at the following Web sites:

- <http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=/com.ibm.db2.udb.uprun.doc/doc/t0025241.htm>
- <http://www-1.ibm.com/support/docview.wss?uid=swg21249656>

### Summary

To secure JDBC on IBM DB2 requires the following:

- An SSL provider must be established on the DB2 server.
- The provider requires a digital certificate and corresponding private key to provide the secure communications.
- The client either needs to have a copy of the digital certificate or trust the signer of the server certificate.
- The client needs to be configured to use the secure service, and optionally use a FIPS-compliant SSL provider.

### Prerequisites

The information in this section is from the DB2 V9 Information Center.

1. Make sure you have the required fix pack version of DB2.

To determine the fix pack level you have, run the `db2level` command at the command line. If you have Version 9.1 with a fix pack version earlier than Fix Pack 3, you need to obtain Fix Pack 3 or a later version.

2. Make sure the GSKit is installed.

On linux, it is located in `/usr/local/ibm/gsk7`.

3. Make sure the GSKit libraries are in the path.

Make sure the `/usr/local/ibm/gsk7/lib` directory is included in `LD_LIBRARY_PATH`.

4. For information on how to check if the connection concentrator is in use, see the IBM documentation.

## Setting up the Key Store

The information in this section is from *Global Security Kit Secure Sockets Layer Introduction* and *iKeyman User's Guide*.

1. If you are not already logged in to the server, log in as the instance owner.
2. Start iKeyman GUI gsk7ikm.  
If the Java Cryptographic Extension(JCE) files were not found, make sure the JAVA\_HOME environment variable points to a JDK that contains the JCE.
3. Click **Key Database File** and then **New**.
4. Select a key database type, filename, and location.  
It is suggested that a CMS key database is created. This is consistent with the DB2 Infocenter example. For example:  

```
/home/db2inst1/GSKit/Keystore/key.kdb
```
5. Click **OK**. The Password Prompt window is displayed.
6. Enter a password for the key database.
7. Click **OK**. A confirmation window is displayed. Click **OK**.

## Creating a Self-signed Digital Certificate for Testing

The information in this section is from *Global Security Kit Secure Sockets Layer Introduction* and *iKeyman User's Guide*.

1. If you are not already logged in to the server, log in as the instance owner.
2. Start iKeyman GUI gsk7ikm.  
If the Java Cryptographic Extension(JCE) files were not found, make sure the JAVA\_HOME environment variable points to a JDK that contains the JCE.
3. Click **Key Database File** and then **Open**.
4. Select the key database file where you want to add the self-signed digital certificate.
5. Click **Open**. The Password Prompt window is displayed.
6. Select **Personal Certificates** from the menu.
7. Click **New Self-Signed**. The Create New Self-Signed Certificate Window is displayed.
8. Type a Key Label, such as `keytest`, for the self-signed digital certificate.
9. Type a **Common Name and Organization**, and select a **Country**. For the remaining fields, accept the default values or enter new values.
10. Click **OK**. The IBM Key Management Window is displayed. The Personal Certificates field shows the name of the self-signed digital certificate you created.

## Configuring the IBM DB2 Server

The information in this section is from the DB2 V9 Information Center.

1. If you are not already logged in to the server, log in as the instance owner.

## 2. Create an SSL configuration file:

- For Linux and UNIX:

<INSTHOME>/cfg/SSLconfig.ini

For example:

/home/db2inst1/sqllib/cfg/SSLconfig.ini

- For Windows:

<INSTHOME>\SSLconfig.ini

For example:

F:\IBM\SQLLIB\DB2\SSLconfig.ini

<INSTHOME> is the home directory of the instance.

---

**Caution:** It is recommended that you set the file permission to limit access to the `SSLconfig.ini`, as the file might contain sensitive data. For example, limit read and write authority on the file to members of the SYSADM group if the file contains the password for Key Store.

---

- ## 3. Add SSL parameters to the SSL configuration file. The `SSLconfig.ini` file contains the SSL parameters that are used to load and start SSL. The list of SSL parameters are shown in the following table:

| SSL parameter name     | Description  |
|------------------------|--|
| DB2_SSL_KEYSTORE_FILE  | Fully qualified file name of the Key Store that stores the Server Certificate.                         |
| DB2_SSL_KEYSTORE_PW    | Password of the Key Store that stores the Server Certificate.  |
| DB2_SSL_KEYSTORE_LABEL | Label for the Server Certificate. If it is omitted, the default certificate for the Key Store is used. |
| DB2_SSL_LISTENER       | Service name or port number for the SSL listener.  |

The following is an example of an `SSLconfig.ini` file:

```
DB2_SSL_KEYSTORE_FILE=/home/db2inst1/GSKit/Keystore/key.kdb
DB2_SSL_LISTENER=20397
DB2_SSL_KEYSTORE_PW=abcd1234
```

- ## 4. Add the value SSL to the DB2COMM registry variable. For example, use the following command:

```
db2set -i <db2inst1> DB2COMM=SSL
```

where <db2inst1> is the IBM DB2 instance name.

The database manager can support multiple protocols at the same time. For example, to enable both TCP/IP and SSL communication protocols:

```
db2set -i <db2inst1> DB2COMM=SSL,TCPIP
```

5. Restart the IBM DB2 instance. For example, use the following commands:

```
db2stop
```

```
db2start
```

At this point, the server should be ready to start serving SSL connections. You can check the `db2diag.log` file for errors. There should be no errors pertaining to SSL after the restart.

## Exporting a Certificate from iKeyman

The information in this section is from *Global Security Kit Secure Sockets Layer Introduction* and *iKeyman User's Guide*.

In order to be able to talk to the server, the clients need to have a copy of the self-signed certificate from the server.

1. Start iKeyman. The IBM Key Management window is displayed.
2. Click **Key Database File** and then **Open**. The Open window is displayed.
3. Select the source key database. This is the database that contains the certificate you want to add to another database as a signer certificate.
4. Click **Open**. The Password Prompt window is displayed.
5. Enter the key database password and click **OK**. The IBM Key Management window is displayed. The title bar shows the name of the selected key database file, indicating that the file is open and ready.
6. Select the type of certificate you want to export: Personal or Signer.
7. Select the certificate that you want to add to another database.
  - If you selected Personal, click **Extract Certificate**.
  - If you selected Signer, click **Extract**.

The Extract a Certificate to a File window is displayed.

8. Click **Data type** and select a data type, such as Base64-encoded ASCII data. The data type needs to match the data type of the certificate stored in the certificate file. The iKeyman tool supports Base64-encoded ASCII files and binary DER-encoded certificates.
9. Enter the certificate file name and location where you want to store the certificate, or click **Browse** to select the name and location.
10. Click **OK**. The certificate is written to the specified file, and the IBM Key Management window is displayed.

## Configuring the IBM FIPS-compliant Provider for SSL (optional)

The information in this section is from the DB2 V9 Information Center.

The Sun JSSE SSL provider works with the IBM DB2 driver by following the above instructions. If you want to use the IBM FIPS-compliant provider, you have to use the IBM JDK and make the following configuration changes.

---

**Note:** If you are following the IBM documentation, note the following issues:

- Prior to the numbered steps, it says to add several lines to `java.security`. Do not add the lines.
  - Step two incorrectly shows setting `ssl.SocketFactory.provider` twice. It only needs to be done once.
- 

1. Set the `IBMJSSE2 FIPS` system property to enable FIPS mode:

```
com.ibm.jsse2.JSSEFIPS=true
```

2. Set security properties to ensure that all JSSE code uses the IBMJSSE2 provider. The following example shows the entries in `java.security`.

```
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
```

3. Add the IBMJCEFIPS cryptographic provider.

Add `com.ibm.crypto.fips.provider.IBMJCEFIPS` to the provider list before the IBMJCE provider. Do not remove the IBMJCE provider. The IBMJCE provider is required for Key Store support.

The following example shows the entries in `java.security`.

```
# List of providers and their preference orders (see above):
#
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
# inserted provider 2 for FIPS
security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.3=com.ibm.crypto.provider.IBMJCE
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
security.provider.5=com.ibm.security.cert.IBMCertPath
security.provider.6=com.ibm.security.sasl.IBMSASL
```

## Configuring Returns Management on IBM WebSphere

It is difficult to configure Oracle Retail Returns Management to use secure JDBC from the start by using the URL that includes the `sslConnection` property and secure port number. The following instructions are for retrofitting it into the configuration after the install is complete.

To complete the configuration:

1. Install the database digital certificate into the application server truststore.
  - a. Log in to the WebSphere Integrated Solutions Console (Admin Console).
  - b. Expand the Security menu.
  - c. Click the **SSL certificate and key management** option.
  - d. In the Related Items list, click **Key stores and certificates**.
  - e. Click the **NodeDefaultTrustStore** link in the list.
  - f. In the Additional Properties list, click the **Signer certificates** link.
  - g. Click the **Add** button.

- h. Enter a distinct alias and the full path to the certificate file on the server in the File name field. Make sure the Data type corresponds to the type in the file. The certificate should appear in the list of Signer certificates.
2. Update all the data sources to use SSL. (jdbc/DataSource, jdbc/DimpDataSource, jdbc/DimpDataSource)
  - a. Log in to the WebSphere Integrated Solutions Console (Admin Console).
  - b. Expand the Resources menu option.
  - c. Expand the JDBC menu option.
  - d. Click the **Data sources** option. The list of data sources is displayed.
  - e. Click on the data source to be edited.
  - f. In the Additional Properties list, click the **Custom properties** link.
  - g. Click the **New** button.
  - h. Enter sslConnection in the Name field, true in the Value field, and click **OK**.
  - i. Click the data source name in the bread crumb trail to return to the data source edit page.
  - j. Change the Port number field from the TCPIP port to the SSL port.
  - k. Click **OK**.
  - l. Edit the remaining data sources.
  - m. Save the configuration.
3. Stop the server.
4. Edit the custom user registry properties in customRegistry.properties.
  - a. Change the JDBC URL to use the SSL port.
  - b. Append :sslConnection=true; to the end.
5. Start the server.

## Useful Links

For more information, see the following Web sites:

- <http://publib.boulder.ibm.com/infocenter/db2luw/v9/topic/com.ibm.db2.udb.apdv.java.doc/doc/rjvdsprp.htm>

This Web site has documentation of all the properties available in the DB2 Driver for JDBC.

- <http://publib.boulder.ibm.com/infocenter/db2luw/v9/topic/com.ibm.db2.udb.apdv.java.doc/doc/tjvjcccn.htm>

This Web site contains documentation of the URL syntax for connecting to DB2 using JDBC.

- <http://www.redbooks.ibm.com/abstracts/sg247555.html>

An IBM Redbook on security related issues with DB2, including auditing and data encryption. The IBM Form Number is SG24-7555-00.

---

# Appendix: Troubleshooting

This appendix has information that can be used to troubleshoot problems after the installation of Returns Management.

## Apache Axis2 Servlet Not Accessible

To workaround the problem:

1. Stop the WebSphere application server in the profile that contains Returns Management.
2. Under InstallApps, navigate to  
`/ReturnsManagement.ear/retwebsvc-webapp.war/WEB-INF/modules.`
3. Copy the `addressing-1.5.mar` module to  
`ReturnsManagement.ear/retwebsvc-webapp.war/WEB-INF/lib.`
4. Rename `addressing-1.5.mar` to `addressing-1.5.jar` under  
`ReturnsManagement.ear/retwebsvc-webapp.war/WEB-INF/lib.`
5. Start the WebSphere application server in the profile.

For more information, see the following Web site:

<http://www-01.ibm.com/support/docview.wss?uid=swg21315686>





---

## Appendix: Installation Order

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

---

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

---

### Enterprise Installation Order

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

---

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

---

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

---

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

---

9. Oracle Retail Central Office (ORCO)
10. Oracle Retail Returns Management (ORRM)
11. Oracle Retail Back Office (ORBO) or Back Office with Labels and Tags (ORLAT)

**12. Oracle Retail Store Inventory Management (SIM)**

---

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

---

- 13. Oracle Retail Predictive Application Server (RPAS)**
- 14. Oracle Retail Demand Forecasting (RDF)**
- 15. Oracle Retail Category Management (CM)**
- 16. Oracle Retail Replenishment Optimization (RO)**
- 17. Oracle Retail Analytic Parameter Calculator Replenishment Optimization (APC RO)**
- 18. Oracle Retail Regular Price Optimzation (RPO)**
- 19. Oracle Retail Merchandise Financial Planning (MFP)**
- 20. Oracle Retail Size Profile Optimization (SPO)**
- 21. Oracle Retail Assortment Planning (AP)**
- 22. Oracle Retail Item Planning (IP)**
- 23. Oracle Retail Item Planning Configured for COE (IP COE)**
- 24. Oracle Retail Advanced Inventory Planning (AIP)**
- 25. Oracle Retail Integration Bus (RIB)**
- 26. Oracle Retail Point-of-Service (ORPOS)**
- 27. Oracle Retail Markdown Optimization (MDO)**
- 28. Oracle Retail Clearance Optimization Engine (COE)**
- 29. Oracle Retail Analytic Parameter Calculator for Markdown Optimization (APC-MDO)**
- 30. Oracle Retail Analytic Parameter Calculator for Regular Price Optimization (APC-RPO)**
- 31. Oracle Retail Promotion Intelligence and Promotion Planning and Optimization (PI-PPO)**
- 32. Oracle Retail Workspace (ORW)**