Oracle® Retail Back Office

Installation Guide

Release 13.0.6

E38090-01

February 2013

ORACLE®

Oracle Retail Back Office Installation Guide, Release 13.0.6

Primary Author: Bernadette Goodman

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

F Appendix: Common Installation Errors

G Appendix: Troubleshooting Problems on the Oracle Stack

H Appendix: Best Practices for Passwords

I Appendix: Secure JDBC with Oracle 11g Database

J Appendix: Secure JDBC with IBM DB2

List of Figures

List of Tables

Send Us Your Comments

Oracle Retail Back Office Installation Guide, Release 13.0.6

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

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

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

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

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

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

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

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

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

Preface

This Installation Guide describes the requirements and procedures to install this Oracle Retail Back Office release.

Audience

This Installation Guide is for the following audiences:

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

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Access to Oracle Support

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

Related Documents

For more information, see the following document in the Oracle Retail Back Office Release 13.0.6 documentation set:

- *Oracle Retail Back Office Release Notes*

Customer Support

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

https://support.oracle.com

When contacting Customer Support, please provide the following:

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

Review Patch Documentation

When you install the application for the first time, you install either a base release (for example, 13.0) or a later patch release (for example, 13.0.6). If you are installing the base release or additional patch releases, read the documentation for all releases that have occurred since the base release before you begin installation. Documentation for patch releases can contain critical information related to the base release, as well as information about code changes since the base release.

Oracle Retail Documentation on the Oracle Technology Network

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

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

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

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

Conventions

The following text conventions are used in this document:

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

1

Pre-installation Tasks

This chapter describes the requirements that must be met before the application can be installed.

> **Note:** The Oracle stack and IBM stack are the configurations that were tested for this release. The components required for each stack are listed in this chapter. For each component, the product and the version that were used for testing are included. While Back Office may work in other configurations, these are the configurations that are supported for this release.

Check for the Current Version of the Installation Guide

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

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

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

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

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

Check Oracle Retail Merchandising Version

The integration with Oracle Retail Merchandising requires version 13.0.6 of the following products:

- Oracle Retail Merchandising System
- Oracle Retail Price Management
- Oracle Retail Sales Audit

Check Database Requirements

Table 1–1 lists the general components required for a database server and the versions tested for this release.

Table 1–1 Database Server Component Versions Tested for this Release

Component	Oracle Stack	IBM Stack
Operating System	Windows 2003 Server	IBM IRES version 2.1.5
Database	Oracle Database 11gR2 Enterprise Edition version 11.2.0.3 (64-bit)	IBM DB2 version 9.1.0.5 (64-bit)

Required Settings for Database Installation

The following settings must be made during database creation:

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

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

- When using the IBM DB2 database server, the default heap size is 256. Increase the heap size to at least 1024. For information on how to set the heap size, refer to your IBM DB2 documentation.

Secure JDBC with Oracle 11g

Creating the Oracle wallet and certificate for the server requires that the Advanced Security options are installed with the database server. For more information, see "Securing the JDBC for the Oracle 11g Database" in Chapter 2.

Check Application Server Requirements

Table 1–2 lists the general components required for an application server capable of running Back Office and the versions tested for this release.

Table 1–2 Application Server Component Versions Tested for this Release

Component	Oracle Stack	IBM Stack
Operating System	Windows 2003 Server	IBM IRES version 2.1.5
J2EE Application Server	Oracle Application Server 10g Enterprise Edition version 10.1.3.5 **Note:** This release of Back Office is only supported in a managed OC4J instance as part of OracleAS 10g. It is not supported on OC4J standalone.	IBM WebSphere version 6.1.0.19
J2EE Application Server JVM	Oracle Java 6 or later within the Java 6 code line	included in IBM WebSphere version 6.1.0.19
Messaging Provider	included in Oracle Application Server	IBM WebSphere MQ 6.0.2.5

Table 1–2 (Cont.) Application Server Component Versions Tested for this Release

Component	Oracle Stack	IBM Stack
System Management Agents	OEM 10.1.3.5	IBM WebSphere Admin Console 6.1.0.19

Install Required Patches for the Oracle Stack

To use Oracle Application Server version 10.1.3.5 with an Oracle 11g database, you must apply patches to the OPatch utility and Oracle Application Server:

1. Download and install OPatch version 10.1.0.0.0 from ARU for your platform. The ARU Checkin number is 6880880.
2. Use OPatch to apply ARU Request Number 10579638.

Check for SSL Certificate

Oracle Retail Back Office 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 Back Office.

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

Check Java KeyStore Requirement

Oracle Retail Back Office requires that a Java KeyStore is created prior to installation. A KeyStore connector RAR file is required to enable the connection between Oracle Retail Back Office and the KeyStore. During installation, the RAR file must be deployed to the application server. Specific information for configing the KeyStore and deploying the RAR file is entered on the Security Setup: KeyStore installer screens.

WARNING: A simulated key management package is bundled with Oracle Retail Back Office. It is not compliant with either the Visa Payment Applications Best Practices (PABP) or Payment Card Industry Data Security Standard (PCI-DSS). It is made available as a convenience for retailers and integrators. If you use the simulated key manager, you will not be PCI-DSS compliant. Therefore, the simulated key manager should be replaced with a compliant key manager.

Hardware Requirements

Specific hardware requirements for the machines running Oracle Retail Back Office depend on variables including the number of users and other applications running on the same machine.

Please note the following about the hardware requirements:

- The CPU requirement depends on variables including the number of registers and the operating system and middleware selected.
- Memory requirements and performance depend on variables including the number of active promotions and best deal calculations.

- Disk size can vary based on the operating system and middleware requirements as well as the amount of data storage needed. Data storage depends on variables including the number of items and promotions defined, data retention period, and so on.

You need to determine your hardware requirements, based on the variables mentioned here, as well as any additional variables specific to your environment.

Check 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 Scalable Vector Graphics (SVG) and Portable Data Format (PDF) files

The following web browsers are tested for this release:

- Microsoft Internet Explorer 7
- Microsoft Internet Explorer 8
- Microsoft Internet Explorer 9
- Mozilla Firefox ESR 10.0.0.6+

Visa Payment Application Best Practices

This release of Oracle Retail Back Office complies with the Visa Payment Application Best Practices (PABP). Where there is a specific PABP requirement to be met during the installation process, a caution is included in this guide advising you how to comply with the requirement.

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

https://support.oracle.com

Oracle Retail Strategic Store Solutions Security Implementation Guide **(Doc ID: 567438.1)**

This guide provides information on the PABP requirements.

2

Installation of the Oracle Stack on Windows

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

During installation, the Back Office database schema will be created and the Back Office application will be deployed to an OC4J instance within the OracleAS 10g installation. The Java JDK that is included with the Oracle Application Server (under `%ORACLE_HOME%\jdk`) will be used to run the application.

Note: J2EE_HOME refers to the directory `%ORACLE_HOME%\j2ee\<instancename>`

Create a New OC4J Instance for Back Office

You can skip this section if you are redeploying to an existing OC4J instance.

The Back Office application must be deployed to its own dedicated OC4J instance. For instructions on how to create a new OC4J instance, see Adding and Deleting OC4J Instances in the Reconfiguring Application Server Instances chapter of the *Oracle Application Server Administrator's Guide*.

To create a new OC4J instance:

1. Log onto the server, which is running your OracleAS 10g installation, as the user who owns the OracleAS 10g installation. Set your `ORACLE_HOME` environment variable to point to this installation. You must use forward slash file separators when setting this variable.
2. Choose a name for the new OC4J instance. In the remainder of this installation guide, `<orbo-inst>` is used for the name.
3. Create this OC4J instance as documented in the *Oracle Application Server Administrator's Guide*, for example:

   ```
   %ORACLE_HOME%\bin\createinstance -instanceName <orbo-inst>
   ```

Note: When prompted for the oc4jadmin password, provide the same administrative password you gave for the OracleAS 10g installation. All OC4J instances running Oracle Retail applications must have the same oc4jadmin password.

Note: The `jms` and `rmi` port numbers should be set so that the numbers do not overlap between all the instances in your configuration. Also, a specific port number should be set rather than a range of port numbers. If a range of port numbers is specified, the same port number may not be used each time the instance is started.

The port numbers are defined in the `%ORACLE_HOME%\opmn\conf\opmn.xml` file. The following is an example definition of the port numbers in that file.

Port number definitions for the home instance:

```
<port id="rmi" range="12401-12401"/>
<port id="jms" range="12601-12601"/>
```

Port number definitions for the Back Office instance:

```
<port id="rmi" range="12403-12403"/>
<port id="jms" range="12603-12603"/>
```

4. Start the OC4J instance. You can do this through the Enterprise Manager web interface, or on the command line using the opmnctl utility:

   ```
   %ORACLE_HOME%\opmn\bin\opmnctl startproc
    process-type=<orbo-inst>
   ```

5. Verify that the OC4J instance was fully started. If you are using the Enterprise Manager web interface, the instance should have a green arrow indicating that it is running. On the command line, verify that the instance has a status of "Alive".

   ```
   %ORACLE_HOME%\opmn\bin\opmnctl status
   ```

   If you are unable to start the OC4J instance after several attempts, try increasing the startup timeouts in `%ORACLE_HOME%\opmn\conf\opmn.xml`. If that does not help, consult the Oracle Application Server documentation for further assistance.

Create the Database Schema Owner and Data Source Connection Users

A user to own the database schema and a data source connection user used by Back Office to access the database must be defined. Specific roles must be defined for each user.

Caution: To meet the requirements of the Visa Payment Application Best Practices (PABP), separate schema owner and data source connection users must be created. The data source connection user cannot have any create privileges.

If other Oracle Retail products are installed, the database schema owner and data source connection users defined for each product must not be the same as any other product. However, for example, if Oracle Retail Back Office and Point-of-Service are sharing a database, the database schema owner would be the same for those products.

For information on the best practices for passwords, see Appendix H.

Note: Do not delete the database schema owner after installation. When using Data Import (DIMP), the schema owner privileges are needed for DIMP processing which includes creating and dropping tables. For information on DIMP, see the *Oracle Retail Strategic Store Solutions Implementation Guide*.

To create the database schema owner and data source connection users:

1. Log in using the database administrator user ID.
2. Create a role in the database to be used for the schema owner.

   ```
   create role <schema_owner_role>;
   ```

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

   ```
   grant CREATE TABLE, CREATE VIEW, CREATE SEQUENCE, CREATE PROCEDURE, ALTER
   SESSION, CONNECT, SELECT_CATALOG_ROLE to <schema_owner_role>;
   ```

4. Create a role in the database to be used for the data source connection user.

   ```
   create role <data_source_connection_role>;
   ```

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

   ```
   grant CONNECT, CREATE SYNONYM, SELECT_CATALOG_ROLE to
   <data_source_connection_role>;
   ```

6. Create the schema owner user in the database.

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

7. Grant the schema owner role to the user.

   ```
   grant <schema_owner_role> to <schema_owner_user>;
   ```

8. Create the data source connection user.

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

9. Grant the data source connection role to the user.

   ```
   grant <data_source_connection_role> to <data_source_user>;
   ```

The installer grants the data source connection 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 Option".

Expand the Back Office Distribution

To extract the Back Office files:

1. Extract the ORBO-13.0.6.zip file from the Back Office distribution.
2. Create a new staging directory for the Back Office application distribution (ORBO-13.0.6.zip) file, for example, c:\tmp\j2ee\orbo-inst\orbo-staging.

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

3. Copy or upload ORBO-13.0.6.zip to *<staging_directory>* and extract its contents. The following files and directories should be created under *<staging_directory>*\ORBO-13.0.6:

```
ant\
ant-ext\
antinstall\
backoffice\
connectors\
external-lib\
installer-resources\
.postinstall.cmd
.postinstall.sh
.preinstall.cmd
.preinstall.sh
.preinstall-oas.cmd
.preinstall-oas.sh
.preinstall-was.cmd
.preinstall-was.sh
ant.install.properties.sample.oas
ant.install.properties.sample.was
antinstall-config.xml
build.xml
build-common.xml
build-common-backoffice.xml
build-common-oas.xml
build-common-was.xml
build-common-webapps.xml
checkdeps.cmd
checkdeps.sh
install.cmd
install.sh
prepare.xml
retail-OCM.zip
```

For the remainder of this chapter, *<staging_directory>*\ORBO-13.0.6 is referred to as *<INSTALL_DIR>*.

Obtain the Third-Party Library File Required by Back Office

The Back Office application uses the Pager Tag Library from JSPTags. You must download the `pager-taglib.jar` file from the JSPTags website before running the Back Office application installer.

1. Download the `pager-taglib-2.0.war` file from the JSPTags website: `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. Copy `pager-taglib.jar` into *<INSTALL_DIR>*`\external-lib\`.

Set Up to Integrate with the Central Office JMS Server

On the Central Office JMS Server Integration installer screen, you select whether Back Office will be integrated with the Central Office JMS server. See Figure A–18 in Appendix A.

If **Yes** is selected on the screen, the Central Office application must be running in order for the Back Office files to be installed correctly.

Securing the JDBC for the Oracle 11g Database

Communication with the database must be secured in order to be compliant with PABP requirements.

On the Enable Secure JDBC screen, you select whether secure JDBC will be used for communication with the database. If **Yes** is selected, the installer sets up the secure JDBC.

If **No** is selected and you want to manually set up the secure JDBC after the installer completes, see Appendix I. If secure JDBC is not used, Back Office will not be compliant with PABP requirements.

Run the Back Office Application Installer

Once you have an OC4J instance that is configured and started, you can run the Back Office application installer. This installer will configure and deploy the Back Office application.

> **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 ORACLE_HOME and JAVA_HOME environment variables.

   ORACLE_HOME should point to your OracleAS 10g installation, for example, `C:\Oracle\10.1.3.5\OracleAS_1`.
   JAVA_HOME should point to `%ORACLE_HOME%\jdk`.

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

3. If you are using an X server such as Exceed, 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.

   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 install.cmd script. This will launch the installer. After installation is complete, a detailed installation log file is created: `orbo-install-app.<timestamp>.log`.

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

   ```
   install.cmd [text | silent oracle]
   ```

5. Verify that the installer was able to delete the `%ORACLE_HOME%\jdk\jre\lib\ext\security-360-ora.jar` file. This is a file that is temporarily created by the installer. If the installer was unable to delete the file, you must shut down all OC4J instances, delete the file manually, and start the OC4J instances back up again.

   Note: If the installer is unable to delete this file, it prints a warning that instructs you to delete it manually. This warning also shows up at the end of the installer log file.

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 C.

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

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

Oracle Configuration Manager

The Oracle Retail OCM Installer packaged with this release does not install the latest version of OCM. Oracle Retail recommends that retailers upgrade to the latest version of OCM from ARU. See OCM documentation for further instructions on how to automatically upgrade.

For more information, see the following:

My Oracle Support Note: 559539.1

The Oracle Configuration Manager Installer 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/ocm.html

Install Database Option

The database must be populated before configuring the application server. On the Install Database Option screen, you select whether the installer completes installation of the database schema and seed data.

- If you chose Yes, you do not need to perform any further steps to populate the database. This is the default selection on the screen.
- If you chose No, the installer did not populate the database schema. If you want to manually populate the database, execute the `ant load_sql` command in the *<INSTALL_DIR>*`\backoffice\configured-output\db` directory.

Install Parameters

The application parameters must be installed before the Back Office application is fully operational. On the Install Parameters screen, you select whether the installer completes installation of the parameters.

- 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".

Manual Deployment Option

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>*`\backoffice\configured-output\`.

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

1. Grant the data source connection user access to the application database objects. For information on these users and roles, see "Create the Database Schema Owner and Data Source Connection Users".

   Note: Before granting the access, the database must be populated. If the database has not been populated, see "Install Database Option" for information on doing this manually.

   a. Log in as the schema owner, *<schema_owner_user>*.

   b. Grant select, insert, update, and delete privileges for all the objects owned by the schema owner to the data source connection role.

   ```
   grant SELECT, INSERT, UPDATE, DELETE ON <object_name> to
   <data source connection role>;
   ```

c. Log in as the data source connection user, <*data_source_user*>.

d. Create synonyms for all objects owned by the schema owner.

```
create synonym <object_name> for <schema_owner_user>.<object_name>;
```

2. Make sure there have not been any application server configuration changes since the installer was run. You can do this by comparing the backup files created by the installer in the staging area to the same files in the application server.

```
comp <INSTALL_DIR>\backoffice\configured-output\appserver\ORACLE_HOME\
j2ee\myinstance\config\jms.xml.<date and time> %ORACLE_HOME%\j2ee\
myinstance\config\jms.xml
```

If there are changes to the application server's configuration file, they should be merged into the local copy under configured-output before proceeding to the next step.

3. Inspect the contents of the <*INSTALL_DIR*>\backoffice\configured-output\appserver\ ORACLE_HOME directory, and then overlay the files in the application server's ORACLE_HOME directory, using the same directory structure. This will install library files required by the application and required application server configuration changes.

4. Set the JAVA_HOME and PATH environment variables to use the JDK located at %ORACLE_HOME%\jdk.

```
SET JAVA_HOME=%ORACLE_HOME%\jdk;
SET PATH=%JAVA_HOME%\bin;%PATH%;
```

5. Copy the <*INSTALL_DIR*>\backoffice\lib\oracle\security-360-ora.jar file to the %ORACLE_HOME%\jdk\jre\lib\ext\ directory.

6. Create the required JAAS configuration for Back Office:

a. Set JAVA_HOME and PATH environment variables to use the JDK located at %ORACLE_HOME%\jdk.

```
SET JAVA_HOME=%ORACLE_HOME%\jdk;
SET PATH=%JAVA_HOME%\bin;%PATH%;
```

b. Grant RMI access permissions for the Back Office application.

```
java -jar ..\home\jazn.jar -grantperm com._
360commerce.commerceservice.security.oracle.CustomPrincipal oracle_rmi_
access com.evermind.server.rmi.RMIPermission login
```

The AbstractLoginModule prompts you for the user name and password. Enter the same user name and password you entered on the OC4J Administrative User installer screen.

7. Delete %ORACLE_HOME%\jdk\jre\lib\ext\security-360-ora.jar. You may need to shut down all OC4J instances to be able to successfully delete this file.

8. Restart the OC4J instance where Back Office will be deployed.

```
%ORACLE_HOME%\opmn\bin\opmnctl restartproc process-type=<orbo-inst>
```

9. Deploy the Back Office ear file using the Enterprise Manager web interface. The configured ear file is located at <*INSTALL_DIR*>\backoffice\configured-output\backoffice.ear.

When deploying the ear file, you should 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 for later reference.

Backups Created by Installer

The Back Office application installer will back up modified application server files and directories by renaming them with a timestamp. This is done to prevent the removal of any custom changes you might have. These backup files and directories can be safely removed without affecting the current installation. For example, the file could be named jms.xml.200605011726.

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 Oracle Retail Back Office. For more information on parameters, see the *Oracle Retail Strategic Store Solutions Configuration Guide*.

This section provides an overview of the procedures for importing an initial set of parameters. You can import the parameters through the Oracle Retail Back Office 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 Back Office User Guide*.

These instructions assume you have already expanded the backofficeDBInstall.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 Oracle Retail Back Office application in a web browser. The address is provided at the end of the installer output and in the log file.

   https:\\<*host name*>:<*port number*>\<*context root*>

2. Log in to the application as any user ID that has full administrative rights.
3. Click the **Admin** tab and then the **Job Manager** subtab. Click the **Available Imports** left navigation link. 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*>\backoffice\db folder.
5. To import the initial set of Oracle Retail Back Office application parameters, click the **File** link in the Import BackOffice Parameters row. Follow the instructions to import backoffice.xml from the <*INSTALL_DIR*>\backoffice\db folder.

Importing Parameters By Using an Ant Target

To import parameters using an ant target:

1. Change to the *<INSTALL_DIR>*\backoffice\configured-output\db directory.
2. Edit the db.properties file. Update the following properties in the "Properties for Parameter Loading" section.
   a. Change ora.home.dir to your installation directory.

      ```
      ora.home.dir=C:\Oracle\10.1.3\OracleAS_1
      ```

   b. Change ORA_HOST_NAME to your host name. Change 12401 to your port number.

      ```
      parameters.apphost=ormi:\\ORA_HOST_NAME:12401\BackOffice
      ```

3. Set the JAVA_HOME, ANT_HOME, and PATH environment variables. See "Creation of the Back Office Database Schema" in Appendix G for the settings to be used.
4. Execute the following command:

   ```
   ant load_parameters
   ```

Load Optional Purge Procedures

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

To load the purge procedures:

1. Log in as the database schema owner, *<schema_owner_user>*.
2. Run the available Ant target to load the procedures.

   ```
   ant load_purge_procedures
   ```

3. Create a user for running the purge procedures. This user should only have the privileges required to run the purge procedures.

Using the Back Office Application

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

After the application installer completes and you have run the initial parameter load, you should have a working Back Office application installation. To launch the application, open a web browser and go to
https:*<servername>*:*<portnumber>**<context root>*

For example, https:\\myhost:8080\backoffice

Note: Before viewing any reports for the first time after Back Office is installed, you must open the store. Opening the store creates data that is needed for Reports functionality to work correctly.

3

Installation of the IBM Stack on IRES

Before proceeding, you must install the database and application server software. See Chapter 1.

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

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

Create the Database Schema Owner and Data Source Connection Users

A user to own the database schema and a data source connection user used by Back Office to access the database must be defined. Specific roles must be defined for each user.

Caution: To meet the requirements of the Visa Payment Application Best Practices (PABP), separate schema owner and data source connection users must be created. The data source connection user cannot have any create privileges.

If other Oracle Retail products are installed, the database schema owner and data source connection users defined for each product must not be the same as any other product. However, for example, if Oracle Retail Back Office and Point-of-Service are sharing a database, the database schema owner would be the same for those products.

For information on the best practices for passwords, see Appendix H.

Note: Do not delete the database schema owner after installation. When using Data Import (DIMP), the schema owner privileges are needed for DIMP processing which includes creating and dropping tables. For information on DIMP, see the *Oracle Retail Strategic Store Solutions Implementation Guide*.

To create the database schema owner and database source users:

1. Log in using the database administrator user ID.
2. Create the schema owner user.

   ```
   create schema <schema_name> authorization <schema_owner_user>
   ```

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

   ```
   grant CREATETAB, BINDADD, CONNECT, IMPLICIT_SCHEMA ON DATABASE to user
   <schema_owner_user>
   ```

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

   ```
   grant CREATEIN, DROPIN, ALTERIN ON SCHEMA <schema_name> to user
   <schema_owner_user> with GRANT OPTION
   ```

5. Create the data source connection user.

   ```
   create schema <data_source_schema_name> authorization <data_source_user>
   ```

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

   ```
   grant CONNECT, IMPLICIT_SCHEMA ON DATABASE to <data_source_user>
   ```

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

   ```
   grant CREATEIN ON SCHEMA <data_source_schema_name> to user <data_source_user>
   with GRANT OPTION
   ```

The installer grants the data source connection 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 Option".

Expand the Back Office Distribution

To extract the Back Office files:

1. Extract the `ORBO-13.0.6.zip` file from the Back Office distribution.
2. Log into the UNIX server as the user who owns the IBM WebSphere installation. Create a new staging directory for the Back Office application distribution (`ORBO-13.0.6.zip`), for example, `/tmp/j2ee/orbo-inst/orbo-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 `ORBO-13.0.6.zip` to *<staging_directory>* and extract its contents. The following files and directories should be created under *<staging_directory>*`/ORBO-13.0.6`:

```
ant/
ant-ext/
antinstall/
backoffice/
connectors/
external-lib/
installer-resources/
.postinstall.cmd
.postinstall.sh
.preinstall.cmd
.preinstall.sh
.preinstall-oas.cmd
.preinstall-oas.sh
.preinstall-was.cmd
.preinstall-was.sh
ant.install.properties.sample.oas
ant.install.properties.sample.was
antinstall-config.xml
build.xml
build-common.xml
build-common-backoffice.xml
build-common-oas.xml
build-common-was.xml
build-common-webapps.xml
checkdeps.cmd
checkdeps.sh
install.cmd
install.sh
prepare.xml
retail-OCM.zip
```

For the remainder of this chapter, *<staging_directory>*`/ORBO-13.0.6` is referred to as *<INSTALL_DIR>*.

Obtain Third-Party Library Files Required by Back Office

The Back Office application uses the Pager Tag Library from JSPTags and the DB2 drivers from IBM. Before running the Back Office application installer, you must download the necessary files from the JSPTags website and the IBM website.

1. Download the `pager-taglib-2.0.war` file from the JSPTags website: 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. Copy `pager-taglib.jar` into *<INSTALL_DIR>*`/external-lib/`.
3. Download the `db2_v9_db2driver_for_jdbc_sqlj.zip` file from the IBM website: http://www.ibm.com/software/data/db2/java/
4. Extract the `db2jcc.jar` and `db2jcc_license_cu.jar` files from the `db2_v9_db2driver_for_jdbc_sqlj` subdirectory in the `db2_v9_db2driver_for_jdbc_sqlj.zip` file. Copy `db2jcc.jar` and `db2jcc_license_cu.jar` into *<INSTALL_DIR>*`/external-lib/`.

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:

- "Install Database Option"
- "Install Parameters"
- "Configure MQ Series"
- "Manual Deployment Option"

Set Up to Integrate with the Central Office JMS Server

On the Central Office JMS Server Integration installer screen, you select whether Back Office will be integrated with the Central Office JMS server. See Figure B–19 in Appendix B.

If **Yes** is selected on the screen, the Central Office application must be running in order for the Back Office files to be installed correctly.

Securing the JDBC for the IBM DB2 Database

Communication with the database must be secured in order to be compliant with PABP requirements.

On the Enable Secure JDBC screen, you select whether secure JDBC will be used for communication with the database. If **Yes** is selected, the installer sets up the secure JDBC.

If **No** is selected and you want to manually set up the secure JDBC after the installer completes, see Appendix J. If secure JDBC is not used, Back Office will not be compliant with PABP requirements.

Run the Back Office Application Installer

The installer will configure and deploy the Back Office application.

Note: To see details on every screen and field in the application installer, see Appendix B.

---

1. Change to the *<INSTALL_DIR>* directory.
2. Set the JAVA_HOME environment variable. JAVA_HOME should point to an installation of IBM Java2 JDK.

Note: The installer is not compatible with versions of Java earlier than 1.5.

---

3. If you are using an X server such as Exceed, 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.

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 the user who owns the IBM WebSphere installation.
   b. Change the mode of `install.sh` 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: `orbo-install-app.<timestamp>.log`

5. The installer leaves behind the `ant.install.properties` file for future reference and repeat installations. This file contains all the inputs you provided, including passwords. As a security precaution, make sure that the file has restrictive permissions.

```
chmod 600 ant.install.properties
```

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 C.

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

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

Oracle Configuration Manager

The Oracle Retail OCM Installer packaged with this release does not install the latest version of OCM. Oracle Retail recommends that retailers upgrade to the latest version of OCM from ARU. See OCM documentation for further instructions on how to automatically upgrade.

For more information, see the following:

My Oracle Support Note: 559539.1

The Oracle Configuration Manager Installer 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/ocm.html

Install Database Option

The database must be populated before configuring the application server. On the Install Database Option screen, you select whether the installer completes installation of the database schema and seed data.

- If you chose Yes, you do not need to perform any further steps to populate the database. This is the default selection on the screen.
- If you chose No, the installer did not populate the database schema. If you want to manually populate the database, execute the `ws_ant load_sql` command in the *<INSTALL_DIR>*`/backoffice/configured-output/db` directory.

Install Parameters

The application parameters must be installed before the Back Office application is fully operational. On the Install Parameters screen, you select whether the installer completes installation of the parameters.

- 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".

Configure MQ Series

MQ Series must be configured with a queue manager and the queues and topics required by Back Office before Back Office can be deployed. On the Configure MQ Series Option screen, you select whether the installer configures MQ Series or if you manually configure it. If MQ Series is installed on a different machine than the WebSphere server, you must manually configure MQ Series.

Use the following commands to configure MQ Series. `MQ_Install_Dir` is the directory where MQ Series 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/runmqlsr -m <input.jms.server.queue> -p
    <input.jms.server.port> -t tcp &
<MQ_Install_Dir>/bin/runmqsc     <input.jms.server.queue> <
    <INSTALL_DIR>/backoffice/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>
```

Manual Deployment Option

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>/backoffice/configured-output/`.

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

1. Grant the data source connection user access to the application database objects. For information on these users and roles, see "Create the Database Schema Owner and Data Source Connection Users".

   Note: Before granting the access, the database must be populated. If the database has not been populated, see "Install Database Option" for information on doing this manually.

   a. Log in as the schema owner, <*schema_owner_user*>.

   b. Grant select, insert, update, and delete privileges for all the objects owned by the schema owner to the data source connection user.

   ```
   grant SELECT, INSERT, UPDATE, DELETE ON <object_name> to
   <data_source_user>
   ```

   c. Log in as the data source connection user, <*data_source_user*>.

   d. Create synonyms for all objects owned by the schema owner.

   ```
   create synonym <object_name> for <schema_owner_user>.<object_name>
   ```

2. Deploy the Back Office application.

   a. Log in to the WebSphere Administrative console.

   b. Deploy the ear file located in `<INSTALL_DIR>/backoffice`. Use the same application name and context root used for the installation. These values are available in the `<INSTALL_DIR>/ant.install.properties` file.

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 Oracle Retail Back Office. For more information on parameters, see the *Oracle Retail Strategic Store Solutions Configuration Guide*.

This section provides an overview of the procedures for importing an initial set of parameters. You can import the parameters through the Oracle Retail Back Office 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 Back Office User Guide*.

These instructions assume you have already expanded the `backofficeDBInstall.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 Oracle Retail Back Office application in a web browser. The address is provided at the end of the installer output and in the log file.

   `https://<your host name>:<port number/<context root>`

2. Log in to the application as user ID **pos** and password **pos**, or any other user ID that has full administrative rights.
3. Click the **Admin** tab and then the **Job Manager** subtab. Click the **Available Imports** left navigation link. 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>*`/backoffice/db` folder.
5. To import the initial set of Oracle Retail Back Office application parameters, click the **File** link in the Import BackOffice Parameters row. Follow the instructions to import `backoffice.xml` from the *<INSTALL_DIR>*`/backoffice/db` folder.

Importing Parameters By Using an Ant Target

To import parameters using an ant target:

1. Change to the *<INSTALL_DIR>*`/backoffice/tmp/db` directory.
2. Execute the following command:

   ```
   ant load_parameters
   ```

Load Optional Purge Procedures

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

To load the purge procedures:

1. Log in as the database schema owner, *<schema_owner_user>*.
2. Run the available Ant target to load the procedures.

   ```
   ant load_purge_procedures
   ```

3. Create a user for running the purge procedures. This user should only have the privileges required to run the purge procedures.

Using the Back Office Application

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

After the application installer completes and you have run the initial parameter load, you should have a working Back Office application installation. To launch the application, open a web browser and go to
`https://<servername>:<portnumber>/<context root>`

For example, https://myhost:8080/backoffice

> **Note:** Before viewing any reports for the first time after Back Office is installed, you must open the store. Opening the store creates data that is needed for Reports functionality to work correctly.

A

Appendix: Back Office Application Installer Screens for the Oracle Stack on Windows

You need specific details about your environment for the installer to successfully deploy the Back Office application on the Oracle 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. If you want to document any specific information about your environment for any field, a Notes row is provided in each table for saving that information.

Figure A–1 Introduction

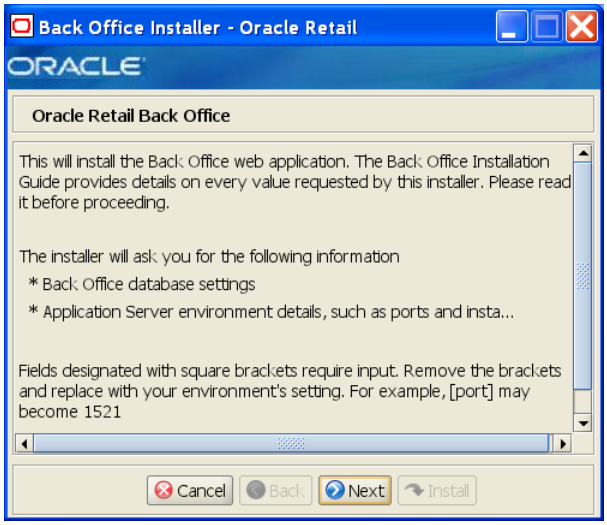


Figure A–2 Requirements

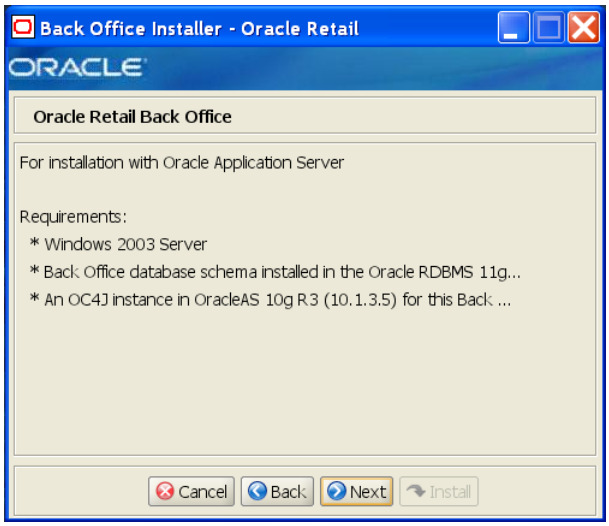
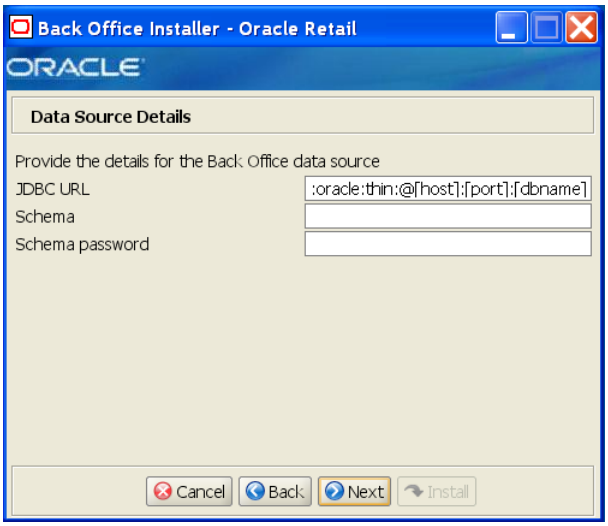


Figure A–3 License Agreement

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

Figure A–4 Data Source Details



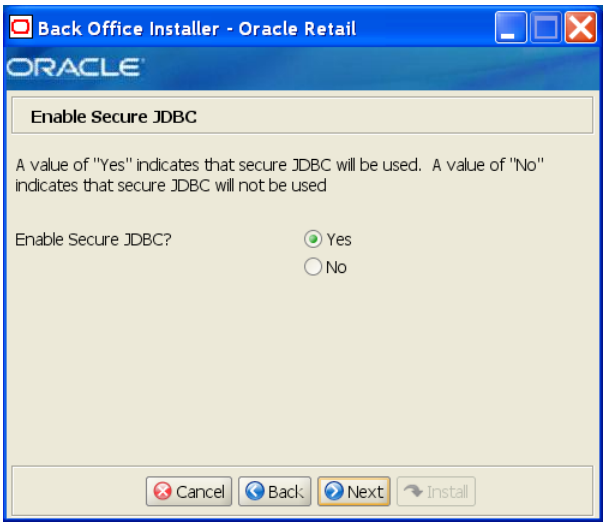
The fields on this screen are described in the following tables.

Field Title	JDBC URL
Field Description	URL used by the Back Office application to access the database schema. See Appendix E for the expected syntax.
Example	`jdbc:oracle:thin:@myhost:1525:mydatabase`
Notes	

Field Title	Schema
Field Description	Data source connection user name used by the Back Office application to access the database. This user name is created prior to running the installer. For information, see "Create the Database Schema Owner and Data Source Connection Users" in Chapter 2.
Example	DBUSER
Notes	

Field Title	Schema password
Field Description	Password for the data source connection user.
Notes	

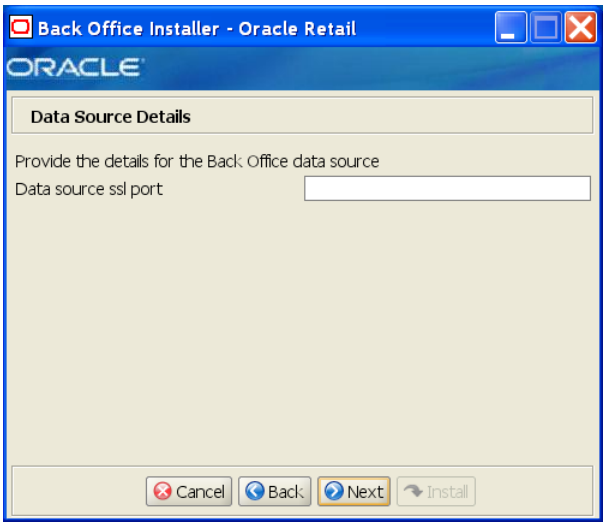
Figure A–5 Enable Secure JDBC



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
Notes	

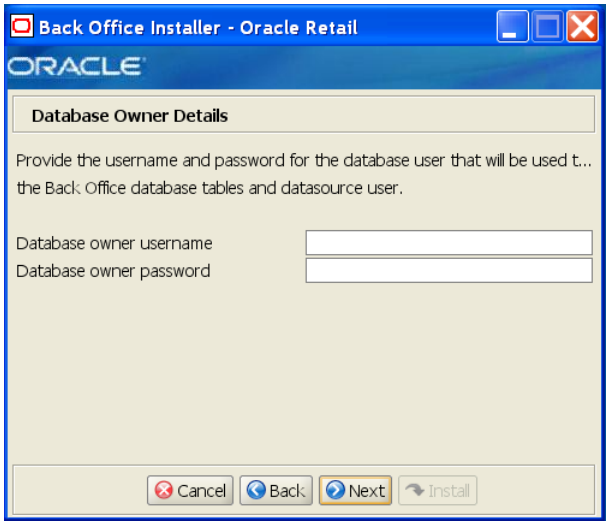
Figure A–6 Data Source Details



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	1521
Notes	

Figure A–7 Database Owner Details Screen

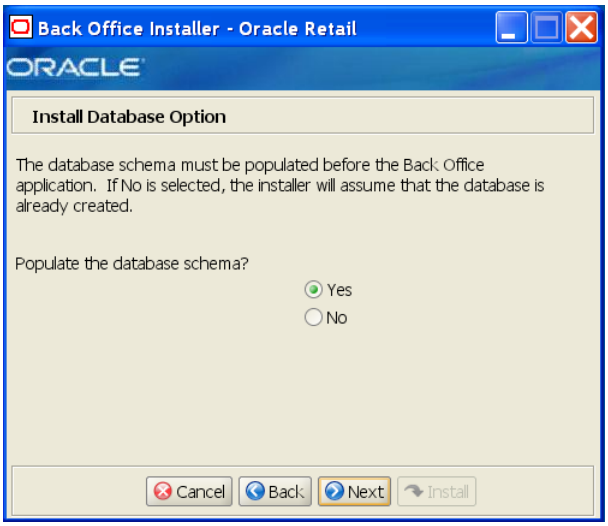


The fields on this screen are described in the following tables.

Field Title	Database owner username
Field Description	Database user name that owns the database schema. This user name is created prior to running the installer. For information, see "Create the Database Schema Owner and Data Source Connection Users" in Chapter 2.
Example	DBOWNER
Notes	

Field Title	Database owner password
Field Description	Password for the database schema owner.
Notes	

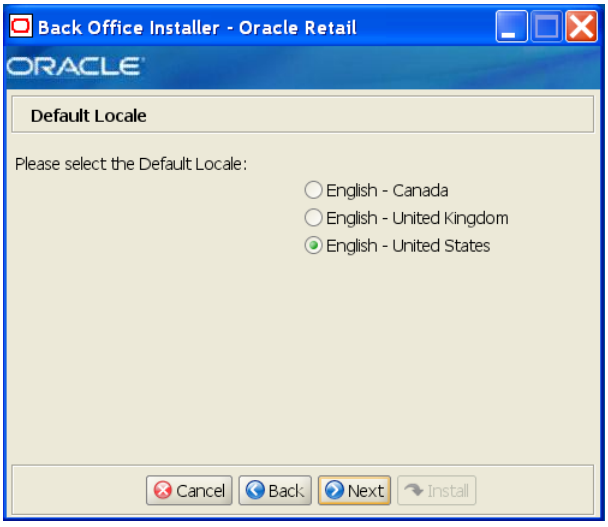
Figure A–8 Install Database Option



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

Field Title	Populate the database schema?
Field Description	The database schema must be populated before Oracle Application Server can be configured for Back Office. This screen gives you the option to leave the database schema unmodified and populate the database schema manually. This can be used if the database is already created. If you choose No, see "Install Database Option" in Chapter 2 for the manual steps you need to perform after the installer completes.
Example	Yes
Notes	

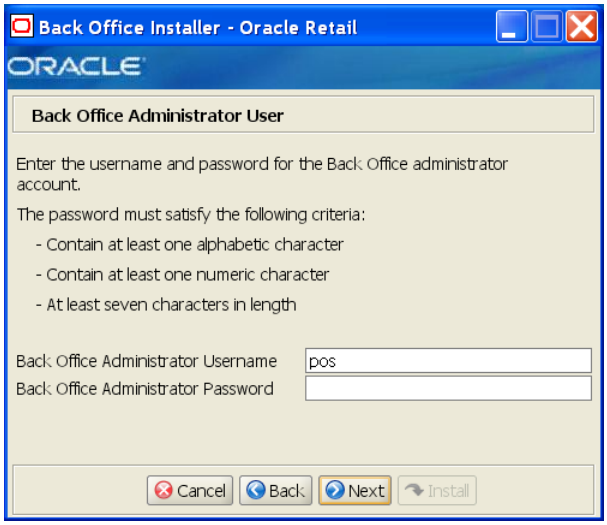
Figure A–9 Default Locale



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

Field Title	Please select the Default Locale
Field Description	Limited locale support in Back Office enables the date, time, currency, and calendar to be displayed in the format for the selected default locale.
Example	English - United States
Notes	

Figure A–10 Back Office Administrator User



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

Field Title	Back Office Administrator Username
Field Description	Administrator user for the Back Office application.
Example	pos
Notes	

Field Title	Back Office Administrator Password
Field Description	Password for the administrator user.
Notes	

Figure A–11 Security Setup: KeyStore

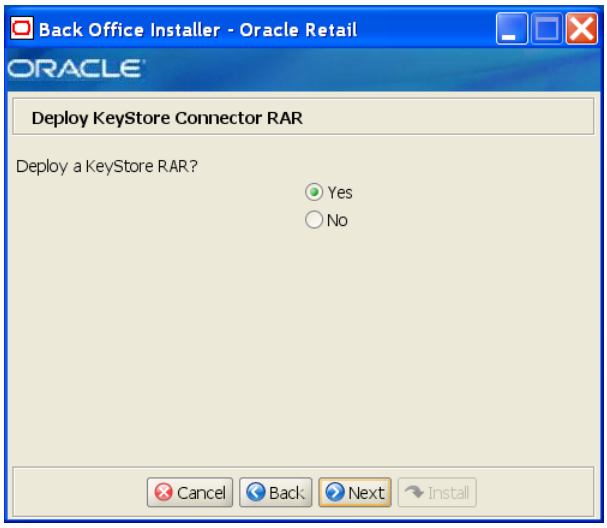
The fields on this screen are described in the following tables.

Field Title	KeyStore Hash Algorithm
Field Description	Enter the name of the algorithm used by the KeyStore to hash sensitive data.
Example	SHA-256
Notes	

Field Title	KeyStore Provider Name
Field Description	Enter the provider for the KeyStore.
Example	SunJCE
Notes	

Field Title	KeyStore JNDI Name
Field Description	Enter the JNDI name for the KeyStore module.
Example	eis/keystoreconnector
Notes	

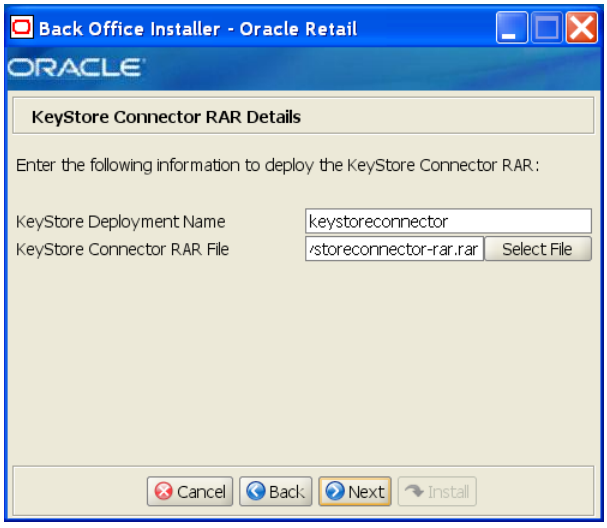
Figure A–12 Deploy KeyStore Connector RAR



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

Field Title	Deploy a KeyStore RAR?
Field Description	Select whether a KeyStore RAR is to be deployed.
Example	Yes
Notes	

Figure A–13 KeyStore Connector RAR Details

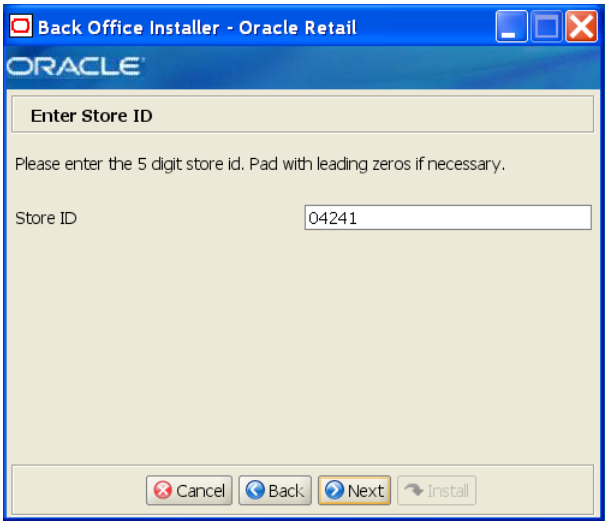


This screen is only displayed if **Yes** is selected on the Deploy KeyStore Connector RAR screen. The fields on this screen are described in the following tables.

Field Title	KeyStore Deployment Name
Field Description	Name to which the KeyStore Connector will be deployed.
Example	keystoreconnector
Notes	

Field Title	KeyStore Connector RAR File
Field Description	Path name to the KeyStore Connector RAR file.
Example	c:\connectors\keystoreconnector-rar.rar
Notes	

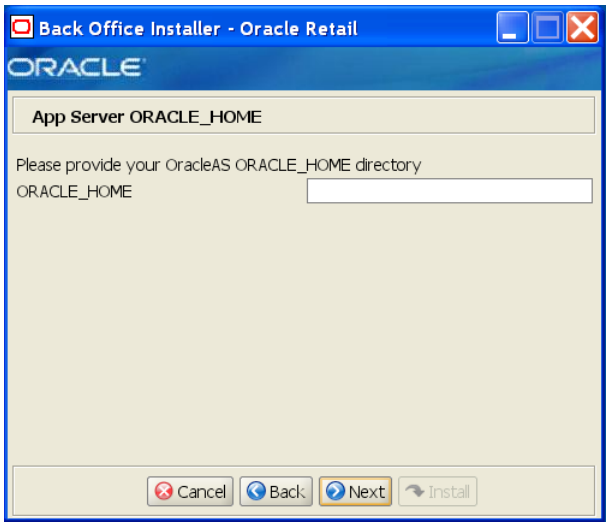
Figure A–14 Enter Store ID



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

Field Title	Store ID
Field Description	ID for this store.
Example	04241
Notes	

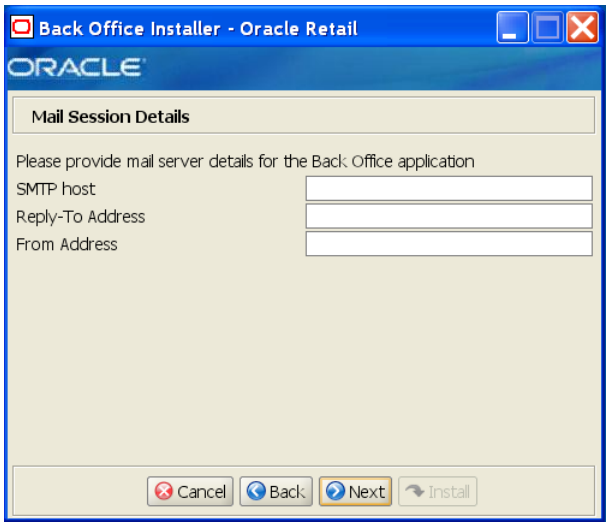
Figure A–15 App Server ORACLE_HOME



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

Field Title	ORACLE_HOME
Field Description	ORACLE_HOME directory for the Oracle Application Server installation.
Example	`C:\Oracle\10.1.3.5\OracleAS_1`
Notes	

Figure A–16 Mail Session Details



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

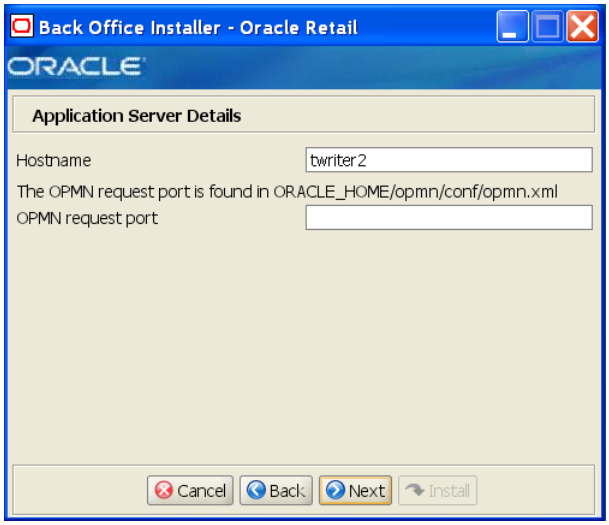
Field Title	SMTP host
Field Description	Host where the SMTP server is running.
Example	`mail.mycompany.com`

Field Title	SMTP host
Notes	

Field Title	Reply-To Address
Field Description	Reply-to address in e-mails generated by Back Office.
Example	`donotreply@mycompany.com`
Notes	

Field Title	From Address
Field Description	From address in e-mails generated by Back Office.
Example	`donotreply@mycompany.com`
Notes	

Figure A–17 Application Server Details

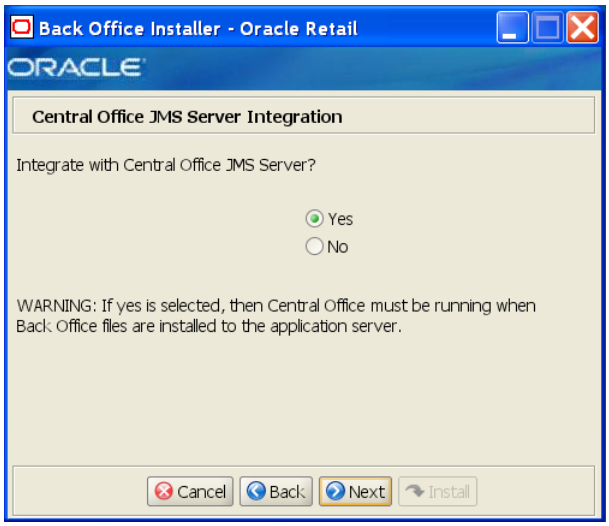


The fields on this screen are described in the following tables.

Field Title	Hostname
Field Description	Host name of the application server.
Example	myhost
Notes	

Field Title	OPMN request port
Field Description	Port on which OPMN listens for requests to forward on to OC4J instances. This port can be found in the `%ORACLE_HOME%\opmn\conf\opmn.xml` file: `<port local="6100" remote="6200" request="6003"/>`
Example	6003
Notes	

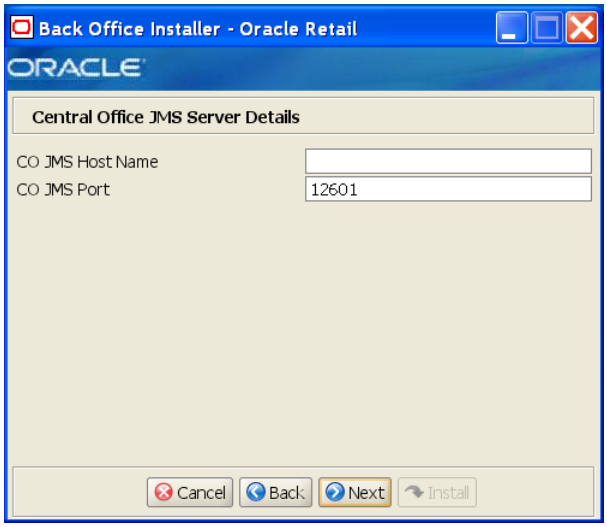
Figure A–18 Central Office JMS Server Integration



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

Field Title	Integrate with Central Office JMS Server?
Field Description	This screen gives you the option to integrate the Back Office application with a Central Office JMS server. **Note:** If you select **Yes**, the Central Office application must be running in order for the Back Office files to be installed correctly.
Example	Yes
Notes	

Figure A–19 Central Office JMS Server Details

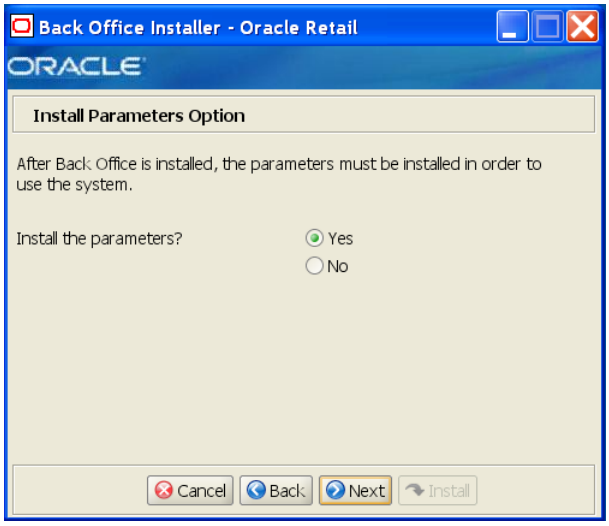


This screen is only displayed if **Yes** is selected on the Central Office JMS Server Integration screen. The fields on this screen are described in the following tables.

Field Title	CO JMS Host Name
Field Description	Name of the Central Office JMS server. **Note:** 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	Server1
Notes	

Field Title	CO JMS Port
Field Description	Port number used by the Central Office JMS server.
Example	12601
Notes	

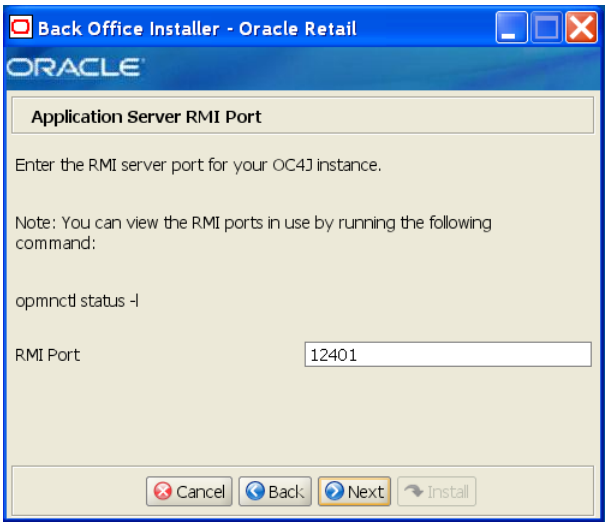
Figure A–20 Install Parameters Options



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 Back Office can be used. This screen gives you the option to set up the parameters manually. If you choose No, see "Install Parameters" in Chapter 2 for the manual steps you need to perform after the installer completes.
Example	Yes
Notes	

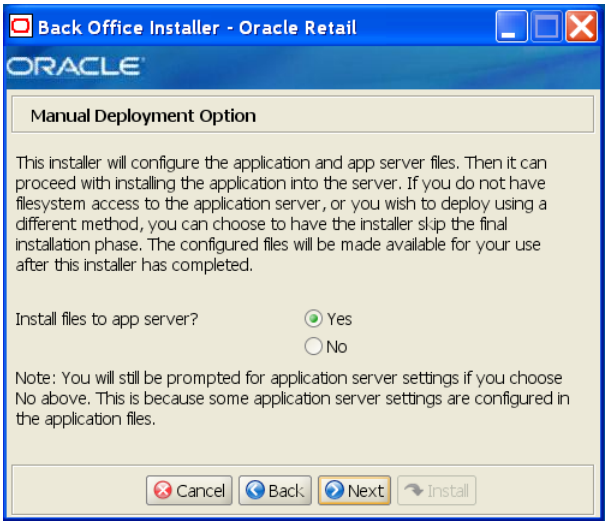
Figure A–21 Application Server RMI Port



This screen is only if **Yes** is selected for the Install the Parameters option. The field on this screen is described in the following table.

Field Title	RMI Port
Field Description	Port to be used for installing parameters. This port can be found in the `%ORACLE_HOME%\opmn\conf\opmn.xml` file.
Example	12402
Notes	

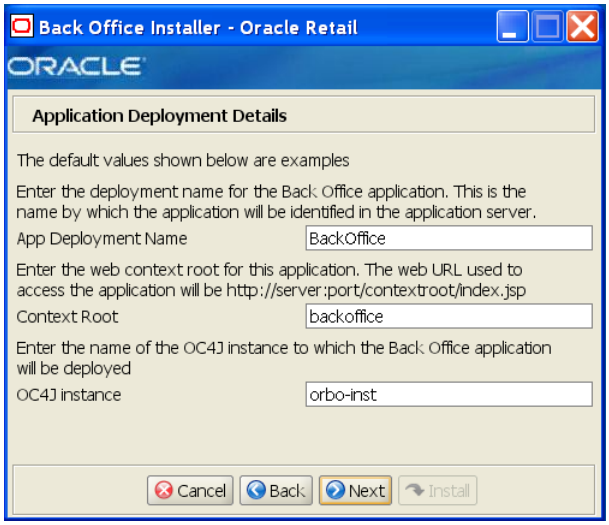
Figure A–22 Manual Deployment Option



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

Field Title	Install files to app server?
Field Description	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. If you choose No, see "Manual Deployment Option" in Chapter 2 for the manual steps you need to perform after the installer completes.
Example	Yes
Notes	

Figure A–23 Application Deployment Details



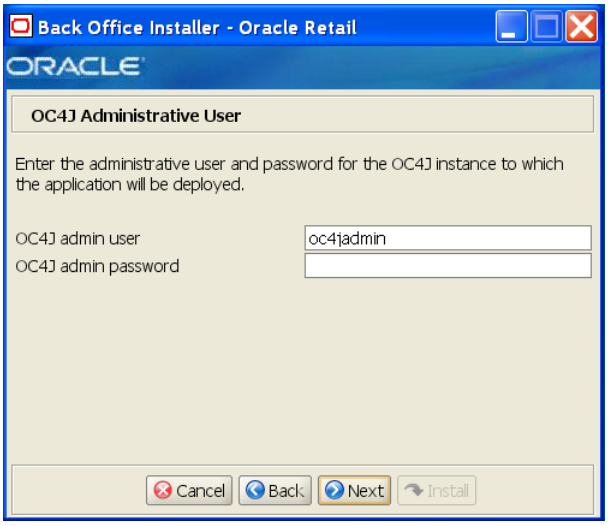
The fields on this screen are described in the following tables.

Field Title	App Deployment Name
Field Description	Name by which this Back Office application will be identified in the application server.
Example	BackOffice
Notes	

Field Title	Context Root
Field Description	Path under the HTTPS URL that will be used to access the Back Office application. For example, a context root of 'backoffice' will result in the application being accessed at `https:\\host:port\backoffice\index.jsp`.
Example	backoffice
Notes	

Field Title	OC4J Instance
Field Description	Name of the OC4J instance that was created for this Back Office application.
Example	orbo-inst
Notes	

Figure A–24 OC4J Administrative User

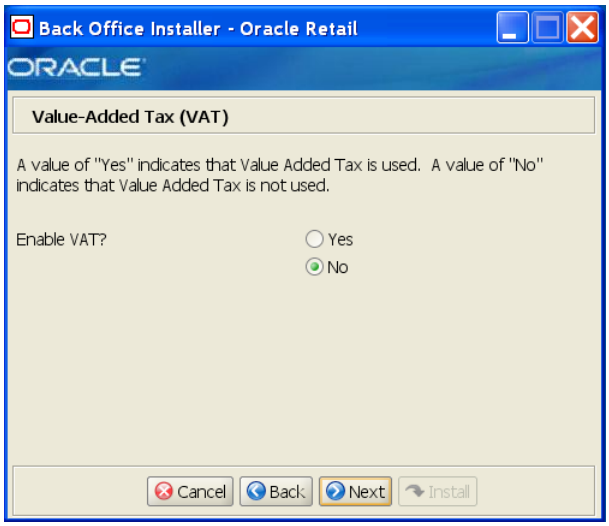


The fields on this screen are described in the following tables.

Field Title	OC4J admin user
Field Description	User name of the administrative user for the OC4J instance to which the Back Office application is being deployed.
Example	oc4jadmin
Notes	

Field Title	OC4J admin password
Field Description	Password for the OC4J administrative user. You chose this password when you created the OC4J instance.
Notes	

Figure A–25 Value-Added Tax (VAT)



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

Field Title	Enable VAT?
Field Description	Sets whether Value-Added Tax is used in Back Office. ■ To enable Back Office to use VAT, choose Yes. ■ To not use VAT, choose No.
Example	No
Notes	

Figure A–26 Installation Progress

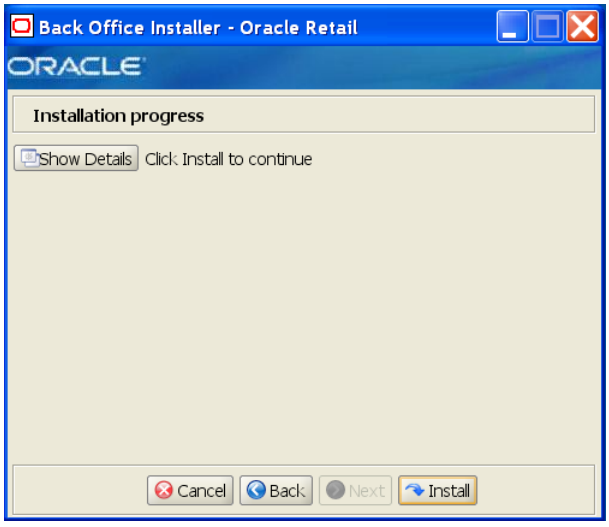
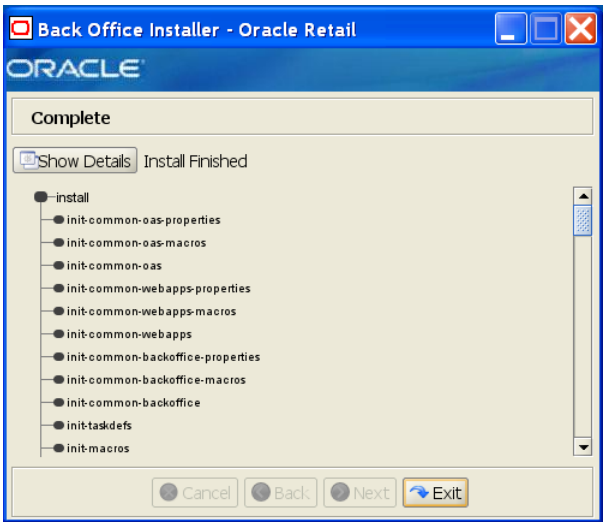


Figure A–27 Installation Complete



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.

B

Appendix: Back Office Application Installer Screens for the IBM Stack

You need specific details about your environment for the installer to successfully deploy the Back Office 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. If you want to document any specific information about your environment for any field, a Notes row is provided in each table for saving that information.

Figure B–1 Introduction

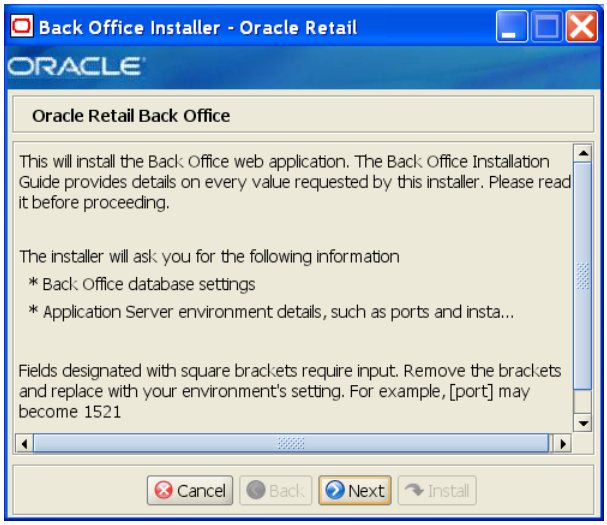


Figure B–2 Requirements

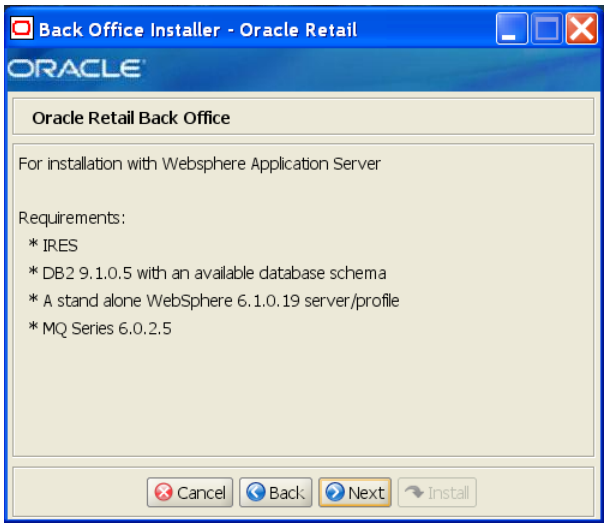
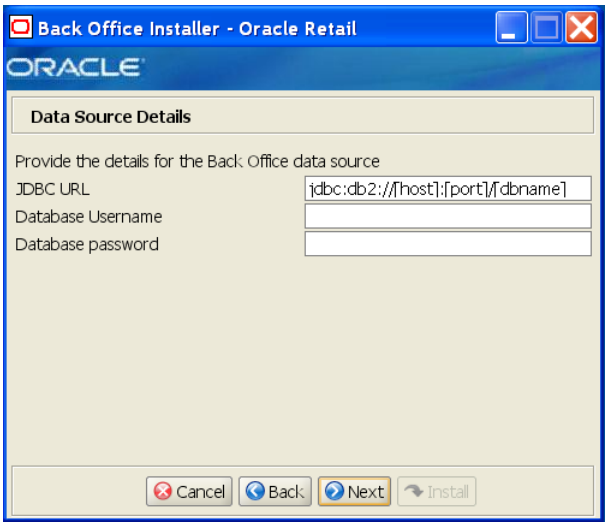


Figure B–3 License Agreement

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

Figure B–4 Data Source Details



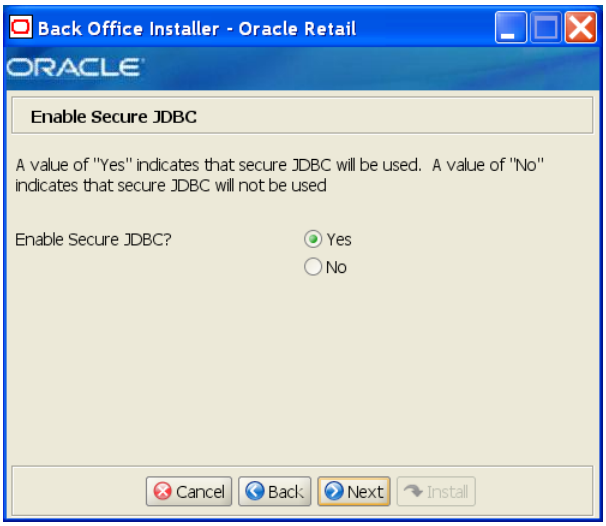
The fields on this screen are described in the following tables.

Field Title	JDBC URL
Field Description	URL used by the Back Office application to access the database schema. See Appendix E for the expected syntax.
Example	`jdbc:db2://myhost:50001/mydb`
Notes	

Field Title	Schema
Field Description	Data source connection name used by the Back Office application to access the database. This user name is created prior to running the installer. For information, see "Create the Database Schema Owner and Data Source Connection Users" in Chapter 3.
Example	DBUSER
Notes	

Field Title	Schema password
Field Description	Password for the data source connection user.
Notes	

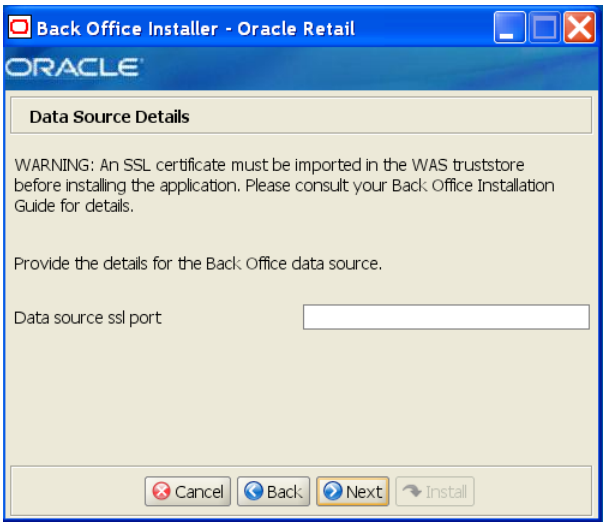
Figure B–5 Enable Secure JDBC



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
Notes	

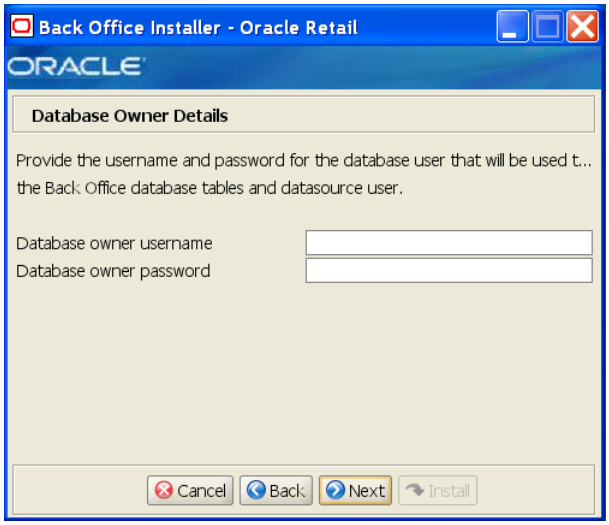
Figure B–6 Data Source Details



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	1521
Notes	

Figure B–7 Database Owner Details Screen

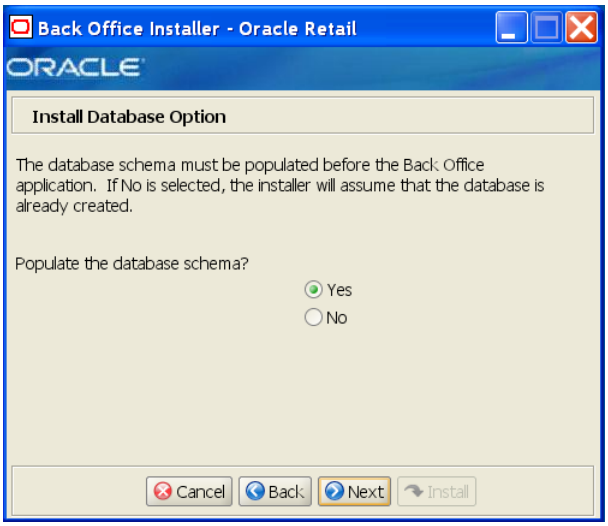


The fields on this screen are described in the following tables.

Field Title	Database owner username
Field Description	Database user name that owns the database schema. This user name is created prior to running the installer. For information, see "Create the Database Schema Owner and Data Source Connection Users" in Chapter 3.
Example	DBOWNER
Notes	

Field Title	Database owner password
Field Description	Password for the database schema owner.
Notes	

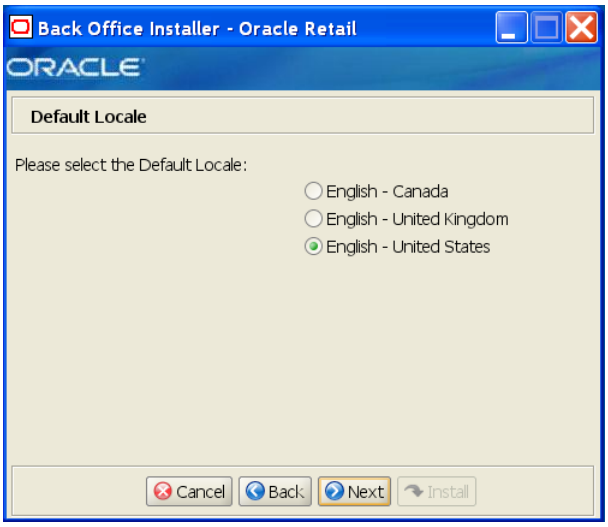
Figure B–8 Install Database Option



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

Field Title	Populate the database schema?
Field Description	The database schema must be populated before WebSphere can be configured for Back Office. This screen gives you the option to leave the database schema unmodified and populate the database schema manually. This can be used if the database is already created. If you choose No, see "Install Database Option" in Chapter 3 for the manual steps you need to perform after the installer completes.
Example	Yes
Notes	

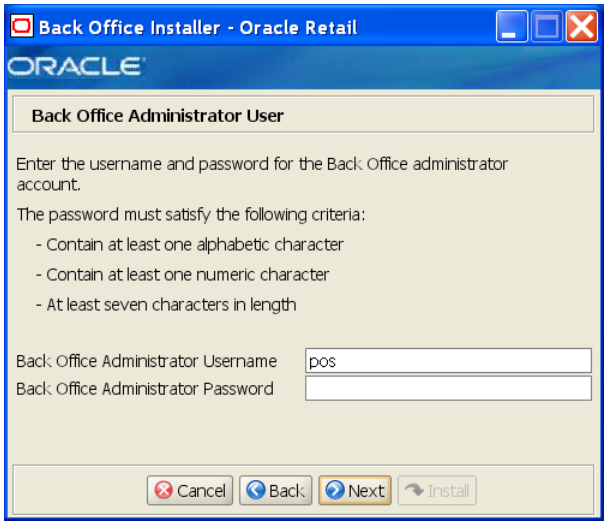
Figure B–9 Default Locale



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

Field Title	Please select the Default Locale
Field Description	Limited locale support in Back Office enables the date, time, currency, and calendar to be displayed in the format for the selected default locale.
Example	English - United States
Notes	

Figure B–10 Back Office Administrator User

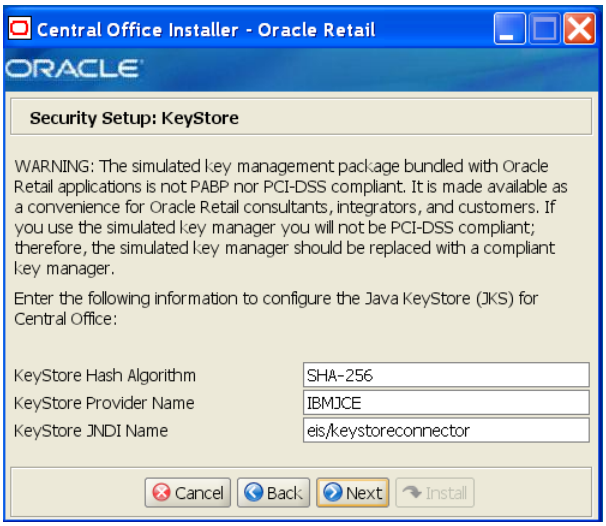


The fields on this screen are described in the following tables.

Field Title	Back Office Administrator Username
Field Description	Administrator user for the Back Office application.
Example	pos
Notes	

Field Title	Back Office Administrator Password
Field Description	Password for the administrator user.
Notes	

Figure B–11 Security Setup: KeyStore



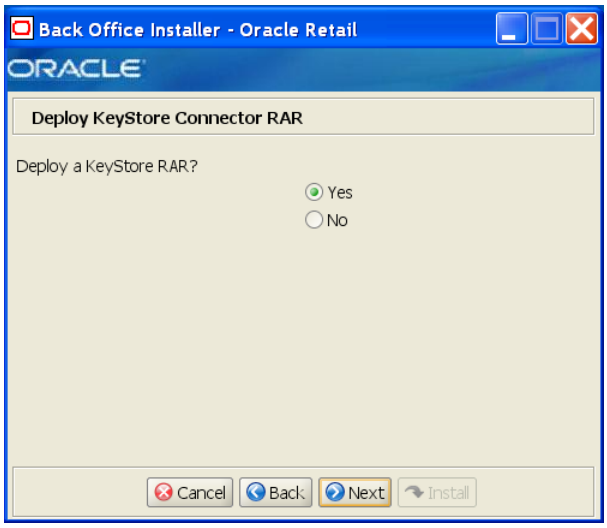
The fields on this screen are described in the following tables.

Field Title	KeyStore Hash Algorithm
Field Description	Enter the name of the algorithm used by the KeyStore to hash sensitive data.
Example	SHA-256
Notes	

Field Title	KeyStore Provider Name
Field Description	Enter the provider for the KeyStore.
Example	IBMJCE
Notes	

Field Title	KeyStore JNDI Name
Field Description	Enter the JNDI name for the KeyStore module.
Example	eis/keystoreconnector
Notes	

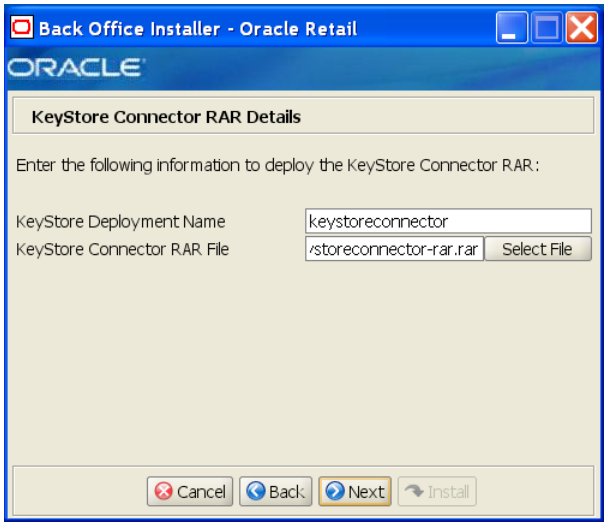
Figure B–12 Deploy KeyStore Connector RAR



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

Field Title	Deploy a KeyStore RAR?
Field Description	Select whether a KeyStore RAR is to be deployed.
Example	Yes
Notes	

Figure B–13 KeyStore Connector RAR Details

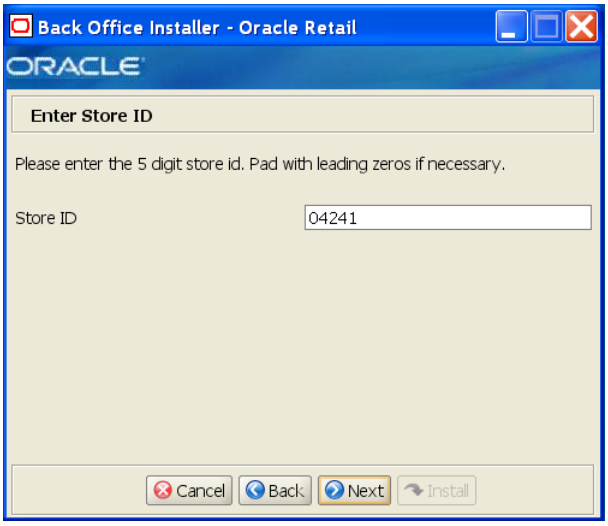


This screen is only displayed if **Yes** is selected on the Deploy KeyStore Connector RAR screen. The fields on this screen are described in the following tables.

Field Title	KeyStore Deployment Name
Field Description	Name to which the KeyStore Connector will be deployed.
Example	keystoreconnector
Notes	

Field Title	KeyStore Connector RAR File
Field Description	Path name to the KeyStore Connector RAR file.
Example	opt/connectors/keystoreconnector-rar.rar
Notes	

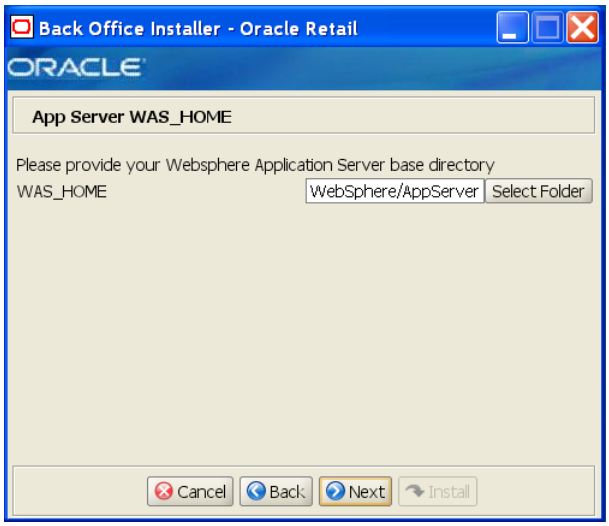
Figure B–14 Enter Store ID



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

Field Title	Store ID
Field Description	ID for this store.
Example	04241
Notes	

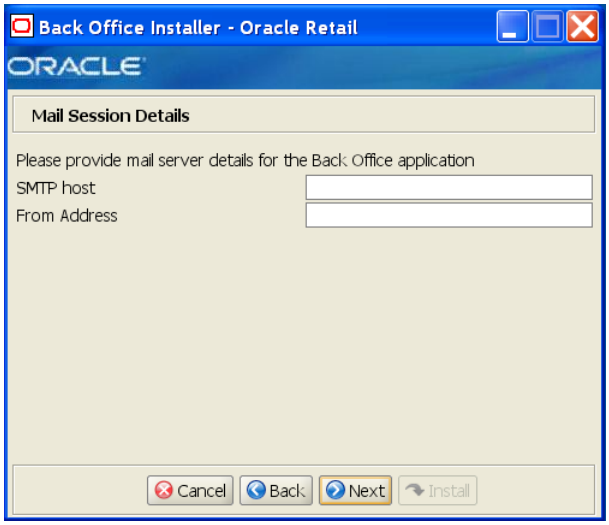
Figure B–15 App Server WAS_HOME



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

Field Title	WAS_HOME
Field Description	Base directory for the WebSphere Application Server installation.
Example	`/opt/IBM/WebSphere/AppServer`
Notes	

Figure B–16 Mail Session Details



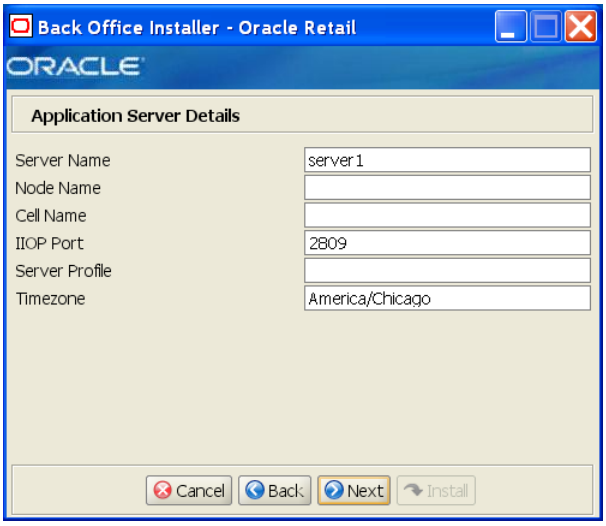
The fields on this screen are described in the following tables.

Field Title	SMTP host
Field Description	Host where the SMTP server is running.
Example	`mail.mycompany.com`

Field Title	SMTP host
Notes	

Field Title	From Address
Field Description	From address in e-mails generated by Back Office.
Example	`donotreply@mycompany.com`
Notes	

Figure B–17 Application Server Details



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

Field Title	Server Name
Field Description	Name of the WebSphere server.
Example	server1
Notes	

Field Title	Node Name
Field Description	Name of the WebSphere node.
Example	myhostNode01
Notes	

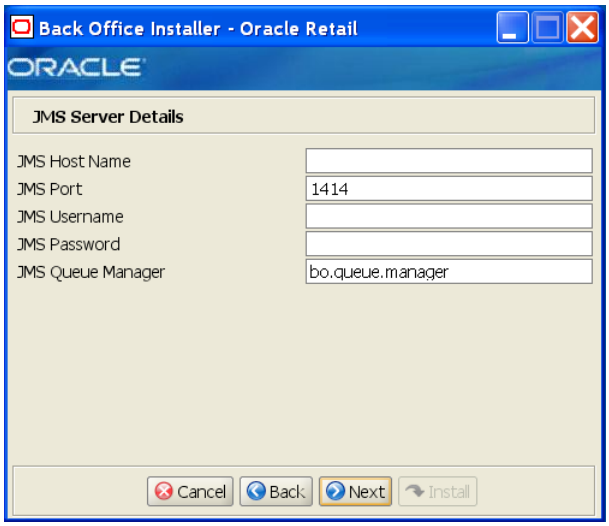
Field Title	Cell Name
Field Description	Name of the WebSphere cell.
Example	myhostNode01Cell
Notes	

Field Title	IIOP port
Field Description	IIOP/BOOTSTRAP_ADDRESS port of the WebSphere server. This port can be found in the *<WAS_HOME>*/profiles/*<profile name>*/properties/portdef.props file.
Example	2809
Notes	

Field Title	Server Profile
Field Description	Name of the WebSphere profile.
Example	AppSrv01
Notes	

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

Figure B–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. **Note:** 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
Notes	

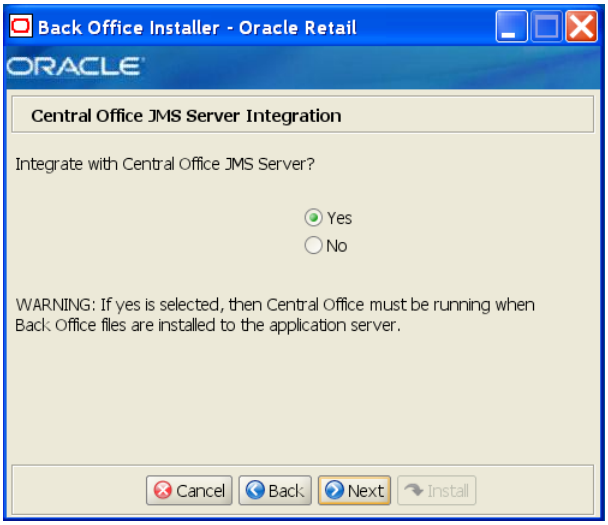
Field Title	JMS Port
Field Description	Port number used by the JMS server.
Example	1414
Notes	

Field Title	JMS Username
Field Description	User name for the JMS server. This user must exist in the Back Office schema.
Example	myuser
Notes	

Field Title	JMS Password
Field Description	Password for the JMS server.
Example	mypassword
Notes	

Field Title	JMS Queue Manager
Field Description	Name of the JMS queue manager.
Example	bo.queue.manager
Notes	

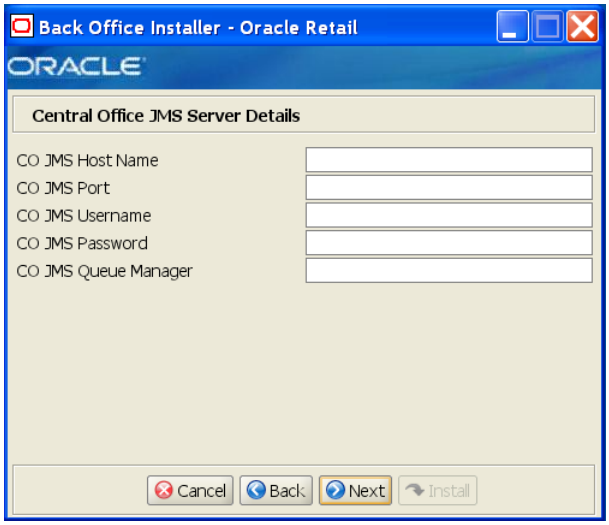
Figure B–19 Central Office JMS Server Integration



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

Field Title	Integrate with Central Office JMS Server?
Field Description	This screen gives you the option to integrate the Back Office application with a Central Office JMS server. **Note:** If you select **Yes**, the Central Office application must be running in order for the Back Office files to be installed correctly.
Example	Yes
Notes	

Figure B–20 Central Office JMS Server Details



This screen is only displayed if **Yes** is selected on the Central Office JMS Server Integration screen. The fields on this screen are described in the following tables.

Field Title	CO JMS Server Name
Field Description	Name of the Central Office JMS server. **Note:** 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	Server1
Notes	

Field Title	CO JMS Server Port
Field Description	Port number used by the Central Office JMS server.
Example	1414
Notes	

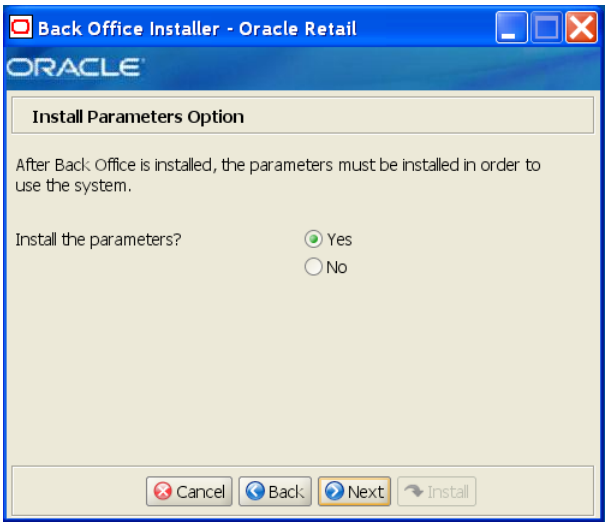
Field Title	CO JMS Username
Field Description	User name for the Central Office JMS server. This user must exist in the operating system where Central Office is running and the user must be in the `mqm` group.

Field Title	CO JMS Username
Example	myuser
Notes	

Field Title	CO JMS Password
Field Description	Password for the user name entered in the CO JMS Username field.
Notes	

Field Title	CO JMS Queue Manager
Field Description	Name of the Central Office JMS queue manager.
Example	co.queue.manager
Notes	

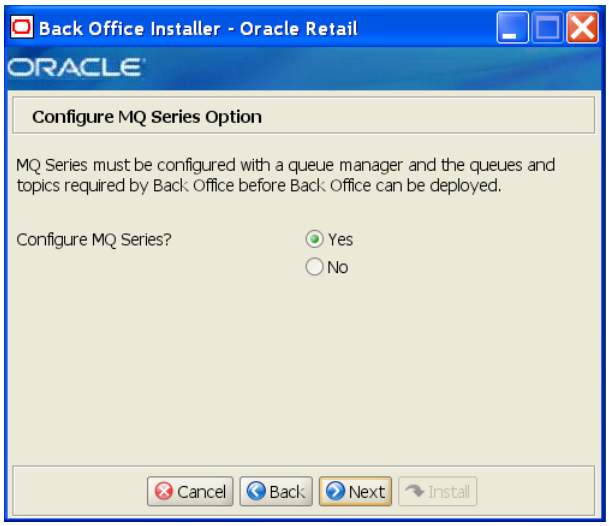
Figure B–21 Install Parameters Option



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 Back Office can be used. This screen gives you the option to set up the parameters manually. If you choose No, see "Install Parameters" in Chapter 3 for the manual steps you need to perform after the installer completes.
Example	Yes
Notes	

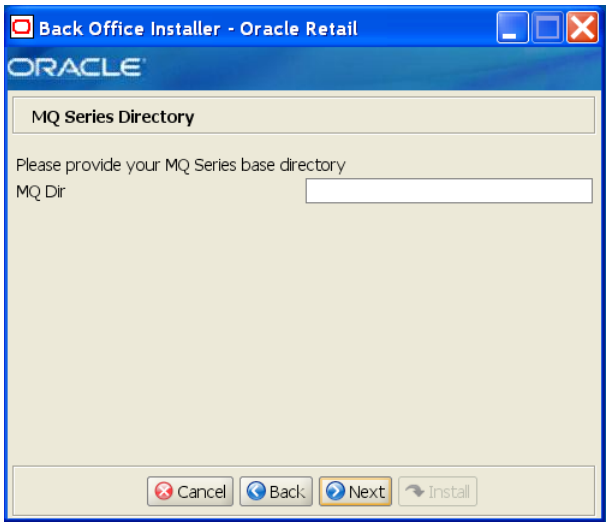
Figure B–22 Configure MQ Series Option



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

Field Title	Configure MQ Series?
Field Description	MQ Series must be configured with a queue manager and the queues and topics required by Back Office before Back Office can be deployed. This screen gives you the option to configure MQ Series manually. If you choose No, see "Configure MQ Series" in Chapter 3 for the manual steps you need to perform after the installer completes.
Example	Yes
Notes	

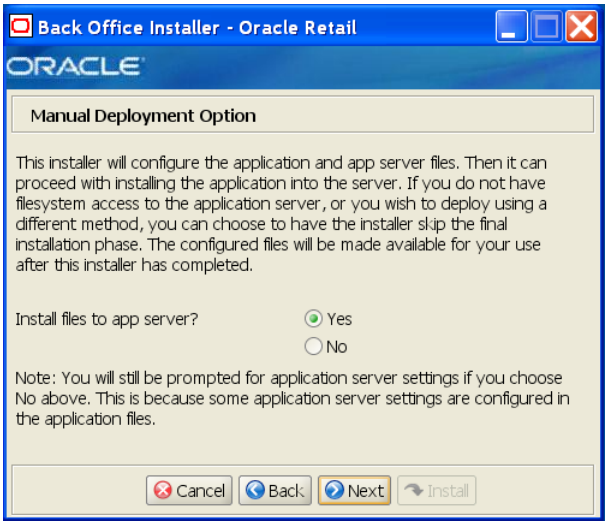
Figure B–23 MQ Series Directory



This screen is only displayed if **Yes** is selected on the Configure MQ Series Option screen. The field on this screen is described in the following table.

Field Title	MQ Dir
Field Description	Base directory for MQ Series.
Example	/opt/mqm
Notes	

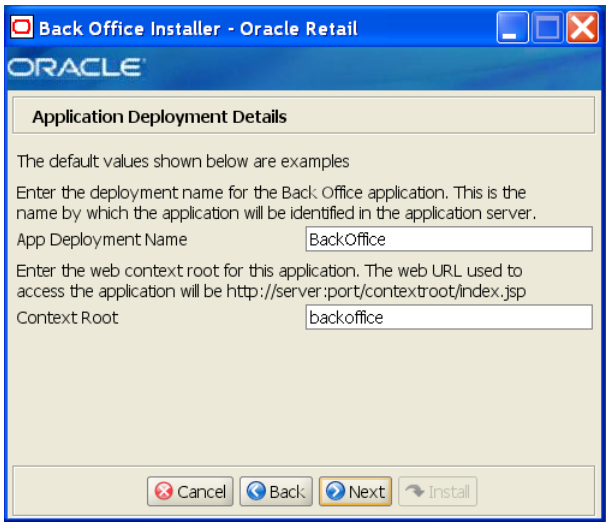
Figure B–24 Manual Deployment Option



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

Field Title	Install files to app server?
Field Description	By default, the installer will deploy the ear file. This screen gives you the option to 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 the deployed files must be reviewed by another party before being applied. If you choose No, see "Manual Deployment Option" in Chapter 3 for the manual steps you need to perform after the installer completes.
Example	Yes
Notes	

Figure B–25 Application Deployment Details

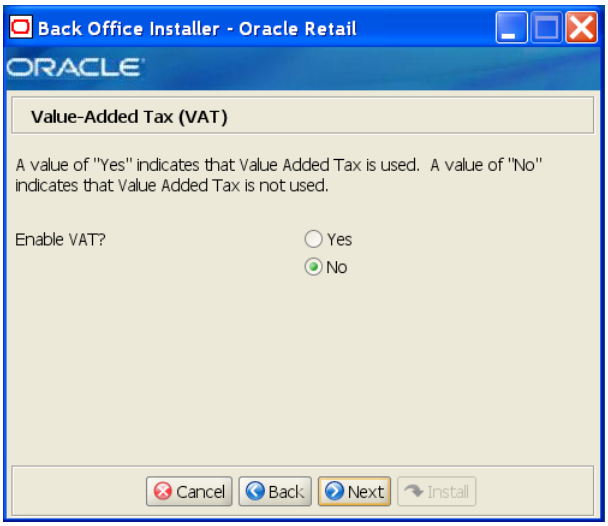


The fields on this screen are described in the following tables.

Field Title	App Deployment Name
Field Description	Name by which this Back Office application will be identified in the application server.
Example	BackOffice
Notes	

Field Title	Context Root
Field Description	Path under the HTTPS URL that will be used to access the Back Office application. For example, a context root of 'backoffice' will result in the application being accessed at `https://host:port/backoffice/index.jsp`.
Example	backoffice
Notes	

Figure B–26 Value-Added Tax (VAT)



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

Field Title	Enable VAT?
Field Description	Sets whether Value-Added Tax is used in Back Office. ▪ To enable Back Office to use VAT, choose Yes. ▪ To not use VAT, choose No.
Example	No
Notes	

Figure B–27 Installation Progress

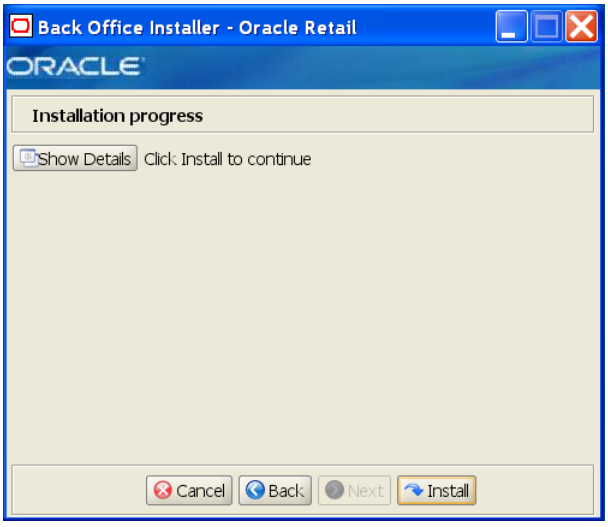
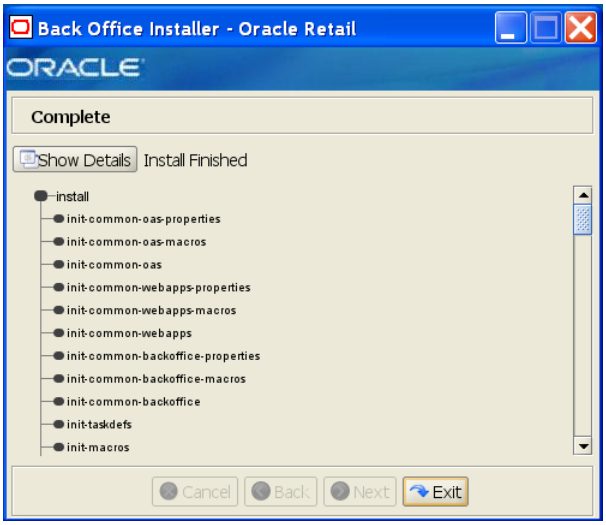


Figure B–28 Installation Complete



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 3.

C

Appendix: Installer Silent Mode

In addition to the GUI and text interfaces of the Back Office installer, there is a silent mode that can be run. This mode is useful if you wish to run a new installation and use the settings you provided in a previous installation. It is also useful if you encounter errors in the middle of 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. 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` file 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. Run the installer again with the silent argument.

```
install.sh silent [oracle | websphere]
```

D

Appendix: Reinstalling Back Office

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

Reinstalling Back Office on the Oracle Stack

To reinstall:

1. Stop the OC4J Back Office instance.
2. Delete the instance.
3. Recreate the OC4J Back Office instance.
4. Start the instance.
5. Run the Back Office installer. For more information, see "Run the Back Office Application Installer" in Chapter 2.

Reinstalling Back Office on the IBM Stack

To reinstall:

1. Stop the WebSphere application server in the profile that contains Back Office.
2. Delete the profile.
3. Stop the WebSphere MQ queue manager and listener. For example, stop `bo.queue.manager`.
4. Delete the queue manager.
5. Recreate the profile.
6. Start the WebSphere application server in the profile.
7. Run the Back Office installer. For more information, see "Run the Back Office Application Installer" in Chapter 3.

E

Appendix: URL Reference

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

URLs for the Oracle Stack

The following sections describe the URLs used for the Oracle stack.

JDBC URL for a Database

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

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

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

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

JNDI Provider URL for an Application

Used for server-to-server calls between applications.

Syntax: `opmn:ormi://<host>:<port>:<instance>/<app>`

- *<host>*: host name of the OracleAS environment
- *<port>*: OPMN request port of the OracleAS environment. This can be found in the *<ORACLE_HOME>*`/opmn/conf/opmn.xml` file
- *<instance>*: name of the OC4J instance running the application
- *<app>*: deployment name for the application

For example, `opmn:ormi://myhost:6003:rpm-oc4j-instance/rpm12`

Note: The JNDI provider URL can have a different format depending on your cluster topology. Consult the Oracle Application Server documentation for further details.

Deployer URI

Used by the Oracle Ant tasks to deploy an application to an OC4J instance. The application installer does not ask the user for this value. It is constructed based on other inputs and written to the `ant.install.properties` file for input to the installation script. For repeat installations using silent mode, you may need to correct mistakes in the deployer URI.

> **Note:** There are several different formats for the deployer URI depending on your cluster topology. Consult the Deploying with the OC4J Ant Tasks chapter of the *OC4J Deployment Guide* for further details.

Syntax (managed OC4J):
`deployer:cluster:opmn://<host>:<port>/<instance>`

- *<host>*: host name of the OracleAS environment
- *<port>*: OPMN request port of the OracleAS environment. This can be found in the *<ORACLE_HOME>*`/opmn/conf/opmn.xml` file.
- *<instance>*: name of the OC4J instance where the application will be deployed

For example, `deployer:cluster:opmn://myhost:6003/orco-inst`

Syntax (standalone OC4J): `deployer:oc4j:`*<host>*`:`*<port>*

- *<host>*: host name of the OracleAS environment
- *<port>*: RMI port of the OC4J server. This can be found in the *<ORACLE_HOME>*`/j2ee/home/config/rmi.xml` file.

For example, `deployer:oc4j:myhost:23791`

URLs for the IBM Stack

The following sections describe the URLs 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>*: host name 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>:<iioport>`

- *<host>*: host name of the WebSphere server
- *<iioport>*: 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`

F

Appendix: Common Installation Errors

This appendix describes some common errors encountered during installation of Back Office.

Unreadable Buttons in the Installer

If you are unable to read the text within the installer buttons, it probably means that your JAVA_HOME points to a pre-1.5 JDK. Set JAVA_HOME to a Java development kit of version 1.5 or later and run the installer again.

Installation Errors for the Oracle Stack Only

The following errors occur only when installing for the Oracle stack.

Oracle Application Server Forceful Shutdown

If an error occurs during installation, Oracle Application Server may not shutdown gracefully but will instead do a forceful shutdown. This is a known problem with Oracle Application Server.

You can use `opmnctl status` to check if the application server has stopped appropriately.

"Unable to get a deployment manager" Message

Symptom:

The application installer quits with the following error message:

```
[oracle:deploy] Unable to get a deployment manager.
[oracle:deploy]
[oracle:deploy] This is typically the result of an invalid deployer URI format
being supplied, the target server not being in a started state or incorrect
authentication details being supplied.
[oracle:deploy]
[oracle:deploy] More information is available by enabling logging -- please see
the Oracle Containers for J2EE Configuration and Administration Guide for details.
```

Solution:

This error can be caused by any of the following conditions:

- OC4J instance provided is not running
- Incorrect OC4J instance name provided
- Incorrect OC4J administrative user name, password, or both
- Incorrect OPMN request port provided

Make sure that the OC4J instance is running, and then check the `ant.install.properties` file for entry mistakes. Pay close attention to the input.deployer.uri (see Appendix E), input.oc4j.instance, input.admin.user, and input.admin.password properties. If you need to make a correction, you can run the installer again with this file as input by running silent mode (see Appendix C).

"Could not create system preferences directory" Warning

Symptom:

The following text appears in the installer Errors tab:

```
[May 22, 2006 11:16:39 AM java.util.prefs.FileSystemPreferences$3 run
WARNING: Could not create system preferences directory. System preferences are
unusable.
May 22, 2006 11:17:09 AM java.util.prefs.FileSystemPreferences
checkLockFile0ErrorCode
WARNING: Could not lock System prefs. Unix error code -264946424
```

Solution:

This is related to Java bug 4838770. The `/etc/.java/.systemPrefs` directory may not have been created on your system. See http://bugs.sun.com for details.

This is an issue with your installation of Java and does not affect the Oracle Retail product installation.

Installation Hangs at "Compiling EJB generated code"

Symptom:

The installer freezes for 10 minutes or more showing this as the last message:

```
[[myinstance.name] 06/11/17 16:51:57 Notification ==>Compiling EJB generated code
```

Solution:

Before cancelling the installation, check the OC4J log file. This file is usually located under `$ORACLE_HOME/opmn/logs` and is named after the OC4J instance. This could be a memory problem if you did not follow the steps to set the PermSize space. See "Create a New OC4J Instance for Back Office" in Chapter 2.

"Failed to set the internal configuration" Message

Symptom:

The following text appears in the log file:

```
07/03/19 14:34:51 *** (SEVERE) Failed to set the internal configuration of the
OC4J JMS Server with: XMLJMSServerConfig[file:/D:/10.1.3/OracleAS_1/
j2ee/home/config/jms.xml]
```

Solution:

Check the OC4J log file. This file is usually located under `$ORACLE_HOME/opmn/logs` and is named after the OC4J instance. A NameNotFoundException for `jms/XAQueueConnectionFactory` appears in the log.

To resolve the problem, do the following:

1. Shutdown the application server.
2. Delete the `OracleAS_1/j2ee/<OC4J instance>/persistence/<OC4J instance>_default_group_1/*.lock` file.
3. Restart the application server.

G

Appendix: Troubleshooting Problems on the Oracle Stack

This appendix contains information that may be useful if you encounter errors running Back Office for the first time after an install. These steps are performed by the installer. If you have problems, you may want to ensure the steps were successfully completed by the installer.

Creation of a New OC4J Instance for Back Office

You can skip this section if you are redeploying to an existing OC4J instance.

To create a new OC4J instance:

1. Increase memory for the new OC4J instance by modifying `%ORACLE_HOME%\opmn\conf\opmn.xml`. Locate the OC4J instance you just created, and add the text, shown in bold in the following example, to the start-parameters section.

```
<process-type id="<orbo-inst>" module-id="OC4J" status="enabled">
   <module-data>
      <category id="start-parameters">
         <data id="java-options" value="-server  -XX:PermSize=128m
-XX:MaxPermSize=256m -Djava.security.policy=$ORACLE_
HOME/j2ee/orbo-inst/config/java2.policy -Djava.awt.headless=true
-Dhttp.webdir.enabled=false"/>
      </category>
```

2. Set the -userThreads OC4J option by modifying `%ORACLE_HOME%\opmn\conf\opmn.xml` similar to the previous step. Add the text shown in bold in the following example:

```
<process-type id="<orbo-inst>" module-id="OC4J" status="enabled">
   <module-data>
      <category id="start-parameters">
         <data id="java-options" value="-server  -XX:PermSize=128m
-XX:MaxPermSize=256m -Djava.security.policy=$ORACLE_
HOME/j2ee/orbo-inst/config/java2.policy -Djava.awt.headless=true
-Dhttp.webdir.enabled=false"/>
         <data id="oc4j-options" value="-userThreads"/>
      </category>
```

3. Reload OPMN for this change to take effect.

```
%ORACLE_HOME%\opmn\bin\opmnctl reload
```

4. Increase the transaction timeout for this OC4J instance:
   a. Log into the Enterprise Manager application.

      `http:\\<myhost>:<portnumber>\em`

   b. Click on the OC4J instance that was just created.

      <orbo-inst>

   c. Click the Administration tab, and then the Transaction Manager (JTA) task.
   d. Click the Administration tab of the Transaction Manager page.
   e. Locate the Transaction Timeout field and increase it to at least 120 seconds.
   f. Click **Apply** and then restart the OC4J instance.

Creation of the Back Office Database Schema

The scripts that create the Back Office database schema can be run from the same staging directory as the application files. The database server can be on the same system as the application server or on a different system.

1. Change to the *<INSTALL_DIR>*`\backoffice\db` directory.
2. Set the JAVA_HOME and ANT_HOME environment variables. You can use the JDK and Ant that are installed with the Oracle Application Server.

   ```
   JAVA_HOME=%ORACLE_HOME%\jdk; ANT_HOME=%ORACLE_HOME%\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 `backofficeDBInstall.jar` file.

   ```
   jar -xvf backofficeDBInstall.jar
   ```

5. Modify `db.properties`.
   a. Verify that the following properties are set correctly:

      `db.product=oracle`

      `db.app.server.product=oracleAS`

   b. Uncomment the Oracle properties and comment out properties for the other vendors such as DB2 and MS-SqlServer.
   c. Provide your database settings in the following properties:

      db_user: database user under which tables will be created

      db_password: password for db_user

      db.jdbc-url: JDBC URL for your database

   d. Set the `ora.home.dir` property to point to your OracleAS 10g installation.
   e. Set the host name and port number for the `parameter.apphost` property to point to your Back Office installation.
   f. To enable VAT functionality, uncomment the tax.enableTaxInclusive property in the tax properties section.

6. Run one of the available Ant targets to create the database schema and load data.

   - load_sql: creates tables and other objects; calls seed_data and load_reports
   - seed_data: loads seed data
   - load_reports: loads report data

   For example: `ant load_sql`

   To specifically load the report data, use the following command:
   `ant -f db.xml load_reports`

H

Appendix: Best Practices for Passwords

This appendix covers information about defining passwords for compliance with PABP. It also has specific information for defining passwords for database users. The following topics are covered:

- "Password Guidelines"
- "Special Security Options for Oracle Databases"
- "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 Oracle Databases

The following information is based on Oracle Database version 11.1.0.7 and is found in the *Oracle Database Security Guide*.

Enforcing Password Policies Using Database Profiles

Password policies can be enforced using database profiles. The options can be changed using a SQL statement, for example:

```
alter profile appsample limit
```

Option	Setting	Description
FAILED_LOGIN_ATTEMPTS	4	Maximum number of login attempts before the account is locked.
PASSWORD_GRACE_TIME	3	Number of days a user has to change an expired password before the account is locked.
PASSWORD_LIFE_TIME	90	Number of days that the current password can be used.
PASSWORD_LOCK_TIME	30	Amount of time in minutes that the account is locked.
PASSWORD_REUSE_MAX	10	Number of unique passwords the user must supply before the first password can be reused.
PASSWORD_VERIFY_FUNCTION	<*routine_name*>	Name of the verification script that is used to ensure that the password meets the requirements of the password policy. See "Enforcing Password Policies Using a Verification Script".

Enforcing Password Policies Using a Verification Script

Password policies can be enforced via a password complexity verification script, for example:

```
UTLPWDMG.SQL
```

The password complexity verification routine ensures that the password meets the following requirements:

- Is at least four characters long
- Differs from the user name
- Has at least one alpha, one numeric, and one punctuation mark character
- Is not simple or obvious, such as welcome, account, database, or user
- Differs from the previous password by at least three characters

For example, to set the password to expire as soon as the user logs in for the first time:

```
CREATE USER jbrown
IDENTIFIED BY zX83yT
...
PASSWORD EXPIRE;
```

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 Oracle 11g Database

This appendix has information on setting up and communicating with a secured Oracle 11g database server based on the following assumptions:

- Client authentication is not needed.
- The Oracle wallet is used as a trust store on the database server.

SSL encryption for Oracle JDBC has been supported in the JDBC-OCI driver since Oracle JDBC 9.2.x, and is supported in the THIN driver starting in 10.2. SSL authentication has been supported in the JDBC-OCI driver since Oracle JDBC 9.2.x. The THIN driver supports Oracle Advanced Security SSL implementation in Oracle Database 11g Release 1 (11.2).

For more information, see the following websites:

- http://www.oracle.com/technology/tech/java/sqlj_jdbc/pdf/wp-oracle-jdbc_thin_ssl.pdf
- http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/toc.htm
- http://download.oracle.com/docs/cd/B28359_01/java.111/b31224/toc.htm

Creating the Oracle Wallet and Certificate for the Server

Note the following information:

- The Advanced Security options must be installed with the database server.
- If you want have a user interface, run `owm` from `$ORACLE_HOME/bin` as `oracle/oracle`.
- The wallet you create must support Auto Login. It must be enabled on the new wallet.
- The following is the wallet directory default:
  - `ORACLE_HOME/admin/ORACLE_SID`
  - Test server wallet information:
    * Wallet password: securedb11g
    * Wallet directory: `/u01/oracle/admin/SECURDB11G`

- When generating a self-signed certificate, note the following:
  - Do not use keytool to create a certificate for using Oracle wallets. They are incompatible.
  - Two wallets are needed to generate a self-signed certificate. One wallet is needed to sign the certificate and another wallet is needed to use the certificate.
  - For command line wallet access, use `orapki`.
  - For instructions on generating a self-signed certificate, see *APPENDIX B CREATING TRUSTSTORES AND KEYSTORES* in the following document:

    http://www.oracle.com/technology/tech/java/sqlj_jdbc/pdf/wp-oracle-jdbc_thin_ssl.pdf
  - The following are examples of `orapki` commands:
    * To create the wallet:

      ```
      orapki wallet create -wallet <wallet directory>
      ```

    * To add the self-signed certificate:

      ```
      orapki wallet add -wallet <wallet directory> -dn
      CN=<certificate name>,C-US -keysize 2048 -self_signed -validity 3650
      ```

    * To view the wallet:

      ```
      orapki wallet display -wallet <wallet directory>
      ```

- The Wallet Manager UI can also be used to import certificates.

Securing the Listener on the Server

The `listener.ora`, `tnsnames.ora`, and `sqlnet.ora` files are found in the `$ORACLE_HOME/network/admin` directory. If the `sqlnet.ora` file does not exist, you need to create it.

To secure the listener on the server:

1. Add TCPS protocol to the `listener.ora` file.
2. Add TCPS protocol to the `tnsnames.ora` file.
3. Add the Oracle Wallet location to the `sqlnet.ora` and `listener.ora` files.
4. Add disabling of client authentication to the `sqlnet.ora` and `listener.ora` files.
5. Add encryption-only cipher suites to the `sqlnet.ora` file.
6. Bounce the listener once the file is updated.

Examples of Network Configuration Files

Examples of the following network configuration files are shown in this section:

- listener.ora
- sqlnet.ora
- tnsnames.ora

listener.ora

```
SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME = PLSExtProc)
      (ORACLE_HOME = /u01/oracle/11g)
      (PROGRAM = extproc)
    )
  )

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = 10.143.44.108)(PORT = 1521))
      (ADDRESS = (PROTOCOL = TCPS)(HOST = 10.143.44.108)(PORT = 2484))
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROCO))
    )
  )

WALLET_LOCATION=(SOURCE=(METHOD=FILE)
  (METHOD_DATA=(DIRECTORY=/u01/oracle/admin/SECURDB11G)))

SSL_CLIENT_AUTHENTICATION=FALSE
```

Caution: To generate a trace log, add the following entries to the `listener.ora` file:

```
TRACE_LEVEL_LISTENER = ADMIN
TRACE_DIRECTORY_LISTENER = /u01/oracle/10g/network/trace
TRACE_FILE_LISTENER = listener.trc
```

sqlnet.ora

```
SSL_CLIENT_AUTHENTICATION=FALSE

SSL_CIPHER_SUITES=(SSL_DH_anon_WITH_3DES_EDE_CBC_SHA, SSL_DH_anon_WITH_RC4_128_
MD5, SSL_DH_anon_WITH_DES_CBC_SHA)

WALLET_LOCATION=(SOURCE=(METHOD=FILE)
  (METHOD_DATA=(DIRECTORY=/u01/oracle/admin/SECURDB11G)))
```

tnsnames.ora

```
SECURDB11G =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = 10.143.44.108)(PORT = 1521))
      (ADDRESS = (PROTOCOL = TCPS)(HOST = 10.143.44.108)(PORT = 2484))
    )
    (CONNECT_DATA =
```

```
    (SERVER = DEDICATED)
    (SERVICE_NAME = SECURDB10G)
  )
)
```

Securing Client Access

> **Caution:** Ensure you are using `ojdbc.jar` version 10.2.x or later. Version 10.1.x or earlier will not connect over TCPS.

To secure client access:

1. Export the self-signed certificate from the server Oracle Wallet and import it into a local trust store.
2. Use the following URL format for the JDBC connection:

   ```
   jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=tcps) (HOST=10.143.44.108)
   (PORT=2484) ) (CONNECT_DATA= (SERVICE_NAME=SECURDB11G)))
   ```

3. The database connection call requires the following properties to be set, either as system properties or JDBC connection properties:

Property	Value
oracle.net.ssl_cipher_suites	(SSL_DH_anon_WITH_3DES_EDE_CBC_SHA, SSL_DH_anon_WITH_RC4_128_MD5, SSL_DH_anon_WITH_DES_CBC_SHA)
javax.net.ssl.trustStore	Path and file name of trust store For example: `/DevTools/Testing/Secure10g/truststore/truststore`
javax.net.ssl.trustStoreType	JKS
javax.net.ssl.trustStorePassword	Password for trust store

Specific Instructions for Back Office

Complete the following steps.

Configuring the Application Server Machine

To configure the application server machine, note the following:

- As a client, the application server machine needs to have the trusted certificate added to a local trust store. Follow the previous instructions for exporting the known certificate and importing it to a local trust store.

  This is not required as Release 13.0 Oracle Retail Back Office uses Diffie-Hellman anonymous authentication. With Diffie-Hellman anonymous authentication, neither the server nor the client will be authenticated.

- Oracle Application Server 10.1.3.5 is using the `ojdcb14.jar` file for 10.1.0.5. You need to update the JDBC driver to a 10.2 version.

- For information on securing a website, see the following website:

  http://download.oracle.com/docs/cd/B31017_01/web.1013/b28957/configssl.htm#CHDHGCDJ

- The following instructions describe creating a JDBC shared lib for application. By default, Oracle Appserver 10.1.3.5 comes up with JDBC drivers but they do not support TCPS protocol. TCPS is supported in database version 10.2.0.3 and later.

  For information on creating a secure JDBC shared library, see the following website:

  http://download.oracle.com/docs/cd/B31017_01/web.1013/b28221/servdats005.htm#BABCEDIG

Securing the Data Source

To edit the data source definition in *<instance>*/config/data-sources.xml:

1. Update the URL to use the expanded Oracle format:

```
***(ex. jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=tcps)
(HOST=10.143.44.108) (PORT=2484) ) (CONNECT_DATA= (SERVICE_NAME=SECURDB11G)))
```

2. Add the SSL JDBC properties. The following example shows part of the data-sources.xml file.

```
<connection-pool name="Oracle11GPool">
   <connection-factory factory-class="oracle.jdbc.pool.OracleDataSource"
user="securuser" password="->securuser"

url="jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=10.143.44.108
)(PORT=2484))(CONNECT_DATA=(SERVICE_NAME=SECURDB11G)))">
     <connection-properties>
  <property name="oracle.net.ssl_cipher_suites"
               value="(SSL_DH_anon_WITH_3DES_EDE_CBC_SHA, SSL_DH_anon_WITH_
RC4_128_MD5, SSL_DH_anon_WITH_DES_CBC_SHA)"/>
       </connection-properties>
    </connection-factory>
</connection-pool>
```

Creating a JDBC Shared Library for the Application

To create the library:

1. Create a directory in $ORACLE_HOME/j2ee/home/shared-lib/oracle.jdbc for the new Oracle JDBC driver shared library. For example, create the following folder:

   $ORACLE_HOME/j2ee/home/shared-lib/oracle.jdbc/10.3

   You reference the actual Oracle JDBC driver jar file relative to this directory. You can either put the Oracle JDBC driver jar file (ojdbc14.jar) from the database into this directory and simply reference the jar file by name, or put it into some other directory and reference the jar file with a partial path relative to this directory.

2. Define the new Oracle JDBC driver shared library and TopLink shared library in the server.xml file.

```
<shared-library name="oracle.jdbc" version="10.3">
<code-source path="ojdbc14.jar"/>
</shared-library>
```

```
<shared-library name="oracle.toplink" version="10.3" library-compatible="true">
<code-source path="../../../toplink/jlib/toplink.jar"/>
<code-source path="../../../toplink/jlib/antlr.jar"/>
<code-source path="../../../toplink/jlib/cciblackbox-tx.jar"/>
<import-shared-library name="oc4j.internal"/>
<import-shared-library name="oracle.xml"/>
<import-shared-library name="oracle.jdbc" max-version="10.3"/>
<import-shared-library name="oracle.dms"/>
</shared-library>
```

3. Import your new shared libraries for your application. To make the new oracle.jdbc and oracle.toplink shared libraries the default for all applications in your OC4J instance, update the `system-applications.xml` file as shown in the following example.

```
<imported-shared-libraries>
   <import-shared-library name="oracle.jdbc" min-version="10.3"
max-version="10.3"/>
   <import-shared-library name="oracle.toplink" min-version="10.3"
max-version="10.3"/>
</imported-shared-libraries>
```

J

Appendix: Secure JDBC with IBM DB2

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 websites:

- 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

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.

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 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 KeyStore

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 KeyStore.

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 KeyStore that stores the Server Certificate.
DB2_SSL_KEYSTORE_PW	Password of the KeyStore that stores the Server Certificate.
DB2_SSL_KEYSTORE_LABEL	Label for the Server Certificate. If it is omitted, the default certificate for the KeyStore 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.

Importing the Server Certificate on the Client

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

1. Copy the certificate to the client.
2. Add the certificate to the trust store used by the JVM using [keytool|Secure Protocols^keytool].

```
keytool -import -file <certificateFile> -keystore <truststoreFile>
```

Caution: It is recommended that the certificate is added to the default `cacerts` truststore or into the `jssecacerts` file located in the same directory as the `cacerts` file.

The password for the default truststore is **changeit**. If you add it to a custom trust store, you need to communicate this to the JVM. Set the location and password for the truststore using the `javax.net.ssl.trustStore` and `javax.net.ssl.trustStorePassword` system properties.

Configuring the Client

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

1. Configure the SSL port.

   This should be a simple change to the JDBC URL. There is no established default SSL port for DB2. You should use what was configured for the server in the server `SSLconfig.ini` file.

2. Configure the `sslConnection` property.

   The property can be configured using either of the following methods:

   - As a property on the datasource/connection:

     ```
     props.setProperty("sslConnection", "true");
     ```

   - As a property in the URL:

     ```
     jdbc:db2://<server>:<port>/<database>:sslConnection=true;
     ```

Note: The IBM documentation references this property as `DB2BaseDataSource.sslConnection`. A review of the driver properties shows the correct value to use is `sslConnection`. A URL reference shows that properties can be set on the URL itself. This should eliminate any need to change code.

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 KeyStore 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 Back Office on IBM WebSphere

It is difficult to configure Oracle Retail Back Office 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.

First, follow in the steps in Configuring the Client. Then 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 websites:

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

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

- http://retailweb.us.oracle.com:8080/download/attachments/12780085/sg247555.pdf?version=1

  An IBM Redbook on security related issues with DB2 including auditing and data encryption. It is dated January 18, 2008 and has a product number SG24-7555-00.