Oracle® Retail Back Office

Installation Guide

Release 13.2.8

E48531-01

January 2014

ORACLE®

Oracle Retail Back Office Installation Guide, Release 13.2.8

E48531-01

Primary Author: Bernadette Goodman

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

G Appendix: Best Practices for Passwords

H Appendix: Secure JDBC with Oracle 11g Database

List of Figures

List of Tables

Send Us Your Comments

Oracle Retail Back Office Installation Guide, Release 13.2.8

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 written for the following audiences:

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

Documentation Accessibility

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

Access to Oracle Support

Oracle customers 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 13.2.8 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, 13.2) or a later patch release (for example, 13.2.8). If you are installing the base release or additional patch releases, read the documentation for all releases that have occurred since the base release before you begin installation. Documentation for patch releases can contain critical information related to the base release, as well as information about code changes since the base release.

Improved Process for Oracle Retail Documentation Corrections

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

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

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

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

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

Oracle Retail Documentation on the Oracle Technology Network

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/technetwork/documentation/oracle-retail-100266.html

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

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

Conventions

The following text conventions are used in this document:

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

1

Preinstallation Tasks

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

Note: The Oracle stack is the configuration that was tested for this release. The components required for an Oracle stack are listed in this chapter. For each component, the tested products and versions are included. While Back Office may work in other configurations, this is the configuration that was tested for this release.

Note: Do not use an IBM stack, as described in a previous release, to install Release 13.2.8. Installing Release 13.2.8 on the IBM stack will result in an unsupported environment.

Check Oracle Retail Merchandising System Version

To integrate with Oracle Retail Merchandising System, version 13.1.8 of Oracle Retail Merchandising System is required. To make the integration work, the hot fix for Oracle Retail Merchandising System bug 14805110 is also needed.

Check Database Server 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
Operating System	Microsoft Windows 2008 Server R2 (64-bit)
Database	Oracle Database 11g Enterprise Edition version 11.2.0.2 (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;
```

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
Operating System	Microsoft Windows 2008 Server R2 (32-bit)
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.
J2EE Application Server JVM	Oracle Java 6 or later in the Java 6 code line
Messaging Provider	included in Oracle Application Server
System Management Agent	OEM 10.1.3.5
Reports publisher	Oracle Business Intelligence Publisher for Retail Back Office, version 10.1.3.4 **Note:** This software is included in the Back Office distribution.

Install Required Patches for the Oracle Stack

To use Oracle Application Server version 10.1.3.5 with an Oracle 11g database, you must use the OPatch utility to apply a patch to Oracle Application Server. Download the patches from My Oracle Support:

https://support.oracle.com

1. Download and install OPatch version 10.1.0.0.0 for your platform. The patch number is 6880880.
2. Use OPatch to apply patch number 5649850.

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 that the Fonts Needed for Reports are Installed

To correctly export reports from Oracle Retail Back Office to a PDF file, any fonts used in the PDF must exist in the application server JVM. To install fonts to the application server:

1. Stop the application server.

2. Copy any needed fonts to the library folder of the JRE used by the application server. The following is an example of the path name to the folder:

   `<Oracle Application Server installation directory>\jdk\jre\lib\fonts`

3. Start the application server.

Check Java Key Store Requirement

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

If you are using the RSA Key Manager, you must use version 3.1 and install the Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files 6.0. See "Install the Java Cryptography Extension (JCE)" in Chapter 2.

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

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 operating system and middleware selected.
- Memory requirements and performance depend on variables including the number of active promotions and best deal calculations when Back Office is installed on the same machine as the Point-of-Service server.
- 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 Portable Data Format (PDF) files

The following Web browsers are supported for this release:

- Microsoft Internet Explorer 8
- Microsoft Internet Explorer 9
- Mozilla Firefox ESR 10+
- Mozilla Firefox ESR 17+

Payment Application Data Security Standard

This release of Oracle Retail Back Office complies with the requirements of the Payment Application Data Security Standard (PA-DSS).

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 Implementation Guide, Volume 3 - Security **(Doc ID: 1081886.1)**

This guide provides information on the PA-DSS requirements.

2

Installation of the Oracle Stack on Windows

Before proceeding, you must install the database and application server software. For a list of tested 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 on to 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>
   -groupName <group name>
   ```

   Including a group name is optional.

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:
   a. `%ORACLE_HOME%\opmn\bin\opmnctl start`
   b. `%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

The following recommendations should be considered for schema owners:

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

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

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 "Enable Data Import".

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 user.

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

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

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

6. Create the schema owner user in the database.

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

7. Grant the schema owner role to the user.

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

8. Create the data source user.

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

9. Grant the data source role to the user.

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

The installer grants the data source connection user access to the application database objects. If you choose **No** on the Manual Deployment Option screen, you need to grant the access after the installer completes. For more information, see "Manual Deployment of the Back Office Application".

Expand the Back Office Distribution

To extract the Back Office files:

1. Extract the `ORBO-13.2.8.zip` file from the Back Office distribution file.
2. Create a new staging directory for the Back Office application distribution (`ORBO-13.2.8.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-13.2.8.zip` to *<staging_directory>* and extract its contents. The following files and directories should be created under *<staging_directory>*`\ORBO-13.2.8`:

```
ant\
ant-ext\
antinstall\
backoffice\
connectors\
external-lib\
installer-resources\
ocm-integration\
retail-public-security-api
.postinstall.cmd
.postinstall.sh
.preinstall.cmd
.preinstall.sh
.preinstall-oas.cmd
.preinstall-oas.sh
.preinstall-was.cmd
.preinstall-was.sh
.preinstall-wl.cmd
antinstall-config.xml
build.xml
build-common.xml
build-common-backoffice.xml
build-common-oas.xml
build-common-was.xml
build-common-webapps.xml
build-test.cmd
checkdeps.cmd
checkdeps.sh
install.cmd
install.sh
jmsconfiguration.dat
prepare.xml
retail-OCM-withAnt.zip
```

For the remainder of this chapter, *<staging_directory>*`\ORBO-13.2.8` 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. Before running the Back Office application installer, you must download the necessary Pager Tag Library files.

To get the Pager Tag library:

1. Download the `pager-taglib-2.0.jar` file from the following Web site: `http://mirrors.ibiblio.org/maven2/jsptags/pager-taglib/2.0/`
2. Rename the jar file to `pager-taglib.jar` and copy that file 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–27 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.

Enable Data Import

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

On the Enable DIMP installer screen, you select whether DIMP will be used. See Figure A–11 in Appendix A. If **Yes** is selected on the screen, you then provide the paths to the directories on the DIMP Configuration installer screen. See Figure A–12 in Appendix A.

For detailed information on DIMP, see the *Oracle Retail Strategic Store Solutions Implementation Guide, Volume 1 - Oracle Retail Strategic Store Solutions to Merchandising Products Integration*.

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 Options"
- "Manual Deployment of the Back Office Application"
- "Install Parameters"

For information on manually deploying the Key Store, see "Manual Deployment of the Key Store".

Install Database Options

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

- If you choose **Create schema with sample dataset**, the installer creates and populates the database with sample data, such as item data. This is the default selection on the screen. The sample dataset includes the minimum dataset and report data. If you want data available to use for demonstrating Back Office functionality after installation, you can select this option.
- If you choose **Create schema with minimum dataset**, the installer creates and populates the database with the minimum amount of data needed to launch and run Back Office. The minimum dataset includes report data. If you want to load your own data after installation, you can select this option.
- If you choose **Skip schema creation and data loading**, the installer does not create and populate the database schema. You choose this option if you want to create and populate the database schema manually. For information on manually creating and populating the database schema, see "Manually Creating the Database Schema".

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

Manually Creating the Database Schema

To manually create and populate the database schema:

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=<INSTALL_DIR>\ant;
   export JAVA_HOME ANT_HOME
   ```

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

   ```
   PATH=$JAVA_HOME\bin:$ANT_HOME\bin:$PATH; export PATH
   ```

4. Expand the backofficeDBInstall.jar file.

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

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

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

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

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

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

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

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

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

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

      Enter the values for the URL used by the Back Office application to access the database schema. See Appendix D for the expected syntax:

      ```
      db.jdbc-url=jdbc:oracle:thin:@DB_HOST_NAME:1521:DB_NAME
      ```

   c. Set the ora.home.dir property to point to your Oracle Application Server installation.

d. Set the host name and rmi port number for the `parameter.apphost` property to point to your Back Office installation.

```
parameters.apphost=ormi://localhost:<rmi_port_number>/BackOffice
```

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

f. To enable VAT functionality, uncomment the tax.enableTaxInclusive property in the tax properties section.

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

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

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

   - load_sample: creates the database schema containing the sample dataset. The sample dataset includes the minimum dataset and report data.
   - load_minimum: creates the database schema containing the minimum dataset. The minimum dataset includes report data.
   - load_reports: loads report data.

   For example: `ant load_sample`

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

Secure the JDBC for the Oracle 11g Database

On the Enable Secure JDBC screen, you select whether secure JDBC will be used for communication with the database. See Figure A–9.

- 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 H.

Install the Java Cryptography Extension (JCE)

If you are using the RSA Key Manager, you must update the security for your JRE. You need to obtain version 6.0 of the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.

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

```
cd %ORACLE_HOME%\jdk\jre\lib\security
copy local_policy.jar local_policy.jar.bak
copy US_export_policy.jar US_export_policy.jar.bak
```

2. Download version 6 of the JCE.

   a. Go to the following web site:

   http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html

   b. Follow the instructions to download the JCE.

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

Run the Back Office Application Installer

An OC4J instance must be configured and started before 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. Set the account of the user running the installer to run as an administrator. Set the account using Microsoft Windows 2008 Server.
4. Run the `install.cmd` script. This will launch the installer. After installation is complete, a detailed installation log file is created: `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 B.

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

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

Oracle Configuration Manager

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

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

https://support.oracle.com

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

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

OCM Documentation Link

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

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`.

Manual Deployment of the Key Store

If you implement a Key Store interface, you can use the rar file to manually deploy the Key Store on the application server.

- To deploy using an ant target:

  1. Copy the following properties into the `ant.install.properties` file:

     ```
     ## Properties from Page:InternalDeployKeyStoreRAR
     input.internal.keystore.rar.deploy.enabled = true
     input.internal.keystore.rar.deploy.name = keystoreconnector
     input.internal.keystore.rar.deploy.file = <INSTALL_DIR>/connectors/
     sim-keystoreconnector-rar.rar
     ```

  2. Run the following ant target:

     ```
     install.cmd ant init keystore-rar-deploy -propertyfile
     ant.install.properties
     ```

- To deploy from the application server console, log in to the application server console and deploy the rar file. The rar file is located at:

  `<INSTALL_DIR>\connectors\sim-keystoreconnector-rar.rar`

Manual Deployment of the Back Office Application

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

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

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

- To deploy using the ant target:
  1. Check that the Key Store JNDI name in the *<orbo-inst>*\applib\spring.properties file matches the JNDI name of the Key Store deployed on the application server.
  2. Update the following property in the ant.install.properties file.

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

  3. Run the following ant target:

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

- To deploy from the application server console, log in to the application server console and deploy the ear file. The ear file is located at:

  <INSTALL_DIR>\backoffice\configured-output

  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.

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".

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\10.1.3.5\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. 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. Run the available Ant target to load the procedures.

   ```
   ant load_purge_procedures
   ```

2. Log in as the database schema owner, <schema_owner_user>.
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.

Figure A–1 Introduction

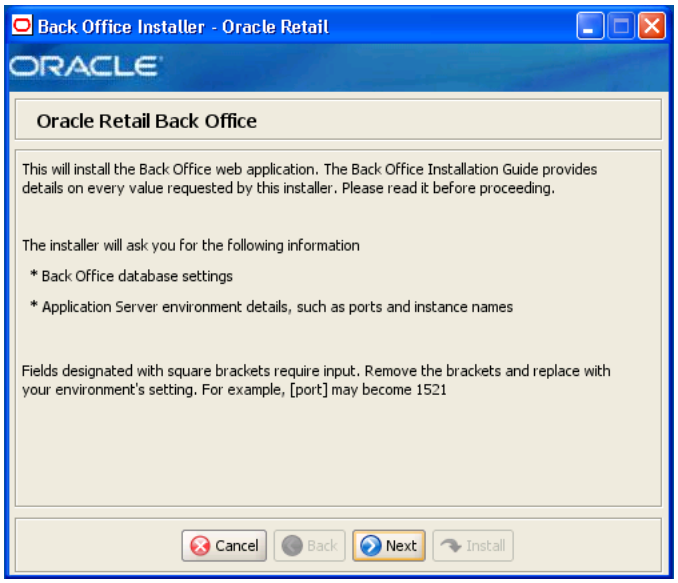
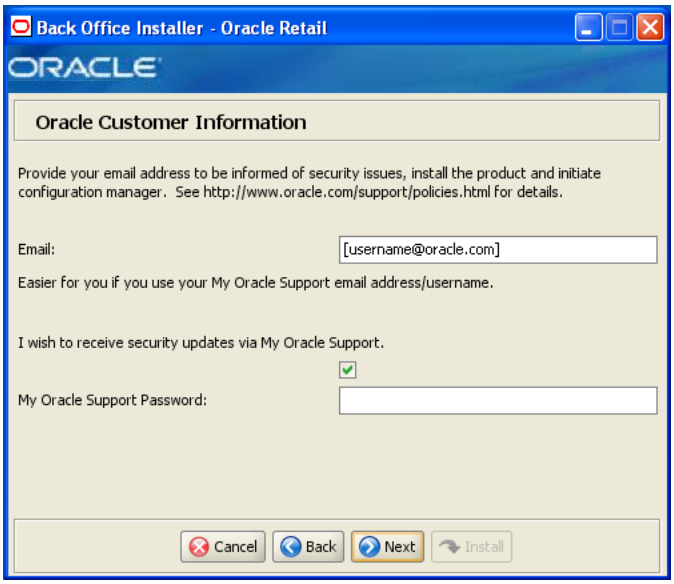


Figure A–2 Oracle Customer Information



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

After the Central Office installer completes, the OCM installer runs if OCM is not already installed. For information on OCM, see "Oracle Configuration Manager" in Chapter 2.

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

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

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

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

Figure A–3 Requirements

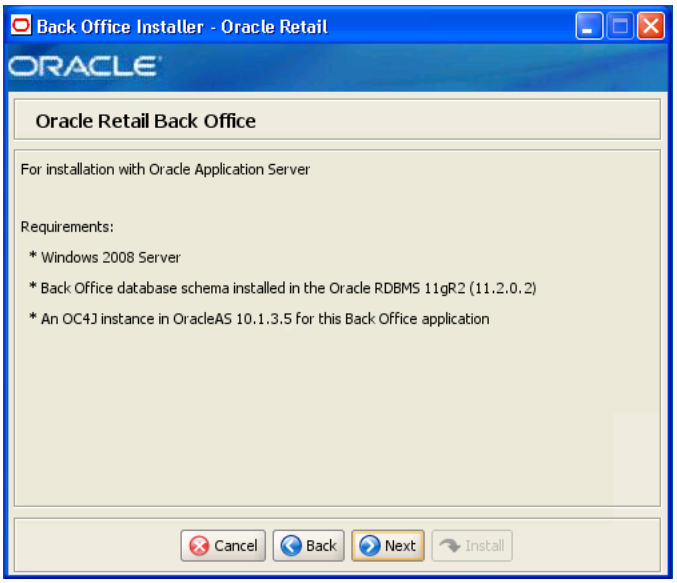
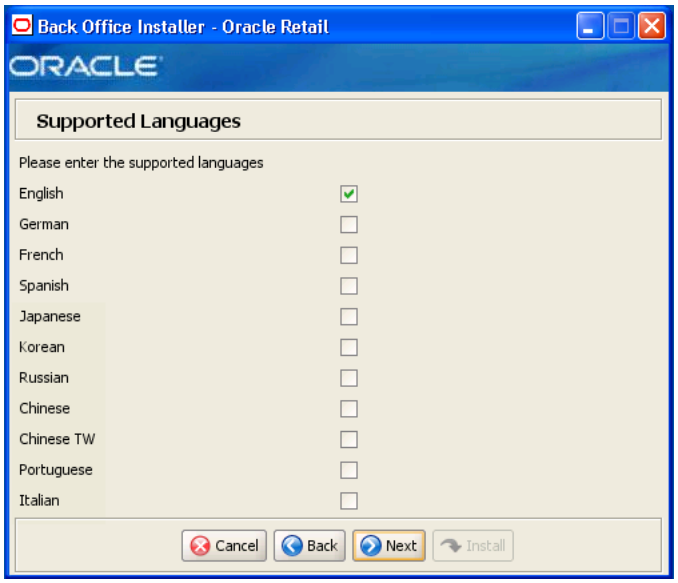


Figure A–4 License Agreement

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

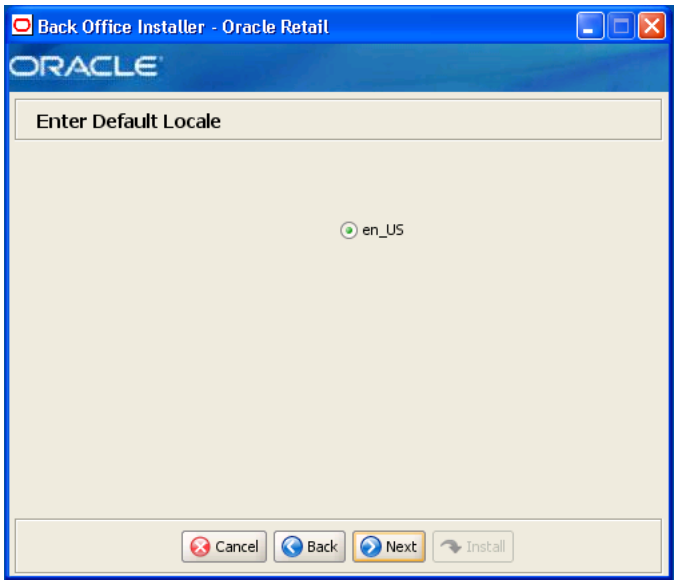
Figure A–5 Supported Languages



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

Field Title	Please enter the supported languages
Field Description	Select the languages that will be available for the Back Office application. The languages selected on this screen determine the available choices on the Enter Default Locale screen.
Example	English

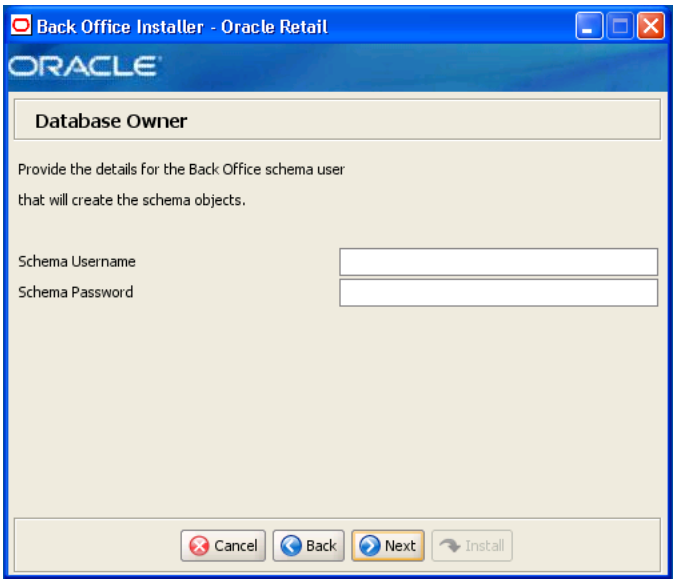
Figure A–6 Default Locale



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

Field Title	Enter Default Locale
Field Description	Locale support in Back Office enables the date, time, currency, calendar, address, and phone number to be displayed in the format for the selected default locale. The choices for default locale are dependent on the selections made on the Supported Languages screen. For example, if English and French are selected on the Supported Languages screen, en_US and fr_FR are the available choices for the default locale.
Example	en_US

Figure A–7 Database Owner

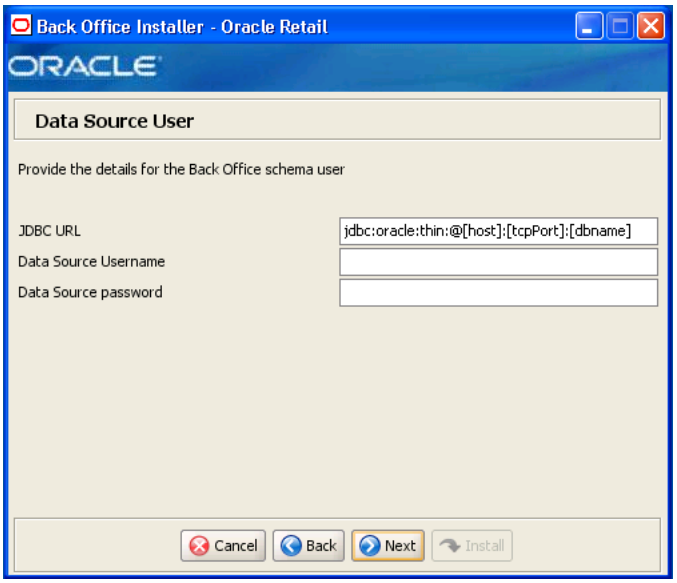


The fields on this screen are described in the following tables.

Field Title	Schema Username
Field Description	Schema user name that manages the objects in the schema. This user has Create, Drop, and Alter privileges in the schema, that is, Data Definition Language (DDL) execution privileges. For information on creating this user, see "Create the Database Schema Owner and Data Source Connection Users" in Chapter 2. **Note:** This user creates the database objects used by Back Office.
Example	DBOWNER

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

Figure A–8 Data Source User



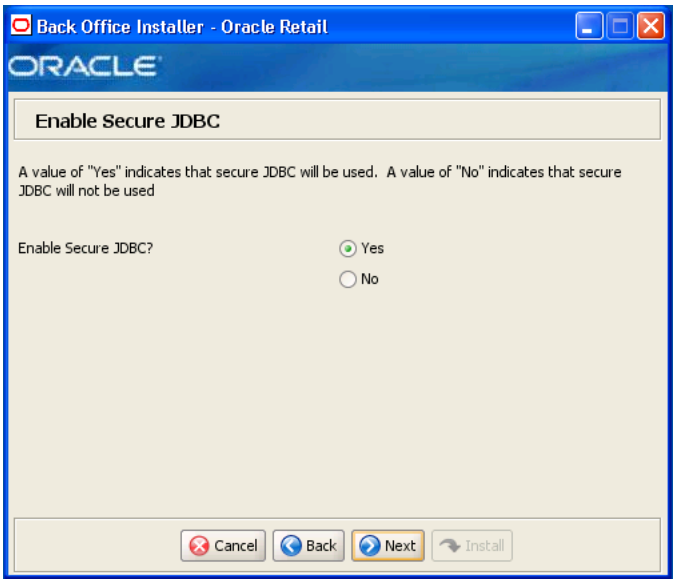
The fields on this screen are described in the following tables.

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

Field Title	Data Source Username
Field Description	Database user name that can access and manipulate the data in the schema. This user can have Select, Insert, Update, Delete, and Execute privileges on objects in the schema, that is, Data Manipulation Language (DML) execution privileges. For information on creating this user, see "Create the Database Schema Owner and Data Source Connection Users" in Chapter 2. **Note:** This schema user is used by Back Office to access the database.
Example	DBUSER

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

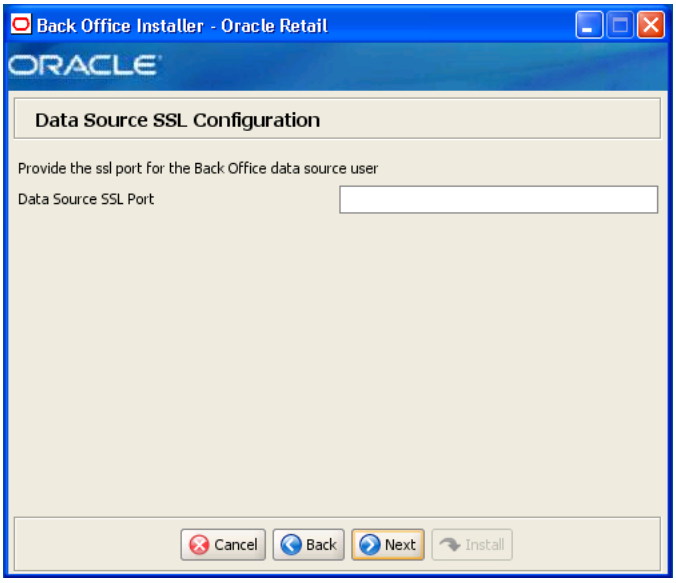
Figure A–9 Enable Secure JDBC



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

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

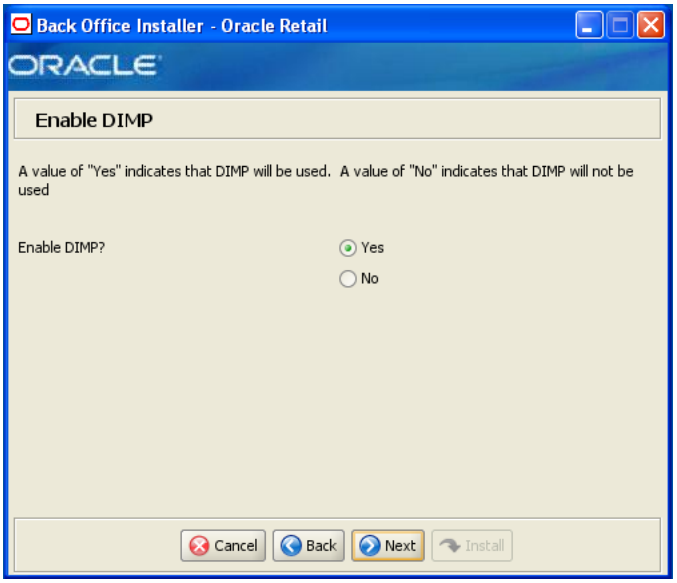
Figure A–10 Data Source SSL Configuration



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

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

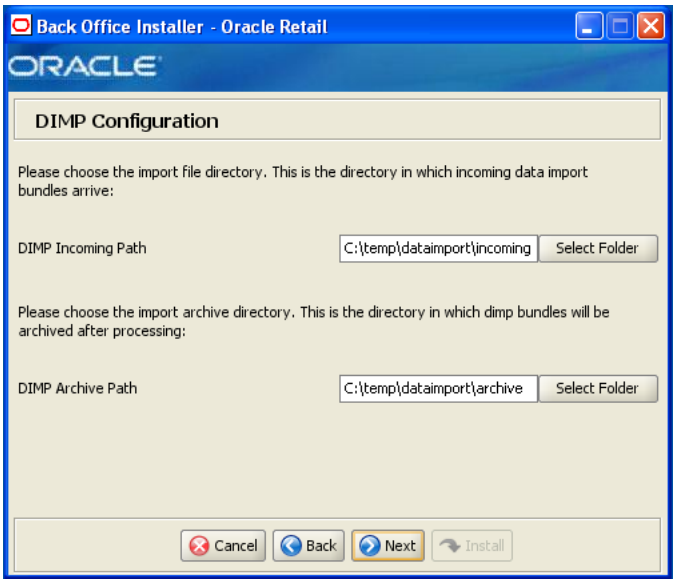
Figure A–11 Enable DIMP



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

Field Title	Enable DIMP?
Field Description	Select whether DIMP will be used. For information on DIMP, see "Enable Data Import" in Chapter 2.
Example	Yes

Figure A–12 DIMP Configuration

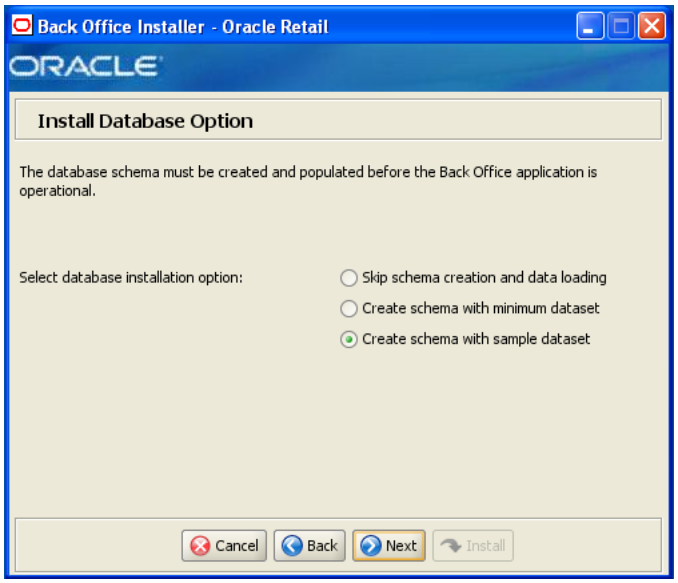


This screen is only displayed if **Yes** is selected on the Enable DIMP screen. The fields on this screen are described in the following tables.

Field Title	DIMP Incoming Path
Field Description	Directory where the incoming data import bundles arrive.
Example	`C:\temp\dataimport\incoming`

Field Title	DIMP Archive Path
Field Description	Directory where the incoming data import bundles are archived after processing.
Example	`C:\temp\dataimport\archive`

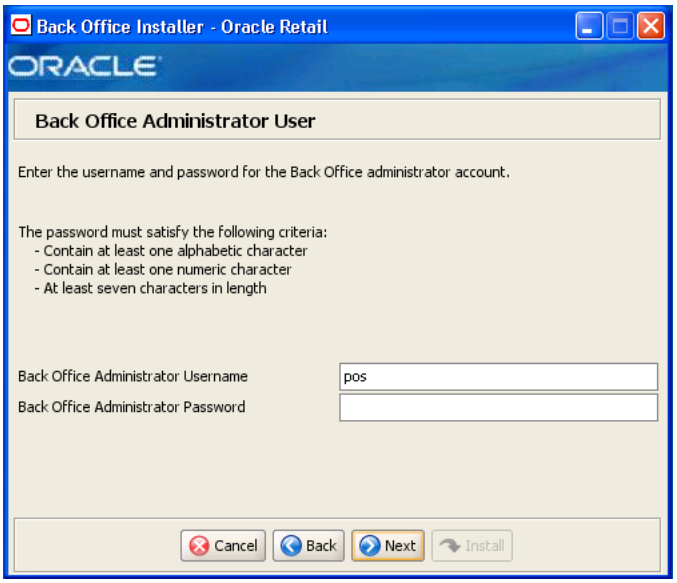
Figure A–13 Install Database Option



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

Field Title	Select database installation option
Field Description	The database schema must be created and populated before starting Back Office. This screen gives you the option to have the installer create and populate the database schema or leave the database schema unmodified. ▪ To have the installer leave the database schema unchanged, select **Skip schema creation and data loading**. ▪ To have the installer create and populate the database schema with the minimum dataset, select **Create schema with minimum dataset**. ▪ To have the installer create and populate the database schema with the sample dataset, select **Create schema with sample dataset**. For more information, see "Install Database Options" in Chapter 2.
Example	Yes

Figure A–14 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

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

Figure A–15 Security Setup: Key Store

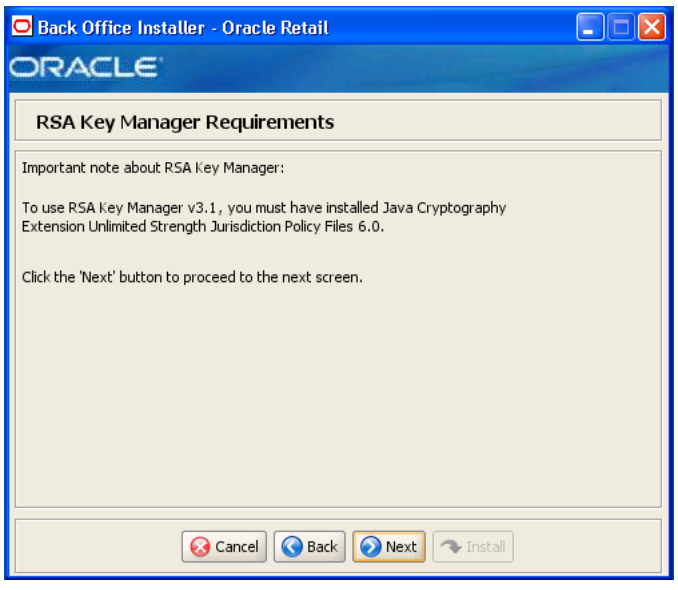
The fields on this screen are described in the following tables.

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

Field Title	Select Key Store Provider
Field Description	Provider for Key Store management. ▪ To use the RSA key management package, select **RSA Key Manager v3.1**. The next screen displayed is Figure A–17. ▪ To use the simulated key management package, select **Simulator**. The next screen displayed is Figure A–19. ▪ To use a different key management provider, select **Other**. The next screen displayed is Figure A–20.
Example	RSA Key Manager v3.1

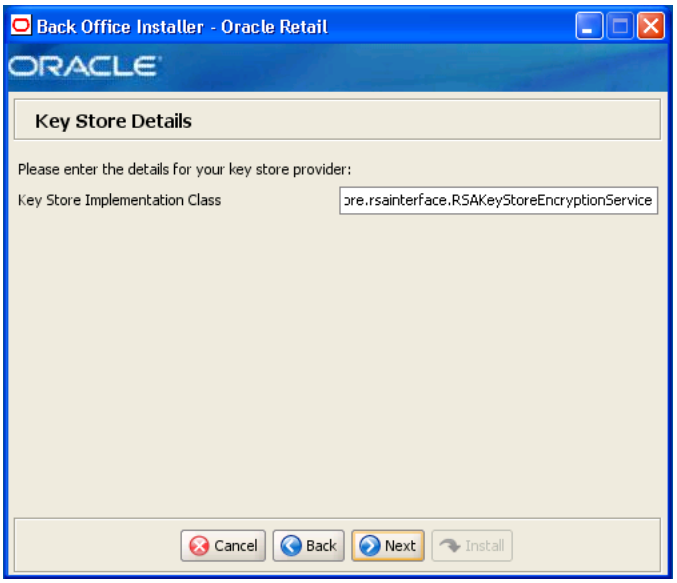
Field Title	Key Store JNDI Name
Field Description	Name of the Key Store JNDI.
Example	eis/keystoreconnector
Notes	

Figure A–16 RSA Key Manager Requirements



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

Figure A–17 Key Store Details

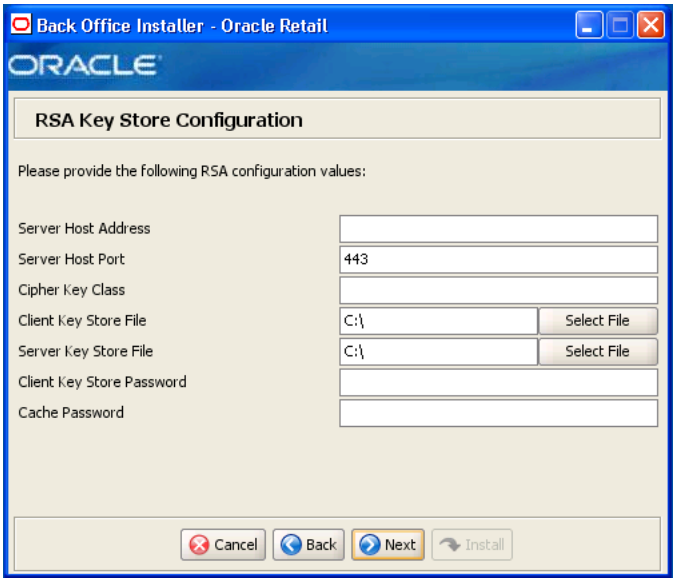


This screen is only displayed if **RSA Key Manager v3.1** is selected for the Key Store provider on the Security Setup: Key Store screen.

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

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

Figure A–18 RSA Key Store Configuration



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

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

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

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

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

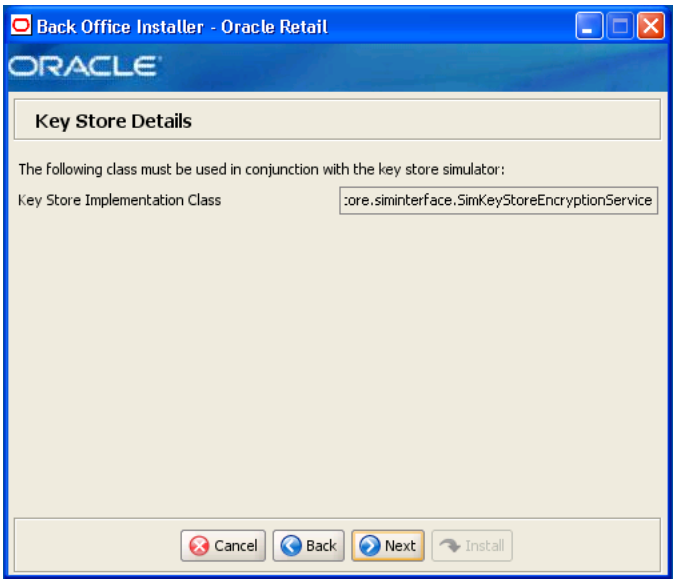
Field Title	Client Keystore File
Field Description	Select the location of the RSA Key Manager client Key Store file.

Field Title	Server Key Store File
Field Description	Select the location of the RSA Key Manager server Key Store file.

Field Title	Client Key Store Password
Field Description	Enter the password used to access the RSA Key Manager client Key Store.

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

Figure A–19 Key Store Details for Simulator Key Manager

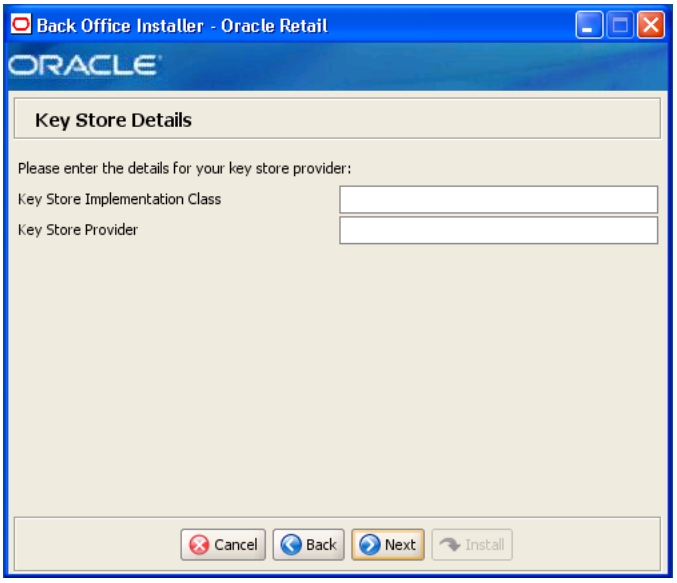


This screen is only displayed if **Simulator** is selected for the Key Store provider on the Security Setup: Key Store screen.

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

Field Title	Key Store Implementation Class
Field Description	Enter the class that invokes the simulated key manager interface.
Example	oracle.retail.stores.simkeystore.siminterface.SimKeyStoreEncryptionService

Figure A–20 Key Store Details for Other Key Manager



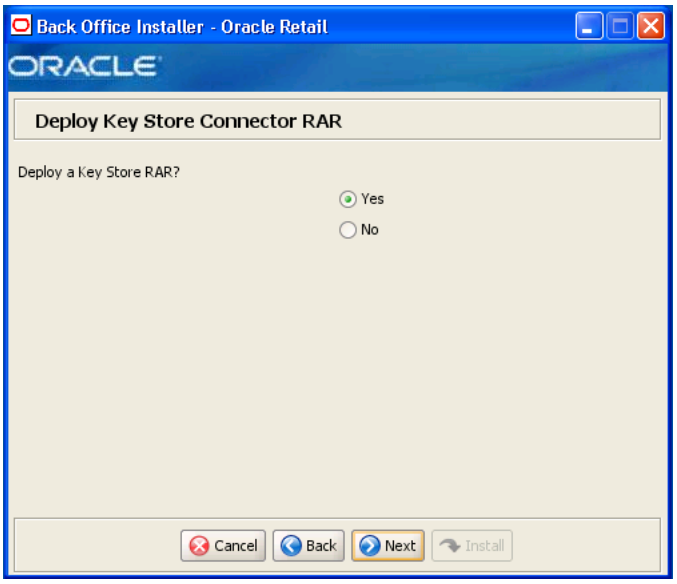
This screen is only displayed if **Other** is selected for the Key Store provider on the Security Setup: Key Store screen.

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

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

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

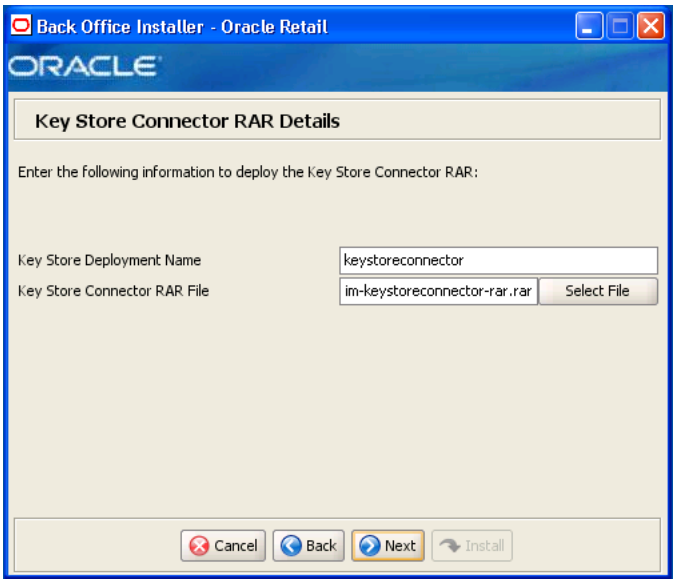
Figure A–21 Deploy Key Store Connector RAR



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

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

Figure A–22 Key Store Connector RAR Details

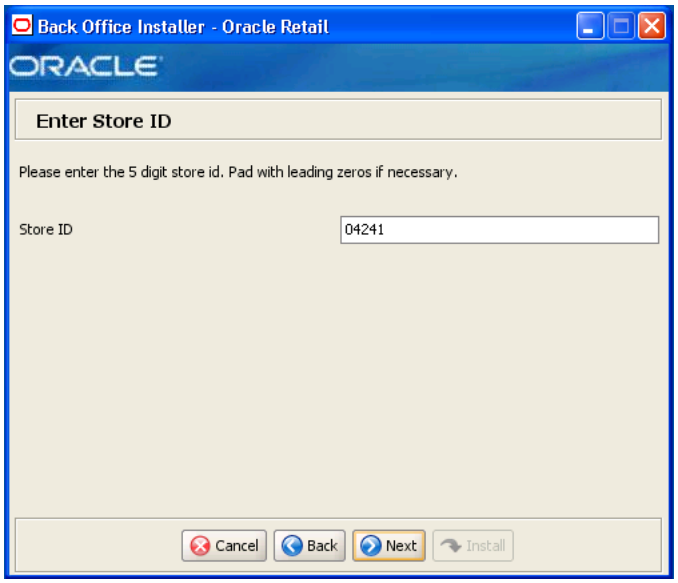


This screen is only displayed if **Yes** is selected on the Deploy Key Store Connector RAR screen. The fields on this screen are described in the following tables.

Field Title	Key Store Deployment Name
Field Description	Name to which the Key Store connector will be deployed.
Example	keystoreconnector

Field Title	Key Store Connector RAR File
Field Description	Path name to the KeyStore Connector RAR file.
Example	`C:\connectors\keystoreconnector-rar.rar`

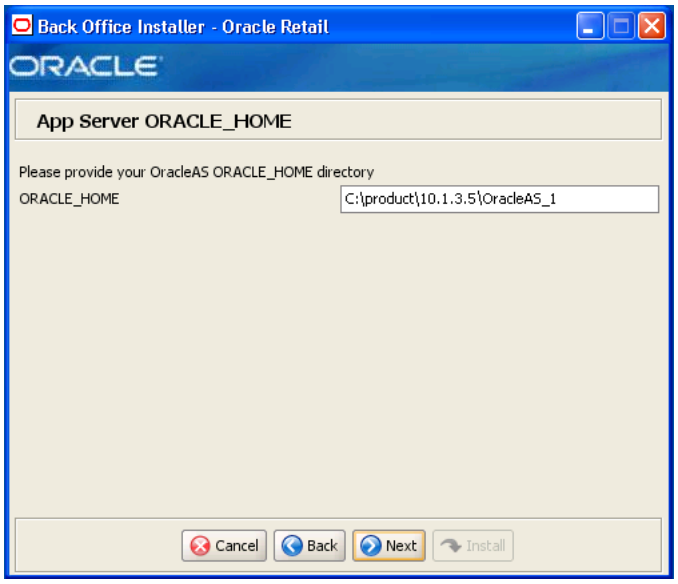
Figure A–23 Enter Store ID



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

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

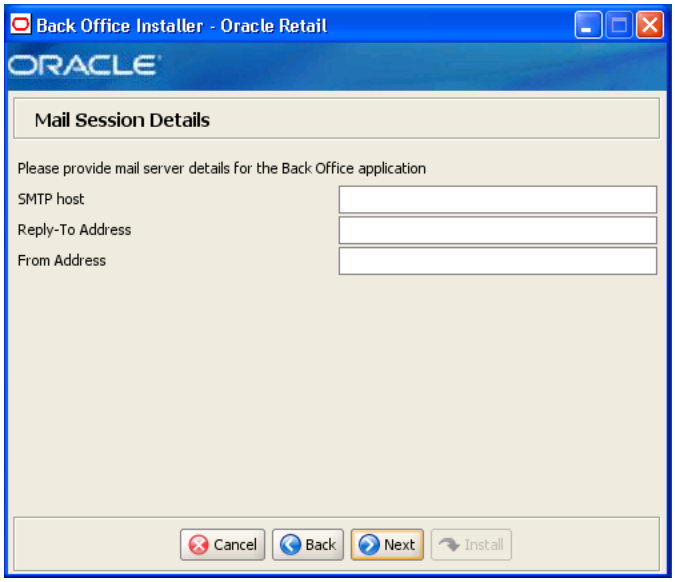
Figure A–24 App Server ORACLE_HOME



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`

Figure A–25 Mail Session Details



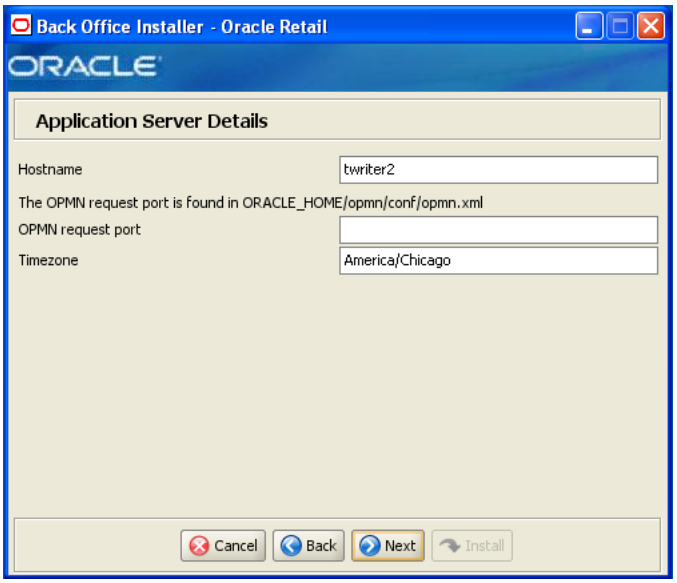
The fields on this screen are described in the following tables.

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

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

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

Figure A–26 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

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

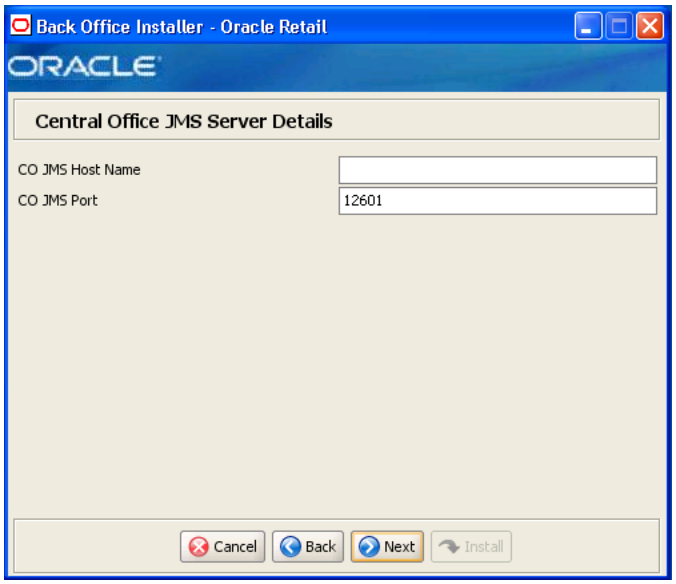
Field Title	Timezone
Field Description	Timezone defined for the application server.
Example	America/Chicago

Figure A–27 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

Figure A–28 Central Office JMS Server Details

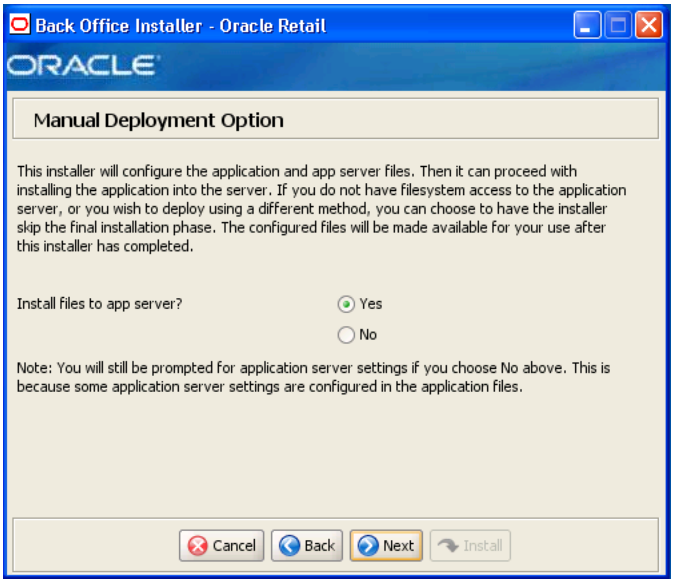


This screen is only displayed if **Yes** is selected on the Central Office JMS Server Integration screen. The fields on this screen are described in the following tables.

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

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

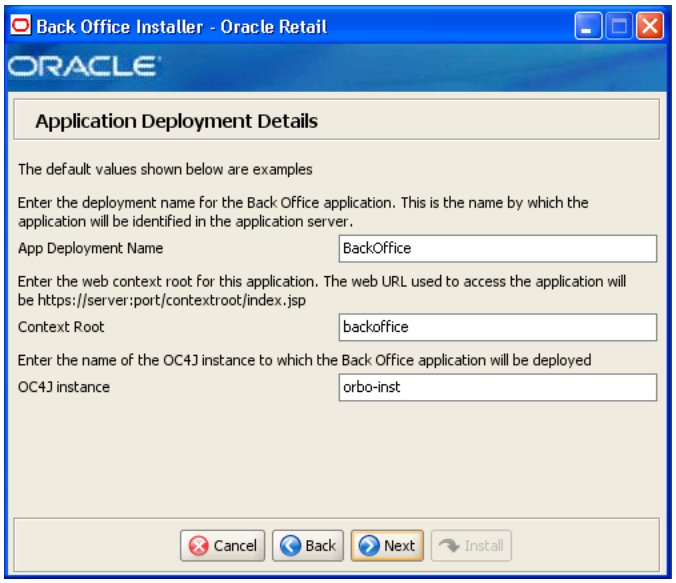
Figure A–29 Manual Deployment Option



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 of the Back Office Application" in Chapter 2 for the manual steps you need to perform after the installer completes.
Example	Yes

Figure A–30 Application Deployment Details



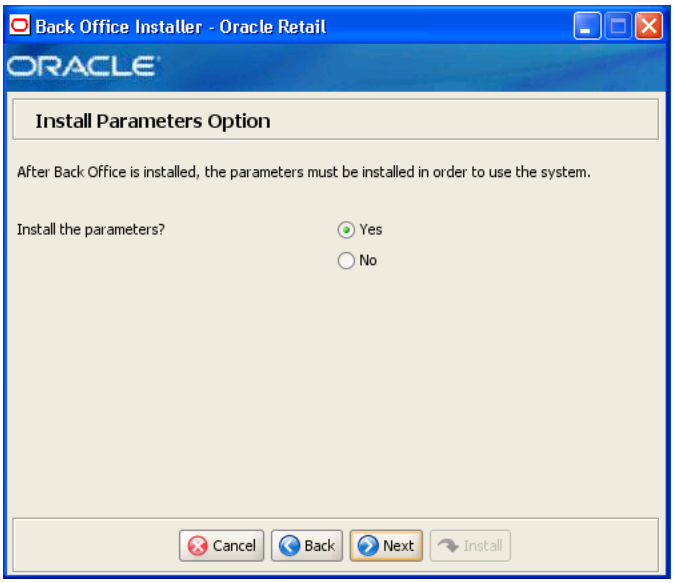
The fields on this screen are described in the following tables.

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

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

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

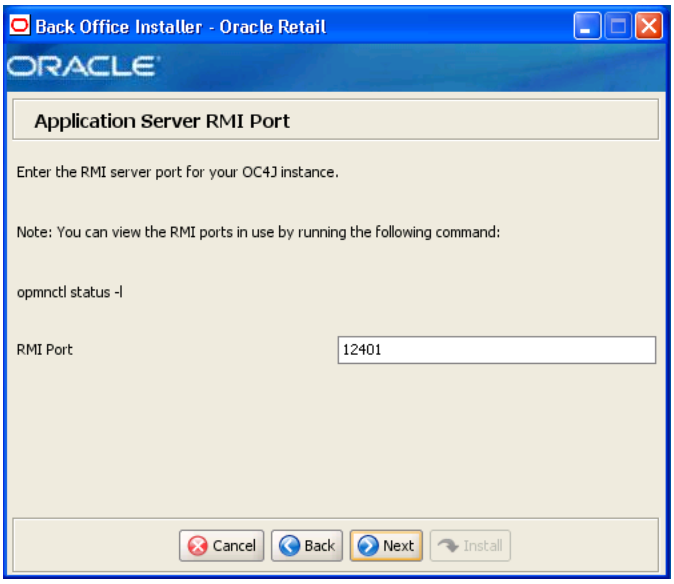
Figure A–31 Install Parameters Options



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

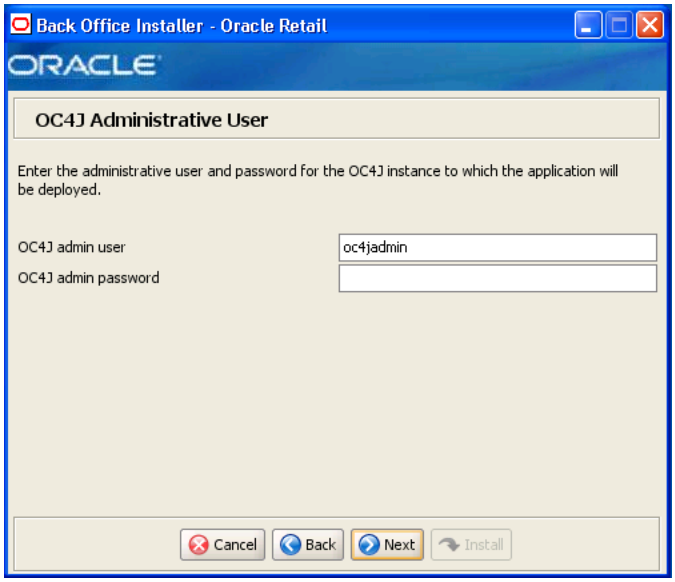
Figure A–32 Application Server RMI Port



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

Figure A–33 OC4J Administrative User

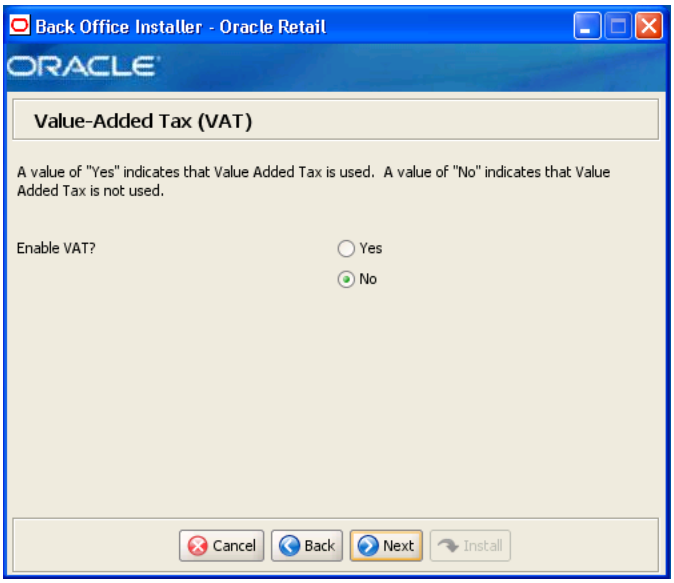


The fields on this screen are described in the following tables.

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

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

Figure A–34 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

Figure A–35 Installation Progress

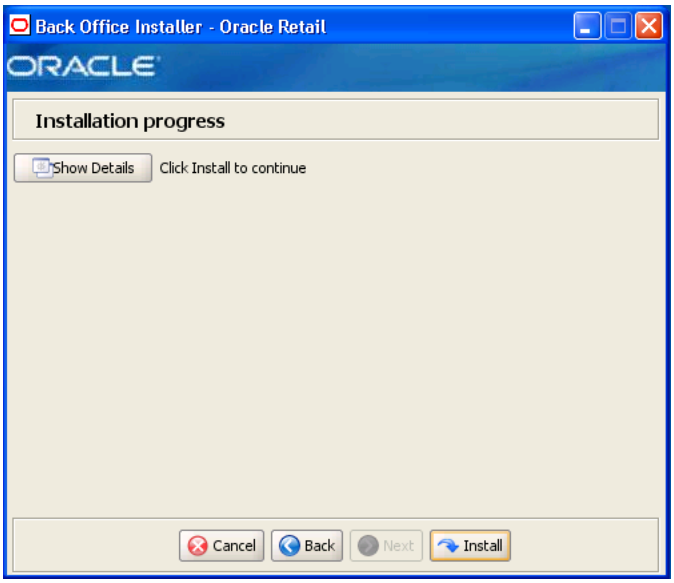
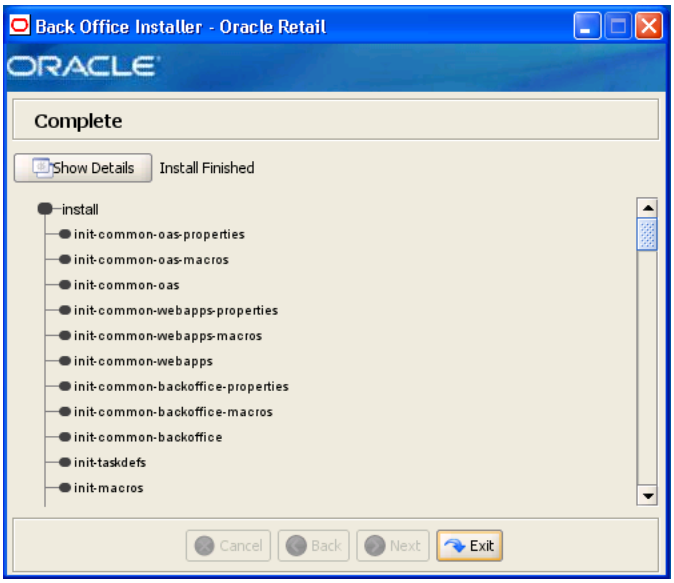


Figure A–36 Installation Complete



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: 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 during an installation and wish to continue after resolving them.

The installer runs in two distinct phases. The first phase involves gathering settings from the user. At the end of the first phase, a properties file named `ant.install.properties` is created with the settings that were provided. 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.cmd silent
   ```

C

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.

D

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`

E

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.

OC4J Instance Does Not Exist

Symptom:

The application installer quits with the following error message:

```
BUILD FAILED

C:\tmp\j2ee\bo\staging\ORBO-trunk\build.xml:697: The following error occurred
while executing this line:
C:\tmp\j2ee\bo\staging\ORBO-trunk\build-common-oas.xml:107: Exiting. OC4J instance
orbo-inst does not exist
```

Solution:

This error occurs because the OC4J instance provided does not exist.

Make sure that the OC4J instance exists, and then check the `ant.install.properties` file for entry mistakes. Pay close attention to the input.deployer.uri (see Appendix D), 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 B).

OC4J Instance is Not Started

Symptom:

The application installer quits with the following error message:

```
BUILD FAILED

C:\tmp\j2ee\bo\staging\ORBO-trunk\build.xml:730: The following error occurred
while executing this line:
C:\tmp\j2ee\bo\staging\ORBO-trunk\build-common-oas.xml:115: Exiting. OC4J instance
orbo-inst exists but is not alive
```

Solution:

This error occurs because the OC4J instance provided is not running.

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 D), 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 B).

"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 D), 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 B).

"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 "Creation of a New OC4J Instance for Back Office" in Appendix F.

"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.

F

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 in to 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.

G

Appendix: Best Practices for Passwords

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

Password Guidelines

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 10.2.0.3 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;
```

H

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 Database Server

Note the following information:

- If you want have a user interface, run `owm` from `$ORACLE_HOME/bin` as `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/11g/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 = SECURDB11G)
    )
  )
```

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/Secure11g/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 13.2 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 `ojdcb5.jar` file for 10.1.0.5 which does not support the SSL protocol. You need to update the JDBC driver to a 11.2.0.2 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 starting in database version 10.2.0.3.

  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 (ojdbc5.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="ojdbc5.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>
```