Oracle® Identity Manager

Installation and Configuration Guide for BEA WebLogic Server

Release 9.1.0

E10370-03

June 2008

Oracle Identity Manager Installation and Configuration Guide for BEA WebLogic Server Release 9.1.0

E10370-03

Primary Author: Lyju Vadassery

Contributing Authors: Shiladitya Guha, Debapriya Datta

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software—Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Contents

11 Installing and Configuring the Oracle Identity Manager Remote Manager

12 Troubleshooting the Oracle Identity Manager Installation

A Java 2 Security Permissions for BEA WebLogic Server

Index

Preface

This guide explains the procedure to install Oracle Identity Manager release 9.1.0 on BEA WebLogic Server.

Audience

This guide is intended for system administrators of Oracle Identity Manager.

Documentation Accessibility

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

`http://www.oracle.com/accessibility/`

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, 7 days a week. For TTY support, call 800.446.2398. Outside the United States, call +1.407.458.2479.

Related Documents

For more information, see the following documents in the Oracle Identity Manager documentation set:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation and Configuration Guide for JBoss Application Server*
- *Oracle Identity Manager Installation and Configuration Guide for IBM WebSphere Application Server*
- *Oracle Identity Manager Installation and Configuration Guide for Oracle Application Server*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Globalization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Tools Reference*
- *Oracle Identity Manager Audit Report Developer's Guide*
- *Oracle Identity Manager Integration Guide for Crystal Reports*
- *Oracle Identity Manager API Usage Guide*
- *Oracle Identity Manager Concepts*
- *Oracle Identity Manager Reference*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager release documentation set, visit Oracle Technology Network at

`http://www.oracle.com/technology/documentation`

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), and names of files, directories, attributes, and parameters.

Convention	Meaning
**_HOME*	This convention represents the directory where an application is installed. The root directory where you install the BEA WebLogic Server is referred to as *BEA_HOME*. The directory where you install the BEA product is referred to as *BEA_PRODUCT_INSTALL*. Typically, *BEA_PRODUCT_INSTALL* is installed in the *BEA_HOME*/`weblogic81` directory. The directory where you install Oracle Identity Manager is referred to as *OIM_HOME*. Each Oracle Identity Manager component includes an abbreviation: *OIM_DC_HOME* for the Design Console and *OIM_RM_HOME* for the Remote Manager.

<Entry 1>.<Entry 2>.<Entry 3>	This convention represents nested XML entries that appear in files as follows:
	`<Entry 1>`
	`    <Entry 2>`
	`        <Entry 3>`

1 Overview of the Installation Procedure

Installing Oracle Identity Manager release 9.1.0 on BEA WebLogic Server involves the following steps:

1. Preparing for the installation: See Chapter 2, "Planning the Installation".
2. Setting up BEA WebLogic Server for Oracle Identity Manager: See Chapter 3, "Installing and Configuring BEA WebLogic Server for Oracle Identity Manager".
3. Setting up a database for Oracle Identity Manager: See Chapter 4, "Installing and Configuring a Database for Oracle Identity Manager".
4. Installing a single Oracle Identity Manager instance: See one of the following chapters based on the operating system:
    - Chapter 5, "Installing Oracle Identity Manager on Microsoft Windows"
    - Chapter 6, "Installing Oracle Identity Manager on UNIX"
5. Performing basic Oracle Identity Manager and BEA WebLogic Server configuration tasks related to the installation setup: See Chapter 7, "Postinstallation Configuration for Oracle Identity Manager and BEA WebLogic Server".
6. Starting Oracle Identity Manager and accessing the Administrative and User Console: See Chapter 8, "Starting and Stopping Oracle Identity Manager".
7. Deploying Oracle Identity Manager in a clustered BEA WebLogic Server installation: See Chapter 9, "Deploying in a Clustered BEA WebLogic Server Configuration".
8. Installing, configuring, and starting the Oracle Identity Manager Design Console: See Chapter 10, "Installing and Configuring the Oracle Identity Manager Design Console".
9. Installing, configuring, and starting the Oracle Identity Manager Remote Manager: See Chapter 11, "Installing and Configuring the Oracle Identity Manager Remote Manager".
10. Troubleshooting the Oracle Identity Manager installation: See Chapter 12, "Troubleshooting the Oracle Identity Manager Installation".

2

Planning the Installation

Oracle recommends that you familiarize yourself with the components required for deployment before installing Oracle Identity Manager. Oracle also recommends that you install and use the Diagnostic Dashboard to ensure that your system is ready for Oracle Identity Manager installation. Refer to the "Using the Diagnostic Dashboard" section on page 2-4 for details of installing the Diagnostic Dashboard.

A basic Oracle Identity Manager installation consists of the following:

- Database server
- Application server
- Oracle Identity Manager running on the application server
- Design Console
- Administrative and User Console running on a Web-browser

This chapter contains the following topics:

- Host Requirements for Oracle Identity Manager Components
- Planning for Non-English Oracle Identity Manager Environments
- Installation Worksheet
- Using the Diagnostic Dashboard

Host Requirements for Oracle Identity Manager Components

This section lists the minimum host system requirements for the various components in an Oracle Identity Manager environment.

> **Note:** Check the Oracle Identity Manager Release Notes for the requirements and supported configurations specific to each version of the Oracle Identity Manager product.

You must obtain the enterprise versions of the application server and database software, complete with valid licenses. Oracle Identity Manager does not include this software.

The Oracle Identity Manager installation program might conflict with other installed applications, utilities, or drivers. Try to remove all nonessential software and drivers from the computer before installing Oracle Identity Manager. This practice also ensures that the database schema can be created in the database host.

Oracle Identity Manager Server (Host) Requirements

Table 2–1 lists the minimum host requirements for Oracle Identity Manager and the guidelines for a basic installation.

Table 2–1 Oracle Identity Manager Server Requirements

Server Platform	Item
Microsoft Windows and Linux	■ Processor Type: Intel Xeon or Pentium IV ■ Processor Speed: 2.4 GHz or higher, 400 MHz FSB or higher ■ Number of Processors: 1 ■ Memory: 2 GB for each Oracle Identity Manager instance ■ Hard Disk Space: 1 GB (initial size)
Solaris	■ Server: Sun Fire V210 ■ Number of Processors: 1 ■ Memory: 2 GB for each Oracle Identity Manager instance ■ Hard Disk Space: 1 GB (initial size)

Database Server Host Requirements

Table 2–2 provides sample database minimum host requirements for selective supported operating systems and should be considered only as guidelines. Refer to database documentation for the specific database host requirements.

Table 2–2 Sample Database Server Host Requirements

Database Server Platform	Item
Microsoft Windows and Linux	■ Processor Type: Intel Xeon ■ Processor Speed: 2.4 GHz or higher, 400 MHz FSB or higher ■ Number of Processors: 2 ■ Memory: 4 GB total or 2 GB for each CPU ■ Hard Disk Space: 40 GB (initial size)
Solaris	■ Server: Sun Fire V250 ■ Number of Processors: 2 ■ Memory: 4 GB total or 2 GB for each CPU ■ Hard Disk Space: 40 GB (initial size) ■ Number of Hard Disks: 1 Disk

Design Console Host Requirements

Table 2–3 lists the minimum host requirements for the Oracle Identity Manager Design Console.

Table 2–3 Design Console Host Requirements

Design Console Platform	Item
Microsoft Windows	■ Processor Type: Intel Pentium IV ■ Processor Speed: 1.4 GHz or higher ■ Number of Processors: 1 ■ Memory: 512 MB ■ Hard Disk Space: 300 MB

Remote Manager Host Requirements

Table 2–4 lists the minimum host requirements for the Oracle Identity Manager Remote Manager.

Table 2–4 Remote Manager Host Requirements

Remote Manager Platform	Item
Microsoft Windows and Linux	■ Processor Type: Intel Pentium IV ■ Processor Speed: 1.4 GHz or higher ■ Number of Processors: 1 ■ Memory: 512 MB ■ Hard Disk Space: 1 GB
Solaris	■ Server: Sun Fire V210 ■ Memory: 1 GB ■ Number of Processors: 1 ■ Hard Disk Space: 10 GB (initial size)
AIX	■ Processor Type: PowerPC ■ Number of Processors: 1 ■ Memory: 512 MB ■ Hard Disk Space: 10 GB

Planning for Non-English Oracle Identity Manager Environments

If you are deploying Oracle Identity Manager components in non-English environments, then review the following guidelines and requirements:

- Before installing any of the Oracle Identity Manager components, ensure that the regional and language settings (locale) on the target system meet the following requirements:
  - An appropriate language version of the operating system is installed.
  - Specific language settings are properly configured.
- Refer to *Oracle Identity Manager Globalization Guide* for information about configuring localized deployments and to ensure that you meet the character restrictions for various components and attributes.
- For Oracle database globalization support, you must configure the database for Unicode. Refer to "Creating an Oracle Database" on page 4-1 for more information.

Installation Worksheet

Table 2–5 provides information about the configuration attributes that you must set during Oracle Identity Manager installation. Print this worksheet and use it to take notes during the installation. Enter information specific to your installation in the User Selection column.

Table 2–5 Installation Worksheet

Item	Default	User Selection
The base directory for installing Oracle Identity Manager	Microsoft Windows: `C:\oracle` UNIX: `/opt/oracle`	
The name or IP address of the computer on which the Oracle Identity Manager database is installed	No default value	
The TCP port number on which the database listens for connections	1521 for Oracle 1433 for Microsoft SQL Server **Note:** Microsoft SQL Server is not supported in Oracle Identity Manager release 9.1.0. See "Certified Components" in *Oracle Identity Manager Release Notes* for information about certified components.	
The name of the database for your installation	No default value	
The name and password of the database account that Oracle Identity Manager uses to access the database	No default value	
The JDK installation directory	Microsoft Windows: `C:\bea\j2sdk`*`version`* or `C:\bea\jrockit`*`version`* UNIX: `/opt/bea/jrockit`*`version`*	
The BEA WebLogic Server root directory	Windows: `C:\bea` UNIX: `/opt/bea`	
The BEA WebLogic Server installation directory	Windows: `C:\bea\weblogic81` UNIX: `/opt/bea/weblogic81`	

Using the Diagnostic Dashboard

The Diagnostic Dashboard is a Web application that runs on the application server. It checks the preinstallation and postinstallation environments for components required by Oracle Identity Manager. Oracle recommends that you install the Diagnostic Dashboard before installing Oracle Identity Manager.

Installing the Diagnostic Dashboard

The Diagnostic Dashboard files are located in the `DiagnosticDashboard directory` on the Oracle Identity Manager Installer CD media.

You must deploy the Diagnostic Dashboard Web application on the application server.

> **See Also:** *Oracle Identity Manager Administrative and User Console Guide* for more information about the Diagnostic Dashboard

Verifying the Preinstallation Environment

You can use the Diagnostic Dashboard to verify that the components required to install Oracle Identity Manager are present:

- A supported Java Virtual Machine (JVM)
- A supported database
- Microsoft SQL Server JDBC libraries (only if you use Microsoft SQL Server)

Note: Microsoft SQL Server is not supported in Oracle Identity Manager release 9.1.0. See "Certified Components" in *Oracle Identity Manager Release Notes* for information about certified components.

See Also: *Oracle Identity Manager Administrative and User Console Guide* for information about the Diagnostic Dashboard

3

Installing and Configuring BEA WebLogic Server for Oracle Identity Manager

This chapter explains the following tasks that you must perform before installing Oracle Identity Manager on BEA WebLogic Server:

1. Installing BEA WebLogic Server
2. Creating a WebLogic Domain, Group, and User for Oracle Identity Manager
3. (Optional and for Solaris only) Preparing to Install Oracle Identity Manager As a Non-Root User on Solaris

After completing the tasks in this chapter, you must install and configure a database by following the steps in Chapter 4, "Installing and Configuring a Database for Oracle Identity Manager" before installing Oracle Identity Manager.

> **Note:** Follow the instructions in Chapter 9, "Deploying in a Clustered BEA WebLogic Server Configuration" if you are deploying BEA WebLogic Server in an application server cluster with Managed Servers.

Installing BEA WebLogic Server

Perform a default (complete) installation of BEA WebLogic Server. Refer to BEA WebLogic Server documentation for detailed procedures.

Creating a WebLogic Domain, Group, and User for Oracle Identity Manager

Before you install Oracle Identity Manager on BEA WebLogic Server, you must create a WebLogic domain, group, and user for Oracle Identity Manager.

To create a WebLogic domain, group, and user for Oracle Identity Manager:

1. Start the WebLogic Configuration Wizard:

   For Microsoft Windows:

   From the **Start** menu, select **BEA WebLogic Platform**, and then select **Configuration Wizard**.

   For UNIX:

   a. Go to the WebLogic bin directory:

      ```
      cd BEA_HOME/weblogic81/common/bin
      ```

   b. Start the Configuration Wizard using the following command:

      ```
      sh config.sh
      ```

2. In the Configuration Wizard:

   a. Select the **Create a new WebLogic configuration** option.

   b. Select the **Basic WebLogic Server Domain** template.

   c. Select the **Express Mode** option.

   d. Enter a user name and password, and confirm the password for the domain.

      Note: This is the account used for Oracle Identity Manager. Make note of the user name and password. You must provide this information when you install Oracle Identity Manager.

      ---

   e. Select either **Development Mode** or **Production Mode.**

   f. Select the appropriate JDK. Before selecting, ensure that it is the certified JDK for BEA WebLogic Server.

   g. Change the location or name of the domain configuration if required.

   h. Exit the Configuration Wizard after creating the domain.

3. Start the BEA WebLogic Server:

   For Microsoft Windows:

   Start BEA WebLogic Server from the **Start** menu by selecting **BEA WebLogic Platform**, then **User Projects**, then `domain name`, and then **Start Server**.

   For UNIX:

   a. Go to the WebLogic user_projects/domains directory.

      For example: `cd BEA_HOME/user_projects/domains/`

   b. Go to the directory of the domain that you just created using the Configuration Wizard. For example:

      ```
      cd domain name
      ```

   c. Start the BEA WebLogic Server using the following command:

      ```
      sh startWebLogic.sh
      ```

4. Log on to the WebLogic Server Administration Console by using your new account and by pointing a Web browser to the following URL:

   ```
   http://hostname:7001/console
   ```

   a. From the left navigation panel, select **Security**, **Realms**, **myrealm**, and then **Groups**.

   b. Select the **Configure a new Group** link in the Groups page.

   c. In the **Name** field on the General tab, enter `User` for the group name and optionally enter a description for the group. Then, click **Apply**.

      Note: The group name `User` is case-sensitive.

      ---

d. From the left navigation panel, select **Security**, **Realms**, **myrealm**, and then **Users**.

e. Select the **Configure a new User** link in the Users page.

f. In the **Name** field on the General tab, enter `Internal` for the user name and optionally enter a description for the user.

> **Note:** The user name *`Internal`* is case-sensitive.

g. Enter and confirm a password associated with the user name Internal and click **Apply**.

h. Select the **Groups** tab.

i. Add the User group to the list of **Current Groups** for the Internal user. To do so, select the user from the list of **Possible Groups** and click the right-arrow button. Then click **Apply**.

Preparing to Install Oracle Identity Manager As a Non-Root User on Solaris

Before installing Oracle Identity Manager as a non-root user account on BEA WebLogic Server running on Solaris, ensure that the user account has the following permissions:

- Write and execute permissions on the specific WebLogic Domain directory
- (Optional) Write permission on the `WebLogic` and `lib/mbeantypes` directories

4

Installing and Configuring a Database for Oracle Identity Manager

Oracle Identity Manager requires a database. You must install and configure your database before you begin the Oracle Identity Manager installation. Refer to the topic that applies to your database:

- Using an Oracle Database for Oracle Identity Manager
- Using Oracle RAC Databases for Oracle Identity Manager
- Using a Microsoft SQL Server Database for Oracle Identity Manager

Using an Oracle Database for Oracle Identity Manager

To use Oracle Database as your database, you must perform the tasks described in the following sections:

- Installing Oracle Database
- Creating an Oracle Database
- Preparing the Oracle Database

Installing Oracle Database

Install Oracle9*i* Database or Oracle Database 10*g* release 2 by referring to the documentation delivered with the Oracle database. See *Oracle Identity Manager Release Notes* for the specific supported versions. Oracle recommends using the Basic installation.

> **Note:** If you choose the Custom installation, then you must include the JVM option, which is required for XA transaction support.

Creating an Oracle Database

You can create a new Oracle database instance for Oracle Identity Manager. When creating the database, ensure that you configure the Oracle JVM feature and enable query rewrite.

You can use the Database Configuration Assistant (DBCA) tool to create the database. To configure the Oracle JVM feature, select the Oracle JVM feature on the Standard Database Features page of the DBCA.

To enable the database for query rewrite, set the initialization parameters `QUERY_REWRITE_ENABLED` to `TRUE` and `QUERY_REWRITE_INTEGRITY` to `TRUSTED` in the **All Initialization Parameters** field of the DBCA.

> **Note:** For the Oracle Identity Manager installation, Oracle recommends that you configure a minimum block size of 8K for Oracle Database.

Refer to the Oracle Database documentation for detailed instructions on creating a database instance.

Configuring the Database for Globalization Support

For globalization support for Oracle Identity Manager, Oracle recommends that for configuring the database for Unicode. To configure the database for Unicode, perform the following steps:

1. Select **AL32UTF8** in the Character Sets tab of the DBCA. This character set supports the Unicode standard.
2. Set the `NLS_LENGTH_SEMANTICS` initialization parameter to `CHAR` in the **All Initialization Parameters** field of the DBCA.

   See Also: *Oracle Identity Manager Globalization Guide* for information about globalization support for Oracle Identity Manager

Preparing the Oracle Database

After you install Oracle Database and create a database instance, you must prepare the database instance for Oracle Identity Manager by completing the following tasks:

1. Verify that query rewrite is enabled.

   > **Note:** Query rewrite is applicable only if you are using Oracle Database Enterprise Edition.

2. Enable XA transactions support.

   > **Note:** Java Virtual Machine (JVM) is required to enable XA transaction support. If you did not install the Oracle JVM component during Oracle Database installation, then you must install it now. See the Oracle Database documentation for specific instructions.

3. Create at least one tablespace for storing Oracle Identity Manager data.
4. Create a database user account for Oracle Identity Manager.

You can perform the preceding tasks to prepare the Oracle database for Oracle Identity Manager by running one of the following scripts:

- On Microsoft Windows, run the following:

  ```
  prepare_xl_db.bat
  ```

- On UNIX, run the following:

  ```
  prepare_xl_db.sh
  ```

Both of these scripts ship with the Oracle Identity Manager Installer and are in the `\installServer\Xellerate\db\oracle\` directory.

You must observe the following prerequisites when using these scripts:

- The script must be run by a user holding DBA privileges. For example, the oracle user on UNIX typically holds these privileges.
- The script must be run on the computer on which the database is installed.

The following sections describe how to prepare the Oracle database for Oracle Identity Manager.

- Preparing the Database on UNIX
- Preparing the Database on Microsoft Windows
- Evaluating Script Results

Perform the steps associated with the operating system on the computer hosting the Oracle database.

Preparing the Database on UNIX

To prepare the database on UNIX:

1. Copy the scripts prepare_xl_db.sh and xell_db_prepare.sql from the distribution CD to a directory on the computer hosting the database in which you (as the account user performing this task) have write permission.
2. Run the following command to enable permission to run the script:

   ```
   chmod 755 prepare_xl_db.sh
   ```

3. Run the prepare_xl_db.sh script by entering the following command:

   ```
   ./prepare_xl_db.sh
   ```

4. Provide information appropriate for your database and host computer when the script prompts you for the following items:
   - The location of your Oracle home, which is *ORACLE_HOME*
   - The name of your database, which is *ORACLE_SID*
   - The name of the Oracle Identity Manager database user to be created
   - The password for the Oracle Identity Manager database user
   - The name of the tablespace to be created for storing Oracle Identity Manager data
   - The directory to store the data file for the Oracle Identity Manager tablespace
   - The name of the data file (You do not append the .dbf extension.)
   - The name of the temporary tablespace
5. Check the prepare_xl_db.lst log file located in the directory in which you ran the prepare_xl_db script to see the execution status and additional information.

Note: If you encounter errors after running the prepare_xl_db.sh script, then run the following command to ensure that the prepare_xl_db.sh is executable on UNIX, and then run the prepare_xl_db.sh script again.

```
$ dos2unix prepare_xl_db.sh
```

Preparing the Database on Microsoft Windows

To prepare the database on Microsoft Windows:

1. Copy the prepare_xl_db.bat and xell_db_prepare.sql scripts from the distribution CD to a directory on the computer hosting the database in which you (as the account user performing this task) have write permission.
2. Open a command prompt, navigate to the directory in which you copied the scripts, and run prepare_xl_db.bat with the following arguments:

   ```
   prepare_xl_db.bat ORACLE_SID ORACLE_HOME
   XELL_USER XELL_USER_PWD TABLESPACE_NAME
   DATAFILE_DIRECTORY DATAFILE_NAME
   XELL_USER_TEMP_TABLESPACE SYS_USER_PASSWORD
   ```

   For example, the string you enter on the command line might look similar to the following:

   ```
   prepare_xl_db.bat XELL C:\oracle\ora92 xladm xladm
   xeltbs C:\oracle\oradata xeltbs_01 TEMP manager
   ```

   Table 4–1 lists the options used in the preceding example of prepare_xl_db.bat.

Table 4–1 Options for the prepare_xl_db.bat Script

Argument	Description
`XELL`	Name of the database
`C:\oracle\ora92`	Directory in which the Oracle database is installed
`xladm`	Name of the Oracle Identity Manager user to be created
`xladm`	Password for the Oracle Identity Manager user
`xeltbs`	Name of the tablespace to be created
`C:\oracle\oradata`	Directory in which the data files will be placed
`xeltbs_01`	Name of the data file (you do not need to include the .dbf extension)
`TEMP`	Name of the temporary tablespace that already exists in the database
`manager`	Password for the SYS user

3. Check the `prepare_xl_db.lst` log file located in the directory in which you have run the xell_db_prepare script to see execution status and additional information.

Evaluating Script Results

If the script returns a message indicating successful execution, then you can continue to the next task, which is Oracle Identity Manager installation.

If the script does not succeed, then you must manually fix all fatal (nonrecoverable) errors so that the database is prepared successfully.

You can ignore all nonfatal errors. For example, when the script tries to drop a nonexistent view, it will return the error `"ORA-00942: table or view does not exist"`.

Scan all the errors in the log file and ignore or resolve them on an individual basis.

Removing Oracle Identity Manager Entries from an Oracle Database

To remove Oracle Identity Manager entries from an Oracle database after removing (deinstalling) the Oracle Identity Manager product, drop the database user holding the Oracle Identity Manager schema.

Using Oracle RAC Databases for Oracle Identity Manager

This section explains how to deploy Oracle Real Application Clusters (Oracle RAC) databases for Oracle Identity Manager. It discusses the following sections:

- Installing Oracle Identity Manager for Oracle RAC
- Oracle RAC Net Services
- JDBC and Oracle RAC
- Configuring BEA WebLogic Server for Oracle RAC

Installing Oracle Identity Manager for Oracle RAC

Oracle RAC is a cluster database with a shared cache architecture that provides highly scalable and available database solutions. Oracle RAC consists of multiple database instances on different computers. These database instances act in tandem to provide database solutions.

> **Note:** The Oracle Identity Manager Installer program does not provide support for Oracle RAC. To deploy Oracle Identity Manager for Oracle RAC, you must install Oracle Identity Manager on a single database instance in Oracle RAC and then change the application server settings, specifically the connection pool parameters, to use the Oracle RAC JDBC connection string.

Perform the following steps to install Oracle Identity Manager for Oracle RAC:

1. Ensure that Oracle RAC is properly set up and configured with the Oracle Identity Manager schema owner.
2. Start the Oracle Identity Manager Installer.
3. On the Database Parameters page of the installer, enter the host name, port number, and database name of a single database instance in Oracle RAC.
4. Complete the Oracle Identity Manager installation by performing the steps in the installer.
5. Configure the application server for RAC. Refer to the "Configuring BEA WebLogic Server for Oracle RAC" section on page 4-7.

Oracle RAC Net Services

The net services name entry for an Oracle RAC database differs from that of a conventional database. The following is an example of the net services name entry for an Oracle RAC database:

```
racdb=
        (DESCRIPTION=
                  (LOAD_BALANCE=off)
                  (FAILOVER=on)
                  (ADDRESS_LIST=
                            (ADDRESS=(protocol=tcp)(host=node1-vip)(port=1521))
                            (ADDRESS=(protocol=tcp)(host=node2-vip)(port=1521)))
        (CONNECT_DATA=
                  (SERVER=DEDICATED)
                  (SERVICE_NAME=racdb)))
```

Table 4–2 describes the parameters in a net services name entry for an Oracle RAC database.

Table 4–2 Parameters for Oracle RAC Database Net Services Name Entries

Parameter	Description
LOAD_BALANCE	Specifies whether client load balancing is enabled (on) or disabled (off). The default setting is on.
FAILOVER	Specifies whether failover is enabled (on) or disabled (off). The default setting is on.
ADDRESS_LIST	Specifies the list of all the nodes in Oracle RAC, including their host names and the ports they listen on.

JDBC and Oracle RAC

JDBC client applications that use the Thin driver to connect to an Oracle RAC database must use the Oracle RAC net services name as a part of the JDBC URL. The entire Oracle RAC net services name is concatenated and the entire string is used in the JDBC URL so that the client application can connect to Oracle RAC.

The following sample code shows how a JDBC URL is used to connect to an Oracle RAC database:

```
//String url = "jdbc:oracle:thin:@dbhost:1521:dbservice"
String racUrl =
"jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=off)(FAILOVER=on)(ADDRESS_LIST=(ADDR
ESS=(protocol=tcp)(host=node1-vip)(port=1521))(ADDRESS=(protocol=tcp)(host=node2-v
ip)(port=1521)))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=racdb)))";

       String strUser = "username";
       String strPW = "password";

       // load Oracle driver
       Class.forName("oracle.jdbc.driver.OracleDriver");

       // create the connection
       con = DriverManager.getConnection(strURL, strUser, strPW);
```

The subsequent sections about configuring application servers for Oracle RAC databases explain how to modify connection pools to use a similar JDBC URL so that the application server can communicate with Oracle RAC.

Configuring BEA WebLogic Server for Oracle RAC

This section explains how to configure BEA WebLogic Server (nonclustered or clustered) for Oracle RAC by ensuring the data sources and connection pools are configured to use the Oracle RAC JDBC connection string.

> **Note:** Before configuring BEA WebLogic Server for Oracle RAC, you must:
>
> - Get the RAC net services name from the tnsnames.ora file.
> - Construct the RAC JDBC URL. Refer to the "JDBC and Oracle RAC" section on page 4-6.

Perform the following steps to configure both nonclustered and clustered BEA WebLogic Server for Oracle RAC:

1. Open the `OIM_HOME/xellerate/config/xlconfig.xml` file.
2. Locate the <DirectDB> section and replace the value of the `<url>...</url>` tag with the Oracle RAC JDBC URL. For example, the new tag might be similar to the following:

   ```
   <url>jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=off)(FAILOVER=on)(ADDRESS_
   LIST=(ADDRESS=(protocol=tcp)(host=node1-vip)(port=1521))(ADDRESS=(protocol=tcp)
   (host=node2-vip)(port=1521)))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_
   NAME=racdb)))</url>
   ```

3. Save and close the `OIM_HOME/xellerate/config/xlconfig.xml` file.
4. Start BEA WebLogic Server and open the WebLogic Server Administration Console by using a Web browser.
5. Log in to the WebLogic Server Administration Console by using the administrator account.
6. Select **Services**, **JDBC**, **Connection Pools**, and then select **xlConnectionPool**.
7. Select the **General** tab for xlConnectionPool.
8. Enter the Oracle RAC JDBC URL described in Step 2 in the **URL** field and save the settings.
9. Select the **Connections** tab for xlConnectionPool.
10. Select **Advanced Options** and set the following:

    - Select **Test Reserved Connections**.
    - Set the **Test Table Name** value to `dual`.

    Save the settings.
11. Select **Services**, **JDBC**, **Connection Pools**, and then select **xlXAConnectionPool**.
12. Select the **General** tab for xlXAConnectionPool.
13. Enter the Oracle RAC JDBC URL described in Step 2 in the **URL** field and save the settings.
14. Select the **Connections** tab for xlXAConnectionPool.
15. Select **Advanced Options** and set the following:

    - Select **Test Reserved Connections**.

- Set the **Test Table Name** value to `dual`.
- Select **Keep XA Connection Till Transaction Complete**.

Save the settings.

16. Restart the Administrative Server and the Managed Server. For BEA WebLogic Server clusters, restart all nodes in the cluster.

Using a Microsoft SQL Server Database for Oracle Identity Manager

> **Note:** Microsoft SQL Server is not supported in Oracle Identity Manager release 9.1.0. See "Certified Components" in *Oracle Identity Manager Release Notes* for information about certified components.

To use Microsoft SQL Server for the database, you must complete the procedures in the following sections:

- Installing and Configuring Microsoft SQL Server
- Registering Microsoft SQL Server
- Creating a Microsoft SQL Server Database
- Creating a Microsoft SQL Server Database Account

After you have completed these tasks, you are ready to install the Oracle Identity Manager components.

Installing and Configuring Microsoft SQL Server

To install and configure Microsoft SQL Server for Oracle Identity Manager:

1. Install Microsoft SQL Server 2000 with Service Pack 3a.

   During installation, select **mixed authentication mode**, and then set the password to `sa`.

2. On the computer hosting the application server, download the SQL Server 2000 Driver for JDBC Service Pack 3 from the following Web site:

   `http://www.microsoft.com`

3. On the computer hosting the application server, install SQL Server 2000 Driver for JDBC Service Pack 3.

> **Note:** Specify a short path for the installation folder, such as `C:\JDBCjars`, so that you can easily add the path to your CLASSPATH (Step 4). If the classpath is more than 256 characters, then the installer does not work properly.

4. On the computer hosting the application server, locate the JDBC driver files mssqlserver.jar, msbase.jar, and msutil.jar.

   Add their location to the system CLASSPATH environment variable. If the CLASSPATH environment variable does not exist, then you must create it. The string you add should look like the following:

   ```
   C:\jdbc_install_folder\lib\mssqlserver.jar;
   ```

```
C:\jdbc_install_folder\lib\msbase.jar;
C:\jdbc_install_folder\lib\msutil.jar;
```

In these sample strings, `jdbc_install_folder` is the location where the SQL Server 2000 Driver for JDBC files is installed.

5. Enable distributed transactions by installing SQL Server JDBC XA procedures.

   Copy the sqljdbc.dll file in the `SQLServer JDBC Driver\SQLServer JTA\` directory to the following directory:

   ```
   C:\Program Files\Microsoft SQl Server\MSSQL\Binn
   ```

6. Run the instjdbc.sql script.

   Follow the instructions for installing stored procedures for Java Transaction APIs (JTA). These instructions are bundled with the SQL Server 2000 Driver for JDBC. See the jdbcsqlsrv9.html Help file.

7. Ensure that the Distributed Transaction Coordinator (MSDTC) service for the Microsoft SQL Server is running.

   If necessary, use the SQL Server Service Manager to start it.

> **Note:** You can set the Distributed Transaction Coordinator to start automatically whenever the operating system is restarted.

Registering Microsoft SQL Server

To register Microsoft SQL server:

1. Start the Microsoft SQL Server Enterprise Manager application.

   From the Windows **Start** menu, select **Programs**, **Microsoft SQL Server**, and then select **Enterprise Manager**.

2. In the left pane of the SQL Server Enterprise Manager application window, select **Console Root**, and then select **Microsoft SQL Servers**.
3. Right-click **SQL Server Group**, and select **New SQL Server Registration**.
4. In the Register SQL Server Wizard dialog box, click **Next**.
5. On the Select a SQL Server page, perform one of the three following steps:
   - Select the server from the list in the right pane, click **Add**, then click **Next**.
   - Select **LOCAL**, click **Add**, and then click **Next**.
   - Enter the host name of the server in the text entry box, click **Add**, and then click **Next**.
6. On the Select an Authentication Mode page, select **The SQL Server login information that is assigned to you by the administrator [SQL Server Authentication]**, and then click **Next**.
7. On the Register Connection Option page, select **Login automatically using my SQL server account information**, and then complete the following steps:

   a. In the **Login name** field, enter the account name used to connect to your SQL server. Typically, this is **sa**.

   b. In the **Password** field, enter the password associated with the account name you specified, and then click **Next**.

8. On the Select SQL Server Group page, select **Add the SQL Server(s) to an existing SQL Server Group**, select a group from the **Group name** list, and then click **Next**.
9. On the Completing the Register SQL Server Wizard page, click **Finish**, and then click **Done**.

Creating a Microsoft SQL Server Database

The following procedure describes how to create a Microsoft SQL Server database.

> **Note:** The following procedure uses the name XELL for the database. You are not required to use XELL as the name for the database. This document refers to the name of the database as XELL throughout.

To create a new database for Oracle Identity Manager:

1. Start the Microsoft SQL Server Enterprise Manager application. To do so, from the Windows **Start** menu, select **Programs**, **Microsoft SQL Server**, and then select **Enterprise Manager**.
2. In the left pane of the SQL Server Enterprise Manager application window, select **Console Root**, **Microsoft SQL Servers**, select the server group to which your server belongs, and then double-click the icon representing your server.
3. Right-click **Databases**, and then select **New Database**.
4. In the Database Properties dialog box, select the **General** tab, and then enter `XELL` in the **Name** field.
5. Select the **Data Files** tab. Then, for the **Initial Size** and **Filegroup** columns in the Database files matrix, enter the information from the corresponding columns in Table 4–3.

Table 4–3 Database Files

File Name	Initial Size in Megabytes (MB)	Filegroup Name	Content
XELL_PRIMARY	100	PRIMARY	System objects required for SQL Server operation
XELL_DATA	500	XELL_DATA	Physical data and primary keys
XELL_INDEX	300	XELL_INDEX	Indexes
XELL_TEXT	500	XELL_TEXT	Large text fields
XELL_UPA	1000	XELL_UPA	Keys for the User Profile Audit component

> **Note:** Table 4–3 lists initial sizes for a production environment. For nonproduction installations, you can use the default initial sizes provided for the filegroups.
>
> To ensure successful installation of Oracle Identity Manager, filegroup names must be entered exactly as they are shown in Table 4–3. You can vary the File Name and Location strings to match the database name and the location of your SQL Server installation.

a. Select **Automatically Grow File**.
b. Select **By Percent**, and then enter **10** in the associated field.
c. Select **Unrestricted file growth**.

> **Note:** The PRIMARY filegroup contains the system objects required for SQL Server to operate. The XELL_DATA filegroup stores the physical data and primary keys, XELL_INDEX filegroup stores indexes, XELL_TEXT stores large text fields, and XELL_UPA stores the physical data and primary keys of the User Profile Audit component.

6. Select the **Transaction Log** tab, and then change the initial size to 500 MB.

   Leave all the other options on the tab at their default values.

> **Note:** For nonproduction installations, you can use the default size for the log file.

7. Click **OK** to trigger database creation.

Creating a Microsoft SQL Server Database Account

The following procedure describes how to create a database account for Oracle Identity Manager and assign appropriate permissions to that account.

> **Note:** The following procedure assumes that the account name is xladm. If you want an account name other than xladm, then specify that name instead of xladm throughout the following procedure and also when installing Oracle Identity Manager.

To create a Microsoft SQL Server database account and permissions:

1. Start the Microsoft SQL Server Enterprise Manager application. To do so, from the Windows **Start** menu, select **Programs**, **Microsoft SQL Server**, and then select **Enterprise Manager**.
2. In the left pane of the SQL Server Enterprise Manager application window, select **Console Root**, **Microsoft SQL Servers**, select the server group to which your server belongs, and then double-click the icon representing your server.
3. Select **Security**, right-click **Logins**, and then select **New Login**.
4. In the SQL Server Login Properties dialog box, select the **General** tab. In the **Name** field, enter **xladm**.
5. Select **SQL Server Authentication**. In the **Password** field, enter the password associated with the account name that you specified in Step 4.
6. In the **Database** list in the **Defaults** section, select **XELL** from the list. Leave the **Language** field set to **<default>**.
7. Select the **Database Access** tab.

   In the upper panel, select the check box associated with **XELL**.
8. In the lower panel, select the check boxes associated with the following:

- public
- db_owner
- db_accessadmin
- db_securityadmin
- db_ddladmin
- db_datareader
- db_datawriter

9. Click **OK** to commit your changes.

   When prompted, confirm the password and click **OK**.

10. To check your database settings, right-click the icon representing your server, and then select **Properties** from the shortcut menu.
11. On the SQL Server Properties page, select the **Security** tab, then verify that Authentication is set to **SQL Server and Windows**.
12. Click the **General** tab, and then verify that the check boxes associated with **Autostart SQL Server** and **Autostart MSDTC** are selected.

    If **Autostart SQL Server Agent** is selected, then do not change the existing setting, because that setting might be required by other applications.

    Click **OK** to close the SQL Server Properties page.

Removing Oracle Identity Manager Entries from a SQL Server Database

To remove Oracle Identity Manager entries from a SQL Server database after removing Oracle Identity Manager, perform the following steps:

1. Delete the Oracle Identity Manager database.
2. Delete the Oracle Identity Manager login account.

5

Installing Oracle Identity Manager on Microsoft Windows

This chapter explains how to install Oracle Identity Manager on Microsoft Windows in a nonclustered installation.

> **See Also:** Chapter 9, "Deploying in a Clustered BEA WebLogic Server Configuration" for information about deploying Oracle Identity Manager in a clustered installation

You must install Oracle Identity Manager on systems running the application server. Oracle Identity Manager components, such as the Remote Manager and Design Console, can be installed on separate systems. Each component has its own installer.

> **Note:** You must ensure that BEA WebLogic Server is running during the Oracle Identity Manager installation.

This chapter discusses the following topics:

- Setting Environment Variables Before Installing Oracle Identity Manager
- Installing the Database Schema
- Installing Documentation
- Installing Oracle Identity Manager on Microsoft Windows
- Removing Oracle Identity Manager

> **Caution:** Do *not* use a remote client tool, such as Symantec pcAnywhere, to install Oracle Identity Manager products.

Setting Environment Variables Before Installing Oracle Identity Manager

Before you install Oracle Identity Manager, perform the following steps to set the environment variables:

- Verify that the JAVA_HOME system variable is set to the appropriate Sun JDK. For example:

  ```
  set JAVA_HOME=c:\j2ksdk1.4.2_15
  ```

See Also: *Oracle Identity Manager Release Notes* for information about certified JDK versions

- Verify that the Sun JVM `C:\j2sdk1.4.2_15\` is being used when a Java command is run. To do this, include the Sun JDK bin directory, for example, `C:\jdk142_15\bin\`, in the PATH ahead of all other path entries, for example:

  ```
  set PATH = C:\j2sdk1.4.2_15\bin;%PATH%
  ```

Installing the Database Schema

As part of the installation, the Oracle Identity Manager Installer loads a schema into the database. You only install the database schema once. It is installed the first time you run the Oracle Identity Manager Installer. Each time you run the installer to deploy other Oracle Identity Manager components, you enter information about the database connection to configure the component for the same schema. If required, contact your database administrator (DBA).

Note: During the schema installation, a log file is created in the *`OIM_HOME`*`\logs` directory.

Installing Documentation

The Oracle Identity Manager documentation is installed automatically in the *`OIM_HOME`* directory. A full documentation set is installed with each Oracle Identity Manager component.

Installing Oracle Identity Manager on Microsoft Windows

This section describes how to install Oracle Identity Manager on a computer running Microsoft Windows.

Caution: Do not install Oracle Identity Manager on top of an existing Oracle Identity Manager installation. For each new installation, use a different home directory. If you want to reuse the name of an existing Oracle Identity Manager home directory, then back up the original Oracle Identity Manager home by renaming that directory.

Remember that all Oracle Identity Manager components must be installed in different home directories. For example, you cannot install the Remote Manager in the same directory as Oracle Identity Manager.

To install Oracle Identity Manager on a Microsoft Windows host:

Note: Microsoft SQL Server is not supported in Oracle Identity Manager release 9.1.0. See “Certified Components” in *Oracle Identity Manager Release Notes* for information about certified components.

1. If you are using Microsoft SQL Server as database, then before installing Oracle Identity Manager, ensure that you copy the following three files located in

`C:\Program Files\`*`Microsoft SQL Server 2000 Driver for JDBC`*`\lib\` to the *`BEA_HOME`*`\weblogic81\server\lib\` directory, and add the driver location to the system CLASSPATH environment variable:

- mssqlserver.jar
- msbase.jar
- msutil.jar

2. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.

> **Note:** If the autostart routine is enabled for your computer, then proceed to Step 4.

3. Using Windows Explorer, navigate to the installServer directory on the installation CD, and double-click the **setup_server.exe** file.
4. Select a language on the Installer page and click **OK**. The Welcome page is displayed.
5. Click **Next** on the Welcome page. The Admin User Information page is displayed.
6. Enter the password that you want to use as the Oracle Identity Manager administrator, confirm the password by entering it again, and then click **Next**. The OIM Application Options page is displayed.
7. Select one of the following applications to install, and then click **Next**:
   - Oracle Identity Manager
   - Oracle Identity Manager with Audit and Compliance Module

   See Also: *Oracle Identity Manager Audit Report Developer's Guide* for information about the Audit and Compliance Module

8. After the Target directory page is displayed, complete one of the following:
   - The default directory for Oracle Identity Manager is `C:\oracle`. To install Oracle Identity Manager into this directory, click **Next**.
   - To install Oracle Identity Manager into another directory, enter the path in the Directory field, and then click **Next**.

     Or:

     Click **Browse**, navigate to the desired location, and then click **Next**.

   > **Note:** If the directory path does not exist, then the Base Directory settings field is displayed. Click **OK**. The directory is automatically created. If you do not have write permission to create the default directory for Oracle Identity Manager, then a message is displayed informing you that the installer could not create the directory. Click **OK** to close the message box, and then contact your system administrator to obtain the appropriate permissions.

9. On the Database Server Selection page, specify the type of database that you are using with Oracle Identity Manager, and then click **Next**.

10. On the Database Information page, provide all database connectivity information that is required to install the database schema.

    You install this schema just once, as part of your initial Oracle Identity Manager installation. Thereafter, you configure all the other Oracle Identity Manager components to point to this common schema.

    > **Note:** To install against an existing database, verify that the version of Oracle Identity Manager you are installing is certified with your existing database version. See *Oracle Identity Manager Release Notes* for information about the certified configurations.
    >
    > When Oracle Identity Manager is installed against an existing database, a warning message is displayed indicating that the database schema already exists and instructing you to copy the .xldatabasekey file from the existing Oracle Identity Manager installation to the new `*OIM_HOME*\xellerate\config\` directory after you complete the installation process.
    >
    > You should create the `\config` directory in the new `*OIM_HOME*\xellerate\` path if it does not already exist.

    Enter the following database information:

    - In the **host** field, enter the host name or the IP address of the computer on which the database is installed.
    - In the **Port** field, enter the port number on which the database listens for connections. The default port is 1521 for Oracle Database and 1433 for Microsoft SQL Server.
    - In the **Database SID** field, enter the name of the database instance.
    - In the **User Name** field, enter the user name of the database account that you created for Oracle Identity Manager.
    - In the **Password** field, enter the Oracle Identity Manager database user password.
    - Click **Next** to commit these settings.

      > **Note:** When you set the preceding items, see the configuration settings specified in "Using an Oracle Database for Oracle Identity Manager" on page 4-1 or "Using a Microsoft SQL Server Database for Oracle Identity Manager" on page 4-8 to verify your settings.

      The installer checks for database connectivity and whether a database schema exists. If the check passes, then the installer proceeds to the next step in the process. If the check fails, then an error message is displayed.

    - Select the appropriate database options:
      - If a database exists and the connectivity is good, then proceed to Step 11.
      - If no connectivity is detected, then you are prompted to enter new information or to fix the connection. After you do that, click **Next**.

11. On the Authentication Information page, select either the **Oracle Identity Manager Default Authentication** or **SSO Authentication** option. If you select

Single Sign-On authentication, then you must provide the header variable used in the Single Sign-On system in the **Enter the header value for SSO Authentication** field. Click **Next**.

12. On the Application Server Selection page, select **BEA WebLogic**, and click **Next**.
13. On the Cluster Information page, specify the server configuration (clustered or nonclustered).

    - Select **No** for nonclustered, and then click **Next**.
    - Select **Yes** for clustered, enter the cluster name, and then click **Next**.

    Note: Refer to Chapter 9, "Deploying in a Clustered BEA WebLogic Server Configuration" if you are deploying in a clustered installation.

14. On the WebLogic Directory page, enter the application server and Java information.

    a. Enter the path to the BEA WebLogic Server product installation directory for the application server.

    Alternatively, click **Browse** and navigate to the BEA WebLogic Server product installation directory for the application server. For example: `C:\bea\weblogic81`.

    b. Enter the path to the JDK directory associated with the application server domain.

    Alternatively, click **Browse** and navigate to the JDK directory associated with the application server domain.

    c. Click **Next**.

15. On the WebLogic Application Server Information page, enter appropriate information for the WebLogic server host.

    Note: The information you enter is different for clustered and nonclustered installations.

    For a nonclustered installation:

    a. Enter the host name or IP address of the application server computer.

    Note: The host name is case-sensitive.

    b. Enter the BEA WebLogic Server name. The default name is myserver.

    c. Enter the Admin Port.

    This is the WebLogic server administrative port. The default is 7001.

    d. Enter the WebLogic Server Port.

    This is the WebLogic server service port. The default is 7001.

    Note: Admin Port and WebLogic Server Port are the same for nonclustered installations. The default port is 7001.

e. Enter the Admin Console user name for the WebLogic domain administrator. This is the administrator account that you configured by using the WebLogic Configuration Wizard.

f. Enter and confirm the domain administrator password.

g. Click **Next** to commit the settings.

For clustered installation:

a. Enter the host name or IP address of the computer hosting the application server.

> **Note:** The host name is case-sensitive.

b. Enter the WebLogic Server Name.

This is the Managed Server name. For example, `xlManagedServer_1`.

c. Enter the Admin Port.

This is the WebLogic Administrative Server port. The default is 7001.

d. Enter the WebLogic Server Port.

This is the WebLogic Managed Server port. The default is 7001.

e. Enter the Login Name for the WebLogic domain administrator. This is the administrator account that you configured by using the WebLogic Configuration Wizard.

f. Enter and confirm the administrator password.

g. Click **Next**.

16. On the WebLogic Domain Information page, enter the appropriate WebLogic domain information.

    a. Specify the path to the WebLogic domains folder.

    b. Enter the configuration directory name. Usually, this is same as the domain name.

    c. Enter the domain name.

    d. Click **Next**.

17. Back up the application server when the Application Server Configuration Backup page is displayed, and then click **Next**.

18. On the Installation Summary page, click **Install** to initiate the server software installation.

    Depending on the processor speed of the computer, the installation script might require a few minutes to load the base database schema script and generate the corresponding log file.

19. If the installer detects an existing encrypted database, then it will display a message to copy the .xldatabasekey file to the new installation location.

    Click **OK** to proceed. If the existing database is not encrypted, then you are prompted to encrypt it. Click **OK** to proceed.

20. After Oracle Identity Manager is installed, a message is displayed listing the location of the installer log file and the next steps you should perform.

Click **OK** and complete the postinstallation steps listed in the message.

21. On the Completed page, click **Finish** to exit the installer.
22. Shut down the application server gracefully and then restart it. For detailed information about this procedure, refer to Chapter 8, "Starting and Stopping Oracle Identity Manager".

After installing Oracle Identity Manager, follow the instructions in Chapter 7, "Postinstallation Configuration for Oracle Identity Manager and BEA WebLogic Server".

Removing Oracle Identity Manager

To remove an Oracle Identity Manager installation:

1. Stop Oracle Identity Manager if it is running, and stop all Oracle Identity Manager processes.
2. Delete the *`OIM_HOME`* directory in which you installed Oracle Identity Manager.
3. Delete the WebLogic domain directory in which Oracle Identity Manager is installed.

6 Installing Oracle Identity Manager on UNIX

This chapter describes how to install Oracle Identity Manager on a computer running UNIX in a nonclustered installation.

See Also:

- *Oracle Identity Manager Release Notes* for information about supported UNIX platforms
- Chapter 9, "Deploying in a Clustered BEA WebLogic Server Configuration" for information about deploying Oracle Identity Manager in a clustered installation

You must install Oracle Identity Manager on systems running the application server. Oracle Identity Manager components such as the Remote Manager can be installed on separate systems. Each component has its own installer.

This chapter discusses the following topics:

- Installation Prerequisites and Notes
- Installing the Database Schema
- Installing Documentation
- Installing Oracle Identity Manager on UNIX
- Removing Oracle Identity Manager

Note: Ensure that BEA WebLogic Server is running during Oracle Identity Manager installation.

Installation Prerequisites and Notes

The following is a list of prerequisites for installing Oracle Identity Manager on UNIX:

- The Oracle Identity Manager Installer program requires at least 200 MB of free space in the home directory of the user installing Oracle Identity Manager. Check the `/etc/passwd` file to determine the home directory. Note that you cannot work around this requirement by changing the value of the $HOME variable.
- There must be at least 200 MB of free space in the `/var/tmp/` directory.
- Before you install Oracle Identity Manager, verify that the JAVA_HOME system variable is set to the appropriate Sun JDK. For example:

```
export JAVA_HOME=/opt/j2sdk1.4.2_15
```

See *Oracle Identity Manager Release Notes* for information about the certified versions of Java JDK.

- Before you install Oracle Identity Manager, verify that the correct Sun JVM is being used when a Java command is run. To do this, include the Sun JVM bin directory in the PATH variable ahead of all other path entries, for example:

```
export PATH=/opt/j2sdk1.4.2_15/bin:$PATH
```

- If you are using SQL Server as the database, before installing Oracle Identity Manager, ensure that the following files are in the `*BEA_HOME*/weblogic81/server/lib/` directory, and add the driver location to the CLASSPATH environment variable:

> **Note:** Microsoft SQL Server is not supported in Oracle Identity Manager release 9.1.0. See “Certified Components” in *Oracle Identity Manager Release Notes* for information about certified components.

  - mssqlserver.jar
  - msbase.jar
  - msutil.jar

- Do not install Oracle Identity Manager on top of an existing Oracle Identity Manager installation. Use a different Oracle Identity Manager home directory. If you want to reuse the same directory name for the Oracle Identity Manager home directory, then back up your previous Oracle Identity Manager home by renaming the original directory.

  In addition, all Oracle Identity Manager components must be installed in different home directories. For example, you cannot install the Remote Manager in the same directory in which Oracle Identity Manager is installed.

Installing the Database Schema

As part of the installation, the Oracle Identity Manager Installer loads a schema into the database. You only install the database schema once. It is installed the first time you run the Oracle Identity Manager Installer. Each subsequent time you run the installer to deploy other Oracle Identity Manager components, you enter information about the database connection to configure the component for the same schema. If required, contact your database administrator (DBA).

> **Note:** During the schema installation, a log file is created in the *OIM_HOME*/`logs` directory.

Installing Documentation

The Oracle Identity Manager documentation is installed automatically in the *OIM_HOME* directory. A full documentation set is installed with each Oracle Identity Manager component.

Installing Oracle Identity Manager on UNIX

If BEA WebLogic Server is installed in nondefault directory (other than WebLogic81), the Oracle Identity Manager Installer fails unless you create a symbolic link of WebLogic81 for a nondefault directory in which BEA WebLogic Server is installed. You can create a symbolic link in UNIX by using the internal `ln` command.

Oracle Identity Manager for UNIX is installed through a console mode installer, which supports the following two input methods:

- Choose from list of options.

  Each option is numbered and accompanied by brackets ([ ]). To select an option, enter its number. When selected, the associated brackets display an X ([X]).

- Enter information at a prompt.

  Type in the information at the prompt, and press **Enter**. Default values are enclosed in brackets after a prompt; to accept a default value, press **Enter**.

The installer contains logical sections or panels. You can perform the following actions in the panels:

- When you have selected an item from a list of options, enter the number zero (0) to indicate that the desired item has been selected.
- To move to the next installation panel, enter **1**.
- To go back to the previous panel, enter **2**.
- To cancel the installation, enter **3**.
- To redisplay the current panel, enter **5**.

To install Oracle Identity Manager on UNIX:

1. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.
2. From the console, change directory (`cd`) to the installServer directory on the installation CD.
3. Run the install_server.sh file by using the following command:

   ```
   sh install_server.sh
   ```

   The installer starts in console mode.

   > **Note:** If you are not installing Oracle Identity Manager from distributed media (CD), then you must set the execute bit of all shell scripts in the installServer directory. To set the execute bit for all shell scripts recursively, navigate to the installServer directory and run the following command:
   >
   > ```
   > find . -name "*.sh" -exec chmod u+x {} \;
   > ```

4. Choose a language by entering a number from the list of languages.

   Enter **0** to apply the language selection. The Welcome Message panel is displayed.

5. Enter **1** on the Welcome Message panel to display the next panel.

   The Admin User Information panel is displayed.

6. Enter a user password that you want to use for the Oracle Identity Manager Administrator, confirm the password by entering it again, and then enter **1** to move to the next panel.

   The OIM Application Options panel is displayed.

7. Enter **1** on the OIM Application Options panel to display the next panel.

   The Select the Oracle Identity Manager application to install panel is displayed.

8. Select the application to install:

   - Enter **1** for Oracle Identity Manager.
   - Enter **2** for Oracle Identity Manager with Audit and Compliance Module.

   Enter **0** when you are finished to move to the next section.

   The Target directory panel is displayed.

9. On the Target directory panel, complete one of the following steps:

   - Enter the path to the directory in which you want to install Oracle Identity Manager. For example, enter `/opt/oracle/`.
   - Enter **1** to move to the next panel.

   If the directory does not exist, then you are asked to create it. Enter **y** for yes.

   The Database Server Selection panel is displayed.

   > **Note:** To install against an existing database, verify that the version of Oracle Identity Manager you are installing is certified with your existing database version. Refer to the *Oracle Identity Manager Release Notes release 9.1.0* to confirm the certified configurations.
   >
   > When Oracle Identity Manager is installed against an existing database, a warning message will appear stating that the database schema already exists and instructing you to copy the .xldatabasekey file from the existing Oracle Identity Manager installation to the new *`OIM_HOME`*`/xellerate/config` directory after you complete the installation process.
   >
   > Create the new *`OIM_HOME`*`/xellerate/config` directory if it does not already exist.

10. Specify the type of database that you are using:

    – Enter **1** to select Oracle Database.

    – Enter **2** to select Microsoft SQL Server.

    > **Note:** Microsoft SQL Server is not supported in Oracle Identity Manager release 9.1.0. See "Certified Components" in *Oracle Identity Manager Release Notes* for information about certified components.

    – Enter **0** to finish.

    – Enter **1** to move to the next panel.

    The Database Information panel is displayed.

11. Enter your database information:

- Enter the database host name or IP address.
- Enter the port number, or accept the default.
- Enter the SID for the database name.
- Enter the database user name for the account that Oracle Identity Manager uses to connect to the database.
- Enter the password for the database account that Oracle Identity Manager uses to connect to the database.
- Enter **1** to move to the next panel.

The Authentication Information panel is displayed.

12. Select the authentication mode for the Oracle Identity Manager Web application.

    - Enter **1** for Oracle Identity Manager Default Authentication.
    - Enter **2** for SSO Authentication.
    - Enter **0** when you are finished.

    If you select SSO authentication, then you must provide the header variable used in the Single Sign-On system when prompted.

    Enter **1** to move to the next panel.

    The Application Server Selection panel is displayed.

13. Specify your application server type.

    - Enter **3** for BEA WebLogic Server.
    - Enter **0** when you are finished.
    - Enter **1** to move to the next panel.

    The Cluster Information panel is displayed.

14. Specify whether or not the application server is clustered:

    - Enter **1** to specify that the application server is clustered. Then, enter the cluster name at the prompt and the cluster details.
    - Enter **2** to specify that the application server is not clustered.
    - Enter **0** when you are finished.

    Enter **1** to move to the next section.

    The Application Server Information panel is displayed.

15. Enter the application server information at the prompts.

    – Enter the path to the application server or press **Enter** to accept the default.

    – Enter the path to the application server's domain JDK directory or press **Enter** to accept the default.

    – Enter **1** to move to the next panel.

    The Application Server Information panel is displayed.

16. Enter the login information for the application server:

    Note: The information that you enter is different for clustered and nonclustered installations.

For a nonclustered installation:

- Enter the host name or IP address of the application server computer.

  > **Note:** The host name is case-sensitive.

- Enter the WebLogic Server Name. The default name is myserver.
- Enter the Admin Port.

  This is the WebLogic Server administrative port. The default is 7001.
- Enter the WebLogic Server Port.

  This is the WebLogic Server service port. The default is 7001.

  > **Note:** Admin Port and WebLogic Server Port are the same for nonclustered installations. The default port is 7001.

- Enter the Admin Console user name for the WebLogic domain administrator. This is the administrator account you configured through the WebLogic configuration wizard.
- Enter and confirm the domain administrator password.
- Enter **1** to move to the next section.

For a clustered installation:

- Enter the host name or IP address of the computer hosting the application server.

  > **Note:** The host name is case-sensitive.

- Enter the WebLogic Server Name.

  This is the Managed Server name. For example, `xlManagedServer_1`.
- Enter the Admin Port.

  This is the WebLogic Managed Server port number. The default is 7001.
- Enter the WebLogic Server Port.

  > **Note:** The default port is 7001. Change it to the port of the Managed Server, for example, 7051.

- Enter the Login Name for the WebLogic domain administrator. This is the administrator account that you configured by using the WebLogic configuration wizard.
- Enter and confirm the administrator password.
- Enter **1** to move to the next section.

  The second Application Server Information panel is displayed.

17. Enter the domain information:

- Enter the domain location. This is the BEA WebLogic Server directory that contains domain directories. This is sometimes called the configuration or target location in WebLogic.
- Enter the configuration directory name. This is the directory that contains the specific domain in which you are installing Oracle Identity Manager.
- Enter the domain name. This is the name of the domain in which you are installing Oracle Identity Manager.
- Enter **1** to move to the next section.

18. When a message is displayed warning you to back up your application server installation, back up your installation, and then enter **1** to move to the next section.
19. When the Information Summary page is displayed, verify the information displayed, then do one of the following:

    - Enter **2** to go back and make changes.
    - Enter **1** to start the installation.

    Oracle Identity Manager installs and the Completed panel is displayed.
20. Enter **3** to finish.
21. Shut down the application server gracefully and then restart it. For detailed information about this procedure, refer to Chapter 8, "Starting and Stopping Oracle Identity Manager".

After installing Oracle Identity Manager, follow the instructions in Chapter 7, "Postinstallation Configuration for Oracle Identity Manager and BEA WebLogic Server".

Removing Oracle Identity Manager

To remove an Oracle Identity Manager installation:

1. Stop Oracle Identity Manager if it is running, and stop all Oracle Identity Manager processes.
2. Delete the *`OIM_HOME`* directory in which you installed Oracle Identity Manager.
3. Delete the WebLogic domain directory in which Oracle Identity Manager is installed.

7

Postinstallation Configuration for Oracle Identity Manager and BEA WebLogic Server

After you have installed Oracle Identity Manager, you must complete some postinstallation tasks before you can use the application. Some of the postinstallation tasks are optional, depending on your deployment.

This chapter discusses the following topics:

- Default JMS Queue Configuration
- Changing Keystore Passwords
- Required Postinstallation Tasks
- Optional Postinstallation Tasks
- Setting the Compiler Path for Adapter Compilation
- Deploying the SPML Web Service

Default JMS Queue Configuration

Previously, Oracle Identity Manager used a single JMS queue (named xlQueue) for all asynchronous operations including requests, reconciliation, attestation, and offline tasks. In release 9.1.0, by default, Oracle Identity Manager uses separate JMS queues for specific operations to optimize JMS queue processing. The following list shows the JMS queues in the default configuration and indicates the operation related to each queue:

- `xlQueue` (for request operations)
- `xlReconQueue` (for reconciliation operations)
- `xlAuditQueue` (for auditing operations)
- `xlAttestationQueue` (for attestation operations)
- `xlProcessQueue` (for use in a future release)

Changing Keystore Passwords

During installation, the passwords for the Oracle Identity Manager keystores are set to `xellerate`. The Installer scripts and installation log contain this default password. It is strongly recommended that you change the keystore passwords for all production installations.

To change the keystore passwords, you must change the storepass of .xlkeystore and the keypass of the xell entry in .xlkeystore, and these two values must be identical. Use the keytool utility to change the keystore passwords by performing the following steps:

1. Open a command prompt on the Oracle Identity Manager host computer.
2. Navigate to the *OIM_HOME*\xellerate\config directory.
3. Run the keytool utility with the following options to change the storepass:

   ```
   JAVA_HOME\jre\bin\keytool -storepasswd -new new_password -storepass xellerate
   -keystore .xlkeystore -storetype JKS
   ```

4. Run the keytool with the following options to change the keypass of the xell entry in .xlkeystore:

   ```
   JAVA_HOME\jre\bin\keytool -keypasswd -alias xell -keypass xellerate -new
   new_password -keystore .xlkeystore -storepass new_password
   ```

   > **Note:** Replace *new_password* with the same password entered in step 3.

   Table 7–1 lists the options used in the preceding example of keytool usage.

Table 7–1 Command Options for the keytool Utility

Option	Description
JAVA_HOME	Location of the Java directory associated with the application server
new_password	New password for the keystore
-keystore *option*	Keystore whose password you are changing (.xlkeystore for Oracle Identity Manager or .xldatabasekey for the database)
-storetype *option*	JKS for .xlkeystore and JCEKS for .xldatabasekey

5. In a text editor, open *OIM_HOME*\xellerate\config\xlconfig.xml.
6. Edit the <xl-configuration>.<Security>.<XLPKIProvider>.<KeyStore> section, <xl-configuration>.<Security>.<XLPKIProvider>.<Keys> section and the <RMSecurity>.<KeyStore> section to specify the keystore password as follows:

   > **Note:** Change the <XLSymmetricProvider>.<KeyStore> section of the configuration file to update the password for the database keystore (.xldatabasekey).

   - Change the password tag to encrypted="false".
   - Enter the password, for example:

     ```
     <Security>
     <XLPKIProvider>
     <KeyStore>
           <Location>.xlkeystore</Location>
           <Password encrypted="false">new_password</Password>
           <Type>JKS</Type>
           <Provider>sun.security.provider.Sun</Provider>
     ```

```
</KeyStore>
<Keys>
<PrivateKey>
<Alias>xell</Alias>
<Password encrypted="false">new_password</Password>
</PrivateKey>
</Keys>
<RMSecurity>
<KeyStore>
<Location>.xlkeystore</Location>
<Password encrypted="false">new_password</Password>
<Type>JKS</Type>
<Provider>sun.security.provider.Sun</Provider>
</KeyStore>
```

7. Save and close the xlconfig.xml file.

> **Note:** When you perform the procedure described in the "Shutting Down and Restarting BEA WebLogic Server" section on page 7-7, a backup of the configuration file is created. The configuration file with the new password is read in, and the password is encrypted in the file. If all of the preceding steps succeed, then you can delete the backup file.
>
> On UNIX, you might also want to clear the command history of the shell by using the following command:
>
> ```
> history -c
> ```

Required Postinstallation Tasks

After you install Oracle Identity Manager on BEA WebLogic Server, you must perform the following tasks:

- Increasing the Memory and Setting the Java Option
- Setting Up Authentication
- Setting Up the XML Registry
- WebLogic JMS Server Configuration Changes
- Setting the Transaction Timeout Parameter
- Copying the Oracle 10.2.0.3 JDBC JAR File in a Clustered Installation
- Shutting Down and Restarting BEA WebLogic Server

Increasing the Memory and Setting the Java Option

To increase the memory and set the Java option:

1. Use the WebLogic Server Administration Console to shut down the application server gracefully.
2. Navigate to `BEA_HOME\user_projects\domains\domain_name`. For example, `C:\bea\user_projects\domains\mydomain`.
3. In a text editor, open the WebLogic start script file. The start script is:
   - For Microsoft Windows:

```
startWebLogic.cmd
```

- For UNIX:

  ```
  startWebLogic.sh
  ```

4. JVM memory settings must be changed for production environments and when processing a large volume of data in nonproduction environments. Edit the script to specify memory options as follows:

   For Microsoft Windows, locate the line that starts with the following:

   ```
   %JAVA_HOME%\bin\java %JAVA_VM% %MEM_ARGS% %JAVA_OPTIONS%
   ```

   Add either of the following lines just before it:

   - If Sun JVM is used:

     ```
     set MEM_ARGS=-Xms1280m -Xmx1280m -XX:PermSize=128m -XX:MaxPermSize=256m
     ```

   - If BEA JRockit JVM is used:

     ```
     set MEM_ARGS=-Xms1280m -Xmx1280m
     ```

   For UNIX, locate the line that starts with the following:

   ```
   $JAVA_HOME/bin/java ${JAVA_VM} ${MEM_ARGS} ${JAVA_OPTIONS}
   ```

   Add either of the following lines just before it:

   - If Sun JVM is used:

     ```
     MEM_ARGS="-Xms1280m -Xmx1280m -XX:PermSize=128m -XX:MaxPermSize=256m"
     export MEM_ARGS
     ```

   - If BEA JRockit JVM is used:

     ```
     MEM_ARGS="-Xms1280m -Xmx1280m"
     export MEM_ARGS
     ```

5. If BEA JRockit JVM is being used, add the -XnoOpt option to the existing JAVA_OPTIONS. This option turns off adaptive optimization and is required for stable Oracle Identity Manager operation.

   For Microsoft Windows, locate the line that starts with the following:

   ```
   %JAVA_HOME%\bin\java %JAVA_VM% %MEM_ARGS% %JAVA_OPTIONS%
   ```

   Add the following line just before it:

   ```
   set JAVA_OPTIONS=%JAVA_OPTIONS% -XnoOpt
   ```

   For UNIX, locate the line that starts with the following:

   ```
   $JAVA_HOME/bin/java ${JAVA_VM} ${MEM_ARGS} ${JAVA_OPTIONS}
   ```

   Add the following line just before it:

   ```
   JAVA_OPTIONS="$JAVA_OPTIONS -XnoOpt"
   export JAVA_OPTIONS
   ```

6. Save and close the file.

Setting Up Authentication

To set up the authentication:

1. Log on to the WebLogic Server Administration Console.
2. In the left frame, select **Security**, **Realms**, **myrealms**, **Providers**, and then select **Authentication**.
3. Click **Configure a new OIMAuthenticator**.
   a. Retain the default value in the Name field.
   b. Set the Control Flag to **Sufficient**, and then click **Create**.
4. In the left frame, click **Authentication**, and then select **DefaultAuthenticator**. Set the **Control Flag** to **Sufficient**, and then click **Apply**.

Setting Up the XML Registry

To set up the XML registry:

1. Log on to the WebLogic Server Administration Console.
2. In the left frame, click **Services**.
3. Right-click **XML**, then select **Configure a new XMLRegistry** from the shortcut menu.
4. Enter the registry information:
   a. Enter a unique name, for example, **Oracle Identity Manager XML registry**.
   b. Use default values for the other fields, then click **Create**.
5. Click the **Target and Deploy** tab.
   a. Select the server option.

   Note: For clustered installations, select all Managed Servers that are part of the cluster.

   b. Click **Apply**.
6. In the left frame, click **XML**, and then click your new XML registry entry to expand it.
7. Right-click **Parser Select Entries**, and then select **Configure a New XMLParserSelectRegistryEntry** from the shortcut menu.
8. Enter the configuration information:
   a. Ensure that the Public ID field is blank.
   b. Ensure that the System ID field is blank.
   c. In the Root Element Tag field, enter **database**.
   d. In the Document Builder Factory field, enter the following:

   ```
   org.apache.crimson.jaxp.DocumentBuilderFactoryImpl
   ```

   e. Ensure that the Parser Class Name field is blank.
   f. In the SAX Parser Factory field, enter the following:

   ```
   org.apache.xerces.jaxp.SAXParserFactoryImpl
   ```

g. Click **Create**.

> **Note:** If you are using SQL Server as the database and the Oracle Identity Manager log shows traces of exceptions related to MS JDBC classes, then you must add three MS JDBC files to the beginning of CLASSPATH in the startWebLogic script located in the domain directory, and restart the server.
>
> Microsoft SQL Server is not supported in Oracle Identity Manager release 9.1.0. See "Certified Components" in *Oracle Identity Manager Release Notes* for information about certified components.
>
> Add the following files located in the `/WebLogic81/server/lib/` directory to the beginning of CLASSPATH in the startWebLogic script, and restart the server:
>
> - mssqlserver.jar
> - msbase.jar
> - msutil.jar
>
> In a clustered installation, add these three JAR files in the Class Path field in the Remote Start tab of all Managed Servers.

WebLogic JMS Server Configuration Changes

Changing the WebLogic JMS Server configuration involves the following steps:

- Set the Redelivery Limit for JMS queues (`xlQueue`, `xlReconQueue`, `xlProcessQueue`, `xlAuditQueue`, and `xlAttestationQueue`) to 5.
- To improve performance, make the following changes for BEA WebLogic Server JMS servers:
  1. Log on to the WebLogic Server Administration Console.
  2. Navigate to **Services**, **JMS**, **Servers**, **xlJMSServer**, and then click the **Thresholds & Quotas** tab.
  3. Set **Messages Threshold High** to `250`, **Messages Threshold Low** to `20`, select **Messages Paging Enabled**, and then click **Apply**.

> **Note:** For a clustered installation of the BEA WebLogic Server, repeat the steps in this section for all the JMS servers with names starting with xlJMSServer, for example, `xlJMSServerMyServer`.

Setting the Transaction Timeout Parameter

To set the transaction timeout parameter:

1. Log in to the WebLogic Server Administration Console.
2. Navigate to **Services**, **JTA**, and then enter `1200` for in the **Timeout Seconds** field.

Copying the Oracle 10.2.0.3 JDBC JAR File in a Clustered Installation

In a BEA WebLogic Server clustered installation, perform the following (mandatory) procedure on all nodes except the first one on which Oracle Identity Manager is installed:

After backing up the `ojdbc14.jar` file, copy the file from the *`OIM_HOME`*`/xellerate/ext` directory to the *`BEA_HOME`*`/weblogic81/server/lib` directory.

> **Note:** In a nonclustered installation, the Oracle Identity Manager Installer automatically performs this procedure.

Shutting Down and Restarting BEA WebLogic Server

After performing the postinstallation tasks, shut down the application server gracefully and then restart it for the changes in settings to take effect. Refer to Chapter 8, "Starting and Stopping Oracle Identity Manager" for detailed information about starting and stopping the application server after deploying Oracle Identity Manager .

Optional Postinstallation Tasks

After installing Oracle Identity Manager, consider performing the following optional postinstallation tasks before using the application. Depending on the Oracle Identity Manager deployment, you might choose not to perform some of these tasks.

> **Note:** After performing any of the optional postinstallation tasks, shut down the application server gracefully and then restart it for the changes in settings to take effect. Refer to Chapter 8, "Starting and Stopping Oracle Identity Manager" for detailed information about starting and stopping the application server after deploying Oracle Identity Manager.

- Setting Log Levels
- Enabling Single Sign-On (SSO) for Oracle Identity Manager
- Configuring Custom Authentication

Setting Log Levels

Oracle Identity Manager uses log4j for logging. Logging levels are configured in the logging properties file, *`OIM_HOME`*`/xellerate/config/log.properties`.

The following is a list of the supported log levels, appearing in descending order of information logged. DEBUG logs the most information and FATAL logs the least information:

- DEBUG
- INFO
- WARN
- ERROR
- FATAL

By default, Oracle Identity Manager is configured to provide output at the WARN level except for DDM, which is configured to provide output at the DEBUG level. You can change the log level universally for all components or for one or more individual component.

Oracle Identity Manager components are listed in the *OIM_HOME*`\xellerate\config\log.properties` file in the XELLERATE section, for example:

```
log4j.logger.XELLERATE=WARN
log4j.logger.XELLERATE.DDM=DEBUG
log4j.logger.XELLERATE.ACCOUNTMANAGEMENT=DEBUG
log4j.logger.XELLERATE.SERVER=DEBUG
log4j.logger.XELLERATE.RESOURCEMANAGEMENT=DEBUG
log4j.logger.XELLERATE.REQUESTS=DEBUG
log4j.logger.XELLERATE.WORKFLOW=DEBUG
log4j.logger.XELLERATE.WEBAPP=DEBUG
log4j.logger.XELLERATE.SCHEDULER=DEBUG
log4j.logger.XELLERATE.SCHEDULER.Task=DEBUG
log4j.logger.XELLERATE.ADAPTERS=DEBUG
log4j.logger.XELLERATE.JAVACLIENT=DEBUG
log4j.logger.XELLERATE.POLICIES=DEBUG
log4j.logger.XELLERATE.RULES=DEBUG
log4j.logger.XELLERATE.DATABASE=DEBUG
log4j.logger.XELLERATE.APIS=DEBUG
log4j.logger.XELLERATE.OBJECTMANAGEMENT=DEBUG
log4j.logger.XELLERATE.JMS=DEBUG
log4j.logger.XELLERATE.REMOTEMANAGER=DEBUG
log4j.logger.XELLERATE.CACHEMANAGEMENT=DEBUG
log4j.logger.XELLERATE.ATTESTATION=DEBUG
log4j.logger.XELLERATE.AUDITOR=DEBUG
```

To set Oracle Identity Manager log levels, edit the logging properties in the *OIM_HOME*`\xellerate\config\log.properties` file as follows:

1. Open the *OIM_HOME*`\xellerate\config\log.properties` file in a text editor.

   This file contains a general setting for Oracle Identity Manager and specific settings for the components and modules that comprise Oracle Identity Manager.

   By default, Oracle Identity Manager is configured to output at the Warning level, as follows:

   ```
   log4j.logger.XELLERATE=WARN
   ```

   This is the general value for Oracle Identity Manager. Individual components and modules are listed following the general value in the properties file. You can set individual components and modules to different log levels. The log level for a specific component overrides the general setting.

2. Set the general value to the desired log level.
3. Set other component log levels as desired.

   Individual components or modules can have different log levels. For example, the following values set the log level for the Account Management module to INFO, whereas the server is at DEBUG, and the rest of Oracle Identity Manager is at the WARN level:

   ```
   log4j.logger.XELLERATE=WARN
   log4j.logger.XELLERATE.ACCOUNTMANAGEMENT=INFO
   log4j.logger.XELLERATE.SERVER=DEBUG
   ```

4. Save your changes.

Enabling Single Sign-On (SSO) for Oracle Identity Manager

The following procedure describes how to enable Single Sign-On for Oracle Identity Manager with ASCII character logins. To enable Single Sign-On with non-ASCII character logins, use the following procedure, but include the additional configuration setting described in Step 3.

> **See Also:** *Oracle Identity Manager Best Practices Guide* for more information about configuring Single Sign-On for Oracle Identity Manager with Oracle Access Manager

> **Note:** Header names can contain only English-language characters, the dash character (-), and the underscore character (_). Oracle recommends that you do not use special characters or numeric characters in header names.

To enable Single Sign-On for Oracle Identity Manager:

1. In a text editor, open the `OIM_HOME\xellerate\config\xlconfig.xml` file:
2. Locate the following Single Sign-On configuration. The following are the default settings without Single Sign-On.

   ```
   <web-client>
   <Authentication>Default</Authentication>
   <AuthHeader>REMOTE_USER</AuthHeader>
   </web-client>
   ```

3. Edit the Single Sign-On configuration to be the following and replace *SSO_HEADER_NAME* with the appropriate header configured in your Single Sign-On system:

   ```
   <web-client>
   <Authentication>SSO</Authentication>
   <AuthHeader>SSO_HEADER_NAME</AuthHeader>
   </web-client>
   ```

   To enable Single Sign-On with non-ASCII character logins, you must include a decoding class name to decode the non-ASCII header value. Add the decoding class name and edit the Single Sign-On configuration as follows:

   ```
   <web-client>
   <Authentication>SSO</Authentication>
   <AuthHeader>SSO_HEADER_NAME</AuthHeader>
   <AuthHeaderDecoder>com.thortech.xl.security.auth.CoreIDSSOAuthHeaderDecoder</Au
   thHeaderDecoder>
   </web-client>
   ```

   Replace *SSO_HEADER_NAME* with the appropriate header configured in your Single Sign-On system.

4. Change the application server and Web server configuration to enable Single Sign-On by referring to the application and Web server vendor documentation.

Configuring Custom Authentication

This section describes how to use custom authentication solutions with Oracle Identity Manager.

Oracle Identity Manager deploys a Java Authentication and Authorization Service (JAAS) module to authenticate users. For unattended logins, which require offline message processing and scheduled task execution, Oracle Identity Manager uses signature-based authentication. Although you should use JAAS to handle signature-based authentication, you can create a custom authentication solution to handle standard authentication requests.

Note: The Oracle Identity Manager JAAS module must be deployed on the application server and should be the first invoked authenticator.

To enable custom authentication on BEA WebLogic Server, you use the WebLogic Server Console, which allows you to add multiple authentication providers and invoke them in a specific order. The custom authentication provider that you specify will handle standard authentication requests, and the Oracle Identity Manager JAAS module will continue to handle signature-based authentication.

Note: The custom authentication provider that you specify must come after the Oracle Identity Manager JAAS module in the WebLogic Server Console's list of authentication providers.

To specify a custom authentication provider for BEA WebLogic Server:

1. Start the **WebLogic Server Console** and open the **Authentication Providers** page from *domain*/Security/Realms/*realm name*/Providers/Authentication.
2. In the Authentication Providers page, select **Oracle Identity Manager Authenticator** from the table at the bottom of the page. The Oracle Identity Manager Authenticator page is displayed.
3. In the Oracle Identity Manager Authenticator page, select the **Allow Custom Authentication** option in the **Details** tab, and then click **Apply**.
4. In the Authentication Providers page, configure a new authentication provider by clicking the **Configure a new ...** link for the custom authentication provider that you want to add.
5. When you finish configuring the new authentication provider, confirm that it is listed after Oracle Identity Manager Authenticator (which is the Oracle Identity Manager JAAS module) in the list of authentication providers. If the Oracle Identity Manager Authenticator is not listed above your custom authentication provider, then click **Reorder the Configured Authentication Providers**.

Protecting the JNDI Namespace

When you specify a custom authentication solution, you should also protect the Java Naming and Directory Interface (JNDI) namespace to ensure that only designated users have permission to view resources. The primary purpose of protecting the JNDI namespace is to protect Oracle Identity Manager from any malicious applications that might be installed in the same application server instance. Even if no other applications, malicious or otherwise, are installed in the same application server instance as Oracle Identity Manager, you should protect your JNDI namespace as a routine security measure.

To protect your JNDI namespace and configure Oracle Identity Manager to access it:

1. From the WebLogic Server Console:
   a. Right-click the server name and go to the JNDI tree view.
   b. Right-click the tree and then define the security policy.
   c. Specify the policy as `User name of the caller xelsysadm` or user name of the caller Internal.

   > **Note:** For a clustered installation, repeat the steps for all the available servers in the domain where Oracle Identity Manager is installed.

2. Open the *`OIM_HOME`*`/config/xlconfig.xml` file in a text editor and add the following elements to the `<Discovery>` element:

   ```
   <java.naming.security.principal>user</java.naming.security.principal>
   <java.naming.security.credentials>user_password</java.naming.security.credentia
   ls>
   ```

   For *`user`*, specify `Internal`. For *`user_password`*, enter the password for Internal.

3. To optionally encrypt the JNDI password, add an encrypted attribute that is assigned a value of true to the `<java.naming.security.credentials>` element, and assign the password as the element's value, as follows:

   ```
   <java.naming.security.credentials
     encrypted="true">password</java.naming.security.credentials>
   ```

   > **Note:** To protect the plaintext password, it is strongly recommended that you add the `encrypted="true"` attribute.

4. Add the following elements to the `<Scheduler>` element:

   ```
   <CustomProperties>
     <org.quartz.dataSource.OracleDS.java.naming.security.principal>user
     </org.quartz.dataSource.OracleDS.java.naming.security.principal>
    <org.quartz.dataSource.OracleDS.java.naming.security.credentials>user_password
     </org.quartz.dataSource.OracleDS.java.naming.security.credentials>
   </CustomProperties>
   ```

Troubleshooting the JNDI Namespace Configuration If you create a user and that is the only user who can perform lookups, you might see the following exception when attempting to start Oracle Identity Manager where *`user_name`* represents the user you created to perform lookups:

```
[XELLERATE.ACCOUNTMANAGEMENT],Class/Method: Authenticate/connect User with ID: user_name was
not found in Xellerate.
[XELLERATE.ACCOUNTMANAGEMENT],Class/Method: Authenticate/connect User with ID: user_name was
not found in Xellerate.
[XELLERATE.ACCOUNTMANAGEMENT],Class/Method: XellerateLoginModuleImpl/login encounter some
problems:
com.thortech.xl.security.tcLoginException:
```

```
at com.thortech.xl.security.tcLoginExceptionUtil.createException(Unknown Source)
at com.thortech.xl.security.tcLoginExceptionUtil.createException(Unknown Source)
at com.thortech.xl.security.Authenticate.connect(Unknown Source)
at com.thortech.xl.security.wl.XellerateLoginModuleImpl.login(Unknown Source)
at weblogic.security.service.DelegateLoginModuleImpl.login(DelegateLoginModuleImpl.java:71)
```

To resolve this issue, refresh the embedded LDAP directory in the Managed Server with the LDAP directory in the Administrative Server after starting Oracle Identity Manager by using the following steps:

1. Log on to the WebLogic Server Administration Console.
2. Click the domain name for the Managed Server.
3. Click **View Domain-wide security settings**.
4. Click the **Embedded LDAP** tab.
5. Select the **Refresh replica at startup** option, and then click **Apply**.

> **Note:** You should only perform these steps once to resolve this issue, and you can disable the **Refresh replica at startup** option after restarting the Admin and Managed Servers.

Setting the Compiler Path for Adapter Compilation

To compile adapters or import Deployment Manager XML files that have adapters, you must set the compiler path. To set the compiler path for adapter compilation, you must first install the Design Console. Refer to Chapter 10, "Installing and Configuring the Oracle Identity Manager Design Console" for instructions on installing the Design Console and then setting the compiler path for adapter compilation.

Deploying the SPML Web Service

Organizations can have multiple provisioning systems that exchange information about the modification of user records. In addition, there can be applications that interact with multiple provisioning systems. The SPML Web Service provides a layer over Oracle Identity Manager to interpret SPML requests and convert them to Oracle Identity Manager calls.

The SPML Web Service is packaged in a deployable Enterprise Archive (EAR) file. This file is generated when you install Oracle Identity Manager.

Because the EAR file is generated while you install Oracle Identity Manager, a separate batch file in the Oracle Identity Manager home directory runs the scripts that deploy the SPML Web Service on the application server on which Oracle Identity Manager is running. You must run the batch file to deploy the SPML Web Service.

For details about the SPML Web Service, see Chapter 12, "The SPML Web Service" in *Oracle Identity Manager Tools Reference*.

8

Starting and Stopping Oracle Identity Manager

This chapter describes how to start and stop Oracle Identity Manager, and how to access the Administrative and User Console. This chapter discusses the following topics:

> **Note:** You must complete all relevant postinstallation steps described in Chapter 7, "Postinstallation Configuration for Oracle Identity Manager and BEA WebLogic Server" before starting Oracle Identity Manager.

Removing Backup xlconfig.xml Files After Starting or Restarting

After you start any Oracle Identity Manager component for the first time, or after you change any passwords in the xlconfig.xml file, Oracle Identity Manager encrypts and saves the passwords. Oracle Identity Manager also creates a backup copy of the xlconfig.xml file before saving changes to the file. These backup files contain old passwords in plaintext. The backup file are named xlconfig.xml.*x*, where *x* is the latest available number, for example xlconfig.xml.0, xlconfig.xml.1, and so on.

> **Note:** You must remove these backup files after starting any Oracle Identity Manager component for the first time, or on restarting after changing any passwords in xlconfig.xml once you have established that the new password is working properly.

Starting Oracle Identity Manager

This section describes how to start Oracle Identity Manager on Microsoft Windows and UNIX.

To start Oracle Identity Manager:

1. Verify that your database is up and running.

2. Start Oracle Identity Manager by running one of the following scripts appropriate for your deployment. Running the Oracle Identity Manager start script also starts BEA WebLogic Server.

   To start an Administrative Server on Microsoft Windows, run the `OIM_HOME\xellerate\bin\xlStartServer.bat` script.

   To start an Administrative Server on UNIX, run the `OIM_HOME/xellerate/bin/xlStartServer.sh` script.

> **Note:** In a clustered enviroment, start the Administrative Server by running the `xlStartServer.bat/xlStartServer.sh` script, and then start the cluster for admin console.

Stopping Oracle Identity Manager

This section describes how to stop Oracle Identity Manager on Microsoft Windows and UNIX. To stop an Administrative Server or Managed Server:

1. Log on to the WebLogic Server Administration Console by using the following URL:

   ```
   http://hostname:port/console
   ```

   In this URL, `hostname` represents the name of the computer hosting the application server and `port` refers to the port on which the server is listening. The default port number for BEA WebLogic Server is 7001.

2. Expand the **Servers** option in the left navigation pane.
3. Right-click the server that you want to stop, and select **Start/Stop Server**.
4. In the main window, select the **Graceful shutdown of this server** option to stop the server.

   Verify that the server is stopped in the Status section at the bottom of the main window.

> **Note:** In a clustered installation, right-click the cluster name you want to stop and select **Start/stop this Cluster**, and then click **Gracefully shutdown of all Managed Servers**. When all the cluster members are shut down, follow steps 2 through 4 to stop the Administrative Servers.

Accessing the Administrative and User Console

After starting the BEA WebLogic Server and Oracle Identity Manager, you can access the Administrative and User Console by performing the following steps:

1. Navigate to the following URL by using a Web browser:

   ```
   http://hostname:port/xlWebApp
   ```

   In this URL, `hostname` represents the name of the computer hosting the application server and `port` refers to the port on which the server is listening. The default port number for BEA WebLogic Server is 7001.

Note: The application name, xlWebApp, is case-sensitive.

For example:

```
http://localhost:7001/xlWebApp
```

2. After the Oracle Identity Manager login page is displayed, log in with your user name and password.

Using the Diagnostic Dashboard to Verify Installation

The Diagnostic Dashboard verifies each component in your postinstallation environment by testing for:

- A trusted store
- Single sign-on configuration
- Messaging capability
- A task scheduler
- A Remote Manager

The Diagnostic Dashboard also checks for all supported versions of components along with their packaging.

See Also: The "Using the Diagnostic Dashboard" section on page 2-4 for information about installing and using the Diagnostic Dashboard

9

Deploying in a Clustered BEA WebLogic Server Configuration

This chapter explains how to deploy Oracle Identity Manager in a clustered BEA WebLogic Server environment.

This chapter discusses the following topics:

- About BEA WebLogic Server Clusters
- Installing and Configuring a Database for Oracle Identity Manager
- Setting Up a BEA WebLogic Server Oracle Identity Manager Cluster
- Adding New Servers to the BEA WebLogic Server Cluster
- Configuring the Microsoft IIS Proxy Plug-in
- Configuring Database-Based HTTP Session Failover

About BEA WebLogic Server Clusters

A clustered installation requires multiple host computers. The instructions in this chapter involve a deployment of 3+n computers. Your configuration can vary.

Table 9–1 describes the entities needed for a cluster, the computers that the entities run on, and the software required for the entities. Host computers and entities are labeled.

Table 9–1 WebLogic-Based Oracle Identity Manager Cluster Host Computers

Host Computers	Entities	Software	Description
ADMIN_SERVER_HOST	Administrative Server	BEA WebLogic Server	The Administrative Server is the BEA WebLogic Server instance that configures and manages the BEA WebLogic Server instances in its domain.
XLMANAGED_SERVER_HOST_n	xlManagedServer_n node manager	BEA WebLogic Server Oracle Identity Manager	Managed servers are BEA WebLogic Server instances that are the cluster members. Members are controlled by the Administrative Server. Each application server in the cluster runs Oracle Identity Manager. The Managed Servers run on one or more host computers. Replace n with the node number, such as xlManagedServer_1. You can have more than one application server for each host computer.
Not applicable	xlCluster		This is the name of the BEA WebLogic Server cluster for Oracle Identity Manager.
IIS_HOST	IIS server	IIS BEA WebLogic Server IIS plug-in	The IIS Web server acts as the front end to the BEA WebLogic Server cluster and handles load balancing.

Caution: Deploying an application in a clustered installation is a complex procedure. This document assumes that you have expertise in installing and running applications on a BEA WebLogic Server cluster. These instructions only provide details specific to Oracle Identity Manager. They are not complete instructions for setting up a BEA WebLogic Server cluster. For more information about clustering, refer to BEA WebLogic Server documentation.

Installing and Configuring a Database for Oracle Identity Manager

Refer to Chapter 4, "Installing and Configuring a Database for Oracle Identity Manager" for information.

Setting Up a BEA WebLogic Server Oracle Identity Manager Cluster

The basic procedure for deploying Oracle Identity Manager in a BEA WebLogic Server cluster is to install and configure an Administrative Server and a single Managed Server, and then clone the Managed Server for the other cluster members.

Note: This chapter assumes that you are running a dedicated Administrative Server host on which Oracle Identity Manager is not running.

To set up a BEA WebLogic Server Oracle Identity Manager cluster:

1. Install BEA WebLogic Server on ADMIN_SERVER_HOST.

2. Install BEA WebLogic Server on all managed hosts (XLMANAGED_SERVER_HOST_1...n).
3. Configure the XLMANAGED_SERVER_HOST_1 to listen to the Administrative Server.

   Refer to the "Configuring a Node Manager for a Managed Server" section on page 9-3 for more information.
4. Create a BEA WebLogic Server configuration.

   Refer to the"Creating a BEA WebLogic Server Configuration" section on page 9-4 for more information.
5. Configure the Remote Start options for xlManagedServer_1 and start the cluster.

   Refer to the "Configuring Remote Start Options" section on page 9-8 for more information.
6. Install Oracle Identity Manager on the ADMIN_SERVER_HOST.

   Refer to the "Installing Oracle Identity Manager" section on page 9-10 for more information.
7. Configure BEA WebLogic Server.

   Refer to the "Configuring BEA WebLogic Server After Installing Oracle Identity Manager" section on page 9-10 for more information.
8. Add new servers to your cluster.

   Refer to the "Adding New Servers to the BEA WebLogic Server Cluster" section on page 9-11 for more information.
9. (Optional) Configure the IIS Proxy Plug-ins.

   Refer to the "Configuring the Microsoft IIS Proxy Plug-in" section on page 9-14 for more information.
10. (Optional) Configure database-based HTTP session failover.

    Refer to the "Configuring Database-Based HTTP Session Failover" section on page 9-15 for more information.

Installing BEA WebLogic Server

Install BEA WebLogic Server on the Administrative Server and XLMANAGED_SERVER_HOST_1 and any other XLMANAGED_SERVER_HOST_n computers. Configure the Node Manager on all MANAGED_SERVER_HOST computers so that they can be controlled by the Administrative Server. Refer to the "Configuring a Node Manager for a Managed Server" section on page 9-3 for more information about configuring the Node Manager.

Configuring a Node Manager for a Managed Server

To control your Managed Servers remotely from the Administrative Server, you must set up and configure Node Manager on each of the remote systems hosting Managed Servers by following the instructions on the BEA e-docs page:

`http://e-docs.bea.com/wls/docs81/adminguide/confignodemgr.html`

On each remote computer, on which BEA WebLogic Server is installed and Managed Servers are configured, edit the `nodemanager.hosts` file and specify the IP address/DNS Name (set `ReverseDnsEnabled=true` in the `nodemanager.properties` file to use DNS name) of the Administrative Server host.

> **Note:** After installing BEA WebLogic Server, you must start (or restart) the Node Manager to generate the initial `nodemanager.hosts` file.

The default location of the `nodemanager.hosts` and `nodemanager.properties` files is:

For Microsoft Windows:

```
BEA_HOME\weblogic81\common\nodemanager
```

For UNIX:

```
BEA_HOME/weblogic81/common/nodemanager
```

Creating a BEA WebLogic Server Configuration

Before installing Oracle Identity Manager, you must prepare your Administrative Server host (ADMIN_SERVER_HOST). Use the WebLogic Configuration Wizard to create a configuration. The configuration includes a domain for Oracle Identity Manager, a cluster, and settings for the Managed Server (xlManagedServer_1) and its host computer (XLMANAGED_SERVER_HOST_1).

To create a BEA WebLogic Server Oracle Identity Manager cluster configuration, install BEA WebLogic Server on ADMIN_SERVER_HOST and create (or edit) a BEA WebLogic Server configuration by using the WebLogic Configuration Wizard.

Summary of the Steps to Create a BEA WebLogic Server Cluster Configuration

The following steps are an overview of the process for creating a BEA WebLogic Server cluster configuration for installing Oracle Identity Manager:

1. Create or use an existing domain to host the Oracle Identity Manager application.
2. Add a Managed Server entry (xlManagedServer_1).
3. Create a cluster (xlCluster).
4. Add xlManagedServer_1 to the cluster.
5. Add a host entry for your Managed Server (XLMANAGED_SERVER_HOST_1).
6. Assign xlManagedServer_1 to XLMANAGED_SERVER_HOST_1.
7. Create the BEA WebLogic Server administrator account.
8. Create the Internal user and the User group.
9. Add the Internal user to the User group.
10. Set start up mode and choose the SDK.
11. Save your configuration.

Steps to Create a BEA WebLogic Server Cluster Configuration

To create a BEA WebLogic Server cluster configuration for installing Oracle Identity Manager:

1. Start the WebLogic Configuration Wizard:

   Microsoft Windows:

Click **Start**, select **Programs**, **BEA WebLogic Platform**, and then select **Configuration Wizard**.

UNIX:

Run the `BEA_HOME/weblogic81/common/bin/config.sh` script.

2. In the Create or Extend a Configuration page, create a new configuration:
   a. Select **Create a new WebLogic configuration**.
   b. Click **Next**.
3. In the Select a Configuration Template page, select the basic template:
   a. Select the **Basic WebLogic Server Domain** template.
   b. Click **Next**.
4. In the Choose Express or Custom Configuration page, select a custom configuration:
   a. Click the **Custom** option to create a custom configuration.
   b. Click **Next**.
5. In the Configure the Administration Server page, enter the Administrative Server information:
   a. Enter a name for the Administrative server (such as AdminServer).
   b. Accept the defaults settings for the other fields.
   c. Click **Next**.
6. In the Managed Servers, Clusters, and Machine Options page, set up your cluster:
   a. Select **Yes** to create the cluster.
   b. Click **Next**.
7. In the Configure Managed Servers page, configure your Managed Server:
   a. Click **Add** to create a Managed Server entry.
   b. Select the IP address from the **Listen Address** list.
   c. Enter the listening port, for example, 7051.
   d. Accept the default values for all other fields.
   e. Click **Next**.
   f. Click **Next** on the Choose SIP Server Type page without selecting any option.
   g. Click **Next** again on the Configure SIP Data-Tier Managed Server Partition page.
8. In the Configure Cluster page, configure your cluster:
   a. Click **Add** to create a cluster entry.
   b. Specify a name for the cluster (such as xlCluster).
   c. Provide a unique multicast address and port number.

      At this time, the Cluster Address is not required.
   d. Click **Next**.
9. In the Assign Servers to Cluster page, assign the Managed Server to your cluster:

a. Highlight the Managed Server name from the **Server** section.

b. Use the right arrow to assign it to the cluster.

c. Click **Next**.

10. In the Configure Machines page, configure your Managed Server host computer:

For a Windows host:

a. Click the **Machine** tab.

b. Click **Add**.

c. Enter the name of the Managed Server host, such as XLMANAGED_SERVER_HOST_1.

d. Enter the Node Manager listen address.

e. Accept the default value of 5555 for the listening port.

f. Click **Next**.

For a UNIX host:

a. Click the **UNIX or Linux Machine** tab.

The Configure Machines page UNIX or Linux machine tab is displayed.

b. Click **Add**.

c. Enter the name of the Managed Server host, such as XLMANAGED_SERVER_HOST_1.

d. Select the option for GID binding, if you want to enable GID binding.

e. Enter the GID to bind as.

f. Select the option for UID binding, if you want to enable UID binding.

g. Enter the UID to bind as.

h. Enter the host address.

i. Enter the listen port.

j. Click **Next**.

11. In the Assign Servers to Machines page, assign the Managed Server to the Managed Server host computer:

a. Select the Managed Server.

b. Select the host computer.

c. Click the right-arrow button to assign the server to the host computer.

d. Click **Next**.

12. In the Database (JDBC) Options page, the JDBC component is defined by the Oracle Identity Manager Installer. Do not define your JDBC component:

a. Click **No**.

b. Click **Next**.

13. In the Messaging (JMS) Options page, the JMS component is defined by the Oracle Identity Manager Installer. Do not define your JMS component:

a. Click **No**.

b. Click **Next**.

14. In the Configure Administrative Username and Password page, enter your administrator information:

    a. The default user name is *weblogic*. Use this name, or enter another name.

    b. Enter a password and confirm it.

    c. Enter a description for the user. (Optional)

    d. Select **Yes** to create an additional user and group that are required by Oracle Identity Manager so that the *Internal* user can be created for Oracle Identity Manager.

    e. Click **Next**.

15. In the Configure Users and Groups page, configure the user and group information:

    a. Click **Add** to create a new user.

    b. Enter **Internal** for the user name.

    Note: The Internal user name is case-sensitive.

    c. Enter a password and confirm it.

    d. Enter a description for this user.

    e. Click the **Group** tab.

16. The Configure Users and Groups page displays the **Group** list. Enter the group information:

    a. Click **Add** to create a user group.

    b. Enter **User** for the group name.

    Note: The User group name is case-sensitive.

    c. Enter a description for the group.

    d. Click **Next**.

17. In the Assign Users Groups page, assign the Internal user to the User group:

    a. Select the User group from the **Group** list on the right side of the page.

    b. Select **Internal user** in the User list.

    c. Click **Next**.

18. In the Assign Groups to Groups page, it is not necessary to assign groups to other groups. To continue, click **Next**.

19. In the Assign Users and Groups to Global Roles page, it is not necessary to assign users or groups a global role. To continue, click **Next**.

    If you are running the wizard on a Windows computer, then the Configure Windows Options page is displayed. Otherwise, The Configure Server Start Mode and Java SDK page is displayed. In this case, skip this step and continue with Step 21.

20. Configure the Microsoft Windows Options.

You can choose to create a start menu shortcut for the Administrative Server, and to run the Administrative Server as a Windows service.

a. Click the **Yes** or **No** options to indicate your preferences.

b. Click **Next**.

> **Note:** If you add a shortcut to the Start menu, then the Build Start Menu Entries page is displayed. Select or decline the options, and then click **Next**.

21. In the Configure Server Start Mode and Java SDK page, select the server start mode and the Java SDK.

    a. Select the desired mode for BEA WebLogic Server.

    b. Select the Sun SDK or JRockit SDK.

    c. Click **Next**.

22. In the Create WebLogic Configuration page, select the configuration directory:

    a. Enter the name of the domain in the **Configuration Name** field.

    b. If required, change the configuration location.

    c. Review other configuration details. If desired, go back to make any changes.

    d. Click **Create**.

23. In the Creating Configuration page, complete your configuration and start the Administrative Server.

    - On Microsoft Windows, select **Start Admin Server** and then click **Done**.

      The wizard exits and the server starts and prompts you for the BEA WebLogic Server user name and password. Enter `weblogic` for the user name and `weblogic` for the password if you accepted the default values for user name and password when you created the WebLogic domain. If you created a unique user name and password when you created the WebLogic domain, enter those values.

    - On UNIX, enter the following commands:

      ```
      cd BEA_HOME/user_projects/domains/domain_name
      sh startWebLogic.sh
      ```

      The Administrative Server starts.

Configuring Remote Start Options

To allow the Managed Servers to be controlled remotely by the administration console, set the server classpath and the memory parameters. Use the WebLogic Server Administration Console to configure the server.

When you clone the Managed Server (to add members to your cluster), these settings are copied to the clone. If you install BEA WebLogic Server in another directory on the new host computer, you must manually edit the remote start settings for the new Managed Server.

To configure the server remote start options:

1. Open the WebLogic Server Administration Console by navigating to the following URL:

   ```
   http://localhost:7001/console
   ```

2. Click the server name, for example xlManagedServer_1, under `*domain name*/Servers`.
3. Click the **Remote Start** tab, and then:
   a. In the **Java Home** field, enter the path of the Sun SDK or JRockit SDK directory, for example, `C:\bea\jdk142_15`.

   b. Set the **BEA Home** field. For example, if BEA WebLogic Server is installed on the C drive, you set the **BEA Home** field to `C:\bea\`.

   c. Increase the memory by appending the following to the Arguments field:

   For Sun SDK:

   ```
   -Xms1280m -Xmx1280m -XX:PermSize=128m -XX:MaxPermSize=256m
   ```

   For JRockit SDK:

   ```
   -Xms1280m -Xmx1280m -XnoOpt
   ```

   d. For deployment on Microsoft Windows, locate the **Class Path** field and add the path to `weblogic.jar`. If you are using **SQL Server** as the database, then you must also add the `mssqlserver.jar`, `msbase.jar`, and `msutil.jar` Microsoft JDBC files to the **Class Path** field. For example:

   > **Note:** Microsoft SQL Server is not supported in Oracle Identity Manager release 9.1.0. See "Certified Components" in *Oracle Identity Manager Release Notes* for information about certified components.

   ```
   BEA_HOME\weblogic81\server\lib\weblogic.jar;C:\sqljars\msbase.jar;C:\sqljar
   s\msutil.jar;C:\sqljars\mssqlserver.jar;
   ```

   > **Note:** Ensure that you perform this step on all Managed Servers.

   e. Click **Apply** to save the setting on the **Remote Start** tab.

4. Ensure that the Node Manager is running on the remote host, for example XLMANAGED_SERVER_HOST_1. If the Node Manager is not running, start it by running the `*BEA_HOME*\weblogic81\server\bin\startNodeManager` script.
5. Start the server from the administration console by performing the following steps:
   a. Click **<domain>**, select **Clusters**, select **xlCluster**, then select **<xlManagedServer_n>** in the navigation bar on the left side of the page.

   b. Select the **Control** tab in the main pane.

   c. To start the server, click **Start this server**.

> **Note:** If you have a problem starting the server because of Host Name validation, then go to **server** for both Admin and Managed servers, select **Key Stores & SSL** under the Configuration tab, change **Hostname Verification** to **None** under the Advanced Options, and restart the server.

The server starts, and its state changes from UNKNOWN to RUNNING.

Installing Oracle Identity Manager

Install Oracle Identity Manager on ADMIN_SERVER_HOST. See either Chapter 5, "Installing Oracle Identity Manager on Microsoft Windows" or Chapter 6, "Installing Oracle Identity Manager on UNIX" for more information.

Configuring BEA WebLogic Server After Installing Oracle Identity Manager

After you have installed Oracle Identity Manager, you must further configure BEA WebLogic Server. Some of the configuration is cluster-specific, and some is the same as you would do for any Oracle Identity Manager system.

To perform postinstallation configuration of BEA WebLogic Server:

1. Stop the Managed Server and Administrative Server. For detailed information about this procedure, refer to Chapter 8, "Starting and Stopping Oracle Identity Manager".
2. Restart the Administrative Server by using the xlStartServer.bat script for Windows, or the xlStartServer.sh script for UNIX. Refer to Chapter 8, "Starting and Stopping Oracle Identity Manager" for more information about starting the Administrative Server.
3. Complete the tasks described in "Required Postinstallation Tasks" on page 7-3.
4. Copy the Oracle Identity Manager directory from ADMIN_SERVER_HOST to XLMANAGED_SERVER_HOST_1 by maintaining the identical directory hierarchy structure.

   > **Note:** If the XLMANAGED_SERVER_HOST_1 is located on the same computer as ADMIN_SERVER_HOST, then you do not need to copy the Oracle Identity Manager directory.

5. Each server in the cluster must know the location of the others. Refer to the "Specifying Cluster Members" section on page 9-13 for more information.
6. If XLMANAGED_SERVER_HOST_1 is a different computer than ADMIN_SERVER_HOST, then copy the following Oracle Identity Manager files to the BEA WebLogic Server installation directory on the XLMANAGED_SERVER_HOST_1:
   - Copy `*OIM_HOME*\ext\nexaweb-common.jar` to the `*BEA_HOME*\weblogic81\server\lib\` directory.
   - Copy `*OIM_HOME*\xellerate\lib\wlXLSecurityProviders.jar` to the `*BEA_HOME*\weblogic81\server\lib\mbeantypes\` directory.
7. Start the cluster.

Adding New Servers to the BEA WebLogic Server Cluster

After you have set up your cluster, you can add more servers by cloning the first Managed Server (`xlManagedServer1`).

> **Note:** If you install BEA WebLogic Server in a different location on a new Managed Server host, then additional configuration is necessary.

To add a server to your cluster:

1. Install BEA WebLogic Server on XLMANAGED_SERVER_HOST_n.

   Refer to the "Installing BEA WebLogic Server" section on page 3-1 for more information.

   > **Note:** To control the server remotely, you must edit the nodemanager.hosts file.

2. Configure the Node Manager for xlManagedServer_n.

   Refer to the "Configuring a Node Manager for a Managed Server" section on page 9-3 and the "Creating a BEA WebLogic Server Configuration"section on page 9-4 for more information.

3. Set up Oracle Identity Manager on XLMANAGED_SERVER_HOST_n.

   Refer to the "Installing Oracle Identity Manager on New Hosts" section on page 9-11 for more information.

4. Configure the XLMANAGED_SERVER_HOST_n computer.

   Refer to the "Configuring New Host Computers" section on page 9-12 for more information.

5. Add the new host computer to the list of cluster members.

   Refer to the "Specifying Cluster Members" section on page 9-13 for more information.

6. Configure new JMS servers corresponding to the new cluster member Managed Servers.

   Refer to the "Creating JMS Entries for New Cluster Members" section on page 9-12 for more information.

Installing Oracle Identity Manager on New Hosts

To install Oracle Identity Manager on a new host in the BEA WebLogic Server cluster:

1. Ensure that the name and path of the *JAVA_HOME* directory used by Oracle Identity Manager is the same across all the nodes of the cluster.
2. Copy the *OIM_HOME* directory, in which Oracle Identity Manager is installed in the cluster, to the new host, by maintaining the identical directory hierarchy structure.
3. Copy the wlXLSecurityProviders.jar file from *OIM_HOME*`\xellerate\lib` directory into the *BEA_HOME*`\weblogic81\server\lib\mbeantypes\` directory.

4. Copy the `*OIM_HOME*\xellerate\ext\nexaweb-common.jar` file to the `*BEA_HOME*\weblogic81\server\lib\` directory.

Configuring New Host Computers

To configure a new host to the BEA WebLogic Server cluster, you must create an entry for the host, clone the server, then set up a JMS server.

To add a new host to the BEA WebLogic Server cluster:

1. Open the WebLogic Server Administration Console by navigating to the following URL:

   ```
   http://localhost:7001/console
   ```

2. Click **<domain_name>**.
3. Click **Machines** on the directory tree in the left pane.
4. Click **Configure a new Machine**.
   - Enter a name for this computer, for example, XLMANAGED_SERVER_HOST_2.
   - Click **Create**.
5. Click the **Node Manager** tab.
   - Enter the listen address (IP address) for this computer.
   - Accept the default for the listen port.
   - Ensure that **Debug Enabled** is selected.
   - Click **Apply**.
6. Right-click the existing manager server name, for example, xlManagedServer_1, and select **Clone <server_name>** from the shortcut menu.
   - Enter a name for the new server, for example, xlManagedServer_2.
   - Select the host computer from the **Machine** menu, for example, XLMANAGED_SERVER_HOST_2.
   - Ensure that the cluster, for example, xlCluster, is selected in the **Cluster** menu.
   - Enter the listen address in the **Listen Address** field.
   - Enter the listen port in the **Listen Port** field.
   - Scroll down and click **Clone**.
7. If BEA WebLogic Server is installed in a different directory than xlManagedServer_1, then change the remote start configuration to include the directory location.
8. Navigate to the host computer and start the node manager.

Creating JMS Entries for New Cluster Members

To create JMS entries for new cluster members:

1. On the Administration Server host, run the setup_wl_server script to configure a new JMS server corresponding to the new Managed Server, and configure the distributed queue.

   To run the setup_wl_server script:

a. Navigate to the *OIM_HOME*/xellerate/setup directory.

b. Run setup_wl_server.cmd for Microsoft Windows and setup_wl_server.sh for UNIX by appending the following parameters:

```
BEA_HOME ADMIN_SERVER_HOST ADMIN_SERVER_HOST_port WEBLOGIC_admin_login
WEBLOGIC_admin_password XLMANAGED_SERVER_n
```

Run the following scripts depending on the operating system of the computer hosting Oracle Identity Manager.

Microsoft Windows:

```
setup_wl_server.cmd c:\bea\weblogic81 t3://192.168.50.172 8001 wladmin
wladmin XLMANAGED_SERVER_2
```

UNIX:

```
./setup_wl_server.sh /opt/bea/weblogic81 t3://192.168.50.172 8001 wladmin
wladmin XLMANAGED_SERVER_2
```

c. Configure the settings for the newly added JMS server. Refer to the "WebLogic JMS Server Configuration Changes" section on page 7-6 for detailed information about this procedure.

d. Stop all Managed Servers gracefully by using the Admin Console and then gracefully stop the Administrative Server.

e. Start the Administrative Server by running the *OIM_HOME*\xellerate\bin\xlStartServer script.

Specifying Cluster Members

To specify the location of all the cluster members, perform the following steps:

1. Edit the *OIM_HOME*\xellerate\config\xlconfig.xml file on each node in the cluster. Modify the Discovery section to specify the cluster members. You can accomplish this one of the following two ways:

   - Specify the cluster address that resolves to multiple computers instead of specifying individual members. This enables you to update the DNS server when adding new members rather than editing the xlconfig.xml file for each Oracle Identity Manager component.

     If you follow this method, then the port number must be the same on all of the computers.

   - In the xlconfig.xml file on each server in the cluster, specify all the URLs (including port) for all servers in the cluster.

     If you use this approach, then the xlconfig.xml file must be updated each time a server is added to the cluster. You must do this for every Oracle Identity Manager component (server or Design Console) in the cluster.

     In the Discovery section of the xlconfig.xml file, add the list of all servers to each of the four occurrences of the <java.naming.provider.url> property, for example:

Note: JBoss Application Server clustered environments are not supported in Oracle Identity Manager release 9.1.0. See “Certified Components” in *Oracle Identity Manager Release Notes* for information about certified components.

```
<Discovery>
<CoreServer>
<java.naming.provider.url>t3://192.168.50.28:7051,192.168.50.184:7051</java
.naming.provider.url>
<java.naming.factory.initial>weblogic.jndi.WLInitialContextFactory</java.na
ming.factory.initial
>
</CoreServer>
<BackOffice>
<java.naming.provider.url>t3://192.168.50.28:7051,192.168.50.184:7051</java
.naming.provider.url>
<java.naming.factory.initial>weblogic.jndi.WLInitialContextFactory</java.na
ming.factory.initial
>
</BackOffice>
<Scheduler>
<java.naming.provider.url>t3://192.168.50.28:7051,192.168.50.184:7051</java
.naming.provider.url>
<java.naming.factory.initial>weblogic.jndi.WLInitialContextFactory</java.na
ming.factory.initial
>
</Scheduler>
<!-- For JBoss use ConnectionFactory
            (non-clustered and HAILXAConnectionFactory (Clustered) -->
<JMSServer>
<connectionFactory>xlConnectionFactory</connectionFactory>
<java.naming.provider.url>t3://192.168.50.28:7051,192.168.50.184:7051</java
.naming.provider.url>
<java.naming.factory.initial>weblogic.jndi.WLInitialContextFactory</java.na
ming.factory.initial
>
</JMSServer>
</Discovery>
```

2. Start all cluster members by using the Admin Console.

Configuring the Microsoft IIS Proxy Plug-in

To configure the Microsoft IIS proxy plug-in:

1. To enable the Web clients to fail over, place the load balancer before the BEA WebLogic Server cluster, and configure it for session affinity. Alternatively, you can configure a BEA WebLogic Server proxy plug-in into the application server.
2. To configure the IIS proxy plug-in, use the iisproxy.dll and iisforward.dll extension and filters.

   Follow the BEA WebLogic Server documentation to perform this activity:

   Use the documentation at the following URL:

   http://e-docs.bea.com/wls/docs81/plugins/isapi.html#113486

   You will be using Request Forwarding based on a context name xlWebApp and Nexaweb, while deploying the whole application.

   The following is a sample iisproxy.ini file.

   ```
   WlForwardPath=/xlWebApp*,/NexaWeb*
   Debug=ON
   WebLogicCluster=192.168.50.28:7051,192.168.50.184:7051
   ```

Configuring Database-Based HTTP Session Failover

Oracle Identity Manager on BEA WebLogic Server cluster is by default configured to provide memory-to-memory session replication and failover. However, it is possible to use database-based replication.

To enable database-based replication:

1. Edit the profile weblogic.profile in `OIM_HOME/Profiles` on the application server host, and change the replication mechanism from InMemory to Database.
2. To patch the application, run the patch_weblogic script found in the `OIM_HOME\xellerate\setup` directory.

   Note: The database tables required for holding the sessions must be created manually. Refer to BEA documentation for information about creating these tables.

   It is possible to use other types of failover mechanisms in BEA WebLogic Server. To use them, change the deployment descriptor (weblogic.xml) in the `OIM_HOME/DDTemplates/xlWebApp` directory, then insert the proper settings for the Web application descriptor. After the change, runthe patch_weblogic script to fix the existing application.

   Note: If the deployment descriptor is changed (for example, during an upgrade), then you must perform the same changes again on the deployment descriptor.

10

Installing and Configuring the Oracle Identity Manager Design Console

This chapter explains how to install the Oracle Identity Manager Design Console, which is a Java client. You can install the Design Console on the same computer as Oracle Identity Manager or on a different computer.

This chapter discusses the following topics:

Requirements for Installing the Design Console

Verify that the following requirements are met for the Design Console installation:

- You must have an Oracle Identity Manager server installed and running.
- If you are installing on a computer other than the host for the application server, then you must know the host name and port number of the computer hosting that application server.
- The Design Console host must be able to ping the application server host by using both IP address and host name.
- For clustered Oracle Identity Manager server installations, you must know the host name and port number of the Web server.

Note: If you cannot resolve the host name of the application server, then try adding the host name and IP address in the hosts file in the following directory:

```
C:\winnt\system32\drivers\etc\
```

Installing the Design Console

The following procedure describes how to install the Design Console.

> **Note:** All Oracle Identity Manager components must be installed in different home directories. If you are installing the Design Console on a computer that is hosting another Oracle Identity Manager component, such as Oracle Identity Manager or the Remote Manager, then you must specify a different installation directory for the Design Console.

To install the Design Console on a Microsoft Windows host:

1. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.
2. Using Windows Explorer, navigate to the installServer directory on the installation CD.
3. Double-click the setup_client.exe file.
4. Choose a language from the list on the Installer page.

   The Welcome page is displayed.
5. In the Welcome page, click **Next**.
6. In the target directory page, complete one of the following steps:
   - The default directory for the Design Console is C:\oracle. To install the Design Console into this directory, click **Next**.
   - To install the Design Console in another directory, specify the path of the directory in the **Directory** field, and then click **Next**.

   > **Note:** If the directory path that you specified does not exist, then the Base Directory settings field is displayed. Click **OK**. This directory is automatically created. If you do not have write permission to create the default directory for Oracle Identity Manager, then a message is displayed informing you that the installer could not create the directory. Click **OK** to close the message, and then contact your system administrator to obtain the appropriate permissions.

7. In the Application Server page, select **BEA WebLogic**, then click **Next**.

   The Application Client Location page is displayed.
8. Select the JRE that is installed with Oracle Identity Manager or specify an existing JRE. Then, click **Next**. The Application Server configuration page is displayed.
9. In the Application Server configuration page, enter the information appropriate for the application server hosting Oracle Identity Manager:

   a. In the first field, enter the host name or IP address.

   > **Note:** The host name is case-sensitive.

   b. In the second field, enter the naming port for the application server on which Oracle Identity Manager is deployed.

   c. Click **Next**.
10. In the Graphical Workflow Rendering Information page, enter the Application server configuration information. To do so:

   a. Enter the Oracle Identity Manager server (host) IP address.
   b. Enter the port number.
   c. Select **Yes** or **No** to specify whether or not the Design Console must use Secure Sockets Layer (SSL).
   d. Click **Next**.

11. In the Shortcut page, select or clear the check boxes for the shortcut options according to your preferences:
    a. Select the option to create a shortcut to the Design Console on the Start Menu.
    b. Select the option to create a shortcut to the Design Console on the desktop.
    c. Click **Next** when you are satisfied with the check box settings.
12. In the Summary page, click **Install** to initiate the Design Console installation.
13. The final installation page displays a reminder to copy certain application server-specific files to the Oracle Identity Manager installation.

    Perform these steps, and click **OK**.
14. Click **Finish** to complete the installation process.

Postinstallation Requirements for the Design Console

Perform the following steps after installing the Design Console:

1. Copy `BEA_HOME\weblogic81\server\lib\weblogic.jar` on the computer hosting Oracle Identity Manager to the `OIM_DC_HOME\xlclient\ext` directory on the computer in which the Design Console is installed.
2. If you are pointing the Design Console to a clustered server installation, edit the `OIM_DC_HOME\xlclient\Config\xlconfig.xml` file to add the cluster members in the URL under the `<Discovery>` section, and point the Application URL for Workflow Visualization to the Web server to access the cluster.

   For example:

   - `<ApplicationURL>http://webserver/xlWebApp/LoginWorkflowRenderer.do</ApplicationURL>`
   - `<Discovery>.<CoreServer>.<java.naming.provider.url>t3://`

     `192.168.50.31:7005,192.168.50.32:7005`
     `</java.naming.provider.url>`
3. In the configuration XML file, change the multicast address to match that of Oracle Identity Manager:
   a. Open the following file:

      ```
      OIM_HOME\xellerate\config\xlconfig.xml
      ```
   b. Search for the `<MultiCastAddress>` element, and copy the value assigned to this element.
   c. Open the following file:

      ```
      OIM_DC_HOME\xlclient\Config\xlconfig.xml
      ```

d. Search for the `<Cache>` element, and replace the value of the `<MultiCastAddress>` element inside this element with the value that you copy in Step b.

Starting the Design Console

To start the Design Console, double-click *`OIM_DC_HOME`*`\xlclient\xlclient.cmd` or select Design Console from the Microsoft Windows Start menu or desktop.

Setting the Compiler Path for Adapter Compilation

In the System Configuration form of the Design Console, you must set the `XL.CompilerPath` system property to include the path of the bin directory inside the JDK directory (*`JDK_HOME`*`\bin`) that is used by the application server on which Oracle Identity Manager is deployed.

Then, restart Oracle Identity Manager.

> **See Also:** The "Rule Elements, Variables, Data Types, and System Properties" section in *Oracle Identity Manager Reference*

Enabling SSL Communication (Optional)

The following topics provide information required for enabling SSL communication between the Design Console and BEA WebLogic Server:

- Prerequisites or Assumptions
- SSL Certificate Setup
- Configuration Changes

Prerequisites or Assumptions

The following are the prerequisites or assumptions for enabling SSL communication:

- BEA WebLogic Server is installed.
- The WebLogic Domain directory is `C:\bea\user_projects\domains\oim`.
- The BEA WebLogic Server home (*`WEBLOGIC_HOME`*) directory is `C:\bea\weblogic81`.
- The identity store is `support.jks` and the password is `support`.
- The certificate request is made for xellerate.oracle.com host and for Oracle Identity Management Group.
- The self-sign certificate is named supportcert.pem.
- The private key alias is `support`, and the password is `weblogic`.
- The `setEnv.cmd` or `setEnv.sh` script is run to set up PATH, CLASSPATH, and other variables.

SSL Certificate Setup

This section discusses the following topics:

- Generating Keys
- Signing the Certificates

- Exporting the Certificate

> **Note:** The preceding steps must be run on the BEA WebLogic Server host.

- Configuring the Trust Store

> **Note:** The preceding step must be run on the Design Console host.

Generating Keys

Generate private/public certificate pairs by using the keytool command provided. The following command creates an identity keystore (`support.jks`). Change the parameter values passed to the keytool command according to your requirements. Ensure that there is no line break in the keytool argument.

```
keytool -genkey
        -alias support
        -keyalg RSA
        -keysize 1024
        -dname "CN=xellerate.oracle.com, OU=Identity, O=Oracle Corporation,
L=RedwoodShores, S=California, C=US"
        -keypass weblogic
        -keystore C:\bea\user_projects\domains\oim\support.jks
        -storepass support
```

> **Note:** Use the same host name that you would use in the `xlconfig.xml` file. For example, if you use `https://localhost:7002` and `t3s://localhost:7002` in the xlconfig.xml file, then the value of CN in the keytool command must be localhost.

Signing the Certificates

Use the following command to sign the certificates that you created.

```
keytool -selfcert -alias support
        -sigalg MD5withRSA
        -validity 2000
        -keypass weblogic
        -keystore C:\bea\user_projects\domains\oim\support.jks
        -storepass support
```

> **Note:** Oracle recommends that you use the trusted certificate authorities, for example, VeriSign or Thawte, for signing the certificates.

Exporting the Certificate

Use the following command to export the certificate from the identity keystore to a file, for example, `supportcert.pem`:

```
keytool -export -alias support
        -file C:\bea\user_projects\domains\oim\supportcert.pem
```

```
-keypass weblogic
-keystore C:\bea\user_projects\domains\oim\support.jks
-storepass support
```

Configuring the Trust Store

To configure the trust store:

1. Copy the `supportcert.pem` file to the following location on the Design Console: *`OIM_DC_HOME`*`\java\lib\security`.
2. Open a command prompt at *`OIM_DC_HOME`*`\java\lib\security` and run the following command:

   ```
   cd OIM_DC_HOME\java\lib\security
   keytool -import
           -alias support
           -trustcacerts
           -file supportcert.pem
           -keystore cacerts
           -storepass changeit
   ```

> **Note:** For a clustered installation, repeat all of the steps for each of the participating nodes in the cluster. However, you do not generate keys or sign and export certificates if the other server in the cluster is located on the same host.

Configuration Changes

The following sections provide information related to the configuration changes required for a successful SSL connection.

- Changes to the Design Console
- Changes to BEA WebLogic Server
- Copying the BEA WebLogic Server License
- (Optional) Enabling SSL Debug for BEA WebLogic Server

Changes to the Design Console

The configuration changes required for successful SSL connection in the Design Console are done by performing the following steps:

1. On the computer in which the Design Console is installed, go to *`OIM_DC_HOME`*`\xlclient\Config\xlconfig.xml`.
2. Modify the `xlconfig.xml` file to use HTTPS and T3S protocol and SSL port to connect to the server, as shown in the following element:

   ```
   <ApplicationURL>https://xellerate.oracle.com:7002/xlWebApp/loginWorkflowRendere
   r.do</ApplicationURL>
   ```

   For a clustered installation, you can send a https request to only one of the servers in the cluster, as shown in the following element:

   ```
   <java.naming.provider.url>t3s://xellerate.oracle.com:7002</java.naming.provider
   .url>
   ```

Else, you can point to the Web server SSL URL based on the Web server configuration. If you choose to use the Web server URL, then repeat the steps in the "Configuring the Trust Store" section on page 10-6 with the Web server certificate.

For a clustered installation, ensure that you add the participating nodes to the corresponding SSL port as comma-separated values in the URL for java.naming.provider.url, as follows:

```
<java.naming.provider.url>t3s://node1:7002,node2:7002</java.naming.provider.url
>
```

Changes to BEA WebLogic Server

The configuration changes required for successful SSL connection in the BEA WebLogic Server are done by performing the following steps:

1. In the WebLogic Server Administration Console, click **Servers, Configuration**, and then click **General.**
2. Select **SSL listen port enabled**. The default port is 7002.
3. In the Administrative Console, click **Servers, Configuration** and then click **Keystores & SSL.**
4. Click the Change link near Keystore Configuration.
5. Select **Custom Identity and Java Standard Trust**, and then click **Continue**.
6. Specify `C:\bea\user_projects\domains\oim\support.jks` as the custom identity keystore file name.
7. Specify `JKS` as the custom identity keystore type.
8. Specify the password.
9. Click **Continue.**
10. Enter `support` as the private key alias.
11. Enter password, for example, `support`, and confirm.
12. Restart the server for the changes to take effect.

> **Note:** For a clustered installation, repeat all the steps for each of the participating nodes in the cluster, and then restart the cluster.

Copying the BEA WebLogic Server License

To copy the BEA WebLogic Server license:

1. Copy `license.bea` from *`WEBLOGIC_HOME`* in the computer in which BEA WebLogic Server is installed to *`OIM_DC_HOME`* in the computer in which the Design Console is installed.
2. Open the *`OIM_DC_HOME`*`/classpath.bat` file and add *`OIM_DC_HOME`* to the classpath at the end of the file.
3. Copy `*webserviceclient+ssl.jar, wlcipher.jar*`, and `*jsafeFIPS.jar*` from *`WEBLOGIC_HOME`*`\server\lib` to *`OIM_DC_HOME`*`\ext`.

   Add `*webserviceclient+ssl.jar*`, `*wlcipher.jar*`, and `*jsafeFIPS.jar*` in the `classpath.bat` file.

(Optional) Enabling SSL Debug for BEA WebLogic Server

To troubleshoot the SSL setup issues, you must enable SSL debug.

To enable SSL debug:

1. Go to the WebLogic domain directory and open:
   - For Windows: `xlStartWLS.cmd`
   - For UNIX: `xlStartWLS.sh`
2. Add the following Java options:

   ```
   -Dssl.debug=true -Dweblogic.StdoutDebugEnabled=true
   ```

Removing the Design Console Installation

To remove the Design Console installation:

1. Stop Oracle Identity Manager and the Design Console if they are running.
2. Stop all Oracle Identity Manager processes.
3. Delete the *`OIM_DC_HOME`* directory in which you installed the Design Console.

11

Installing and Configuring the Oracle Identity Manager Remote Manager

This chapter explains how to install Oracle Identity Manager Remote Manager. It discusses the following topics:

- Installing the Remote Manager on Microsoft Windows
- Installing the Remote Manager on UNIX
- Configuring the Remote Manager
- Starting the Remote Manager
- Removing the Remote Manager Installation

Installing the Remote Manager on Microsoft Windows

This section describes how to install the Remote Manager on Microsoft Windows.

> **Note:** All Oracle Identity Manager components must be installed in different home directories. If you are installing the Remote Manager on a computer that is hosting another Oracle Identity Manager component (the server or the Design Console), then specify an installation directory that has not been used.

To install the Remote Manager on a Microsoft Windows host:

1. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.
2. Using Windows Explorer, navigate to the installServer directory on the installation CD.
3. Double-click the **setup_rm.exe** file.
4. Choose a language from the list on the Installer page.

   The Welcome page is displayed.
5. In the Welcome page, click **Next**.
6. In the Target directory page, complete one of the following steps:
   - The default directory for Oracle Identity Manager products is `C:\oracle`. To install the Remote Manager into this directory, click **Next**.
   - To install Remote Manager in a different directory, specify the path of the directory in the **Directory name** field, and then click **Next**.

> **Note:** If the directory path that you specified does not exist, then the Base Directory settings field is displayed. Click **OK**. The directory is automatically created. If you do not have write permission to create the default directory for Oracle Identity Manager, then a message is displayed informing you that the installer could not create the directory. Click **OK** to close the message, and then contact your system administrator to obtain the appropriate permissions.

7. Select either the JRE that is installed with Oracle Identity Manager or specify an existing JRE. Click **Next**. The Remote Manager Configuration page is displayed.
8. In the Remote Manager Configuration page, enter the appropriate information for the Remote Manager:
   a. Enter the service name. The default value is RManager.
   b. Enter the Remote Manager binding port. The default value is 12346.
   c. Enter the Remote Manager Secure Sockets Layer (SSL) port. The default value is 12345.
   d. Click **Next**.
9. In the Shortcut page, select or clear the check boxes for the shortcut options according to your preferences:
   a. Choose to create a shortcut for the Remote Manager on the desktop.
   b. Choose to create a shortcut for the Remote Manager on the Start Menu.
   c. After completing the settings, click **Next**.
10. In the Installation page, review the configuration details, and then click **Install** to start the installation.
11. Click **Finish** to complete the installation.

Installing the Remote Manager on UNIX

To install the Remote Manager on UNIX:

> **Note:** Before installing the Remote Manager you must set the JAVA_HOME variable to the JRE that is included with the Remote Manager installer.

1. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.

> **Note:** If the autostart routine is enabled for your computer, then proceed to Step 3.

2. From the console, change directories to the installServer directory on the installation CD by using the `cd` command, and run the install_rm.sh file.

   The command-line installer starts.
3. Choose a language from the list by entering a number and then by entering **0** to apply the language.

The Welcome panel is displayed.

4. In the Welcome panel, enter **1** to move to the next panel. The Target directory panel is displayed.

5. In the Target directory panel, enter the path to the directory in which you want to install the Oracle Identity Manager Remote Manager. The default directory is `/opt/oracle`.

   - Enter **1** to move to the next panel.
   - If the directory does not exist, then you are asked to create it. Enter **y** for yes.

   > **Note:** All Oracle Identity Manager components must be installed in different home directories. If you are installing the Remote Manager on a computer that is hosting an Oracle Identity Manager server, then you must specify a unique installation directory.

6. Specify the JRE to use with the Remote Manager:

   - Enter **1** to install the JRE included with Oracle Identity Manager.
   - Enter **2** to use an existing JRE at a specified location.

   After specifying the JRE, enter **0** to accept your selection and then enter **1** to move to the next panel.

7. In the Remote Manager Configuration panel, enter the Remote Manager configuration information:

   a. Enter the Service Name, or press the Enter key to accept the default.

   b. Enter the Remote Manager binding port, or press the Enter key to accept the default.

   c. Enter the Remote Manager SSL port, or press the Enter key to accept the default.

   After entering the Remote Manager configuration information, enter **1** to move to the next panel.

   The Remote Manager installation summary panel is displayed.

8. Check the information.

   - Enter **2** to go back and make changes.
   - Enter **1** to start the installation.

9. Enter **3** to finish the Remote Manager installation.

Configuring the Remote Manager

The Remote Manager and Oracle Identity Manager server communicate by using SSL. If you are using the Remote Manager, then you must enable a trust relationship between Oracle Identity Manager and the Remote Manager. Oracle Identity Manager must trust the Remote Manager certificate.

Optionally, you can enable client-side authentication in which the Remote Manager checks the server certificate. Import the Remote Manager certificate into the Oracle Identity Manager keystore and make it trusted. For client-side authentication, import the certificate for Oracle Identity Manager into the keystore for the Remote Manager, and then make that certificate trusted. You must also manually edit the configuration file associated with the server, and depending on the options you selected during the Remote Manager installation, edit the Remote Manager configuration file as well.

Changing the Remote Manager Keystore Passwords

During installation, the password for the Remote Manager keystore is set to `xellerate`. Oracle recommends that for changing the keystore passwords for all production installations.

To change the keystore password, you must change the storepass of .xlkeystore and the keypass of the xell entry in .xlkeystore; these two values must be identical. Use the keytool utility and perform the following steps to change the keystore passwords:

1. Open a command prompt on the Oracle Identity Manager host computer.
2. Navigate to the *`OIM_RM_HOME`*`\xellerate\config` directory.
3. Run the keytool utility with the following options to change the storepass:

   ```
   JAVA_HOME\jre\bin\keytool -storepasswd -new new_password -storepass xellerate
   -keystore .xlkeystore -storetype JKS
   ```

4. Run the keytool utility with the following options to change the keypass of the xell entry in .xlkeystore:

   ```
   JAVA_HOME\jre\bin\keytool -keypasswd -alias xell -keypass xellerate
   -new new_password -keystore .xlkeystore -storepass xellerate
   ```

   `JAVA_HOME` represents the location of the Java installation associated with the Remote Manager installation.

5. In a text editor, open *`OIM_RM_HOME`*`\xlremote\config\xlconfig.xml`.
6. Edit the *`<RMSecurity>.<KeyStore>`* tag to specify the keystore password as follows:

   - Change the password tag to `encrypted=false`.
   - Enter the password, for example:

     ```
     <RMSecurity>
     <KeyStore>
     <Location>.xlkeystore</Location>
     <Password encrypted="false">new_password</Password>
     <Type>JKS</Type>
     <Provider>sun.security.provider.Sun</Provider>
     </KeyStore>
     ```

> **Note:** If you are using client-side authentication for the Remote Manager, then enter the Oracle Identity Manager keystore password in the `<RMSecurity>.<TrustStore>` section of *`OIM_RM_HOME`*`\xlremote\config\xlconfig.xml` as follows:
>
> ```
> <TrustStore>
> <Location>.xlkeystore</Location>
> <Password encrypted="false">OIM_Server_keystore_password</Password>
> <Type>JKS</Type>
> <Provider>sun.security.provider.Sun</Provider>
> </TrustStore>
> ```

7. Save and close the xlconfig.xml file.

8. Restart the Remote Manager.

9. In a text editor, open *OIM_HOME*`\xellerate\config\xlconfig.xml`.

10. Edit the `<RMSecurity>.<TrustStore>` section to specify the new Remote Manager keystore password as follows:

    - Change the password tag to `encrypted=false`.
    - Enter the password, for example:

    ```
    <TrustStore>
    <Location>.xlkeystore</Location>
    <Password encrypted="false">new_password</Password>
    <Type>JKS</Type>
    <Provider>sun.security.provider.Sun</Provider>
    </TrustStore>
    ```

11. Save and close the xlconfig.xml file, and then restart Oracle Identity Manager.

Trusting the Remote Manager Certificate

To establish a trust relationship between Oracle Identity Manager and the Remote Manager:

1. Copy the Remote Manager certificate to the server computer. On the Remote Manager computer, locate the *OIM_RM_HOME*`\xlremote\config\xlserver.cert` file, and copy it to the server computer.

    Note: The server certificate in *OIM_HOME* is also named `xlserver.cert`. Ensure that you do not overwrite that certificate.

2. Open a command prompt on the server computer.

3. To import the certificate by using the keytool utility, use the following command:

    ```
    JAVA_HOME\jre\bin\keytool -import -alias rm_trusted_cert -file
    RM_cert_location\xlserver.cert -trustcacerts -keystore
    OIM_HOME\xellerate\config\.xlkeystore -storepass xellerate
    ```

    JAVA_HOME is the location of the Java directory for the application server, the value of `alias` is an arbitrary name for the certificate in the store, and *RM_cert_location* is the location in which you copied the certificate.

    Note: If you changed the keystore password, then substitute that for xellerate for the value of the storepass variable.

4. Enter **Y** at the prompt to trust the certificate.

5. In a text editor, open the *OIM_HOME*`\xellerate\config\xlconfig.xml` file.

6. Locate the `<RMIOverSSL>` property and set the value to `true`, for example:

    ```
    <RMIOverSSL>true</RMIOverSSL>
    ```

7. Locate the <KeyManagerFactory> property. If you are using the IBM JRE, then set the value to IBMX509. For all other JREs, set the value to SUNX509. For example:

   ```
   <KeyManagerFactory>IBMX509</KeyManagerFactory>
   ```

   Or:

   ```
   <KeyManagerFactory>SUNX509</KeyManagerFactory>
   ```

8. Save the file.
9. Restart Oracle Identity Manager.

Using Your Own Certificate

To configure the Remote Manager by using your own certificate on the Remote Manager system:

1. Import your custom key in a new keystore (new_keystore_name) other than .xlkeystore. Remember the password (new_keystore_pwd) that you use for the new keystore.
2. Copy this new keystore to the *OIM_RM_HOME*\xlremote\config\ directory.
3. Open the following file in a text editor:

   OIM_RM_HOME\xlremote\config\xlconfig.xml

4. Locate the <RMSecurity> tag and change the value in the <Location> and <Password> tags as follows:

   - If you are using the IBM JRE, change the values to:

     ```
     <KeyStore>
          <Location>new_keystore_name</Location>
          <Password encrypted="false">new_keystore_pwd</Password>
          <Type>JKS</Type>
          <Provider>com.ibm.crypto.provider.IBMJCE</Provider>
     </KeyStore>
     ```

   - For all other JREs, change the values to:

     ```
     <KeyStore>
          <Location>new_keystore_name</Location>
          <Password encrypted="false">new_keystore_pwd</Password>
          <Type>JKS</Type>
          <Provider>sun.security.provider.Sun</Provider>
     </KeyStore>
     ```

5. Restart the Remote Manager server, and open the xlconfig.xml file to ensure that the password for the new keystore was encrypted.

To configure the Remote Manager by using your own certificate on the Oracle Identity Manager server:

1. Import the same certificate key used in the Remote Manager system to a new keystore (new_svrkeystore_name) other than .xlkeystore. Remember the password (new_svrkeystor_pwd) that you use for the new keystore.
2. Copy this new keystore to the *OIM_HOME*\xellerate\config directory.
3. Open the following file in a text editor:

   OIM_HOME\xellerate\config\xlconfig.xml

4. Locate the `<RMSecurity>` tag and change the value in the `<Location>` and `<Password>` tags as follows:

   ```
   <TrustStore>
      <Location>new_svrkeystore_name</Location>
      <Password encrypted="false">new_svrkeystor_pwd</Password>
      <Type>JKS</Type>
      <Provider>sun.security.provider.Sun</Provider>
   </TrustStore>
   ```

5. Restart Oracle Identity Manager and open the `xlconfig.xml` file to ensure that the password for the new keystore is encrypted.

Enabling Client-Side Authentication for the Remote Manager

To enable client-side authentication:

1. On the computer hosting the Remote Manager, in a text editor, open the *`OIM_RM_HOME`*`\xlremote\config\xlconfig.xml` file.

2. Set the `<ClientAuth>` property to `true`, for example:

   ```
   <ClientAuth>true</ClientAuth>
   ```

3. Ensure that the `<RMIOverSSL>` property is set to `true`, for example:

   ```
   <RMIOverSSL>true</RMIOverSSL>
   ```

4. Locate the `<KeyManagerFactory>` property.

   If you are using the IBM JRE, then set the value to `IBMX509`. For all other JREs, set the value to `SUNX509`. For example:

   ```
   <KeyManagerFactory>IBMX509</KeyManagerFactory>
   ```

   Or:

   ```
   <KeyManagerFactory>SUNX509</KeyManagerFactory>
   ```

5. Save the file.

6. Copy the server certificate to the Remote Manager computer.

   On the server computer, locate the *`OIM_HOME`*`\xellerate\config\xlserver.cert` file, and copy it to the Remote Manager computer.

   > **Note:** The Remote Manager certificate is also named xlserver.cert. Ensure that you do not overwrite that certificate.

7. Open a command prompt on the Remote Manager computer.

8. Import the certificate by using the following keytool command:

   ```
   JAVA_HOME\jre\bin\keytool -import -alias trusted_server_cert -file
   server_cert_location\xlserver.cert -trustcacerts -keystore
   OIM_RM_HOME\xlremote\config\.xlkeystore -storepass xellerate
   ```

   `JAVA_HOME` is the location of the Java directory for the Remote Manager, the value of `alias` is an arbitrary name for the certificate in the store, *`OIM_RM_HOME`* is the home directory for the Remote Manager, and *`server_cert_location`* is the location to which you copied the server certificate.

Note: If you changed the keystore password, then substitute that value for xellerate, which is the default value of the storepass variable.

9. Enter **Y** at the prompt to trust the certificate.
10. Restart the Remote Manager.

Starting the Remote Manager

Use the following script to start the Remote Manager:

- On Microsoft Windows:

  ```
  OIM_RM_HOME\xlremote\remotemanager.bat
  ```

- On UNIX:

  ```
  OIM_RM_HOME/xlremote/remotemanager.sh
  ```

Removing the Remote Manager Installation

To remove the Remote Manager installation, perform the following steps:

1. Stop Oracle Identity Manager and the Remote Manager if they are running.
2. Stop all Oracle Identity Manager processes.
3. Delete the *`OIM_RM_HOME`* directory in which you installed the Remote Manager.

12

Troubleshooting the Oracle Identity Manager Installation

This section describes the following problems that can occur during the Oracle Identity Manager installation:

- Oracle Identity Manager Installation Fails During Installation in a BEA WebLogic Server Cluster
- Task Scheduler Fails in a Clustered Installation
- Default Login Does Not Work

> **Note:** You can use the Diagnostic Dashboard tool for assistance when you troubleshoot the Oracle Identity Manager Installation. See *Oracle Identity Manager Administrative and User Console Guide* for detailed information.

Oracle Identity Manager Installation Fails During Installation in a BEA WebLogic Server Cluster

The Oracle Identity Manager installation will fail during installation in a BEA WebLogic Server cluster if incorrect values are defined for the target server and server port number. Do not define the Administrative Server as a target during the installation process; the setup script must create the JMS Server on a cluster member.

Workaround Example

The following is a sample procedure to clean up the BEA WebLogic Server services so that you can continue with the installation:

1. Open the WebLogic Server Administration Console to clean up the services that have been created for the cluster.
2. Select the **JDBC** tab and delete:
   - The connection pools
   - Both the data sources
3. Select the **JMS** tab and delete:
   - The xleConnectionFactory
   - Every xlJDBCStore
   - Every xlJMSServer

4. Open the *OIM_HOME*\Profile\weblogic.profile file, and then change the following:

    a. The BEA WebLogic Server target name from myserver to <cluster_member1>.

    b. The BEA WebLogic Server target port from 7001 to 7051.

5. Run the setup_weblogic.cmd script.
6. Review the log file to see that it runs successfully.
7. When the setup script runs successfully, restart BEA WebLogic Server.

You can either continue with your installation (restart the Oracle Identity Manager Installer at this point), or start the Oracle Identity Manager installation by removing all installed Oracle Identity Manager products as well as the WebLogic domain.

Task Scheduler Fails in a Clustered Installation

The Task Scheduler fails to work properly when the cluster members, which are computers that are part of the cluster, have different settings on their system clocks. Oracle recommends that the system clocks for all cluster members be synchronized within a second of each other.

Default Login Does Not Work

If the default login is not working for the Design Console or Administrative and User Console and you are using Microsoft SQL Server, then ensure that the Distributed Transaction Coordinator is running.

Note: Microsoft SQL Server is not supported in Oracle Identity Manager release 9.1.0. See "Certified Components" in *Oracle Identity Manager Release Notes* for information about certified components.

A

Java 2 Security Permissions for BEA WebLogic Server

Note: The application might fail to start because of syntax errors in the policy files.

Be careful when you edit the policy files. Oracle recommends that you use the policy tool provided by the JDK for editing the policy files. The tool is available in the following directory:

JAVA_HOME/jre/bin/policytool

To enable Java 2 Security for Oracle Identity Manager running on BEA WebLogic Server:

1. Go to the $*BEA_HOME*/user_projects/domains/$OIM_DOMAIN/ directory and open the run script (xlStartWLS.bat for Windows and xlStartWLS.sh for UNIX).
2. Search for JAVA_OPTIONS and add the following:

```
-Djava.security.manager
-Djava.security.policy=$WL_HOME/server/lib/weblogic.policy
-Dbea.home=$BEA_HOME
-Dserver.name=$SERVER_NAME
-Doim.domain=$BEA_HOME/user_projects/domains/$OIM_DOMAIN
```

Note: Remember the following:

Change *$WL_HOME* to the actual BEA WebLogic Server home directory location.

Change *$BEA_HOME* to the actual BEA home directory location.

Change *$SERVER_NAME* to the actual server name of BEA WebLogic Server.

Change *$OIM_DOMAIN* to the actual domain name where Oracle Identity Manager is deployed.

The following table describes the options:

Option	Description
`-Djava.security.manager`	Enables the Java 2 Security manager.
`-Djava.security.policy`	Specifies the policy file to use for Java 2 Security.
`-Dbea.home`	Specifies the root of the WebLogic Server install. Typically it is `/opt/bea` or `c:\bea`.
`-Dserver.name`	Specifies the name of the server on which Oracle Identity Manager is installed. Typically it is myserver.
`-Doim.domain`	Specifies the directory of the domain on which Oracle Identity Manager is installed.

3. Check if the *$WL_HOME*`/weblogic81/server/lib/weblogic.policy` file exists. If the file exists, then edit it and add the Java 2 Security permissions specified in the "Policy File"section on page A-2. If it does not exist, then create it.
4. After making the changes mentioned in steps 1 through 3, you must restart all the servers.

Policy File

Append the following code at the end of the `weblogic.policy` file:

> **Note:** The instructions to change the code in the policy file are given in comments, which are in bold font.
>
> This `weblogic.policy` example is for UNIX installation. For Microsoft Windows, ensure that you change the slash (/) character between the directory names to two backslash characters (\\) in every `permission java.io.FilePermission` property.
>
> Ensure that you change the multicast IP `231.167.157.106` in this example to reflect the multicast IP address of the Oracle Identity Manager installation. You can find the Oracle Identity Manager multicast IP address in the `xlconfig.xml` file.

```
// ********************************************
 //  Default WebLogic Permissions ends
 // ********************************************

 grant codeBase "file:${java.home}/lib/-" {
 permission java.security.AllPermission;
 };

 grant codeBase "file:${java.home}/jre/lib/-" {
 permission java.security.AllPermission;
 };

 grant codebase "file:${oim.domain}/${server.name}/.internal/-" {
 permission java.security.AllPermission;
 };


 // ********************************************
 // From here, OIM application permission start
 // ********************************************
 // OIM codebase permissions
```

```
grant codeBase
    "file:${oim.domain}/XLApplications/WLXellerateFull.ear/-" {
      // File permissions

      // Need read,write,delete permissions on $OIM_HOME/config folder
      // to read various config files, write the
      // xlconfig.xml.{0,1,2..} files upon re-encryption and delete
      // the last xlconfig.xml if the numbers go above 9.

      permission java.io.FilePermission "${XL.HomeDir}/config/-",
        "read, write, delete";
      permission java.io.FilePermission "${XL.HomeDir}/-", "read";

      // Need read,write,delete permissions to generate adapter java
      // code, delete the .class file when the adapter is loaded into
      // the database
      permission java.io.FilePermission "${XL.HomeDir}/adapters/-",
        "read,write,delete";

      // This is required by the connectors and connector installer
      permission java.io.FilePermission
        "${XL.HomeDir}/ConnectorDefaultDirectory/-", "read,write,delete";
      permission java.io.FilePermission
        "${XL.HomeDir}/connectorResources/-", "read,write,delete";

      // Read Globalization resource bundle files for various
      // locales
      permission java.io.FilePermission
        "${XL.HomeDir}/customResources/-", "read";

      // Read code from "JavaTasks", "ScheduleTask",
      // "ThirdParty", "EventHandlers" folder
      permission java.io.FilePermission
        "${XL.HomeDir}/EventHandlers/-", "read";
      permission java.io.FilePermission
        "${XL.HomeDir}/JavaTasks/-", "read";
      permission java.io.FilePermission
        "${XL.HomeDir}/ScheduleTask/-", "read";
      permission java.io.FilePermission
        "${XL.HomeDir}/ThirdParty/-", "read";

      // Required by the Generic Technology connector
      permission java.io.FilePermission  "${XL.HomeDir}/GTC/-", "read";

      // OIM server codebase requires read permissions on the
      // deploy directory, the .wlnotdelete directory, the
      // "applications" folder, the "XLApplications" folder
      // and the BEA WebLogic Server lib directory
      // All these permissions are specific to the BEA WebLogic Server.
      permission java.io.FilePermission
        "${oim.domain}/XLApplications/WLXellerateFull.ear/-", "read";
      permission java.io.FilePermission
        "${oim.domain}/${server.name}/.wlnotdelete/-",
        "read,write,delete";
      permission java.io.FilePermission
        "${oim.domain}/applications/-", "read";
      permission java.io.FilePermission
        "${oim.domain}/XLApplications/-", "read";
      permission java.io.FilePermission "http:${/}-", "read";
      permission java.io.FilePermission ".${/}http:${/}-", "read";
      permission java.io.FilePermission
        "${bea.home}/weblogic81/server/lib/-", "read";
      permission java.io.FilePermission
        "${oim.domain}/${server.name}/ldap/ldapfiles/-", "read,write";
      permission java.io.FilePermission
        "${oim.domain}/${server.name}/-", "read,write,delete";

      // OIM server codebase requires read permissions on the
      // $JAVA_HOME/lib directory
      permission java.io.FilePermission "${java.home}/lib/-", "read";

      // OIM server invokes the java compiler. You need "execute"
      // permissions on all files.
      permission java.io.FilePermission "<<ALL FILES>>", "execute";

      // Socket permissions
      // Basically we allow all permissions on non-privileged sockets
      // The multicast address should be the same as the one in
      // xlconfig.xml for javagroups communication
      permission java.net.SocketPermission "*:1024-",
        "connect,listen,resolve,accept";
      permission java.net.SocketPermission "231.167.157.106",
        "connect,accept,resolve";

      // Property permissions
      // Read and write OIM properties
      // Read XL.*, java.* and log4j.* properties
      permission java.util.PropertyPermission "XL.HomeDir", "read";
      permission java.util.PropertyPermission "XL.*", "read";
      permission java.util.PropertyPermission "XL.ConfigAutoReload",
        "read";
      permission java.util.PropertyPermission "log4j.*", "read";
      permission java.util.PropertyPermission "user.dir", "read";
      permission java.util.PropertyPermission "weblogic.xml.debug",
        "read";
      permission java.util.PropertyPermission "file.encoding", "read";
      permission java.util.PropertyPermission "java.class.path", "read";
      permission java.util.PropertyPermission "java.ext.dirs", "read";
      permission java.util.PropertyPermission "java.library.path",
        "read";
      permission java.util.PropertyPermission "sun.boot.class.path",
        "read";
      permission java.util.PropertyPermission "weblogic.*", "read";

      // Run time permissions
      // OIM server needs permissions to create its own class loader,
      // get the class loader, modify threads and register shutdown
      // hooks
      permission java.lang.RuntimePermission "createClassLoader";
      permission java.lang.RuntimePermission "getClassLoader";
      permission java.lang.RuntimePermission "setContextClassLoader";
      permission java.lang.RuntimePermission  "setFactory";
      permission java.lang.RuntimePermission "modifyThread";
      permission java.lang.RuntimePermission "modifyThreadGroup";
      permission java.lang.RuntimePermission "shutdownHooks";

      // OIM server needs run time permissions to generate and load
      // classes in the following specified packages. Also access the
      // declared members of a class.
      // weblogic.kernelPermission is required by BEA WebLogic Server
```

```
          permission java.lang.RuntimePermission
            "defineClassInPackage.com.thortech.xl.adapterGlue.ScheduleItemEvents";
          permission java.lang.RuntimePermission
            "defineClassInPackage.com.thortech.xl.dataobj.rulegenerators";
          permission java.lang.RuntimePermission
            "defineClassInPackage.com.thortech.xl.adapterGlue";
          permission java.lang.RuntimePermission "accessDeclaredMembers";
          permission java.lang.RuntimePermission "weblogic.kernelPermission";
          permission java.lang.RuntimePermission
            "accessClassInPackage.sun.net.www.protocol.c";
          permission java.lang.RuntimePermission "accessClassInPackage.sun.io";
          permission java.lang.RuntimePermission
            "accessClassInPackage.sun.security.provider";
          permission java.lang.RuntimePermission
            "accessClassInPackage.sun.security.action";

          // Reflection permissions
          // Give permissions to access and invoke fields/methods from
          // reflected classes.
          permission java.lang.reflect.ReflectPermission "suppressAccessChecks";

          // Security permissions for OIM server
          permission java.security.SecurityPermission "*";
          permission java.security.SecurityPermission "insertProvider.SunJCE";
          permission java.security.SecurityPermission "insertProvider.SUN";
          permission javax.security.auth.AuthPermission "doAs";
          permission javax.security.auth.AuthPermission "doPrivileged";
          permission javax.security.auth.AuthPermission "getSubject";
          permission javax.security.auth.AuthPermission "modifyPrincipals";
          permission javax.security.auth.AuthPermission "createLoginContext";
          permission javax.security.auth.AuthPermission "getLoginConfiguration";
          permission javax.security.auth.AuthPermission "setLoginConfiguration";
          permission java.security.SecurityPermission
            "getProperty.policy.allowSystemProperty";
          permission java.security.SecurityPermission
            "getProperty.login.config.url.1";
          permission javax.security.auth.AuthPermission
            "refreshLoginConfiguration";

          // SSL permission (for remote manager)
          permission javax.net.ssl.SSLPermission  "getSSLSessionContext";

          // Serializable permissions
          permission java.io.SerializablePermission "enableSubstitution";
    };


    // You must give the codebase in xlWebApp.war/WEB-INF/classes
    // the following permissions
    grant codeBase

"file:${oim.domain}/XLApplications/WLXellerateFull.ear/xlWebApp.war/WEB-INF/classe
s/-" {
          permission java.io.FilePermission

"${oim.domain}/XLApplications/WLXellerateFull.ear/xlWebApp.war/cabo/styles/-",
"read,write";
          permission java.io.FilePermission

"${oim.domain}/XLApplications/WLXellerateFull.ear/xlWebApp.war/cabo/images/-",
"read,write";
    };

    // nexaweb-common.jar from WebLogic server/lib is given AllPermissions
    // The classes in this JAR must be loaded by WebLogic's classloader
    grant codeBase "file:${bea.home}/weblogic81/server/lib/nexaweb-common.jar" {
          permission java.security.AllPermission;
    };

    // Permissions for nexaweb-common.jar from OIM_HOME/ext
    grant codeBase "file:${XL.HomeDir}/ext/nexaweb-common.jar" {
          permission java.security.AllPermission;
    };

    // Permissions for xlCrypto.jar from $OIM_HOME/lib
    grant codeBase "file:${XL.HomeDir}/lib/xlCrypto.jar" {
          permission java.security.SecurityPermission "insertProvider.SunJCE";
          permission java.security.SecurityPermission "insertProvider.SUN";
    };

    // Permissions for xlUtils.jar from $OIM_HOME/lib
    grant codeBase "file:${XL.HomeDir}/lib/xlUtils.jar" {
          permission java.io.FilePermission
            "${bea.home}/weblogic81/server/lib/-", "read";
          permission java.io.FilePermission "${java.home}/jre/lib/-", "read";

          // Serializable permissions
          permission java.io.SerializablePermission "enableSubstitution";
    };

    // Permissions for log4j-1.2.8.jar from $OIM_HOME/ext
    grant codeBase "file:${XL.HomeDir}/ext/log4j-1.2.8.jar" {
          permission java.io.FilePermission
            "${oim.domain}/XLApplications/WLXellerateFull.ear/xlVO.jar",
            "read";
    };

    // Permissions for xlLogger.jar from $OIM_HOME/lib
    // The Filewatchdog class from this jar file must periodically scan
    // these directories for updated/new jar files.
    // We also scan the classes in xlAdapterUtilities.jar by default
    grant codeBase "file:${XL.HomeDir}/lib/xlLogger.jar" {
          permission java.io.FilePermission "${XL.HomeDir}/EventHandlers",
            "read";
          permission java.io.FilePermission "${XL.HomeDir}/JavaTasks", "read";
          permission java.io.FilePermission "${XL.HomeDir}/ScheduleTask",
            "read";
          permission java.io.FilePermission "${XL.HomeDir}/ThirdParty",
            "read";
          permission java.io.FilePermission "${XL.HomeDir}/EventHandlers/-",
            "read";
          permission java.io.FilePermission "${XL.HomeDir}/JavaTasks/-",
            "read";
          permission java.io.FilePermission "${XL.HomeDir}/ScheduleTask/-",
            "read";
          permission java.io.FilePermission "${XL.HomeDir}/ThirdParty/-",
            "read";
          permission java.io.FilePermission
            "${XL.HomeDir}/lib/xlAdapterUtilities.jar", "read";
    };
```

```
// Permissions for .wlnotdelete folder
grant codeBase "file:${oim.domain}/${server.name}/.wlnotdelete/-" {
      permission java.security.AllPermission;
};

// Nexaweb server codebase permissions
grant codeBase "file:${oim.domain}/XLApplications/WLNexaweb.ear/-" {
      // File permissions
      permission java.io.FilePermission "${user.home}", "read, write";
      permission java.io.FilePermission
        "${oim.domain}/XLApplications/WLNexaweb.ear/-", "read";
      permission java.io.FilePermission
        "${oim.domain}/XLApplications/WLXellerateFull.ear/-", "read";
      permission java.io.FilePermission
        "${bea.home}/weblogic81/server/lib/-", "read";

      permission java.io.FilePermission "${XL.HomeDir}/adapters/-",
        "read,write,delete";
      permission java.io.FilePermission "<<ALL FILES>>", "execute";

      // Property permissions
      permission java.util.PropertyPermission "weblogic.xml.debug", "read";
      permission java.util.PropertyPermission "user.dir", "read";
      permission java.util.PropertyPermission "*", "read,write";

      // Run time permissions
      permission java.lang.RuntimePermission "createClassLoader";
      permission java.lang.RuntimePermission "getClassLoader";
      permission java.lang.RuntimePermission "setContextClassLoader";
      permission java.lang.RuntimePermission  "setFactory";

      // Nexaweb server security permissions to load the Cryptix
      // extension
      permission java.security.SecurityPermission "insertProvider.Cryptix";
      permission java.lang.RuntimePermission "weblogic.kernelPermission";
      permission java.lang.RuntimePermission
        "accessClassInPackage.sun.net.www.protocol.c";

      // Socket permissions
      // Permissions on all non-privileged ports.
      permission java.net.SocketPermission "*:1024-",
        "listen, connect, resolve";

      // Security permissions
      permission javax.security.auth.AuthPermission "doAs";
      permission javax.security.auth.AuthPermission "modifyPrincipals";
      permission javax.security.auth.AuthPermission "createLoginContext";

};


// The following are permissions given to codebase in the OIM server
// directory
grant codeBase "file:${XL.HomeDir}/-" {
      // File permissions
      permission java.io.FilePermission "${XL.HomeDir}/config/-", "read";
      permission java.io.FilePermission "${XL.HomeDir}/JavaTasks/-", "read";
      permission java.io.FilePermission "${XL.HomeDir}/ScheduleTasks/-",
        "read";
      permission java.io.FilePermission "${XL.HomeDir}/ThirdParty/-",
        "read";
      permission java.io.FilePermission "${XL.HomeDir}/adapters/-",
        "read,write,delete";

      // Socket permissions
      permission java.net.SocketPermission "*:1024-",
        "connect,listen,resolve,accept";

      // Property permissions
      permission java.util.PropertyPermission "XL.HomeDir", "read";
      permission java.util.PropertyPermission "XL.ConfigAutoReload", "read";
      permission java.util.PropertyPermission "XL.*", "read";
      permission java.util.PropertyPermission "log4j.*", "read";
      permission java.util.PropertyPermission "user.dir", "read";
      permission java.util.PropertyPermission "weblogic.xml.debug", "read";

      // Security permissions
      permission javax.security.auth.AuthPermission "doAs";
      permission javax.security.auth.AuthPermission "modifyPrincipals";
      permission javax.security.auth.AuthPermission "createLoginContext";

      // Run time Permissions
      permission java.lang.RuntimePermission
        "accessClassInPackage.sun.security.provider";
};

// Minimal permissions are allowed to everyone else
grant {
// "standard" properties that can be read by anyone

permission java.util.PropertyPermission "java.version", "read";
permission java.util.PropertyPermission "java.vendor", "read";
permission java.util.PropertyPermission "java.vendor.url", "read";
permission java.util.PropertyPermission "java.class.version", "read";
permission java.util.PropertyPermission "os.name", "read";
permission java.util.PropertyPermission "os.version", "read";
permission java.util.PropertyPermission "os.arch", "read";
permission java.util.PropertyPermission "file.separator", "read";
permission java.util.PropertyPermission "path.separator", "read";
permission java.util.PropertyPermission "line.separator", "read";

permission java.util.PropertyPermission "java.specification.version",
        "read";
permission java.util.PropertyPermission "java.specification.vendor",
        "read";
permission java.util.PropertyPermission "java.specification.name",
        "read";
permission java.util.PropertyPermission
        "java.vm.specification.version", "read";
permission java.util.PropertyPermission
        "java.vm.specification.vendor", "read";
permission java.util.PropertyPermission "java.vm.specification.name",
        "read";
permission java.util.PropertyPermission "java.vm.version", "read";
permission java.util.PropertyPermission "java.vm.vendor", "read";
permission java.util.PropertyPermission "java.vm.name", "read";
permission java.util.PropertyPermission "sun.boot.class.path", "read";
permission java.util.PropertyPermission "weblogic.xml.debug", "read";
```

```
    permission java.lang.reflect.ReflectPermission "suppressAccessChecks";
        permission java.lang.RuntimePermission "accessDeclaredMembers";
        permission java.util.PropertyPermission "XL.*", "read";
        permission java.util.PropertyPermission "user.dir", "read";
        permission java.util.PropertyPermission "*", "read,write";

        permission java.lang.RuntimePermission "weblogic.kernelPermission";
        permission java.lang.RuntimePermission "getClassLoader";
        permission java.lang.RuntimePermission "createClassLoader";
    permission java.lang.RuntimePermission "setContextClassLoader";
    permission java.util.PropertyPermission "nexaweb.logs", "read,write";
       permission java.util.PropertyPermission
            "sun.net.client.defaultConnectTimeout", "read,write";
        permission java.io.FilePermission
            "${oim.domain}/XLApplications/WLNexaweb.ear/-", "read";
        permission java.io.FilePermission
            "${oim.domain}/XLApplications/WLXellerateFull.ear/-", "read";
        permission java.io.FilePermission
            "${bea.home}/weblogic81/server/lib/weblogic.jar", "read";
        permission java.io.FilePermission
            "${oim.domain}/${server.name}/.wlnotdelete/-", "read";
        permission java.io.FilePermission "${nexaweb.home}/-", "read";

        permission java.lang.RuntimePermission "loadLibrary.*";
        permission java.lang.RuntimePermission "queuePrintJob";
        permission java.net.SocketPermission    "*", "connect";
        permission java.io.FilePermission       "<<ALL FILES>>",
"read,write,execute";
        permission java.lang.RuntimePermission   "modifyThreadGroup";
        permission java.lang.RuntimePermission "accessClassInPackage.sun.io";
        permission java.io.FilePermission "${XL.HomeDir}/adapters/-",
            "read,write,delete";
};
```

Java 2 Security Permissions for WebLogic Cluster

Note: The application might fail to start because of syntax errors in the policy files.

Be careful when editing the policy files. Oracle recommends that you use the policy tool provided by the JDK for editing the policy files. The tool is available in the following directory:

JAVA_HOME/jre/bin/policytool

To enable Java 2 Security for Oracle Identity Manager running on a BEA WebLogic Server cluster:

1. Go to the *$BEA_HOME*/user_projects/domains/$OIM_DOMAIN/ and open the run script (xlStartWLS.bat for Windows and xlStartWLS.sh for UNIX).
2. Add the following:

```
-Djava.security.manager
-Djava.security.policy=$WL_HOME/server/lib/weblogic.policy
-Dbea.home=$BEA_HOME
-Dserver.name=$SERVER_NAME
```

```
-Doim.domain=$BEA_HOME/user_projects/domains/$OIM_DOMAIN
```

> **Note:** Remember the following:
>
> Change *$WL_HOME* to the actual BEA WebLogic Server home directory location.
>
> Change *$BEA_HOME* to the actual BEA home directory location.
>
> Change *$SERVER_NAME* to the actual first server name on which Oracle Identity Manager is deployed.
>
> Change *$OIM_DOMAIN* to the actual domain name where Oracle Identity Manager is deployed.

The following table describes the options:

Option	Description
-Djava.security.manager	Enables the Java 2 Security manager.
-Djava.security.policy	Specifies the policy file to use for Java 2 Security.
-Dbea.home	Specifies the root of the WebLogic Server installation directory. Typically, it is /opt/bea or c:\bea.
-Dserver.name	Specifies the name of the server on which Oracle Identity Manager is installed. Typically, it is myserver.
-Doim.domain	Specifies the directory of the domain on which Oracle Identity Manager is installed.

3. Check if the *$WL_HOME*/weblogic81/server/lib/weblogic.policy file exists. If the file exists, then edit it and add the Java 2 Security permissions specified in the "Policy File" section on page A-11. If the file does not exist, then create it.

4. For each Managed Server in the clustered installation:

   a. In the WebLogic Server Console, expand **Servers**, select the cluster server node, click the **Configuration** tab, and then click the **Remote Start** tab.

   b. Add the following to the Arguments field:

   ```
   -DXL.HomeDir=$OIM_HOME
   -Djava.security.auth.login.config=$OIM_HOME\config\authwl.conf
   -Dlog4j.configuration=file:/$OIM_HOME/config/log.properties
   -Djava.awt.headless=true
   -Djava.security.manager
   -Djava.security.policy==$BEA_HOME/weblogic81/server/lib/weblogic.policy
   -Dbea.home=$BEA_HOME
   -Dserver.name=$SERVER_NAME
   -Doim.domain=$BEA_HOME/user_projects/domains/$OIM_DOMAIN
   ```

Note: Remember the following:

Change *$OIM_HOME* to the actual Oracle Identity Manager home directory location.

Change *$BEA_HOME* to the actual BEA home directory location.

Change *$SERVER_NAME* to the actual server name of BEA WebLogic Server.

Change *$OIM_DOMAIN* to the actual domain name on which Oracle Identity Manager is deployed.

---

5. After making the changes mentioned in steps 1 through 4, you must restart all the servers.

Policy File

The `weblogic.policy` file contains the following code:

Note:

- The instructions to change the code in the policy file are given in comments, which are in bold font.
- This `weblogic.policy` example is for UNIX installation. For Microsoft Windows, change the slash (/) character between the directory names to two backslash characters (\\) in every `permission java.io.FilePermission` property.
- Ensure that you change the multicast IP address `231.116.117.171` in this example to reflect the multicast IP address of the Oracle Identity Manager installation. You can find the Oracle Identity Manager multicast IP address in the `xlconfig.xml` file.

```
    // *******************************************
    //  Default WebLogic Permissions
    // *******************************************
    //
    // To use this file you must turn on the Java security manager by
    // defining java.security.manager and setting the java.security.policy
    // property to point to the security policy which should be in the lib
    // directory.
    // For example:
    //   java -Djava.security.manager
    //
-Djava.security.policy==${/}opt${/}bea${/}weblogic81/server/lib/weblogic.policy
    //           weblogic.Server
    //
    // You can edit this file and change the permissions for your
    // applications or update the codeBase line to point to where your
    // server is installed.
    //
    // You should grant all permissions to classes in
    // .internal, and .wlnotdelete folders located in your server directory.
    // You can set
    //   -Duser.domain=<user domain folder>
    //   -Dweblogic.Name=<server name>
    // command-line properties and use them in your policy file.
    // For example, the basic grant statements for servers in a user
    // domain would be:
    // grant codeBase "file:${user.domain}/${weblogic.Name}/.internal/-" {
    //   permission java.security.AllPermission;
    // };
    // grant codeBase "file:${user.domain}/${weblogic.Name}/.wlnotdelete/-"
    // {
    //   permission java.security.AllPermission;
    // };
    //
    // The codeBase location must be a URL, not a file path,
    // so Windows users beware of backslashes.
    //
    //

grant codeBase "file:D:${/}wl_cluster${/}bea${/}weblogic81/server/lib/-" {
  permission java.security.AllPermission;
};

grant codeBase "file:D:${/}wl_cluster${/}bea${/}weblogic81/server/ext/-" {
  permission java.security.AllPermission;
};

grant codeBase
"file:D:${/}wl_cluster${/}bea${/}weblogic81/samples/server/eval/pointbase/lib/-" {
  permission java.security.AllPermission;
};

// For the petstore demo

grant codeBase
"file:D:${/}wl_cluster${/}bea${/}weblogic81/samples/server/config/petstore/petstor
eServer/.internal/-" {
permission java.security.AllPermission;
};

grant codeBase
"file:D:${/}wl_cluster${/}bea${/}weblogic81/samples/server/config/petstore/petstor
eServer/.wlnotdelete/-" {
permission java.security.AllPermission;
};

grant codeBase
"file:D:${/}wl_cluster${/}bea${/}weblogic81/samples/server/config/petstore/-" {
permission java.util.PropertyPermission "*", "read";
};

// For the examples

grant codeBase
"file:D:${/}wl_cluster${/}bea${/}weblogic81/samples/server/config/examples/example
sServer/.internal/-" {
permission java.security.AllPermission;
};

grant codeBase
"file:D:${/}wl_cluster${/}bea${/}weblogic81/samples/server/config/examples/example
sServer/.wlnotdelete/-" {
```

```
permission java.security.AllPermission;
};

grant codeBase
"file:D:${/}wl_cluster${/}bea${/}weblogic81/samples/server/config/examples/example
sServer/stage/-" {
permission java.util.PropertyPermission "*", "read";
permission java.io.FilePermission
"D:${/}wl_cluster${/}bea${/}weblogic81${/}samples${/}server${/}config${/}examples$
{/}examplesServer${/}ldap", "read,write";
};

grant codeBase
"file:D:${/}wl_cluster${/}bea${/}weblogic81/samples/server/stage/examples/-" {
permission java.io.FilePermission
"D:${/}wl_cluster${/}bea${/}weblogic81${/}samples${/}server${/}src${/}examples${/}
-", "read";
permission java.io.FilePermission
"D:${/}wl_cluster${/}bea${/}weblogic81${/}samples${/}server${/}config${/}examples$
{/}examplesServer${/}ldap", "read,write";
};

// For the workshop

grant codeBase "file:D:${/}wl_cluster${/}bea${/}weblogic81/samples/workshop/-" {
  permission java.security.AllPermission;
};

// These are for the three app types

// EJB default permissions
grant codebase "file:/weblogic/application/defaults/EJB" {
    permission java.lang.RuntimePermission "queuePrintJob";
    permission java.net.SocketPermission "*", "connect";
    permission java.util.PropertyPermission "*", "read";
};

// Web App default permissions
grant codebase "file:/weblogic/application/defaults/Web" {
    permission java.lang.RuntimePermission "loadLibrary";
    permission java.lang.RuntimePermission "queuePrintJob";
    permission java.net.SocketPermission "*", "connect";
    permission java.io.FilePermission "WEBLOGIC-APPLICATION-ROOT${/}-",
"read,write";
    permission java.util.PropertyPermission "*", "read";
};

// Connector default permissions
grant codebase "file:/weblogic/application/defaults/Connector" {
    permission java.net.SocketPermission "*", "connect";
    permission java.io.FilePermission "WEBLOGIC-APPLICATION-ROOT${/}-",
"read,write";
    permission java.util.PropertyPermission "*", "read";
};


// Standard extensions get all permissions by default

grant codeBase "file:${java.home}/lib/ext/-" {
permission java.security.AllPermission;
```

```
};

// default permissions granted to all domains

grant {
// "standard" properties that can be read by anyone

permission java.util.PropertyPermission "java.version", "read";
permission java.util.PropertyPermission "java.vendor", "read";
permission java.util.PropertyPermission "java.vendor.url", "read";
permission java.util.PropertyPermission "java.class.version", "read";
permission java.util.PropertyPermission "os.name", "read";
permission java.util.PropertyPermission "os.version", "read";
permission java.util.PropertyPermission "os.arch", "read";
permission java.util.PropertyPermission "file.separator", "read";
permission java.util.PropertyPermission "path.separator", "read";
permission java.util.PropertyPermission "line.separator", "read";


permission java.util.PropertyPermission "java.specification.version", "read";
permission java.util.PropertyPermission "java.specification.vendor", "read";
permission java.util.PropertyPermission "java.specification.name", "read";

permission java.util.PropertyPermission "java.vm.specification.version", "read";
permission java.util.PropertyPermission "java.vm.specification.vendor", "read";
permission java.util.PropertyPermission "java.vm.specification.name", "read";
permission java.util.PropertyPermission "java.vm.version", "read";
permission java.util.PropertyPermission "java.vm.vendor", "read";
permission java.util.PropertyPermission "java.vm.name", "read";
};

grant codeBase
   "file:${/}opt${/}bea${/}weblogic81/samples/server/eval/pointbase/lib/-" {
permission java.security.AllPermission;
};

// For the petstore demo

grant codeBase

"file:${/}opt${/}bea${/}weblogic81/samples/server/config/petstore/petstoreServer/.
internal/-" {
    permission java.security.AllPermission;
    };

    grant codeBase

"file:${/}opt${/}bea${/}weblogic81/samples/server/config/petstore/petstoreServer/.
wlnotdelete/-" {
    permission java.security.AllPermission;
    };

    grant codeBase
        "file:${/}opt${/}bea${/}weblogic81/samples/server/config/petstore/-" {
    permission java.util.PropertyPermission "*", "read";
    };

    // For the examples

    grant codeBase
```

```
"file:${/}opt${/}bea${/}weblogic81/samples/server/config/examples/examplesServer/.
internal/-" {
    permission java.security.AllPermission;
    };

    grant codeBase

"file:${/}opt${/}bea${/}weblogic81/samples/server/config/examples/examplesServer/.
wlnotdelete/-" {
    permission java.security.AllPermission;
    };

    grant codeBase

"file:${/}opt${/}bea${/}weblogic81/samples/server/config/examples/examplesServer/s
tage/-" {
    permission java.util.PropertyPermission "*", "read";
    permission java.io.FilePermission

"${/}opt${/}bea${/}weblogic81${/}samples${/}server${/}config${/}examples${/}exampl
esServer${/}ldap", "read,write";
    };

    grant codeBase
        "file:${/}opt${/}bea${/}weblogic81/samples/server/stage/examples/-" {
    permission java.io.FilePermission

"${/}opt${/}bea${/}weblogic81${/}samples${/}server${/}src${/}examples${/}-",
"read";
    permission java.io.FilePermission

"${/}opt${/}bea${/}weblogic81${/}samples${/}server${/}config${/}examples${/}exampl
esServer${/}ldap", "read,write";
    };

    // For the workshop

    grant codeBase "file:${/}opt${/}bea${/}weblogic81/samples/workshop/-" {
      permission java.security.AllPermission;
    };

    // These are for the three app types


    // EJB default permissions
    grant codebase "file:/weblogic/application/defaults/EJB" {
        permission java.lang.RuntimePermission "queuePrintJob";
        permission java.net.SocketPermission "*", "connect";
        permission java.util.PropertyPermission "*", "read";
    };

    // Web App default permissions
    grant codebase "file:/weblogic/application/defaults/Web" {
        permission java.lang.RuntimePermission "loadLibrary";
        permission java.lang.RuntimePermission "queuePrintJob";
        permission java.net.SocketPermission "*", "connect";
        permission java.io.FilePermission
            "WEBLOGIC-APPLICATION-ROOT${/}-", "read,write";
        permission java.util.PropertyPermission "*", "read";
```

```
};

// Connector default permissions
grant codebase "file:/weblogic/application/defaults/Connector" {
    permission java.net.SocketPermission "*", "connect";
    permission java.io.FilePermission
        "WEBLOGIC-APPLICATION-ROOT${/}-", "read,write";
    permission java.util.PropertyPermission "*", "read";
};


// Standard extensions get all permissions by default
grant codeBase "file:${java.home}/lib/ext/-" {
permission java.security.AllPermission;
};

grant codeBase "file:${java.home}/lib/-" {
permission java.security.AllPermission;
};

grant codeBase "file:${java.home}/jre/lib/-" {
permission java.security.AllPermission;
};

grant codebase "file:${oim.domain}/${server.name}/.internal/-" {
permission java.security.AllPermission;
};

// *******************************************
//  Default WebLogic Permissions end
// *******************************************


// *******************************************
// From here, OIM application permission starts
// *******************************************
// OIM codebase permissions
grant codeBase
    "file:${oim.domain}/XLApplications/WLXellerateFull.ear/-" {
      // File permissions

      // Need read,write,delete permissions on $OIM_HOME/config folder
      // to read various config files, write the
      // xlconfig.xml.{0,1,2..} files upon re-encryption and delete
      // the last xlconfig.xml if the numbers go above 9.

      permission java.io.FilePermission "${XL.HomeDir}/config/-",
        "read, write, delete";
      permission java.io.FilePermission "${XL.HomeDir}/-", "read";

      // Need read,write,delete permissions to generate adapter java
      // code, delete the .class file when the adapter is loaded into
      // the database
      permission java.io.FilePermission "${XL.HomeDir}/adapters/-",
        "read,write,delete";

      // This is required by the connectors and connector installer
      permission java.io.FilePermission
        "${XL.HomeDir}/ConnectorDefaultDirectory/-", "read,write,delete";
      permission java.io.FilePermission
```

```
  "${XL.HomeDir}/connectorResources/-", "read,write,delete";

// Read Globalization resource bundle files for various
// locales
permission java.io.FilePermission
  "${XL.HomeDir}/customResources/-", "read";

// Read code from "JavaTasks", "ScheduleTask",
// "ThirdParty", "EventHandlers" folder
permission java.io.FilePermission
  "${XL.HomeDir}/EventHandlers/-", "read";
permission java.io.FilePermission
  "${XL.HomeDir}/JavaTasks/-", "read";
permission java.io.FilePermission
  "${XL.HomeDir}/ScheduleTask/-", "read";
permission java.io.FilePermission
  "${XL.HomeDir}/ThirdParty/-", "read";

// Required by the Generic Technology connector
permission java.io.FilePermission  "${XL.HomeDir}/GTC/-", "read";

// OIM server codebase requires read permissions on the
// deploy directory, the .wlnotdelete directory, the
// "applications" folder, the "XLApplications" folder
// and the WebLogic server lib directory
// All these permissions are specific to the weblogic server.
permission java.io.FilePermission
  "${oim.domain}/XLApplications/WLXellerateFull.ear/-", "read";
permission java.io.FilePermission
  "${oim.domain}/${server.name}/.wlnotdelete/-",
  "read,write,delete";
permission java.io.FilePermission
  "${oim.domain}/applications/-", "read";
permission java.io.FilePermission
  "${oim.domain}/XLApplications/-", "read";
permission java.io.FilePermission "http:${/}-", "read";
permission java.io.FilePermission ".${/}http:${/}-", "read";
permission java.io.FilePermission
  "${bea.home}/weblogic81/server/lib/-", "read";
permission java.io.FilePermission
  "${oim.domain}/${server.name}/ldap/ldapfiles/-", "read,write";
permission java.io.FilePermission
  "${oim.domain}/${server.name}/-", "read,write,delete";

// OIM server codebase requires read permissions on the
// $JAVA_HOME/lib directory
permission java.io.FilePermission "${java.home}/lib/-", "read";

// OIM server invokes the java compiler. You need "execute"
// permissions on all files.
permission java.io.FilePermission "<<ALL FILES>>", "execute";

// Socket permissions
// Basically, all permissions are allowed on non-privileged sockets
// The multicast address should be the same as the one in
// xlconfig.xml for javagroups communication
permission java.net.SocketPermission "*:1024-",
  "connect,listen,resolve,accept";
permission java.net.SocketPermission "231.116.117.171",
  "connect,accept,resolve";
```

```
// Property permissions
// Read and write OIM properties
// Read XL.*, java.* and log4j.* properties
permission java.util.PropertyPermission "XL.HomeDir", "read";
permission java.util.PropertyPermission "XL.*", "read";
permission java.util.PropertyPermission "XL.ConfigAutoReload",
  "read";
permission java.util.PropertyPermission "log4j.*", "read";
permission java.util.PropertyPermission "user.dir", "read";
permission java.util.PropertyPermission "weblogic.xml.debug",
  "read";
permission java.util.PropertyPermission "file.encoding", "read";
permission java.util.PropertyPermission "java.class.path", "read";
permission java.util.PropertyPermission "java.ext.dirs", "read";
permission java.util.PropertyPermission "java.library.path",
  "read";
permission java.util.PropertyPermission "sun.boot.class.path",
  "read";
permission java.util.PropertyPermission "weblogic.*", "read";

// Run time permissions
// OIM server needs permissions to create its own class loader,
// get the class loader, modify threads and register shutdown
// hooks
permission java.lang.RuntimePermission "createClassLoader";
permission java.lang.RuntimePermission "getClassLoader";
permission java.lang.RuntimePermission "setContextClassLoader";
permission java.lang.RuntimePermission  "setFactory";
permission java.lang.RuntimePermission "modifyThread";
permission java.lang.RuntimePermission "modifyThreadGroup";
permission java.lang.RuntimePermission "shutdownHooks";

// OIM server needs run time permissions to generate and load
// classes in the following specified packages. Also access the
// declared members of a class.
// weblogic.kernelPermission is required by weblogic
permission java.lang.RuntimePermission
  "defineClassInPackage.com.thortech.xl.adapterGlue.ScheduleItemEvents";
permission java.lang.RuntimePermission
  "defineClassInPackage.com.thortech.xl.dataobj.rulegenerators";
permission java.lang.RuntimePermission
  "defineClassInPackage.com.thortech.xl.adapterGlue";
permission java.lang.RuntimePermission "accessDeclaredMembers";
permission java.lang.RuntimePermission "weblogic.kernelPermission";
permission java.lang.RuntimePermission
  "accessClassInPackage.sun.net.www.protocol.c";
permission java.lang.RuntimePermission "accessClassInPackage.sun.io";
permission java.lang.RuntimePermission
  "accessClassInPackage.sun.security.provider";
permission java.lang.RuntimePermission
  "accessClassInPackage.sun.security.action";

// Reflection permissions
// Give permissions to access and invoke fields/methods from
// reflected classes.
permission java.lang.reflect.ReflectPermission "suppressAccessChecks";

// Security permissions for OIM server
permission java.security.SecurityPermission "*";
```

```
        permission java.security.SecurityPermission "insertProvider.SunJCE";
        permission java.security.SecurityPermission "insertProvider.SUN";
        permission javax.security.auth.AuthPermission "doAs";
        permission javax.security.auth.AuthPermission "doPrivileged";
        permission javax.security.auth.AuthPermission "getSubject";
        permission javax.security.auth.AuthPermission "modifyPrincipals";
        permission javax.security.auth.AuthPermission "createLoginContext";
        permission javax.security.auth.AuthPermission "getLoginConfiguration";
        permission javax.security.auth.AuthPermission "setLoginConfiguration";
        permission java.security.SecurityPermission
          "getProperty.policy.allowSystemProperty";
        permission java.security.SecurityPermission
          "getProperty.login.config.url.1";
        permission javax.security.auth.AuthPermission
          "refreshLoginConfiguration";


        // SSL permission (for remote manager)
        permission javax.net.ssl.SSLPermission  "getSSLSessionContext";

        // Serializable permissions
        permission java.io.SerializablePermission "enableSubstitution";
  };


  // You must give the codebase in xlWebApp.war/WEB-INF/classes
  // the following permissions
  grant codeBase

"file:${oim.domain}/XLApplications/WLXellerateFull.ear/xlWebApp.war/WEB-INF/classe
s/-" {
        permission java.io.FilePermission

"${oim.domain}/XLApplications/WLXellerateFull.ear/xlWebApp.war/cabo/styles/-",
"read,write";
        permission java.io.FilePermission

"${oim.domain}/XLApplications/WLXellerateFull.ear/xlWebApp.war/cabo/images/-",
"read,write";
  };

  // nexaweb-common.jar from WebLogic server/lib is given AllPermissions
  // These classes in this jar can be loaded by WebLogic's classloader
  grant codeBase "file:${bea.home}/weblogic81/server/lib/nexaweb-common.jar" {
        permission java.security.AllPermission;
  };

  // Permissions for nexaweb-common.jar from OIM_HOME/ext
  grant codeBase "file:${XL.HomeDir}/ext/nexaweb-common.jar" {
        permission java.security.AllPermission;
  };

  // Permissions for xlCrypto.jar from $OIM_HOME/lib
  grant codeBase "file:${XL.HomeDir}/lib/xlCrypto.jar" {
        permission java.security.SecurityPermission "insertProvider.SunJCE";
        permission java.security.SecurityPermission "insertProvider.SUN";
  };

  // Permissions for xlUtils.jar from $OIM_HOME/lib
  grant codeBase "file:${XL.HomeDir}/lib/xlUtils.jar" {
        permission java.io.FilePermission
          "${bea.home}/weblogic81/server/lib/-", "read";
        permission java.io.FilePermission "${java.home}/jre/lib/-", "read";

        // Serializable permissions
        permission java.io.SerializablePermission "enableSubstitution";
  };

  // Permissions for log4j-1.2.8.jar from $OIM_HOME/ext
  grant codeBase "file:${XL.HomeDir}/ext/log4j-1.2.8.jar" {
        permission java.io.FilePermission
          "${oim.domain}/XLApplications/WLXellerateFull.ear/xlVO.jar",
          "read";
  };

  // Permissions for xlLogger.jar from $OIM_HOME/lib
  // The Filewatchdog class from this jar file must periodically scan
  // these directories for updated/new jar files.
  // We also scan the classes in xlAdapterUtilities.jar by default
  grant codeBase "file:${XL.HomeDir}/lib/xlLogger.jar" {
        permission java.io.FilePermission "${XL.HomeDir}/EventHandlers",
          "read";
        permission java.io.FilePermission "${XL.HomeDir}/JavaTasks", "read";
        permission java.io.FilePermission "${XL.HomeDir}/ScheduleTask",
          "read";
        permission java.io.FilePermission "${XL.HomeDir}/ThirdParty",
          "read";
        permission java.io.FilePermission "${XL.HomeDir}/EventHandlers/-",
          "read";
        permission java.io.FilePermission "${XL.HomeDir}/JavaTasks/-",
          "read";
        permission java.io.FilePermission "${XL.HomeDir}/ScheduleTask/-",
          "read";
        permission java.io.FilePermission "${XL.HomeDir}/ThirdParty/-",
          "read";
        permission java.io.FilePermission
          "${XL.HomeDir}/lib/xlAdapterUtilities.jar", "read";
  };

  // Permissions for .wlnotdelete folder
  grant codeBase "file:${oim.domain}/${server.name}/.wlnotdelete/-" {
        permission java.security.AllPermission;
  };

  // Nexaweb server codebase permissions
  grant codeBase "file:${oim.domain}/XLApplications/WLNexaweb.ear/-" {
        // File permissions
        permission java.io.FilePermission "${user.home}", "read, write";
        permission java.io.FilePermission
          "${oim.domain}/XLApplications/WLNexaweb.ear/-", "read";
        permission java.io.FilePermission
          "${oim.domain}/XLApplications/WLXellerateFull.ear/-", "read";
        permission java.io.FilePermission
          "${bea.home}/weblogic81/server/lib/-", "read";

        permission java.io.FilePermission "${XL.HomeDir}/adapters/-",
          "read,write,delete";
        permission java.io.FilePermission "<<ALL FILES>>", "execute";

        // Property permissions
        permission java.util.PropertyPermission "weblogic.xml.debug", "read";
        permission java.util.PropertyPermission "user.dir", "read";
        permission java.util.PropertyPermission "*", "read,write";

        // Run time permissions
        permission java.lang.RuntimePermission "createClassLoader";
        permission java.lang.RuntimePermission "getClassLoader";
        permission java.lang.RuntimePermission "setContextClassLoader";
        permission java.lang.RuntimePermission  "setFactory";

        // Nexaweb server security permissions to load the Cryptix
        // extension
        permission java.security.SecurityPermission "insertProvider.Cryptix";
        permission java.lang.RuntimePermission "weblogic.kernelPermission";
        permission java.lang.RuntimePermission
          "accessClassInPackage.sun.net.www.protocol.c";

        // Socket permissions
        // Permissions on all non-privileged ports.
        permission java.net.SocketPermission "*:1024-",
          "listen, connect, resolve";

        // Security permissions
        permission javax.security.auth.AuthPermission "doAs";
        permission javax.security.auth.AuthPermission "modifyPrincipals";
        permission javax.security.auth.AuthPermission "createLoginContext";

  };


  // The following are permissions given to codebase in the OIM server
  // directory
  grant codeBase "file:${XL.HomeDir}/-" {
        // File permissions
        permission java.io.FilePermission "${XL.HomeDir}/config/-", "read";
        permission java.io.FilePermission "${XL.HomeDir}/JavaTasks/-", "read";
        permission java.io.FilePermission "${XL.HomeDir}/ScheduleTasks/-",
          "read";
        permission java.io.FilePermission "${XL.HomeDir}/ThirdParty/-",
          "read";
        permission java.io.FilePermission "${XL.HomeDir}/adapters/-",
          "read,write,delete";

        // Socket permissions
        permission java.net.SocketPermission "*:1024-",
          "connect,listen,resolve,accept";

        // Property permissions
        permission java.util.PropertyPermission "XL.HomeDir", "read";
        permission java.util.PropertyPermission "XL.ConfigAutoReload", "read";
        permission java.util.PropertyPermission "XL.*", "read";
        permission java.util.PropertyPermission "log4j.*", "read";
        permission java.util.PropertyPermission "user.dir", "read";
        permission java.util.PropertyPermission "weblogic.xml.debug", "read";

        // Security permissions
        permission javax.security.auth.AuthPermission "doAs";
        permission javax.security.auth.AuthPermission "modifyPrincipals";
        permission javax.security.auth.AuthPermission "createLoginContext";
```

```
          // Run time Permissions
          permission java.lang.RuntimePermission
            "accessClassInPackage.sun.security.provider";
    };

    // Minimal permissions are allowed to everyone else
    grant {
    // "standard" properties that can be read by anyone

// Socket permissions
          permission java.net.SocketPermission "*:1024-",
            "connect,listen,resolve,accept";

//Change the following IP address to the same value as that of
//your WebLogic cluster multicast IP address
permission java.net.SocketPermission "237.0.0.1", "connect,accept,resolve";

//Change the following IP address to the same value as that of
//the multicast address in the xlConfig.xml file
permission java.net.SocketPermission "231.116.117.171", "connect,accept,resolve";

permission java.lang.RuntimePermission "accessClassInPackage.*";
permission java.security.SecurityPermission "getPolicy";
permission java.security.SecurityPermission "setPolicy";
permission java.lang.RuntimePermission "createSecurityManager";
permission java.lang.RuntimePermission "setSecurityManager";
permission java.security.SecurityPermission "getProperty.*";
permission java.security.SecurityPermission "setProperty.*";
permission javax.security.auth.AuthPermission "createLoginContext.*";
permission java.lang.RuntimePermission "shutdownHooks";
permission java.io.SerializablePermission "enableSubstitution";
permission javax.security.auth.AuthPermission "refreshLoginConfiguration";
permission java.util.logging.LoggingPermission "control";
permission java.security.SecurityPermission "insertProvider.SunJCE";
permission java.security.SecurityPermission "insertProvider.SUN";

permission java.util.PropertyPermission "java.version", "read";
permission java.util.PropertyPermission "java.vendor", "read";
permission java.util.PropertyPermission "java.vendor.url", "read";
permission java.util.PropertyPermission "java.class.version", "read";
permission java.util.PropertyPermission "os.name", "read";
permission java.util.PropertyPermission "os.version", "read";
permission java.util.PropertyPermission "os.arch", "read";
permission java.util.PropertyPermission "file.separator", "read";
    permission java.util.PropertyPermission "path.separator", "read";
    permission java.util.PropertyPermission "line.separator", "read";

    permission java.util.PropertyPermission "java.specification.version",
            "read";
    permission java.util.PropertyPermission "java.specification.vendor",
            "read";
    permission java.util.PropertyPermission "java.specification.name",
            "read";
    permission java.util.PropertyPermission
            "java.vm.specification.version", "read";
    permission java.util.PropertyPermission
            "java.vm.specification.vendor", "read";
    permission java.util.PropertyPermission "java.vm.specification.name",
            "read";
    permission java.util.PropertyPermission "java.vm.version", "read";
    permission java.util.PropertyPermission "java.vm.vendor", "read";
    permission java.util.PropertyPermission "java.vm.name", "read";
    permission java.util.PropertyPermission "sun.boot.class.path", "read";
    permission java.util.PropertyPermission "weblogic.xml.debug", "read";


    permission java.lang.reflect.ReflectPermission "suppressAccessChecks";
    permission java.lang.RuntimePermission "accessDeclaredMembers";
    permission java.util.PropertyPermission "XL.*", "read";
    permission java.util.PropertyPermission "user.dir", "read";
    permission java.util.PropertyPermission "*", "read,write";

    permission java.lang.RuntimePermission "weblogic.kernelPermission";
    permission java.lang.RuntimePermission "getClassLoader";
    permission java.lang.RuntimePermission "createClassLoader";
    permission java.lang.RuntimePermission "setContextClassLoader";
    permission java.util.PropertyPermission "nexaweb.logs", "read,write";
    permission java.util.PropertyPermission
            "sun.net.client.defaultConnectTimeout", "read,write";
    permission java.io.FilePermission
            "${oim.domain}/XLApplications/WLNexaweb.ear/-", "read";
    permission java.io.FilePermission
            "${oim.domain}/XLApplications/WLXellerateFull.ear/-", "read";
    permission java.io.FilePermission
            "${bea.home}/weblogic81/server/lib/weblogic.jar", "read";
    permission java.io.FilePermission
            "${oim.domain}/${server.name}/.wlnotdelete/-", "read";
    permission java.io.FilePermission "${nexaweb.home}/-", "read";

    permission java.lang.RuntimePermission "loadLibrary.*";
    permission java.lang.RuntimePermission "queuePrintJob";
    permission java.net.SocketPermission    "*", "connect";
    permission java.io.FilePermission       "<<ALL FILES>>", "read,write,execute";
    permission java.lang.RuntimePermission   "modifyThreadGroup";
    permission java.lang.RuntimePermission "accessClassInPackage.sun.io";
    permission java.io.FilePermission "${XL.HomeDir}/adapters/-",
            "read,write,delete";
};
```

Index