Oracle® Identity Manager

Installation and Configuration Guide for Oracle WebLogic Server

Release 9.1.0.1

E14047-02

February 2009

ORACLE®

Oracle Identity Manager Installation and Configuration Guide for Oracle WebLogic Server Release 9.1.0.1

E14047-02

Primary Author: Lyju Vadassery

Contributing Author: Debapriya Datta

Contents

8 Installing and Configuring the Oracle Identity Manager Design Console

9 Postinstallation Configuration for Oracle Identity Manager and Oracle WebLogic Server

10 Installing and Configuring the Oracle Identity Manager Remote Manager

Preface

This guide explains the procedure to install Oracle Identity Manager release 9.1.0.1 on Oracle 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 to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at `http://www.oracle.com/accessibility/`.

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

To reach AT&T Customer Assistants, dial 711 or 1.800.855.2880. An AT&T Customer Assistant will relay information between the customer and Oracle Support Services at 1.800.223.1711. Complete instructions for using the AT&T relay services are available at `http://www.consumer.att.com/relay/tty/standard2.html`. After the AT&T Customer Assistant contacts Oracle Support Services, an Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process.

Related Documents

For more information, see the other documents in the Oracle Identity Manager documentation set for this release.

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.
`*_HOME`	This convention represents the directory where an application is installed. The root directory in which you install Oracle WebLogic Server is referred to as *`BEA_HOME`*, for example, `c:\bea`. The directory in which you install the Oracle WebLogic product is referred to as *`WL_HOME`*, for example *`BEA_HOME`*`/wlserver_10.3`. The WebLogic domain directory where Oracle Identity Manager is installed is referred to as *`DOMAIN_HOME`*, for example, *`BEA_HOME`*`/user_projects/domains/oimdomain`. 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 9.1.0.1 on Oracle WebLogic Server involves the following steps:

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

2.1 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:** See *Oracle Identity Manager Readme* 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 on the database host.

2.1.1 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)

2.1.2 Database Server Host Requirements

Table 2–2 provides sample database host requirements for some supported operating systems. The information in this table should be considered only as a guideline. See the database documentation for 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

2.1.3 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

2.1.4 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

2.2 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.
- See *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. See "Creating an Oracle Database" on page 3-1 for more information.

2.3 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	1433 for Microsoft SQL Server 1521 for Oracle Database	
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 Oracle WebLogic Server root directory	Microsoft Windows: `C:\bea` UNIX: `/opt/bea`	
The Oracle WebLogic Server installation directory	Microsoft Windows: `C:\bea\wlserver_10.3` UNIX: `/opt/bea/wlserver_10.3`	

2.4 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.

2.4.1 Installing the Diagnostic Dashboard

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

To deploy the Diagnostic Dashboard on Oracle WebLogic:

1. Log in to the administrative console of the application server.
2. In the Change Center region, click **Lock & Edit**.
3. In the Domain Structure region, click **Deployments**.

4. In the Deployments region on the right pane, click **Install**.
5. Click the **Upload your file(s)** link.
6. In the **Deployment Archive** field, enter the full path of the XIMDD.war file. This file is in the *OIM9101INSTALLER*/DiagnosticDashboard directory.
7. Click **Next** and then click **Next** again.
8. Ensure that the **Install this deployment as an application** option is selected, and then click **Next**.
9. On the Optional Settings page, ensure that:
   - **XIMDD** is shown as the name of the application
   - The **DD Only: Use only roles and policies that are defined in the deployment descriptors** option is selected.
   - The **Use the defaults defined by the deployment's targets** option is selected.
10. Click **Finish**.
11. In the Change center region, click **Activate changes**.
12. In the Summary of Deployments region, select the check box for the XIMDD deployment.
13. From the **Start List** (after the table), select **Servicing all requests**.
14. Click **Yes** to confirm that you want the XIMDD deployment to be started.

At this stage, the State column of the Deployments table shows `Active`.

To open the DD console, use a URL of the following format:

`http://`*`HOSTNAME`*`_or_`*`IP_ADDRESS`*`:7001/XIMDD/`

2.4.2 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)

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

3

Installing and Configuring a Database

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

3.1 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

3.1.1 Installing Oracle Database

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

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

3.1.2 Creating an Oracle Database

Note: Oracle recommends that you increase the number of connections allowed to the Oracle Database. For this, you must increase the value of the processes parameter as follows:

1. Log in as the database administrator and then run the following query:

   ```
   ALTER SYSTEM SET PROCESSES = 300 SCOPE = SPFILE;
   ```

2. Restart the database for the changes to take effect.

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.

See Oracle Database documentation for detailed instructions on creating a database instance.

3.1.2.1 Configuring the Database for Globalization Support

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

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

3.1.3 Preparing the Oracle Database

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

- Verify that query rewrite is enabled.

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

- Enable XA transactions support.

> **Note:** A 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.

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

You can perform the preceding tasks to prepare 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
  ```

These scripts are located in the `\installServer\Xellerate\db\oracle\` directory.

Apply the following guidelines when you run this script:

- The script must be run by a user who has 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.

> **Note:** Perform the steps associated with the operating system on the computer hosting the Oracle database.

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

3.1.3.1 Preparing the Database on UNIX

To prepare the database on UNIX:

1. Copy the prepare_xl_db.sh 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. 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:
   - Location of your Oracle home, which is *ORACLE_HOME*
   - Name of your database, which is *ORACLE_SID*
   - Name of the Oracle Identity Manager database user to be created
   - Password for the Oracle Identity Manager database user
   - Name of the tablespace to be created for storing Oracle Identity Manager data
   - Directory to store the data file for the Oracle Identity Manager tablespace
   - Name of the data file (do not append the .dbf extension)
   - 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
```

3.1.3.2 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 window, navigate to the directory in which you copied the scripts, and then 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:

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

   Table 3–1 lists the options used in the preceding example of prepare_xl_db.bat.

Table 3–1 Options for the prepare_xl_db.bat Script

Argument	Description
XELL	Name of the database
C:\oracle\ora92	Directory in which 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 (do not 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.

3.1.3.3 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 following error:

```
ORA-00942: table or view does not exist"
```

Look for errors in the log file and ignore or resolve them on an individual basis. Remember that you must successfully prepare the database for Oracle Identity Manager before you can install Oracle Identity Manager.

3.1.4 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.

3.2 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 Oracle WebLogic Server for Oracle RAC

3.2.1 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.

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 Oracle WebLogic Server for Oracle RAC" section on page 3-7.

3.2.2 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 3–2 describes the parameters in a net services name entry for an Oracle RAC database.

Table 3–2 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 at which they listen.

3.2.3 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.

3.2.4 Configuring Oracle WebLogic Server for Oracle RAC

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

Note: Before configuring Oracle 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 3-6.

To configure nonclustered or clustered Oracle 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 Oracle 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**, **Data Sources**, and then select **xlDS**.
7. Select the **ConnectionPool** tab.
8. In the Change center region, click **Lock and Edit**.
9. Enter the Oracle RAC JDBC URL described in Step 2 in the **URL** field and save the settings.
10. Save the settings.
11. Select **Services**, **JDBC**, **Data Sources**, and then select **xlXADS**.
12. Select the **ConnectionPool** tab.
13. Enter the Oracle RAC JDBC URL described in Step 2 in the **URL** field and save the settings.
14. Save the settings.
15. In the Change center region, click **Activate Changes**.

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

Note: For a clustered installation, stop the Managed servers and Administrative server. Then, restart the Administrative server and Managed servers.

See the following sections for detailed information:

- Starting Oracle Identity Manager
- Stopping Oracle Identity Manager

3.3 Using a Microsoft SQL Server Database for Oracle Identity Manager

To use Microsoft SQL Server as the database, perform the procedures described in the following sections:

- Installing and Configuring Microsoft SQL Server
- Creating a Microsoft SQL Server 2005 Database
- Creating a Microsoft SQL Server Database Account
- Removing Oracle Identity Manager Entries from a Microsoft SQL Server Database

3.3.1 Installing and Configuring Microsoft SQL Server

To install and configure Microsoft SQL Server 2005 for Oracle Identity Manager:

1. Install Microsoft SQL Server 2005 with Service Pack 2.

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

   Note: Perform Steps 2 through 4 on the computer hosting the application server.

   ---

2. Download the SQL Server 2005 Driver for JDBC from the Microsoft Web site.
3. Install SQL Server 2005 Driver for JDBC.

   Instructions to install JDBC drivers for SQL Server 2005 are available at the following location:

   SQL_SERVER_HOME\sqljdbc_1.2\enu\help\html\574e326f-0520-4003-bdf1-62d92c3db457.htm

   ---

   Note: Specify a short path for the installation folder, such as C:\JDBCjars, so that you can easily add the path to your CLASSPATH in the next step. If the classpath is more than 256 characters, then the installer does not work properly.

   ---

4. Locate the JDBC driver file (sqljdbc.jar) from the *SQL2005_JDBC_DRIVER_HOME*\sqljdbc_1.2\enu\ directory.

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

```
C:\jdbc_install_folder\sqljdbc.jar;
```

In this sample string, *jdbc_install_folder* is the location where the SQL Server 2005 Driver for JDBC files is installed.

Note: Perform Steps 5 through 7 on the computer hosting the Microsoft SQL Server database.

5. On the computer hosting the Microsoft SQL Server database, enable distributed transactions by installing SQL Server 2005 JDBC XA procedures.

   Copy the sqljdbc.dll file from the *SQL2005_JDBC_DRIVER_HOME*\sqljdbc_1.2\enu\xa\x86\ directory to the *Microsoft_SQL_Server_HOME*\MSSQL\Binn\ directory.

6. Run the *SQL2005_JDBC_DRIVER_HOME*\sqljdbc_1.2\enu\xa\xa_install.sql script.

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

   If necessary, restart SQL Server 2005.

3.3.2 Creating a Microsoft SQL Server 2005 Database

The following procedure describes how to create a new database for Oracle Identity Manager.

Note: From this point onward in the guide, the name XELL is used to refer to the database. You can set any name for the database.

To create a SQL Server database:

1. Start the Microsoft SQL Server Management Studio application as follows:

   a. From the Windows Start menu, expand **All Programs**, expand **Microsoft SQL Server 2005**, and then select **SQL Server Management Studio**.

   b. In the Connect to Server dialog box, verify the default settings. Ensure that the name of the computer on which SQL Server is installed is specified in the Server name box. Then, click **Connect**.

2. On the left pane of the SQL Server Management Studio application window, right-click **Databases**, and then select **New Database**.

3. In the New Database Properties dialog box, on the left pane, select **General**, and then enter **XELL** in the Database Name field.

4. In the Database Files section, for the **Initial Size** and **Filegroup** columns in the Database files matrix, enter the information from the corresponding columns in Table 3–3.

Table 3–3 Database Files

Logical Name	File Type	File Group	Initial Size in Megabytes (MB)	Auto Growth	Path	File Name
XELL_PRIMARY	Data	PRIMARY	100	By 1 MB, unrestricted growth (by default)	Specify the default path to save the datafiles	Left Blank (Default)
XELL_DATA	Data	XELL_DATA	500	By 1 MB, unrestricted growth (by default)	Specify the default path to save the datafiles	Left Blank (Default)
XELL_INDEX	Data	XELL_INDEX	300	By 1 MB, unrestricted growth (by default)	Specify the default path to save the datafiles	Left Blank (Default)
XELL_TEXT	Data	XELL_TEXT	500	By 1 MB, unrestricted growth (by default)	Specify the default path to save the datafiles	Left Blank (Default)
XELL_UPA	Data	XELL_UPA	1000	By 1 MB, unrestricted growth (by default)	Specify the default path to save the datafiles	Left Blank (Default)

Note:

- Table 3–3 lists initial sizes for a production environment. For non-production 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 appear in Table 3–3. You can vary the File Name and Location strings to match the database name and the location of your SQL Server installation.
- 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 physical data and primary keys of the User Profile Audit component.

5. Select the log file, 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 initial size for the log file.

6. Click **OK** to start creating the database.

3.3.3 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 the account name xladm. If you want to use an account name other than xladm, then specify that login 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 Management Studio application.
2. On the left pane of the SQL Server Management Studio application window, select **Security**, right-click **Logins**, and then select **New Login**.
3. In the SQL Server Login Properties dialog box, from the left pane, click the **General** tab, and perform the following steps:
   a. In the Login Name field, enter **xladm** (or a different account name that you prefer).
   b. Select the **Enforce Password Policy** check box. Deselect all other check boxes.
4. Select **SQL Server Authentication**, and then enter the password associated with the account you specified in the Password field.
5. In the **Database** box within the **Defaults** section, select **XELL** from the list.

   Leave the **Language** box set to <default>.
6. Select the **User Mapping** option from the left pane.
7. In the upper panel, select the check box associated with **XELL**. Set the XELL in the Default Schema column.
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. Select the check box associated with master. Set the XELL in the Default Schema column.
10. In the lower panel, select the check boxes associated with the following:
    - public
    - SqlJDBCXAUser
11. Click **OK** to commit your changes.

12. On the Microsoft SQL Server Management Studio, in the left pane, right-click registered server, click Properties. In the Properties dialog box, select the Security option, and then verify that Authentication is set to SQL Server and Windows.
13. Start the Microsoft SQL Server 2005 Surface Area Configuration application. To do so:
    a. From the Start menu, expand **All Programs**, expand **Microsoft SQL Server 2005**, expand **Configuration Tools**, and then click **SQL Server 2005 Surface Area Configuration**. A dialog box is displayed.
    b. Click **Surface Area Configuration for Services and Connection**. On the left pane, select the **MSSQLSERVER-> Database Engine**, and then verify that the Startup Type is set to **Automatic**.
    c. If Autostart SQL Server Agent is selected, do not change the existing setting, because that setting may be required by other applications. Click **OK** to close the SQL Server Properties page.

3.3.4 Removing Oracle Identity Manager Entries from a Microsoft SQL Server Database

To remove Oracle Identity Manager entries from a Microsoft SQL Server 2005 database after removing (deinstalling) the Oracle Identity Manager product:

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

4

Installing and Configuring Oracle WebLogic Server in a Nonclustered Mode

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

- Installing Oracle WebLogic Server
- Creating a WebLogic Domain

4.1 Installing Oracle WebLogic Server

Perform a default (complete) installation of Oracle WebLogic Server. Oracle Identity Manager requires the following components if you select custom installation.

- Core Application Server
- Administration Console
- Configuration Wizard and Upgrade Framework
- WebLogic JDBC Drivers
- WebLogic Web Server Plugins
- Select One or Both of the Bundled JDKs

Refer to Oracle WebLogic Server documentation for detailed information about installation.

4.2 Creating a WebLogic Domain

Before you install Oracle Identity Manager on Oracle WebLogic Server, you must create a WebLogic domain.

To create a WebLogic domain:

1. Start the WebLogic Configuration Wizard:

   For Microsoft Windows:

   From the Start menu, navigate to **Programs**, **Oracle WebLogic**, **WebLogic Server 10.3**, **Tools**, and then select **Configuration Wizard**.

   For UNIX:

   a. Go to the WebLogic bin directory by using the following command:

      ```
      cd WL_HOME/common/bin
      ```

b. Start the Configuration Wizard by using the following command:

```
sh config.sh
```

2. In the Configuration Wizard:

a. Select the **Create a new WebLogic configuration** option and then click **Next**.

b. Select **Generate a domain configured automatically to support the following products** and then click **Next**.

c. Enter a user name and password, and confirm the password for the domain and then click **Next**.

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.

---

d. Select either **Development Mode** or **Production Mode.** Oracle recommends that you select production mode for performance reasons.

Caution: For the Development mode installation of WebLogic, you ***must*** deselect the Automatically acquire lock option of the Administrative Console. This must be done before starting Oracle Identity Manager. To do so:

1. Log in to the WebLogic Administrative Console.
2. Click **Preference** at the top of the right pane.
3. Deselect **Automatically acquire lock**.
4. Click **Save** to save the changes.
5. On the left pane of Administrative and User Console, click **Release Configuration**.

---

e. Click **Next**.

f. Select the appropriate JDK. Before selecting a JDK, ensure that it is the certified JDK for Oracle WebLogic Server. Then, click **Next**.

g. Select **No** for the Customize Environment and Services Settings option and then click **Next**.

h. Change the location and/or name of the domain configuration if required and then click **Next**.

i. Create the domain and exit the Configuration Wizard and then click **Next**.

3. Start the Oracle WebLogic Server:

For Microsoft Windows:

From the **Start** menu, select **Programs**, **Oracle WebLogic**, **User Projects**, **DOMAIN_NAME**, and then **Start Admin Server**.

For UNIX:

Go to the WebLogic domain directory (the default is *BEA_HOME*/user_projects/domains/DOMAIN_NAME), and start the WebLogic server as follows:

```
sh startWebLogic.sh
```

5

Installing and Configuring Oracle WebLogic Server in a Clustered Mode

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

This chapter discusses the following topics:

- About Oracle WebLogic Server Clusters
- Steps to Install WebLogic Server and Oracle Identity Manager
- Configuring the Web Server

5.1 About Oracle WebLogic Server Clusters

A clustered installation requires multiple host computers. The instructions in this chapter involve deployment and running of Oracle Identity Manager on four host computers. These instructions assume that you have four computers, of which one is used to host the Web server and the other is used to host the WebLogic Admin Server.

Table 5–1 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 5–1 WebLogic-Based Oracle Identity Manager Cluster Host Computers

Host Computers	Entities	Software	Description
ADMIN_SERVER_HOST	WebLogic Admin Server WebLogic Node Manager	WebLogic Server Oracle Identity Manager	Administrative server for the WebLogic domain
OIM_SERVER1_HOST	OIM_SERVER1 WebLogic Node Manager OIM_CLUSTER	WebLogic Server Oracle Identity Manager	WebLogic Managed Server 1 Part of OIM_CLUSTER Name of the WebLogic cluster that hosts Oracle Identity Manager (logical entity).
OIM_SERVER2_HOST	OIM_SERVER2 WebLogic Node Manager OIM_CLUSTER	WebLogic Server Oracle Identity Manager	WebLogic Managed Server 2 Part of OIM_CLUSTER Name of the WebLogic cluster that hosts Oracle Identity Manager (logical entity).
WEB_SERVER_HOST	Web server	WebLogic Server plug-in Web server software	Web server (can be the Apache server or any other WebLogic supported Web server).

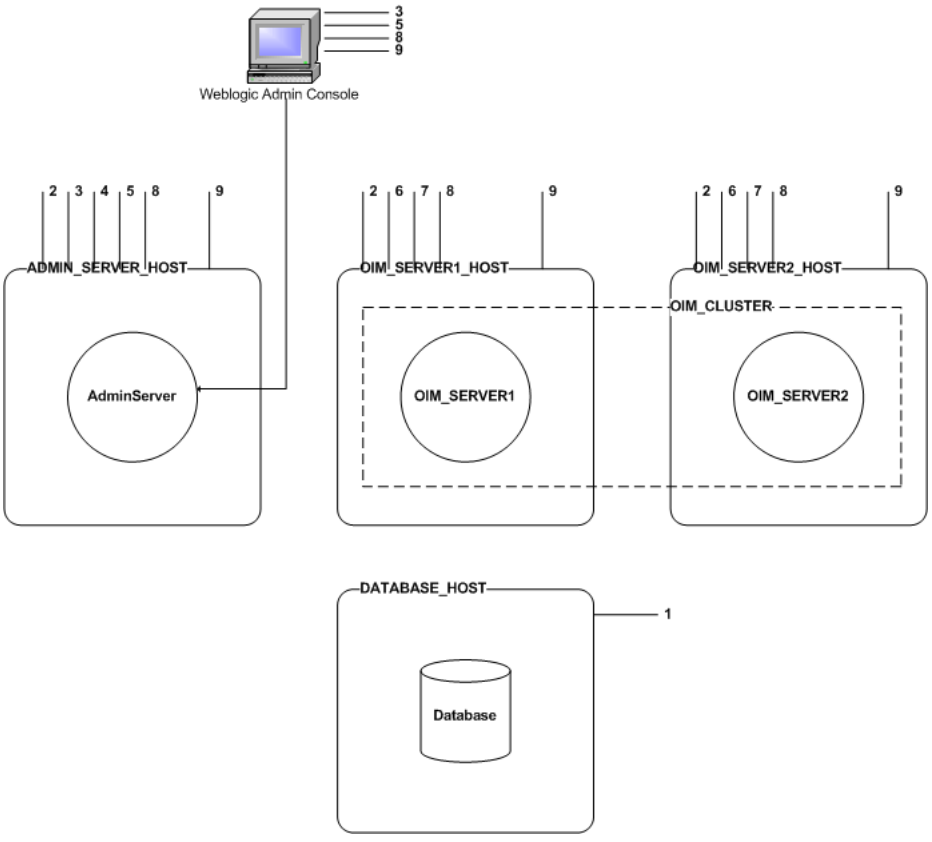
Caution: Deploying an application in a clustered installation is a complex procedure. This document assumes that you have expertise in installing and running applications on an Oracle WebLogic Server cluster. This chapter provides Oracle Identity Manager-specific information only. It does not cover the procedure to set up an Oracle WebLogic Server cluster. For more information about clustering, refer to Oracle WebLogic Server documentation.

5.2 Steps to Install WebLogic Server and Oracle Identity Manager

Note: If the WebLogic Admin server and one of the managed servers are installed on the same computer, then assume that *ADMIN_SERVER_HOST* and *OIM_SERVER1_HOST* are installed on the same computer in the instructions given in this section. In addition, do not perform the steps for *OIM_SERVER1_HOST* configuration.

This section provides an overview of the steps required to install Oracle WebLogic Server and Oracle Identity Manager in a clustered environment. Figure 5–1 represents the overview of these steps.

Figure 5–1 Steps to Install WebLogic and Oracle Identity Manager in a Cluster



Installing WebLogic and Oracle Identity Manager in a clustered environment involves the following steps:

- 1. Installing and Configuring a Database
- 2. Installing WebLogic Server on ADMIN_SERVER_HOST, OIM_SERVER1_HOST and OIM_SERVER2_HOST
- 3. Configuring Oracle WebLogic Server for an Oracle Identity Manager Installation
- 4. Installing Oracle Identity Manager on ADMIN_SERVER_HOST
- 5. Configuring OIM_SERVER2 in the AdminServer on ADMIN_SERVER_HOST
- 6. Copying the WebLogic Domain Directory
- 7. Copying the OIM_HOME Directory
- 8. Configuring the Node Manager
- 9. Restarting the WebLogic Server

5.2.1 1. Installing and Configuring a Database

Refer to Chapter 3, "Installing and Configuring a Database" for information about this step.

5.2.2 2. Installing WebLogic Server on ADMIN_SERVER_HOST, OIM_SERVER1_HOST and OIM_SERVER2_HOST

The basic procedure for deploying Oracle Identity Manager in an Oracle WebLogic Server cluster involves installing Oracle WebLogic Server first. Refer to the "Installing Oracle WebLogic Server" section on page 4-1.

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

5.2.3 3. Configuring Oracle WebLogic Server for an Oracle Identity Manager Installation

To configure Oracle WebLogic Server for an Oracle Identity Manager installation on ADMIN_SERVER_HOST, perform the following procedures:

- Creating a WebLogic Domain
- Creating a Cluster and Managed Server

5.2.3.1 Creating a WebLogic Domain

Refer to the "Creating a WebLogic Domain" section on page 4-1.

5.2.3.2 Creating a Cluster and Managed Server

To create a cluster and managed server:

1. Log in to the WebLogic Administrative Console.
2. In the Change center region, click **Lock and Edit**.
3. Navigate to **Environment**, **Clusters**, and then click **New**. Enter `OIM_CLUSTER` as the name of the cluster and then click **OK**.
4. Select OIM_CLUSTER, click the **Servers** tab, and then click **Add**.
5. Select the **Create a new server and add it to this cluster** option, and then click **Next**. Enter `OIM_SERVER1` as the name of the server.

6. Check the values of Server Listen Address and Server Listen Port. If required, set appropriate values for these fields. Then, click **Finish**.

> **Note:** At this stage, do not configure OIM_SERVER2. It must be configured after Oracle Identity Manager is installed.

7. In the Change center region, click **Activate changes**.

5.2.4 4. Installing Oracle Identity Manager on ADMIN_SERVER_HOST

Refer to Chapter 6, "Installing Oracle Identity Manager on Microsoft Windows" if the environment is running Microsoft Windows, or Chapter 7, "Installing Oracle Identity Manager on UNIX" if the environment is running UNIX.

> **Note:** While installing Oracle Identity Manager, it is recommended that you use a shared file system such as NFS on ADMIN_SERVER_HOST for installing Oracle Identity Manager. The shared files must be available on all the managed server hosts (OIM_SERVER1_HOST and OIM_SERVER2_HOST). If you are using the shared file system, then you do not have to perform Step "7. Copying the OIM_HOME Directory" on all the computers.

5.2.5 5. Configuring OIM_SERVER2 in the AdminServer on ADMIN_SERVER_HOST

After Oracle Identity Manager is installed, you must perform additional configuration steps. Oracle WebLogic Server is stopped automatically after the installation of Oracle Identity Manager. You must start Oracle WebLogic Server by running the following file:

For UNIX:

DOMAIN_HOME/bin/xlStartWLS.sh

For Microsoft Windows:

DOMAIN_HOME\bin\xlStartWLS.cmd

> **See Also:** The "Starting Oracle Identity Manager" section on page 9-1 for more information about starting WebLogic Administrative Server.

After you start Oracle WebLogic Server, perform the following steps:

1. Log in to the WebLogic Administrative Console.
2. In the Change center region, click **Lock and Edit**.
3. Navigate to **Environment**, and then **Servers**. Select **OIM_SERVER1** and click **Clone**.
4. Enter **OIM_SERVER2** as the server name.
5. Check the values of Server Listen Address and Server Listen Port. If required, set appropriate values for these fields. Then, click **OK**.
6. In the Change center region, click **Activate changes**.

By default, the Oracle Identity Manager installer configures JMS servers for OIM_SERVER1. For each additional server, you must perform the following step to create JMS servers for the newly created servers:

Go to OIM_HOME/setup and run the following command:

On Microsoft Windows:

```
config_clustsvr.cmd WebLogic_Admin_Password OIM_SERVER2
```

On UNIX:

```
config_clustsvr.sh WebLogic_Admin_Password OIM_SERVER2
```

5.2.6 6. Copying the WebLogic Domain Directory

The WebLogic domain directory must be copied from ADMIN_SERVER_HOST to OIM_SERVER1_HOST and OIM_SERVER2_HOST.

For example, if you have created the WebLogic domain in the *BEA_HOME*/user_projects/domains/oimdomain directory, then:

1. Create the user_projects/domains directory on the OIM_SERVER1_HOST and OIM_SERVER2_HOST computers.
2. Copy the oimdomain directory from the ADMIN_SERVER_HOST computer to the newly created user_projects/domains directory on each computer.

5.2.7 7. Copying the *OIM_HOME* Directory

Copy the *OIM_HOME* directory and all its contents from the ADMIN_SERVER_HOST computer to the OIM_SERVER1_HOST and OIM_SERVER2_HOST computers.

Note: The directory structure must be same across all the computers. For example, if you have installed Oracle Identity Manager in C:\oim\oimserver on ADMIN_SERVER_HOST, then the OIM_HOME directory must be copied to C:\oim\oimserver on the OIM_SERVER1_HOST and OIM_SERVER2_HOST computers.

5.2.8 8. Configuring the Node Manager

To configure a node manager on ADMIN_SERVER_HOST, OIM_SERVER1_HOST and OIM_SERVER2_HOST, perform the following steps:

1. Log in to the WebLogic Administrative Console.
2. In the Change center region, click **Lock and Edit**.
3. Navigate to **Environment**, and then **Machines**. Click **New.** Enter `ADMIN_SERVER_HOST` as the name of the new computer. For Microsoft Windows, select **Other** as the Machine OS. For UNIX, select **UNIX** as the Machine OS.
4. Navigate to **ADMIN_SERVER_HOST**, and then **Server**. Assign AdminServer to the computer you created in Step 2.
5. Navigate to **ADMIN_SERVER_HOST**, and then **Node Manager**. Check the values of Server Listen Address and Server Listen Port. If required, set appropriate values for these fields.
6. In the Change center region, click **Activate changes**.

7. Repeat Steps 2 through 4 to create OIM_SERVER1_HOST and OIM_SERVER2_HOST, and assign OIM_SERVER1 and OIM_SERVER2 to those computers, respectively.

   Note: Change Hostname Verification to "None" for all WebLogic servers (AdminServer, OIM_SERVER1, OIM_SERVER2, and so on) if you are planning to use default certificates on WebLogic. To do so:

   1. Navigate to **Environment**, **Servers**, ***SERVER_NAME***, **SSL**, and then **Advanced**.
   2. Set Hostname Verification to **None**.

   If you are deploying OIM_SERVER1 on the same computer as AdminServer, then also add OIM_SERVER1 to the computer configuration ADMIN_SERVER_HOST.

8. Repeat the following procedure on all the managed server computers (OIM_SERVER1_HOST and OIM_SERVER2_HOST):

   Enter the domain name in the WL_HOME\common\nodemanager\nodemanager.domains file.

   For example:

   oimdomain=C\:\\bea\\user_projects\\domains\\oimclusterdomain

5.2.9 9. Restarting the WebLogic Server

To restart WebLogic Server:

1. Use the Admin Console to shut down the WebLogic Admin Server. You must also shut down the node manager.

   See Also: "Stopping Oracle Identity Manager"

2. Start the WebLogic Admin Server by using the *DOMAIN_HOME*/bin/xlStartWLS.cmd/sh file.

   Note: In a clustered environment, perform the following step if you are using Microsoft SQL Server as the database:

   Before starting the Managed Servers, ensure that the CLASSPATH is set for all managed servers and add the driver location to the CLASSPATH of the environment variables.

3. Start Node Manager on all the computers by running the *WL_HOME*/server/bin/startNodeManager.cmd/sh file.
4. Start all the managed servers. You can do so in any one of the following ways:

   See Also: "Starting Oracle Identity Manager"

   - Using the node manager: Use the WebLogic Admin Console to navigate to **SERVER_NAME** and **Control**, and then start the server.
   - Without using the node manager, start the managed servers by using the *DOMAIN_HOME*`/bin/xlStartManagedServer script` as follows:

```
xlStartManagedServer.cmd/sh MANAGEDSERVERNAME
http://ADMINSERVERHOST:ADMINPORT
```

For example:

```
xlStartManagedServer.cmd/sh OIM_SERVER1 http://ADMIN_SERVER_HOST:7001
```

Note: To add more managed servers to OIM_CLUSTER (for example, OIM_SERVER3), repeat the following steps for the new host computer:

- 2. Installing WebLogic Server on ADMIN_SERVER_HOST, OIM_SERVER1_HOST and OIM_SERVER2_HOST
- 5. Configuring OIM_SERVER2 in the AdminServer on ADMIN_SERVER_HOST
- 6. Copying the WebLogic Domain Directory
- 7. Copying the OIM_HOME Directory
- 8. Configuring the Node Manager
- 9. Restarting the WebLogic Server

5.3 Configuring the Web Server

To configure the Web server, install the plug-in by following the instructions given in the Web server documentation and WebLogic documentation. Refer to the WebLogic documentation for information about supported Web servers and their versions.

Note: Appendix B, "Configuring the Apache Proxy Plug-in" briefly discusses the procedure to configure the Apache Web server. This information is for reference purposes only. Refer to the WebLogic and Apache documentation for detailed information.

6

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 5, "Installing and Configuring Oracle WebLogic Server in a Clustered Mode" 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 Oracle WebLogic Server is running during the Oracle Identity Manager installation.

This chapter discusses the following topics:

- Installation Prerequisites and Notes
- 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.

6.1 Installation Prerequisites and Notes

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

- 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.

- You cannot install Oracle Identity Manager on a WebLogic domain that already has Oracle Identity Manager or other applications deployed on it. You must use a new domain for installing Oracle Identity Manager.

6.2 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:\jdk160_10
```

> **See Also:** *Oracle Identity Manager Readme* for information about certified JDK versions

- Verify that the Sun JVM `C:\jdk160_10` is being used when a Java command is run. To do this, include the Sun JDK bin directory, for example, `C:\jdk160_10\bin\`, in the PATH ahead of all other path entries, for example:

```
set PATH = C:\jdk160_10\bin;%PATH%
```

6.3 Installing the Database Schema

As part of the installation, the Oracle Identity Manager Installer loads a schema into the database. 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.

6.4 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.

6.5 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:

1. If you are using Microsoft SQL Server as the database, then before installing Oracle Identity Manager, ensure that you copy the sqljdbc.jar file located in C:\Program Files\Microsoft SQL Server 2005Driver forJDBC\lib\ to the *BEA_HOME*\user_projects\domains*DOMAIN_NAME*\lib\ directory, and add the driver location to the system CLASSPATH environment variable:
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 Microsoft 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. On the Target directory page, perform one of the following steps:
   - 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**.

     Alternatively, click **Browse**, navigate to the required 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 required permissions.

9. On the Database Server Selection page, specify either **Oracle** or **SQL Server** as the type of database that you are using with Oracle Identity Manager and then click **Next**.
10. On the Database Information page, enter all database connectivity information that is required to install the database schema.

    You install this schema 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 Readme* 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 3-1.

The installer checks for database connectivity and whether or not 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 detected, then proceed to Step 11.
  - If no connectivity is detected, then you are prompted to enter new information or to fix the connection. Click **Next** after entering new information or fixing the connection.

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 **Oracle 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 5, "Installing and Configuring Oracle WebLogic Server in a Clustered Mode" if you are deploying in a clustered installation.

14. On the WebLogic Directory page, enter information about your application server and Java installation as follows:
    a. Enter the path to the Oracle WebLogic Server product installation directory for the application server.

       Alternatively, click **Browse** and navigate to the Oracle WebLogic Server product installation directory for the application server. For example: `C:\bea\wlserver_10.3`.

    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. For example, the path can be `C:\jdk160_10`.

    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 nonclustered and clustered 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 Admin Port.

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

c. Enter the Oracle WebLogic Server name. The default name is `AdminServer`.

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 a 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 Admin Port.

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

c. Enter the WebLogic Server Name.

This is the Managed Server name. For example, OIM_SERVER1.

d. Enter the WebLogic Server Port.

This is the WebLogic Managed Server port. The default is 7051.

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 domain name.

c. Click **Next**.

17. On the Installation Summary page, click **Install** to start 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.

18. 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.

19. After Oracle Identity Manager is installed, a message is displayed listing the location of the installer log file and the steps to be performed.

    Click **OK** and then perform the postinstallation steps listed in the message.

20. On the Completed page, click **Finish** to exit the installer.

> **Note:** During the installation, WebLogic Server is restarted automatically. After successful installation, the server is automatically shut down. Therefore, you do not have to shut down the server.

21. Start the server. For detailed information about this procedure, refer to the "Starting Oracle Identity Manager" section on page 9-1.

After installing Oracle Identity Manager, follow the instructions in Chapter 9, "Postinstallation Configuration for Oracle Identity Manager and Oracle WebLogic Server".

6.6 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

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 Readme* for information about supported UNIX platforms
- Chapter 5, "Installing and Configuring Oracle WebLogic Server in a Clustered Mode" 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:

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

7.1 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 installing Oracle Identity Manager as a non-root user account on Oracle WebLogic Server, 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

- 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/jdk160_10
  ```

  See *Oracle Identity Manager Readme* 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/jdk160_10/bin:$PATH
  ```

- If you are using Microsoft SQL Server as the database, before installing Oracle Identity Manager, ensure that the sqljdbc.jar file is in the *BEA_HOME*`/user_projects/domains/`*DOMAIN_NAME*`/lib` directory, and add the driver location to the CLASSPATH environment variable. For example:

  ```
  export CLASSPATH=/opt/sql_driver_location/sqljdbc.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.

- You cannot install Oracle Identity Manager on a WebLogic domain that already has Oracle Identity Manager or other applications deployed on it. You must use a new domain for installing Oracle Identity Manager.

7.2 Installing the Database Schema

As part of the installation, the Oracle Identity Manager Installer loads a schema into the database. 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.

7.3 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.

7.4 Installing Oracle Identity Manager on UNIX

If Oracle WebLogic Server is installed in nondefault directory (other than wlserver_10.3), the Oracle Identity Manager Installer fails unless you create a symbolic link of wlserver_10.3 for a nondefault directory in which Oracle 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 input methods:

- Select from a 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 select an item from a list of options, enter the number zero (0) to indicate that the required 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 the distribution 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. Specify 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 the 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 ready to move to the next panel. The Target directory panel is displayed.

9. On the Target directory panel, perform 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 prompted 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. See *Oracle Identity Manager Readme* 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. On the Database Server Selection panel, specify the type of database that you are using:

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

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

    – Enter **0** after you select a database.

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

    The Database Information panel is displayed.

11. Enter the 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 ready to move to the next panel.

    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 **1** for Oracle WebLogic Server.
    - Enter **0** when you are ready to move to the next panel.
    - 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 ready to move to the next panel.

    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 Admin Port.

  This is the WebLogic Server administrative port. The default is 7001.
- Enter the WebLogic Server Name. The default name is AdminServer.
- 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 Admin Port.

  This is the WebLogic Admin Server port number. The default is 7001.
- Enter the WebLogic Server Name.

  This is the Managed Server name. The default is OIM_SERVER1.
- 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 Oracle WebLogic Server directory that contains domain directories. This is sometimes called the configuration or target location in WebLogic.

- 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 the Information Summary page is displayed, verify the information displayed, then perform one of the following steps:
    - Enter **2** to return to earlier panels and make changes.
    - Enter **1** to start the installation.

    Oracle Identity Manager installs and the Completed panel is displayed.
19. Enter **3** to complete the procedure.

> **Note:** During the installation, WebLogic Server is restarted automatically. After successful installation, the server is automatically shut down. Therefore, you do not have to shut down the server.

20. Start the server. For detailed information about this procedure, refer to the "Starting Oracle Identity Manager" section on page 9-1.

After installing Oracle Identity Manager, follow the instructions in Chapter 9, "Postinstallation Configuration for Oracle Identity Manager and Oracle WebLogic Server".

7.5 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.

8

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:

8.1 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\
```

8.2 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 Microsoft Windows Explorer, navigate to the installServer directory on the installation CD.
3. Double-click the setup_client.exe file.
4. Specify a language from the list on the Installer page.

   The Welcome page is displayed.
5. On the Welcome page, click **Next**.
6. On the target directory page, perform 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. On the Application Server page, select **Oracle WebLogic**, then click **Next**.

   The Application Client Location page is displayed.
8. Specify an existing JRE. Then, click **Next**. The Application Server configuration page is displayed.

   Note: Select the JRE for the application server that is in use.
9. On 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. On 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. On 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.

    Click **Next** to move to the next page.
12. On the Summary page, click **Install** to initiate the Design Console installation.
13. Click **Finish** to complete the installation process.

8.3 Postinstallation Requirements for the Design Console

Perform the following steps after installing the Design Console:

1. 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>
2. 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.

8.4 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.

8.5 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*

8.6 Enabling SSL Communication (Optional)

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

- Prerequisites or Assumptions
- SSL Certificate Setup
- Configuration Changes

8.6.1 Prerequisites or Assumptions

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

- Oracle WebLogic Server is installed.
- The WebLogic Domain directory is C:\bea\user_projects\domains\oim.
- The Oracle WebLogic Server home (*WL_HOME*) directory is C:\bea\wlserver_10.3.
- 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.

8.6.2 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 Oracle WebLogic Server host.

- Configuring the Trust Store

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

8.6.2.1 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://xellerate.oracle.com:7002` and `t3s://xellerate.oracle.com:7002` in the `xlconfig.xml` file, then the value of CN in the keytool command must be `xellerate.oracle.com`. Oracle recommends that you generate an SSL certificate by using the domain name (for example, `xellerate.oracle.com`) instead of the IP address.

8.6.2.2 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 trusted certificate authorities, for example, VeriSign or Thawte, for signing the certificates.

8.6.2.3 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
```

8.6.2.4 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.

8.6.3 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 Oracle WebLogic Server
- Copying the Oracle WebLogic Server License

8.6.3.1 Changes to the Design Console

Perform 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 an 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>
```

Alternatively, you can point to the Web server SSL URL based on the Web server configuration. If you want to use the Web server URL, then repeat the steps in the "Configuring the Trust Store" section on page 8-6 with the Web server certificate.

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

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

8.6.3.2 Changes to Oracle WebLogic Server

Perform the following steps:

1. In the WebLogic Server Administration Console, click **Environment**, **Servers**, ***Server_Name***, **Configuration**, and then **General**.
2. Click **Lock & Edit**.
3. Select **SSL listen port enabled**. The default port is 7002.
4. Click the **Keystores** tab
5. From the **Keystore** list, select **Custom Identity and Java Standard Trust**.
6. In the **Custom Identity Keystore** field, 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. Enter the password in the **Custom Identity Keystore Passphrase** and **Confirm Custom Identity Keystore Passphrase** fields.
9. Click **Save**.
10. Click the **SSL** tab.
11. Enter `support` as the private key alias.
12. Enter the password (for example, support) in the **Private Key Passphrase** and **Confirm Private Key Passphrase** fields.
13. Click **Save**.
14. Click **Activate changes**.
15. 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.

8.6.3.3 Copying the Oracle WebLogic Server License

To copy the Oracle WebLogic Server license:

1. Copy `license.bea` from *`WL_HOME`* in the computer on which Oracle WebLogic Server is installed to *`OIM_DC_HOME`* in the computer on 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 *`WL_HOME`*`\server\lib` to *`OIM_DC_HOME`*`\ext`.

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

8.7 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.

9

Postinstallation Configuration for Oracle Identity Manager and Oracle WebLogic Server

After you install Oracle Identity Manager, you may have to perform certain postinstallation tasks before you can use the application. Some of the postinstallation tasks are optional, depending on your deployment and requirement.

This chapter discusses the following topics:

9.1 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. Running the Oracle Identity Manager start script also starts Oracle 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: ■If you are using Microsoft SQL Server as the database, then before starting Oracle Identity Manager (Administrative Server) on UNIX, ensure that you copy the sqljdbc.jar file to the *BEA_HOME*/user_projects/domains/*DOMAIN_NAME*/lib directory and add the driver location to the CLASSPATH environment variable. For example:

```
export CLASSPATH=/opt/sql_driver_location/sqljdbc.jar
```

- In a clustered environment, start the Administrative Server by running the xlStartWLS.bat or xlStartWLS.sh script, and then start the managed servers in the cluster by using the WebLogic Administration Console if you are using WebLogic Node Manager. Otherwise, you can start the managed servers by using the *DOMAIN_HOME*/bin/xlStartManagedServer script as follows:

  ```
  xlStartManagedServer.cmd/sh MANAGEDSERVERNAME
  http://ADMINSERVERHOST:ADMINPORT
  ```

  For example:

  ```
  xlStartManagedServer.cmd/sh OIM_SERVER1
  http://ADMIN_SERVER_HOST:7001
  ```

9.2 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 in 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 Oracle WebLogic Server is 7001.

2. In the Domain Structure tree on the left pane, expand **Environment** and then select **Servers**.
3. On the right pane, select the **Control** tab.
4. Select the check box for the server that you would want to shut down.
5. From the Shutdown list (at the top or bottom of the table), select either **When work completes** or **Force Shutdown Now**.

Note: In a clustered environment, first stop the Managed servers and then stop the Administrative Server.

9.3 Accessing the Administrative and User Console

After starting the Oracle 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 Oracle 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.

9.4 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

9.5 Increasing the Memory and Setting the Java Option

This section describes how to increase the JVM memory settings when Oracle Identity Manager is:

- Deployed on WebLogic Admin Server
- Deployed on WebLogic Managed Servers

9.5.1 Deployed on WebLogic Admin Server

When Oracle Identity Manager is deployed on WebLogic admin server, to increase the JVM memory settings:

1. Use the WebLogic Server Administration Console to shut down the application server gracefully.

2. Navigate to Weblogic *DOMAIN_HOME*/bin. For example, C:\bea103\user_projects\domains\base_domain\bin or /opt/bea103/user_projects/domains/base_domain/bin.
3. Open xlStartWLS.cmd for Microsoft Windows. For UNIX, open xlStartWLS.sh.

   For Microsoft Windows:

   Before "SET JAVA_OPTIONS=....", add any one of the following lines depending on the type of JVM:

   - For Sun and HP JVMs, add: `set USER_MEM_ARGS=-Xms1280m -Xmx1280m -XX:PermSize=128m -XX:MaxPermSize=256m`
   - For JRockit JVMs, add: `set USER_MEM_ARGS=-Xms1280m -Xmx1280m -XnoOpt`
   - For IBM JVMs, add: `set USER_MEM_ARGS=-Xms1280m -Xmx1280`

   For UNIX:

   a. Before "JAVA_OPTIONS=...", add any one of the following lines depending on the type of JVM:

      For Sun and HP JVMs, add: `USER_MEM_ARGS=-Xms1280m -Xmx1280m -XX:PermSize=128m -XX:MaxPermSize=256m`

      For JRockit JVMs, add: `USER_MEM_ARGS=-Xms1280m -Xmx1280 -XnoOpt`

      For IBM JVMs, add: `USER_MEM_ARGS=-Xms1280m -Xmx1280`

   b. Add the following line:

      ```
      export USER_MEM_ARGS
      ```

9.5.2 Deployed on WebLogic Managed Servers

You can deploy Oracle Identity Manager on WebLogic managed servers. This is the only option for clustered installation. Depending on how you start the managed server, such as by using WebLogic admin console or Node Manager, or by running the scripts, changes must be made in different locations.

9.5.2.1 Starting the Server By Using the xlStartManagedServer script

When managed servers are started by running the xlStartManagedServer script, repeat the steps for increasing the JVM memory settings when Oracle Identity Manager is deployed on Weblogic admin server for script *DOMAIN_HOME*/bin/xlStartManagedServer.sh or *DOMAIN_HOME*/bin/xlStartManagedServer.cmd. For more information, see "Deployed on WebLogic Admin Server" on page 9-3.

9.5.2.2 Starting the Server By Using Admin Console or Node Manager

When Managed Servers are started by using the Admin console or Node Manager, to increase the JVM memory settings:

1. Open the WebLogic Server Administration Console.
2. Click **Environment**, **Servers**, *SERVER_NAME*, for example OIM_SERVER1.
3. Click the **Server Start** tab.
4. Change the JVM Memory values as shown in the procedure when Oracle Identity Manager is deployed on WebLogic admin server.

9.6 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. These two values must be identical. Use the keytool utility to change the keystore passwords as follows:

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 9–1 lists the options used in the preceding example of keytool usage.

Table 9–1 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 the *OIM_HOME*`\xellerate\config\xlconfig.xml` file.
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 procedures described in the "Starting Oracle Identity Manager" and "Stopping Oracle Identity Manager" sections, 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
```

9.7 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 8, "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.

9.8 Removing Backup xlconfig.xml Files After Starting or Restarting (Optional)

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 files 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.

9.9 Configuring Proxies to Access Web Application URLs (Optional)

By default, Oracle Identity Manager uses the following Web application URLs. You may have to configure proxies to allow access to the following URLs:

- /xlWebApp
- /xlScheduler
- /Nexaweb
- /spmlws

9.10 Setting Log Levels (Optional)

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:

> **Note:** For a clustered installation, perform this procedure on all the nodes of the cluster.

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 provide output at the WARN level:

   ```
   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 required log level.

3. Set other component log levels according to your requirement.

   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.

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

The following procedure describes how to enable Single Sign-On 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 4.

> **See Also:** *Oracle Identity Manager Best Practices Guide* for more information about configuring Single Sign-On 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. Stop the application server gracefully.
2. In a text editor, open the *OIM_HOME*\xellerate\config\xlconfig.xml file:
3. 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>
```

4. 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.

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

9.12 Configuring Custom Authentication (Optional)

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 must be the first invoked authenticator.

To enable custom authentication on Oracle 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 appear after the Oracle Identity Manager JAAS module in the WebLogic Server Console's list of authentication providers.

To specify a custom authentication provider for Oracle WebLogic Server:

1. Start the **WebLogic Server Console** and open the **Authentication Providers** page from *domain*/Security/Realms/*realm name*/Providers/Authentication.
2. On 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. On the Oracle Identity Manager Authenticator page, select the **Allow Custom Authentication** option on the **Details** tab, and then click **Apply**.
4. On 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**.

9.13 Protecting the JNDI Namespace (Optional)

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. Click **Environment**, **Servers**, and then **AdminServer**.
   b. Click the **View JNDI Tree** link.
   c. On the page that is displayed, click the **Security** tab.
   d. On the Security tab, click the **Policies** tab.

e. Click **Add Conditions** in the Policy Conditions section. The Choose a Predicate page is displayed.

f. From the Predicate List list, you must select a predicate to create a security condition policy. For Oracle Identity Manager, select **User** from the list and click **Next**.

g. In the User Argument Name field, enter `Internal` or `xelsysadm` based on your requirements and click **Add**.

h. Click **Finish**.

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 plain 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>
```

5. Restart the server.

9.14 Deploying the SPML Web Service (Optional)

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 more information, see Chapter 12, "The SPML Web Service" in *Oracle Identity Manager Tools Reference*.

9.15 Configuring Database-Based HTTP Session Failover (Optional)

Oracle Identity Manager on Oracle 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. Delete the *OIM_HOME*\xellerate\OIMApplications directory.
3. To patch the application, run the patch_weblogic script, which is located in the *OIM_HOME*\xellerate\setup directory.

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

It is possible to use other types of failover mechanisms in Oracle WebLogic Server. To use them, change the deployment descriptor (weblogic.xml) in the *OIM_HOME*/DDTemplates/xlWebApp directory, then insert the 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 Remote Manager

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

10.1 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 Microsoft Windows Explorer, navigate to the installServer directory on the installation CD.
3. Double-click the `setup_rm.exe` file.
4. Specify a language from the list on the Installer page.

   The Welcome page is displayed.
5. On the Welcome page, click **Next**.
6. On the Target directory page, perform 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 the 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 required permissions.

7. On the page that is displayed, select the target system JRE by using the **Browse** button.

> **Note:** Select the JRE that is in use by the application server.
>
> See *Oracle Identity Manager Readme* for information about supported JRE versions for the Remote Manager.

8. On the Remote Manager Configuration page:
   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. On the Shortcut page, select or clear check boxes for shortcut options according to your preferences:
   a. Create a shortcut for the Remote Manager on the desktop.
   b. Create a shortcut for the Remote Manager on the Start Menu.

   Click **Next** to move to the next page.
10. On the Installation page, review the configuration details, and then click **Install** to start the installation.
11. After the installation is complete, click **Finish** on the Completed page to exit.

10.2 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 to the installServer directory on the installation CD by using the `cd` command, and then run the `install_rm.sh` file.

   The command-line installer starts.

3. Specify a language from the list by entering a number and then enter **0** to apply the selection.

   The Welcome panel is displayed.

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

5. On 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. On the Remote Manager Configuration panel, enter the Remote Manager configuration information:

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

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

   c. Enter the Remote Manager SSL port, or press Enter 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 complete the Remote Manager installation.

10.3 Configuring the Remote Manager

The Remote Manager and Oracle Identity Manager communicate by using SSL. You must enable a trust relationship between Oracle Identity Manager and the Remote Manager.

Oracle Identity Manager must trust the Remote Manager certificate. To achieve this, you must import the Remote Manager certificate into the Oracle Identity Manager keystore and set it up as a trusted certificate.

If required, you can also enable client-side authentication in which the Remote Manager trusts the server certificate. For client-side authentication, import the certificate for Oracle Identity Manager into the Remote Manager keystore and set it up as a trusted certificate.

You might have to manually edit the configuration file (`xlconfig.xml`) associated with Oracle Identity Manager and the Remote Manager.

10.3.1 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`, which is 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 ensure that the value is set 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 example:

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

   For all other JREs, set the value to `SUNX509`. For example:

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

8. Save the file.

9. Restart Oracle Identity Manager.

10.3.1.1 Using Your Own Certificate

> **Note:** Perform the procedure given in this section only if you want to use your own certificate instead of the default Oracle Identity Manager keystores and certificates. Otherwise, skip this section.

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, then 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 the 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 then open the `xlconfig.xml` file to ensure that the password for the new keystore is encrypted.

10.3.2 Enabling Client-Side Authentication for the Remote Manager

> **Note:** Perform the procedure given in this section only if you want to to enable two-way SSL communication. Otherwise, skip this section.

To enable client-side authentication:

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

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

   For all other JREs, set the value to `SUNX509`. For example:

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

5. Save the file.
6. On the Oracle Identity Manager host 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.

10.3.3 Changing the Remote Manager Keystore Passwords

During installation, the password for the Remote Manager keystore is set to `xellerate`. Oracle recommends that you change 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 to change the keystore passwords as follows:

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 the *OIM_RM_HOME*`\xlremote\config\xlconfig.xml` file.
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 the *OIM_RM_HOME*`\xlremote\config\xlconfig.xml` file 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 the *OIM_HOME*`\xellerate\config\xlconfig.xml` file.
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.

10.4 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`

10.5 Removing the Remote Manager Installation

To remove the Remote Manager installation:

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.

11

Troubleshooting the Oracle Identity Manager Installation

The following sections describe problems that can occur during Oracle Identity Manager installation:

- Oracle Identity Manager Installation Fails During Installation in an Oracle WebLogic Server Cluster
- Task Scheduler Fails in a Clustered Installation
- Default Login Does Not Work
- Installation Fails If Required Operating System Patches for HP-JDK are Not Installed for HP-UX platform
- Disk Space Issue Might Be Encountered While installing Oracle WebLogic Server 10.3 on AIX 5.3
- Troubleshooting the JNDI Namespace Configuration

> **Note:** You can use the Diagnostic Dashboard tool for assistance when you troubleshoot Oracle Identity Manager. See *Oracle Identity Manager Administrative and User Console Guide* for detailed information.

11.1 Oracle Identity Manager Installation Fails During Installation in an Oracle WebLogic Server Cluster

The Oracle Identity Manager installation will fail during installation in an Oracle 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.

11.1.1 Workaround Example

The following is a sample procedure to clean up the Oracle 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. Navigate to **Services**, **JDBC**, **Data Sources**, and then delete both data sources.
3. Navigate to **Services**, **Messaging**, **JMS Servers**, and delete the JMS servers.

4. Navigate to **Services**, **Messaging**, **JMS Modules**, and delete the JMS modules.
5. Navigate to **Services**, **Persistence Stores**, and delete the JDBC stores.
6. Open the *OIM_HOME*\Profile\weblogic.profile file, and then change the following:
   a. The Oracle WebLogic Server target name from myserver to <cluster_member1>.
   b. The Oracle WebLogic Server target port from 7001 to 7051.
7. Run the setup_weblogic.cmd script.
8. Review the log file to verify that the script has run successfully.
9. After the setup script runs successfully, restart Oracle WebLogic Server.

You can either continue with your installation (restart the Oracle Identity Manager Installer at this point), or start Oracle Identity Manager installation by removing all installed Oracle Identity Manager products as well as the WebLogic domain.

11.2 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 strongly recommends that the system clocks for all cluster members be synchronized within a second of each other.

11.3 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.

11.4 Installation Fails If Required Operating System Patches for HP-JDK are Not Installed for HP-UX platform

If you are installing Oracle Identity Manager on Oracle WebLogic Server running on an HP-UX computer, then ensure that the operating system patches needed for the JDK shipped with the operating system have been applied. If this is not done, then Oracle Identity Manager installation fails.

11.5 Disk Space Issue Might Be Encountered While installing Oracle WebLogic Server 10.3 on AIX 5.3

If a disk space issue is encountered while installing Oracle WebLogic Server 10.3 on AIX 5.3, then run the following command to restart the WebLogic Installer:

```
java -Dspace.detection=false -jar server103_generic.jar
```

This command will ensure that disk space is not checked while running the installer.

11.6 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 as follows:

1. Log on to the WebLogic Server Administration Console.
2. Click the domain name under Domain Structure on the left pane.
3. Click the **Security and Embedded LDAP** tab.
4. Select the **Refresh replica at startup** option, and then click **Save**.

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

A

Java 2 Security Permissions for Oracle WebLogic Server

This chapter describes the Java 2 security permissions required for Oracle WebLogic Server. This information is described in the following sections:

- Java 2 Security Permissions for WebLogic Nonclustered Installation
- Java 2 Security Permissions for WebLogic Cluster

A.1 Java 2 Security Permissions for WebLogic Nonclustered Installation

To enable Java 2 Security for Oracle Identity Manager running on Oracle WebLogic Server 10.3:

> **Caution:** The application might fail to start because of syntax errors in the policy files. Therefore, you must exercise caution 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

1. Go to the $*BEA_HOME*/user_projects/domains/$OIM_DOMAIN/ directory and then open the run script (`xlStartWLS.bat` for Microsoft Windows and `xlStartWLS.sh` for UNIX) in a text editor.
2. Search for `JAVA_OPTIONS` and then 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: Make the following changes in the lines that you copy:

Change *$WL_HOME* to the actual Oracle WebLogic Server home directory location.

Change *$BEA_HOME* to the actual BEA home directory location.

Change *$SERVER_NAME* to the actual server name of Oracle 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 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*`/wlserver_10.3/server/lib/weblogic.policy` file exists. If the file exists, then edit it and add the Java 2 Security permissions specified in "Policy File". 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 a 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 address `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.

After you make these changes, restart the server to apply Java 2 Security.

```
// ******************************************
 //  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 permissions 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";

      // Need to 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 Oracle WebLogic Server lib directory
// All these permissions are specific to the Oracle 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
  "${bea.home}/wlserver_10.3/server/lib/-", "read";
permission java.io.FilePermission
  "${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 you must 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 Oracle 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}/wlserver_10.3/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
            "${bea.home}/wlserver_10.3/server/lib/-", "read";
          permission java.io.FilePermission "${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.
```

```
// You 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}/wlserver_10.3/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
            "${bea.home}/wlserver_10.3/server/lib/weblogic.jar", "read";
        permission java.io.FilePermission
            "${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";
};
```

A.2 Java 2 Security Permissions for WebLogic Cluster

To enable Java 2 Security for Oracle Identity Manager running on a Oracle WebLogic Server 10.3 cluster:

Caution: The application might fail to start because of syntax errors in the policy files. Therefore, you must exercise caution 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

---

1. Go to the *$BEA_HOME*/user_projects/domains/$OIM_DOMAIN/ directory and then open the run script (`xlStartWLS.bat` for Microsoft Windows and `xlStartWLS.sh` for UNIX) in a text editor.
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: Make the following changes in the lines that you copy:

Change *$WL_HOME* to the actual Oracle 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*/wlserver_10.3/server/lib/weblogic.policy file exists. If the file exists, then edit it and add the Java 2 Security permissions specified in "Policy File". If the file does not exist, then create it.
4. For clustered nodes that are remotely managed:
   a. On the WebLogic Server Console, click **Configure Servers**, **Server**, **Configuration**, and then click **Remote Start**.
   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/wlserver_10.3/server/lib/weblogic.policy
-Dbea.home=$BEA_HOME
-Dserver.name=$SERVER_NAME
-Doim.domain=$BEA_HOME/user_projects/domains/$OIM_DOMAIN
```

Note: Make the following changes in the lines that you copy:

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 Oracle 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.
- After you make these changes, restart the server to apply Java 2 Security.

```
    // ****************************************
    //  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${/}wlserver_10.3/server/lib/weblogic.policy
    //           weblogic.Server
    //
    // You can edit this file and change the permissions for your
    // applications or update the codeBase line to point to where your
    // server is installed.
    //
    // You should grant all permissions to classes in
    // .internal, and .wlnotdelete folders located in your server directory.
    // You can set
    //   -Duser.domain=<user domain folder>
    //   -Dweblogic.Name=<server name>
    // command-line properties and use them in your policy file.
    // For example, the basic grant statements for servers in a user
    // domain would be:
    // grant codeBase "file:${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${/}wlserver_10.3/server/lib/-" {
  permission java.security.AllPermission;
};

grant codeBase "file:D:${/}wl_cluster${/}bea${/}wlserver_10.3/server/ext/-" {
  permission java.security.AllPermission;
};

grant codeBase
"file:D:${/}wl_cluster${/}bea${/}wlserver_10.3/samples/server/eval/pointbase/lib/-
" {
  permission java.security.AllPermission;
};

// For the petstore demo

grant codeBase
"file:D:${/}wl_cluster${/}bea${/}wlserver_10.3/samples/server/config/petstore/pets
toreServer/.internal/-" {
permission java.security.AllPermission;
};
```

```
grant codeBase
"file:D:${/}wl_cluster${/}bea${/}wlserver_10.3/samples/server/config/petstore/pets
toreServer/.wlnotdelete/-" {
permission java.security.AllPermission;
};

grant codeBase
"file:D:${/}wl_cluster${/}bea${/}wlserver_10.3/samples/server/config/petstore/-" {
permission java.util.PropertyPermission "*", "read";
};

// For the examples

grant codeBase
"file:D:${/}wl_cluster${/}bea${/}wlserver_10.3/samples/server/config/examples/exam
plesServer/.internal/-" {
permission java.security.AllPermission;
};

grant codeBase
"file:D:${/}wl_cluster${/}bea${/}wlserver_10.3/samples/server/config/examples/exam
plesServer/.wlnotdelete/-" {
permission java.security.AllPermission;
};

grant codeBase
"file:D:${/}wl_cluster${/}bea${/}wlserver_10.3/samples/server/config/examples/exam
plesServer/stage/-" {
permission java.util.PropertyPermission "*", "read";
permission java.io.FilePermission
"D:${/}wl_cluster${/}bea${/}wlserver_10.3${/}samples${/}server${/}config${/}exampl
es${/}examplesServer${/}ldap", "read,write";
};

grant codeBase
"file:D:${/}wl_cluster${/}bea${/}wlserver_10.3/samples/server/stage/examples/-" {
permission java.io.FilePermission
"D:${/}wl_cluster${/}bea${/}wlserver_10.3${/}samples${/}server${/}src${/}examples$
{/}-", "read";
permission java.io.FilePermission
"D:${/}wl_cluster${/}bea${/}wlserver_10.3${/}samples${/}server${/}config${/}exampl
es${/}examplesServer${/}ldap", "read,write";
};

// For the workshop

grant codeBase "file:D:${/}wl_cluster${/}bea${/}wlserver_10.3/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${/}wlserver_10.3/samples/server/eval/pointbase/lib/-" {
permission java.security.AllPermission;
};
```

```
// For the petstore demo

grant codeBase

"file:${/}opt${/}bea${/}wlserver_10.3/samples/server/config/petstore/petstoreServe
r/.internal/-" {
    permission java.security.AllPermission;
    };

    grant codeBase

"file:${/}opt${/}bea${/}wlserver_10.3/samples/server/config/petstore/petstoreServe
r/.wlnotdelete/-" {
    permission java.security.AllPermission;
    };

    grant codeBase
        "file:${/}opt${/}bea${/}wlserver_10.3/samples/server/config/petstore/-" {
    permission java.util.PropertyPermission "*", "read";
    };

    // For the examples

    grant codeBase

"file:${/}opt${/}bea${/}wlserver_10.3/samples/server/config/examples/examplesServe
r/.internal/-" {
    permission java.security.AllPermission;
    };

    grant codeBase

"file:${/}opt${/}bea${/}wlserver_10.3/samples/server/config/examples/examplesServe
r/.wlnotdelete/-" {
    permission java.security.AllPermission;
    };

    grant codeBase

"file:${/}opt${/}bea${/}wlserver_10.3/samples/server/config/examples/examplesServe
r/stage/-" {
    permission java.util.PropertyPermission "*", "read";
    permission java.io.FilePermission

"${/}opt${/}bea${/}wlserver_10.3${/}samples${/}server${/}config${/}examples${/}exa
mplesServer${/}ldap", "read,write";
    };

    grant codeBase
        "file:${/}opt${/}bea${/}wlserver_10.3/samples/server/stage/examples/-" {
    permission java.io.FilePermission

"${/}opt${/}bea${/}wlserver_10.3${/}samples${/}server${/}src${/}examples${/}-",
"read";
    permission java.io.FilePermission

"${/}opt${/}bea${/}wlserver_10.3${/}samples${/}server${/}config${/}examples${/}exa
mplesServer${/}ldap", "read,write";
    };
```

```
// For the workshop

grant codeBase "file:${/}opt${/}bea${/}wlserver_10.3/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";

      // Need to read Globalization resource bundle files for various
      // locales
      permission java.io.FilePermission
        "${XL.HomeDir}/customResources/-", "read";

      // Need to 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 code base 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
  "${bea.home}/wlserver_10.3/server/lib/-", "read";
permission java.io.FilePermission
  "${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}/wlserver_10.3/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
            "${bea.home}/wlserver_10.3/server/lib/-", "read";
          permission java.io.FilePermission "${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}/wlserver_10.3/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
            "${bea.home}/wlserver_10.3/server/lib/weblogic.jar", "read";
    permission java.io.FilePermission
            "${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";
};
```

B

Configuring the Apache Proxy Plug-in

To configure the Apache proxy plug-in:

See Also: The Apache Web site for detailed instructions

1. Download Apache Web server version 2.0 or later.
2. Copy the `mod_wl_20.so` file from the *BEA_HOME*`\server\plugin\win\32` directory to the *APACHE_HOME*`\modules` directory.
3. Open the `httpd.conf` file from the *APACHE_HOME*`\conf` directory, and add the following at the end of this file:

```
a> LoadModule weblogic_module modules\mod_wl_20.so

b> <IfModule mod_weblogic.c>
    WebLogicCluster node1:node1_port,node2:node2_port
    DebugConfigInfo ON
    MatchExpression *.jsp
    MatchExpression *.xyz
   </IfModule>

c> <Location /xlWebApp>
    SetHandler weblogic-handler
    DebugConfigInfo ON
    PathTrim /weblogic
   </Location>


d> <Location /xlScheduler>
    SetHandler weblogic-handler
    DebugConfigInfo ON
    PathTrim /weblogic
   </Location>

e> <Location /Nexaweb>
    SetHandler weblogic-handler
    DebugConfigInfo ON
    PathTrim /weblogic
   </Location>

f> <Location /spmlws>
   SetHandler weblogic-handler
   DebugConfigInfo ON
   PathTrim /weblogic
   </Location>
```

```
g> <Location /HTTPClnt>
    SetHandler weblogic-handler
   </Location>
```

4. Run the `Apache.exe` file from *APACHE_HOME*`\bin`.
5. Access the following URL:

   `http://`*apache_installed_hostname_OR_IP_address*`/xlWebApp`

Note: Ensure that the Admin Server and the Managed Server are running.

Index

N

O

P

R

S

T

W

X