Oracle® Identity Manager

Installation Guide for JBoss

Release 9.0

B32138-01

October 2006

ORACLE®

Oracle Identity Manager Installation Guide for JBoss Release 9.0

B32138-01

Primary Author: Don Biasotti

Contents

Preface

Oracle Identity Manager has formerly been known as both Oracle Xellerate Identity Provisioning and Thor Xellerate Identity Manager. The Oracle Identity Manager Audit and Compliance module, formerly known as Oracle Xellerate Audit and Compliance Manager, is a new, optional module that installs on top of Oracle Identity Manager and facilitates user profile auditing.

This document explains how to install Oracle Identity Manager 9.0 on a JBoss application server.

Note: This is a transitional release following Oracle's acquisition of Thor Technologies. Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

Note: The information in this guide applies generally to all Oracle Identity Manager 9.0.x versions.

Audience

The *Oracle Identity Manager Installation Guide for JBoss* is intended for system administrators who plan to install Oracle Identity Manager 9.0 on a JBoss application server.

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

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

- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager API Usage Guide*
- *Oracle Identity Manager Audit Report Developer's Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Globalization Guide*
- *Oracle Identity Manager Glossary of Terms*
- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Tools Reference Guide*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0 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.

Convention	Meaning
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.
*<*_HOME>*	The directory where an application is installed. The directory where you install Oracle Identity Manager server is referred to as *<XL_HOME>*. Each Oracle Identity Manager component includes an abbreviation: *<XL_DC_HOME>* for the Design Console and *<XL_RM_HOME>* for the Remote Manager.

1

Introduction

This chapter provides a brief introduction to the Oracle Identity Manager product and its architecture. It contains the following sections:

Product Overview

Oracle Identity Manager is an advanced, secure enterprise provisioning system that helps streamline the creation of user accounts, management of those accounts, and revocation of user access rights and privileges. Oracle Identity Manager automates access rights management, security, and provisioning of IT resources.

Oracle Identity Manager instantly connects users to the resources they need to be productive. It also prevents unauthorized access to protected, sensitive corporate information.

Access rights management is the process that grants and revokes permissions to access enterprise resources.

Provisioning is the process that grants employees, customers, suppliers, and business partners appropriate access rights to enterprise systems and applications. The provisioning process involves setting up user accounts, groups, and attributes for each user, so that they can access the information they need to work within your company. The Oracle Identity Manager provisioning solution automates these time-consuming manual tasks and secures the correct approvals so that users are connected quickly and securely.

Reconciliation is the process by which any action to create, modify, or delete a target system identity initiated in the target system (using traditional means) is communicated back to the provisioning system and recorded.

De-provisioning is the process of revoking access rights and privileges.

Oracle Identity Manager Components

Oracle Identity Manager includes the following components:

- Oracle Identity Manager Server
- Oracle Identity Manager Remote Manager

- Oracle Identity Manager Design Console (for Windows only)

All components use a single database schema and include documentation. These components can be deployed on one or more host machines that meet the supported requirements. Refer to "Hardware and Software Requirements" on page 2-1 for more information.

Product Architecture

Oracle Identity Manager uses a three-tier architecture: the presentation tier, the server tier, and the data and enterprise integration tier.

The presentation tier contains the following components:

- Design Console
- Administrative and User Console
- Any installed custom client applications

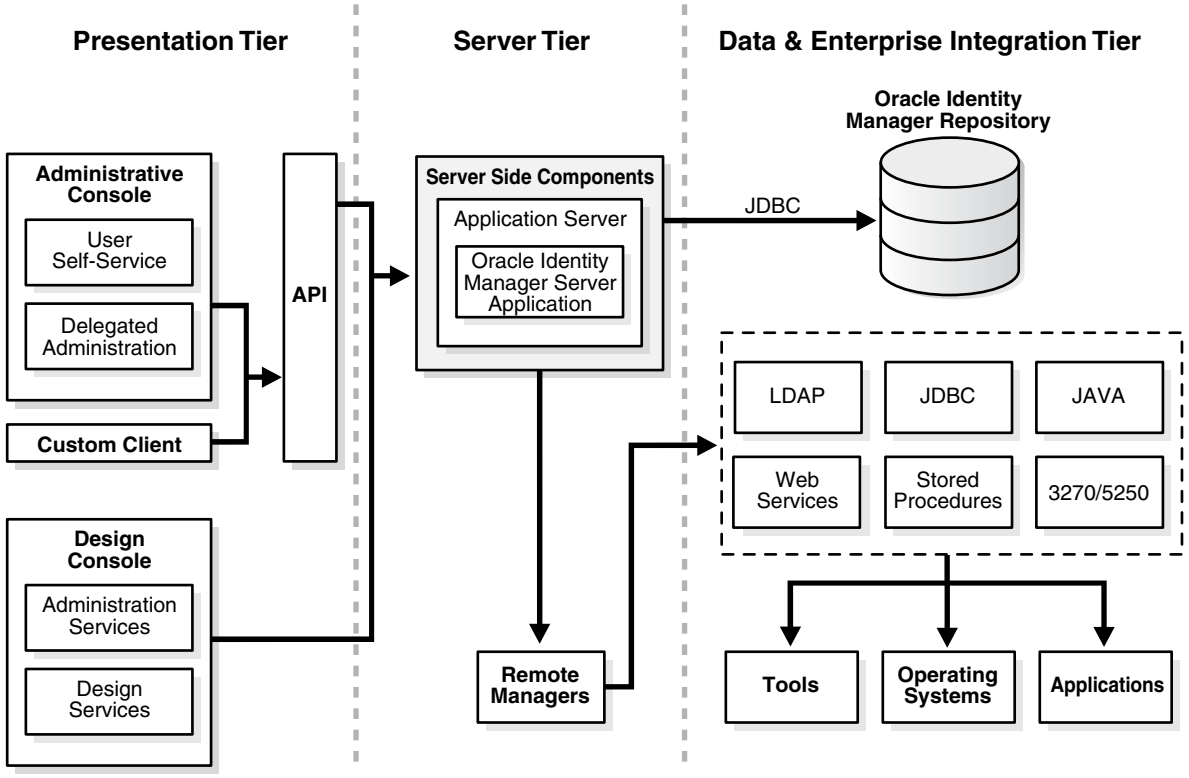
The server tier contains the Oracle Identity Manager Server component, which serves as a bridge between the presentation tier and the data and enterprise integration tier. All requests between the clients and the database are processed through the server tier.

The data and enterprise integration tier contains the database server, which holds the Oracle Identity Manager data structure.

Note: Throughout this document, the Oracle Identity Manager Server is referred to as "the server." The JBoss application server that hosts the Oracle Identity Manager Server is referred to as "the application server."

Figure 1–1 illustrates the Oracle Identity Manager architecture:

Figure 1–1 Oracle Identity Manager Architecture



Installation Overview

The following steps explain how to use this guide for installing Oracle Identity Manager on JBoss:

1. Use Chapter 2, "Planning the Installation" on page 2-1 to prepare for the installation.
2. Use Chapter 3, "Installing and Configuring JBoss for Oracle Identity Manager" on page 3-1 to set up JBoss for Oracle Identity Manager.
3. Use Chapter 4, "Installing and Configuring a Database For Oracle Identity Manager" on page 4-1 to set up a database for Oracle Identity Manager.
4. Use one of the following chapters to install a single Oracle Identity Manager instance:
   - Chapter 5, "Installing Oracle Identity Manager Server on Windows" on page 5-1
   - Chapter 6, "Installing Oracle Identity Manager Server on UNIX or Linux" on page 6-1
5. Use Chapter 7, "Post-Install Configuration for Oracle Identity Manager Server and JBoss" on page 7-1 to perform basic Oracle Identity Manager Server and JBoss configuration tasks related to the installation setup.
6. Use Chapter 8, "Starting and Stopping the Oracle Identity Manager Server" on page 8-1 to start the Oracle Identity Manager server and access the Administrative and User Console.

7. Use Chapter 9, "Deploying in a Clustered JBoss Configuration" on page 9-1 to deploy Oracle Identity Manager in a JBoss cluster.
8. Use Chapter 10, "Installing and Configuring the Oracle Identity Manager Design Console" on page 10-1 to install, configure, and start the Oracle Identity Manager Design Console.
9. Use Chapter 11, "Installing and Configuring the Oracle Identity Manager Remote Manager" on page 11-1 to install, configure, and start the Oracle Identity Manager Remote Manager.
10. Use Chapter 12, "Troubleshooting Your Oracle Identity Manager Installation" on page 12-1 to help troubleshoot your Oracle Identity Manager installation.

2

Planning the Installation

Oracle strongly recommends that you familiarize yourself with the components required for your deployment before starting to install Oracle Identity Manager. Oracle also recommends that you install and use the included Diagnostic Dashboard to ensure that your system is ready for installation. See "Using the Diagnostic Dashboard" on page 2-6 for more information.

A basic Oracle Identity Manager installation consists of the following:

- A database server
- An application server
- An Oracle Identity Manager server (running in the application server)
- A Design Console
- An Administrative and User Console (running in a Web browser)

This chapter contains the following topics:

Release 9.0.2 for Initial Deployments Only

Oracle Identity Manager Release 9.0.2 is intended only for customers performing initial deployments of the Oracle Identity Manager product. Do not install Release 9.0.2 over existing legacy Oracle Identity Manager installations. Contact your Oracle Support representative if you want to upgrade to Release 9.0.2 from previous releases.

Hardware and Software Requirements

The following sections list the supported host computer, application server, and databases required for installing Oracle Identity Manager Release 9.0 and its components.

Note: 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.

Caution: The Oracle Identity Manager installation program may conflict with other installed applications, utilities, or drivers. Try to remove all non-essential software and drivers from the installation machine before loading Oracle Identity Manager. This practice also ensures that the database host can create the database schema.

Important: Always check the Oracle Identity Manager Release Notes for the hardware and software requirements and supported configurations specific to each version of the Oracle Identity Manager product. The information in this guide applies generally to all Oracle Identity Manager 9.0.x versions.

Supported JBoss Application Servers

Oracle Identity Manager Release 9.0 is certified on the JBoss 4.0.2 application server.

Important: Oracle Identity Manager for JBoss requires Java JDK 1.4.2_08 or higher, for example 1.4.2_xx—but not versions 1.5 or higher.

Supported Operating Systems

Oracle Identity Manager Release 9.0 for the JBoss 4.0.2 application server is supported on the following operating systems:

- Microsoft Windows Server 2003 Enterprise Edition with SP1 and 2003 R2 Enterprise Edition
- RedHat Linux AS 4.1
- Solaris 10

Supported Databases

Select one database for your Oracle Identity Manager installation. Oracle Identity Manager supports the following databases:

- Oracle9i Enterprise Edition Release 9.2.0.7
- Oracle 10g Enterprise Edition Release 10.2.0.1.0
- Microsoft SQL Server 2000 with Service Pack 3a

Host System Requirements for Oracle Identity Manager Components

The tables in this section list the minimum host system requirements for the various components in an Oracle Identity Manager environment.

Oracle Identity Manager Server Host Requirements

Table 2–1 lists the minimum host requirements for Oracle Identity Manager Server. It provides guidelines for a basic deployment. Increase each measurement if more size is needed for your deployment.

Table 2–1 Oracle Identity Manager Server Host Requirements

Server Platform	Item
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 Server instance ■ Hard Disk Space: 20 GB (initial size) ■ Operating System: Microsoft Windows Server 2003 Enterprise Edition with SP1 and 2003 R2 Enterprise Edition, or RedHat Linux AS 4.1
Solaris	■ Server: Sun Fire V210 ■ Number of Processors: 1 ■ Memory: 2 GB for each Oracle Identity Manager Server instance ■ Hard Disk Space: 20 GB (initial size) ■ Operating System: Solaris 10

Database Server Host Requirements

Table 2–2 provides examples of minimum host requirements for the database, with selected supported operating systems. These should be considered only as guidelines. Increase each measurement if more size is needed for your deployment. Consult your SQL Server or Oracle database documentation for the specific database host requirements.

Table 2–2 Sample Database Server Host Requirement

Database Server Platform	Item
Windows and Linux	■ Processor Type: Intel Xeon ■ Processor Speed: 2.4 GHz or higher, 400 MHz FSB or higher ■ Number of Processors: 2 ■ Memory: 2 GB for each CPU ■ Hard Disk Space: 40 GB (initial size) for Windows, 20 GB (initial size) for Linux ■ Operating System: Microsoft Windows 2000 (Server, Advanced Server, Professional), Windows 2003 Server SP1 and Windows XP, or RedHat Linux AS 4.1
Solaris	■ Server: Sun Fire V250 ■ Number of Processors: 2 ■ Memory: 2 GB for each CPU ■ Hard Disk Space: 40 GB (initial size) ■ Number of Hard Disks: 1 Disk ■ Operating System: Solaris 10

Design Console Host Requirements

Table 2–3 lists the minimum host requirements for the Oracle Identity Manager Design Console. Increase each measurement if more size is needed for your deployment.

Table 2–3 Design Console Host Requirements

Design Console Platform	Item
Windows	■ Processor Type: Intel Pentium IV ■ Processor Speed: 1.4 GHz or higher ■ Number of Processors: 1 ■ Memory: 512 MB ■ Hard Disk Space: 1 GB ■ Operating System: Windows 2003 (all versions) and Windows XP (all versions)

Remote Manager Host Requirements

Table 2–4 lists the minimum host requirements for the Oracle Identity Manager Remote Manager. Increase each measurement if more size is needed for your deployment.

Table 2–4 Remote Manager Host Requirements

Remote Manager Platform	Item
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 ■ Operating System: Microsoft Windows 2003 Server SP1 and 2003 R2 Enterprise Edition, or RedHat Linux AS 4.1
Solaris	■ Server: Sun Fire V100 Server ■ Number of Processors: 1 ■ Memory: 512 MB ■ Hard Disk Space: 10 GB ■ Operating System: Solaris 10
AIX	■ Processor Type: PowerPC ■ Number of Processors: 1 ■ Memory: 512 MB ■ Hard Disk Space: 10 GB ■ Operating System: AIX 5L 5.3

Supported Versions Details

Table 2–5 lists version details for third-party components compatible with Oracle Identity Manager, version 9.0.

Table 2–5 Support Details for Third-Party Components

Item	Version Details
JBoss	4.0.2
Oracle 10g Release 2	10.2.0.1.0
Oracle9i	9.2.0.7

Table 2–5 (Cont.) Support Details for Third-Party Components

Item	Version Details
SQL Server	2000, with SP3a
Microsoft Windows Server	2003 Enterprise Edition with SP1 and 2003 R2 Enterprise Edition
RedHat Linux	AS 4.1
Solaris	10
Sun JDK	1.4.2_08 or higher, for example 1.4.2_xx—but not versions 1.5 or higher
Microsoft Internet Explorer	6.x

Planning for Non-English Oracle Identity Manager Environments

If you are deploying Oracle Identity Manager Release 9.0.2 components in non-English environments, be sure to review the following guidelines and requirements:

- Before installing any of the Oracle Identity Manager Release 9.0.2 components, ensure the regional and language settings (locale) on the target system meet the following requirements:
  - An appropriate language version of the operating system is installed.
  - Specific language settings are properly configured.
- Refer to the *Oracle Identity Manager Globalization Guide* for information about configuring localized deployments and to ensure you meet the character restrictions for various components and attributes.
- For Oracle database globalization support, you must configure the database for Unicode.

  Refer to "Creating an Oracle Database" on page 4-1 for more information.

Before You Start

To help plan your installation Oracle Identity Manager, read "Hardware and Software Requirements" on page 2-1 and "Installation Worksheet" on page 2-6.

Since the Database Administrator (DBA), System Administrator, and IT Developer typically handle tasks specific to their specific areas of expertise, you should share Oracle Identity Manager installation information among your team members. Table 2–6 indicates the document sections each installation team member should read.

Table 2–6 Installation Roles and Documentation

Installation Role	Sections to Read
Database Administrator	■ Planning Your Installation (this section) ■ Database Setup
System Administrator	■ Planning Your Installation (this section) ■ Pre-Installation ■ Oracle Identity Manager Installation ■ Post-Installation ■ Advance Configuration

Table 2–6 (Cont.) Installation Roles and Documentation

Installation Role	Sections to Read
IT Developer	▪ Planning Your Installation (this section) ▪ Oracle Identity Manager Installation ▪ Installing the Design Console

Installation Worksheet

Table 2–7, the Installation Worksheet, enables you to identify configuration attributes you need before starting the Oracle Identity Manager installation. Print this worksheet and use it to take notes as you go through your installation. Use the *User Selection* column to fill in information specific to your installation:

Table 2–7 Installation Worksheet

Item	Default	User Selection
The base directory for installing Oracle Identity Manager	Windows: C:\oracle UNIX or Linux: /opt/oracle	
The name or IP address of the machine where the Oracle Identity Manager database is installed	N/A[1]	
The TCP port number on which the database listens for connections	1433 for SQL Server 1521 for Oracle	
The name of the database for your installation	N/A	
The name and password of the database account Oracle Identity Manager uses to access the database	N/A	
The JDK install directory	Windows: C:\j2sdk<*version*> UNIX or Linux: /opt/j2sdk<*version*>	
The JBoss install directory	Windows: C:\jboss-<*version*> UNIX or Linux: /opt/jboss-<*version*>	

[1] N/A = Not Applicable for a default. However you must enter a value for this item when you install Oracle Identity Manager.

Using the Diagnostic Dashboard

The Diagnostic Dashboard is a web application that runs in your application server. It checks your pre- and post-installation environments for components required by Oracle Identity Manager. Oracle highly recommends that you install the Diagnostic Dashboard before installing Oracle Identity Manager.

Installing the Diagnostic Dashboard

The Diagnostic Dashboard tool is distributed on the Oracle Identity Manager Installer CD media. It is located in the DiagnosticDashboard directory.

You must deploy the Diagnostic Dashboard web application on your application server. For more information, refer to the *Oracle Identity Manager Administrative and User Console Guide*.

Note: If you install the Diagnostic Dashboard XIMDD application on JBoss before you install the Oracle Identity Manager server, you may encounter an exception when you start JBoss. To avoid this exception, set the `UseJBossWebLoader` property in the jboss-4.0.2\server\default\deploy\jbossweb-tomcat55.sar\META-INF\jboss-service.xml file to `true`.

Verifying Your Pre-installation Environment

The Diagnostic Dashboard verifies the presence of the following components required to install Oracle Identity Manager:

- A supported Application Server
- A supported Java Virtual Machine (JVM)
- A supported Database
- Microsoft SQL Server JDBC Libraries Test

3

Installing and Configuring JBoss for Oracle Identity Manager

This chapter explains how to set up JBoss before installing Oracle Identity Manager.

You must perform the following tasks described in this chapter:

- Installing the Java JDK
- Installing JBoss
- Setting Memory Parameters

> **Note:** See Chapter 9, "Deploying in a Clustered JBoss Configuration" on page 9-1 for information about preparing to deploy Oracle Identity Manager in a JBoss cluster.

Installing the Java JDK

You must have Java JDK 1.4.2_08 or higher, for example 1.4.2_xx—but not versions 1.5 or higher—installed to deploy Oracle Identity Manager on JBoss.

The following procedure explains how to verify that the correct version of the Java JDK has been installed on a Windows system:

1. Open a console window.
2. Enter `java -version`

   For example, the information that appears might look like the following:

```
C:\>java -version
java version "1.4.2_12"
Java(TM) 2 Runtime Environment, Standard Edition
Java HotSpot(TM) Client VM (build 1.4.2_12-b03, mixed mode)
```

Installing JBoss

Install JBoss on the computer where you are going to install Oracle Identity Manager. Consult your JBoss application server documentation for detailed installation procedures.

> **Note:** You can obtain JBoss 4.0.2 from: `http://www.jboss.org`

Setting Environment Variables

Perform the following procedures to set your environment variables:

Windows

To set environment variables on windows:

1. From the Windows **Start Menu**, select **Settings**, select **Control Panel**, select **System**, select **Advanced**, then select **Environment Variables**.
2. In the **System Variables** list, select **Path**, then click **Edit**.

   In the Variable Value field, add the location of your JDK to the beginning of the existing path. For example, if your existing path is the following:

   ```
   %SystemRoot%\system32;%SystemRoot%;C:\Program Files;
   ```

   Change it to the following:

   ```
   c:\j2sdk1.4.2_12\bin;%SystemRoot%\system32;%SystemRoot%;C:\Program Files
   ```

   Click **OK** to commit your change.
3. In the System Variables list, search for JAVA_HOME.

   If JAVA_HOME does not exist, complete Step a. If JAVA_HOME does exist, complete Step b.

   a. Click **New**. In the **Variable Name** field, enter `JAVA_HOME`. In the **Variable Value** field, enter the path to your JDK. Click **OK** to commit your entries, then click **OK** twice more to close the Environment Variables and System Properties windows.

   b. Click **Edit**. Verify the path to your JDK exists in the **Variable Value** field. If the path to your JDK does not, enter the path to your JDK in the **Variable Value** field. Click **OK** to commit your entry, then click **OK** twice more to close the Environment Variables and System Properties windows.

   Note: A window may appear displaying a message asking if you want to update the JDK. Oracle Identity Manager Release 9.0 supports Java JDK 1.4.2_08 or higher, for example 1.4.2_xx—but not versions 1.5 or higher.

UNIX and Linux

To set environment variables on UNIX and Linux:

1. Run the following command:

   ```
   export PATH=/<JAVA_HOME>/bin:$PATH
   ```

Setting Memory Parameters

After installing JBoss, configure the memory allocation for JBoss. The instructions for setting the memory parameters, which appear in the following sub-sections, depend on whether the application server host is running on Windows, or on UNIX or Linux.

Setting Memory Allocation for Windows

To set JBoss memory on a Windows host:

1. Launch a plain-text editor and open the <*JBOSS_HOME*>\bin\run.bat file.
2. Locate the line that contains the following:

   ```
   set JAVA_OPTS=%JAVA_OPTS% -Xms128m -Xmx512m
   ```

3. If necessary, uncomment this line, then change the minimum value to 512 MB and the maximum value to 1024 MB. The altered line should now read as follows:

   ```
   set JAVA_OPTS=%JAVA_OPTS% -Xms512m -Xmx1024m
   ```

4. Save and close the run.bat file.

Setting Memory Allocation for UNIX or Linux

To set the memory allocation for JBoss on UNIX or Linux:

1. Open the <*JBOSS_HOME*>/bin/run.sh file in a text editor.
2. Locate the following line:

   ```
   JAVA_OPTS="$JAVA_OPTS -Dprogram.name=$PROGNAME"
   ```

3. Add the following new line immediately after the line shown in the preceding step:

   ```
   JAVA_OPTS="$JAVA_OPTS -Xms512m -Xmx1024m"
   ```

4. Save and close the run.sh file.

4

Installing and Configuring a Database For Oracle Identity Manager

Oracle Identity Manager requires a database. You must have your database installed and configured before you begin the Oracle Identity Manager installation. Refer to the section that applies to your particular database:

- Using an Oracle Database for Oracle Identity Manager
- Using a SQL Server Database for Oracle Identity Manager

Using an Oracle Database for Oracle Identity Manager

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

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

Installing Oracle

Install the Oracle9i or 10g Release 2 database by referring to the documentation delivered with the Oracle database. See "Supported Databases" on page 2-2 for the specific supported versions. Oracle recommends using the Basic installation.

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

Creating an Oracle Database

You need to create a new Oracle database instance for Oracle Identity Manager. When creating the database, make sure to 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 init.ora parameters `QUERY_REWRITE_ENABLED` to `TRUE` and `QUERY_REWRITE_INTEGRITY` to `TRUSTED` in the **All Initialization Parameters** field of the DBCA.

Consult your Oracle database documentation for detailed instructions on creating a database instance.

Configuring the Database for Globalization Support

For globalization support for Oracle Identity Manager Release 9.0.2, Oracle recommends configuring the database for Unicode. To configure the database for Unicode, perform the following steps:

1. Set the database character to AL32UTF8, which supports the Unicode standard, by selecting AL32UTF8 in the **Character Sets** tab of the DBCA.
2. Set the `NLS_LENGTH_SEMANTICS` init.ora parameter to `CHAR` in the **All Initialization Parameters** field of the DBCA.

See Also: *Oracle Identity Manager Globalization Guide*

Preparing the Oracle Database

After you have installed Oracle and created a database instance, you must prepare it for Oracle Identity Manager by completing the following tasks:

- Verify that query rewrites is enabled
- Enable XA transactions support

Note: The Java JVM is required to enable XA transaction support. If you did not install the JVM during your Oracle installation, you must install it now. Consult Oracle 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 your Oracle database for Oracle Identity Manager by running one of the following scripts:

- On UNIX or Linux, run the following:

  ```
  prepare_xl_db.sh
  ```

- On Windows, run the following:

  ```
  prepare_xl_db.bat
  ```

Both of these scripts ship with the Oracle Identity Manager installer and reside in the \installServer\Xellerate\db\oracle\ directory.

You must observe the following prerequisites when using these scripts:

- The script must be run by the user holding dba privilege (for example, the oracle user on UNIX or Linux typically holds these privileges).
- The script must be run on the machine where the database resides.

The following procedures describe how to prepare your Oracle database for Oracle Identity Manager. Complete the steps associated with the operating system on the machine hosting your Oracle database.

Preparing the Database on UNIX or Linux

To prepare the database on UNIX or Linux:

1. Copy the scripts prepare_xl_db.sh and xell_db_prepare.sql from the distribution CD to a directory on the machine hosting your database where 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 machine when the script prompts you for the following items:
   a. The location of your Oracle home (*ORACLE_HOME*)
   b. The name of your database (*ORACLE_SID*)
   c. The name of the Oracle Identity Manager database user to be created
   d. The password for the Oracle Identity Manager database user
   e. The name of the tablespace to be created for storing Oracle Identity Manager data
   f. The directory in which to store the data file for the Oracle Identity Manager tablespace
   g. The name of the data file (you do not need to append the .dbf extension)
   h. The name of the temporary tablespace
5. Check the prepare_xell_db.lst log file located in the directory where you ran the xell_db_prepare script from to see execution status and additional information.

Preparing the Database on Windows

To prepare the database on Windows:

1. Copy the scripts prepare_xl_db.bat and xell_db_prepare.sql from the distribution CD to a directory on the machine hosting your database where you (as the account user performing this task) have write permission.
2. Open a command window, navigate to the directory where you just copied the scripts, 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, the string you enter on the command line might look something like the following:

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

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

Table 4–1 Options for the prepare_xl_db.bat Script

Argument	Description
`XELL`	Name of the database
`C:\oracle\ora92`	Directory where the Oracle database is installed

Table 4–1 (Cont.) Options for the prepare_xl_db.bat Script

Argument	Description
`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 where the datafiles will be placed
`xeltbs_01`	Name of the datafile (you do not need to give .dbf extension)
`TEMP`	Name of the temporary tablespace that already exists in your database
`manager`	Password for the SYS user

3. Check the prepare_xell_db.lst log file located in the directory where you ran the xell_db_prepare script from to see execution status and additional information.

Evaluating Script Results

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

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

You can ignore non-fatal errors. For example, when the script tries to drop a non-existent view, it will return the error "ORA-00942: table or view does not exist". This can be ignored without adverse consequences.

Make sure to scan all the 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.

Using a SQL Server Database for Oracle Identity Manager

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

- Installing and Configuring SQL Server
- Configuring JBoss for SQL Server
- Registering SQL Server
- Creating a SQL Server Database
- Creating a SQL Server Database Account

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

Installing and Configuring SQL Server

To install and configure SQL Server for Oracle Identity Manager:

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

   During installation, choose **mixed authentication mode**, then set the password to **sa**.

Note: Perform steps 2–4 on the machine hosting the application server.

2. Download the SQL Server 2000 Driver for JDBC Service Pack 3 from http://www.microsoft.com.
3. Install SQL Server 2000 Driver for JDBC Service Pack 3.

Note: Make sure to 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 your classpath is more than 256 characters, the installer does not work properly.

4. Locate the JDBC driver files (mssqlserver.jar, msbase.jar, and msutil.jar).

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

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

   `C:\<jdbc_install_folder>\lib\msbase.jar;`

   `C:\<jdbc_install_folder>\lib\msutil.jar;`

   Where <*jdbc_install_folder*> is the location where the SQL Server 2000 Driver for JDBC files is installed.

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

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

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

6. Run the script instjdbc.sql.

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

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

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

   Tip: Set the Distributed Transaction Coordinator to auto-start whenever your operating system starts.

Configuring JBoss for SQL Server

After installing JBoss, set up JBoss to work with SQL Server by copying (not moving) the following JDBC driver files to the lib directory of your default JBoss server:

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

Copy the files from the SQL Server 2000 Driver for JDBC library directory (the default is C:\Program Files\Microsoft SQL Server 2000 Driver for JDBC\lib) to <*JBOSS_HOME*>\server\default\lib.

Note: For a JBoss cluster, copy (do not move) the files from the SQL Server 2000 Driver for JDBC library directory to <*JBOSS_HOME*>\server\all\lib.

Registering SQL Server

To register the SQL Server:

1. Start the Microsoft SQL Server Enterprise Manager application.

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

2. In the left pane of the SQL Server Enterprise Manager application window, select **Console Root**, then select **Microsoft SQL Servers**.

3. Right-click **SQL Server Group** and select **New SQL Server Registration**.

4. In the Register SQL Server Wizard dialog, click **Next**.

5. On the Select a SQL Server page, perform one of the three following sub-steps:

   a. Select your server from the list in the right pane, click **Add**, then click **Next**.

   b. Select **LOCAL**, then click **Add**, then click **Next**.

   c. Enter the host name of your server in the text entry box, click Add, then click Next.

6. On the Select an Authentication Mode page, select **The SQL Server login information that was assigned to me by the administrator [SQL Server Authentication]**, then click **Next**.

7. On the Register Connection Option page, select **Login automatically using my SQL server account information**, then complete the following sub-steps:

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

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

8. On the Select SQL Server Group page, select **Add the SQL Server(s) to an existing SQL Server Group**, select a group from the **Group name** list, then click **Next**.

9. On the Completing the Register SQL Server Wizard page, click **Finish**, then click **Done**.

Creating a SQL Server Database

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

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

To create a SQL Server database, complete these steps:

1. Start the Microsoft SQL Server Enterprise Manager application.

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

2. In the left pane of the SQL Server Enterprise Manager application window, select **Console Root**, select **Microsoft SQL Servers**, select the server group to which your server belongs, then double-click the icon representing your server.

3. Right-click **Databases**, then select **New Database**.

4. In the Database Properties dialog, select the **General** tab, then enter **XELL** in the **Name** field.

5. Select the **Data Files** tab, then, for the **Initial Size** and **Filegroup** columns in the Database files matrix, enter the information from the corresponding columns in Table 4–2.

Table 4–2 Database Files

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

Note: Table 4–2 lists initial sizes for a production environment. For non-production installations, you can use the default initial sizes provided for the filegroups.

Note: To ensure successful installation of Oracle Identity Manager, filegroup names must be entered exactly as they appear in Table 4–2. You can vary the File Name and Location strings to match the database name and the location of your SQL Server installation.

   a. Select **Automatically Grow File**.

   b. Select **By Percent**, then enter `10` in the associated text box.

   c. Select **Unrestricted file growth**.

   Tip: 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.

6. Select the **Transaction Log** tab, then change the initial size to 500MB. Leave all the other options on the tab at their default values.

Note: For non-production installations you can use the default initial size for the log file.

7. Click **OK** to initiate the database creation.

Creating a 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 an account name other than xladm, make sure to specify that login instead of xladm throughout the following procedure and also when installing Oracle Identity Manager.

To create a SQL Server database account and permissions:

1. Launch the Microsoft SQL Server Enterprise Manager application.

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

2. In the left pane of the SQL Server Enterprise Manager application window, select **Console Root**, select **Microsoft SQL Servers**, select the server group to which your server belongs, then double-click the icon representing your server.
3. Select **Security**, right-click **Logins**, then select **New Login**.
4. In the SQL Server Login Properties dialog, select the **General** tab.

   In the **Name** field, enter xladm (or a different account name that you prefer).

5. Select **SQL Server Authentication**, then enter the password associated with the account you specified in the Password text box.
6. In the **Database** box within the **Defaults** section, select **XELL** from the list.

   Leave the **Language** box set to <default>.

7. Select the **Database Access** tab. In the upper panel, select the check box associated with **XELL**.
8. In the lower panel, select the check-boxes associated with the following:
   - public
   - db_owner
   - db_accessadmin
   - db_securityadmin
   - db_ddladmin
   - db_datareader
   - db_datawriter
9. Click **OK** to commit your changes.

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

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

    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.

5

Installing Oracle Identity Manager Server on Windows

This chapter explains how to install Oracle Identity Manager on Windows. You must install the Oracle Identity Manager server 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.

This chapter contains the following topics:

Caution: *DO NOT* use a remote client tool such as PCAnywhere to install Oracle Identity Manager products.

Installing the Database Schema

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

Note: During the schema installation, a corresponding log file is created under the <*XL_HOME*>\logs\ directory.

Installing Documentation

The Oracle Identity Manager documentation is installed automatically under the <XL_HOME> directory. No special input is required. A full documentation set is installed with each Oracle Identity Manager component.

Installing the Oracle Identity Manager Server on Windows

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

Note: During the installation process, an unused log file named log.conf is created in the <XL_HOME>\xellerate\config\ directory. You can safely ignore this file.

Important: 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 same name of an existing Oracle Identity Manager home directory, then back up your original Oracle Identity Manager home by renaming that directory.

Remember at all times 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 the Oracle Identity Manager server.

To install the Oracle Identity Manager server on a Windows host:

1. If you are using SQL Server as your database, before installing the Oracle Identity Manager server be sure to copy the following three files located in C:\Program Files\<*Microsoft SQL Server 2000 Driver for JDBC*>\lib\ to the <*JBOSS_HOME*>\server\default\lib\ directory and add the driver location to the system CLASSPATH environment variable:
   - mssqlserver.jar
   - msbase.jar
   - msutil.jar
2. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.
3. From Windows Explorer, access the installServer directory on the installation CD and double-click the setup_server.exe file.
4. Select a language on the Installer screen and click **OK**.

   The Welcome screen appears.
5. On the Welcome screen, click **Next**.
6. On the Oracle Identity Manager Application Options screen, select to install one of the following applications:
   - Oracle Identity Manager
   - Oracle Identity Manager with Audit and Compliance Module
7. Click **Next**.
8. After the Target directory screen appears, complete one of the following bulleted actions:
   - The default directory for the Oracle Identity Manager server is C:\oracle. To install the Oracle Identity Manager server into this directory, click **Next**.
   - To install the Oracle Identity Manager server into another directory, enter the path in the **Directory** field, then click **Next**.

     or

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

Note: If the directory path does not exist, the Base Directory settings text box appears. Click **OK**. Oracle Identity Manager creates this directory for the Oracle Identity Manager server. If you do not have write permission to create the default directory for the Oracle Identity Manager server, a dialog appears informing you that the installer could not create the directory. Click **OK** to dismiss the dialog, then contact your System Administrator to obtain the appropriate permissions.

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

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

    Note: To install against an existing database, verify that the version of Oracle Identity Manager you are installing is certified with your existing database version. Refer to the *Oracle Identity Manager Release Notes* to confirm the certified configurations.

    When Oracle Identity Manager is installed against an existing database, the .xldatabasekey file from the earlier Oracle Identity Manager installation must be copied to the new <*XL_HOME*>\xellerate\config directory. You should create the \config directory in the new <*XL_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 resides.
    - In the **PORT** field, enter the port number on which the database listens for connections. The default port is 1521 for Oracle and 1433 for 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 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 setting the preceding items, refer to the configuration settings specified in "Using an Oracle Database for Oracle Identity Manager" on page 4-1 or "Using a SQL Server Database for Oracle Identity Manager" on page 4-4 to be sure you set consistent information.

The installer checks for database connectivity and if a database schema exists. If the check passes, the installer proceeds to the next step in the process. If the check fails, an error message will appear.

- Select the appropriate database options:
  - If a database exists, and the connectivity is good, proceed to step 11.
  - If no connectivity is detected, 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** (Single Sign-On) **Authentication** option. If you select Single Sign-On authentication, 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 **JBoss**, then click **Next**.
13. On the Cluster Information page, specify the server configuration (clustered or non-clustered).
    - For a non-clustered environment, select **No** and click **Next**.
    - If you are deploying in a clustered environment, select **Yes**, enter the unique partition name, and see Chapter 9, "Deploying in a Clustered JBoss Configuration" on page 5-1 for more information.
14. On the Application Server Information page, enter the information pertaining to your application server and Java installation:
    a. Enter the path to your application server installation

       or

       Click **Browse** and navigate to your application server installation

    b. Enter the path to your JDK directory

       or

       Click **Browse** and navigate to your JDK directory

       Note: If you enter an invalid directory, an error message appears.

    c. Click **Next**.
15. Back up your application server when the Application Server Configuration Backup screen appears, then click **Next** to initiate server installation.
16. If the installer detects an existing database, you can choose to use that database.

    Select **Yes**, then click **Next**. If the existing database is not encrypted, you are prompted to encrypt it. Select **Yes**, then click **Next**.
17. The Summary screen appears.

    Click **Install** to install the Oracle Identity Manager application.
18. After the Oracle Identity Manager server installs, a message appears listing the location of the installer log file and the next steps you should perform.

    Click **OK** and complete the post-installation steps listed in the message.

19. The Completed screen appears.

    Click **Finish** to exit the installer.

After installing the Oracle Identity Manager server, perform the steps in Chapter 7, "Post-Install Configuration for Oracle Identity Manager Server and JBoss" on page 7-1 to continue the installation process.

Removing the Oracle Identity Manager Server Installation

To remove the Oracle Identity Manager server installation:

1. Stop the Oracle Identity Manager server if it is running and stop all Oracle Identity Manager processes.
2. Delete the <*XL_HOME*> directory where you installed the Oracle Identity Manager server.

6

Installing Oracle Identity Manager Server on UNIX or Linux

This chapter explains how to install Oracle Identity Manager on UNIX and Linux. Refer to Supported Operating Systems on page 2-2 for more information on the supported UNIX and Linux platforms. You must install the Oracle Identity Manager server 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 contains the following topics:

Note: The default logging package included by the base RedHat Linux installation causes installation problems and exceptions for Oracle Identity Manager. Before installing Oracle Identity Manager on RedHat Linux, delete the commons-logging-1.0.2 library from the base operating system installation. The commons-logging-1.0.2 library is typically installed with any standard RedHat installation. Also, be sure to delete the symbolic links in the /usr/share/java/ directory. Deleting these symbolic links will force Oracle Identity Manager to use its own internal logger jar files during installation.

Installing the Database Schema

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

Note: During the schema installation, a corresponding log file is created under the <*XL_HOME*>/logs/ directory.

Installing Documentation

The Oracle Identity Manager documentation is installed automatically under the <*XL_HOME*> directory. No special input is required. A full documentation set is installed with each Oracle Identity Manager component

Installing the Oracle Identity Manager Server on UNIX or Linux

This section describes pre-installation considerations and the installation program.

Before installation Oracle Identity Manager, do the following:

- Set the `JAVA_HOME` variable to Sun JDK 1.4.2_08 or higher.

  Oracle Identity Manager Release 9.0 supports JDK 1.4.2_08 or higher, for example 1.4.2_xx—but not versions 1.5 or higher.

- If you are using SQL Server as your database, before installing Oracle Identity Manager server, be sure to copy the three Microsoft SQL Server JDBC driver .jar files to the UNIX or Linux server and add the files to the CLASSPATH.

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

- Choose from among a list of options

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

- Enter information at a prompt

  To enter information at the prompt, enter the information and press the Enter key. To accept a default value—default values are enclosed in brackets after a prompt—simply press the Enter key to accept them.

The installer contains logical sections (panels).

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

The following procedure describes the installation process.

Note: During the installation process, an unused log file named log.conf is created in the <*XL_HOME*>/xellerate/config/ directory. You can safely ignore this file.

Important: 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, back up your previous Oracle Identity Manager home by renaming the original directory.

All Oracle Identity Manager components must be installed in different home directories. For example, you cannot install the Remote Manager in the same directory where the Oracle Identity Manager server is installed.

To install Oracle Identity Manager server on UNIX or Linux:

1. If you are using SQL Server as your database, before installing the Oracle Identity Manager server be sure the following three files are in the *<JBOSS_HOME>*/server/default/lib/ directory and add the driver location to the system CLASSPATH environment variable:
   - mssqlserver.jar
   - msbase.jar
   - msutil.jar
2. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.
3. From the console, change directory (cd) to the installServer directory on the installation CD and run the install_server.sh file using the following command:

   ```
   sh install_server.sh
   ```

   The installer starts in console mode.

   Note: If you are not installing Oracle Identity Manager from distributed media (CD), you must set the execute bit of all shell scripts under in the installServer directory. To set the execute bit for all shell scripts recursively, cd to the installServer directory and run the following command:

   ```
   # chmod -R u+x *.sh
   ```

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

   Enter **0** to apply the language selection. The product Welcome Message panel appears.
5. Enter **1** on the Welcome Message panel to display the next panel.

   The Oracle Identity Manager Application Options panel appears.
6. Enter **1** on the Oracle Identity Manager Application Options panel to display the next panel.

   The Select the Oracle Identity Manager application to install panel appears.
7. Select the application to install:
   - Enter **1** for Oracle Identity Manager.
   - Enter **2** for the Oracle Identity Manager with Audit and Compliance Module.

Enter **0** when you are finished and then enter **1** to move to the next section. The Target directory panel appears.

8. On the Target directory panel, complete one of the sub-steps that follow:
   - Enter the path to the directory where 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, you are asked to create it. Enter **y**, for yes.

   The Database Server Selection panel appears.

   Note: To install against an existing database, verify that the version of Oracle Identity Manager you are installing is certified with your existing database version. Refer to the *Oracle Identity Manager Release Notes* to confirm the certified configurations.

   When Oracle Identity Manager is installed against an existing database, the .xldatabasekey file from the earlier Oracle Identity Manager installation must be copied to the new <*XL_HOME*>/xellerate/config directory. You should create the /config directory in the new <*XL_HOME*>/xellerate/ path if it does not already exist.

   ---

9. On the Database Server Selection panel, specify the type of database you are using.
   - Enter 1 for Oracle.
   - Enter 2 for SQL Server.
   - Enter 0 when you are finished.
   - Enter 1 to move to the next panel.
10. Enter your database information:
    a. Enter the database host name or IP address.
    b. Enter the port number (or accept the default).
    c. Enter the SID for the database name.
    d. Enter the database user name for the account that Oracle Identity Manager uses to connect to the database.
    e. Enter the password for the database account that Oracle Identity Manager uses to connect to the database.
    f. Enter 1 to move to the next panel.

    The Authentication Information panel appears.
11. Select the authentication mode for the Oracle Identity Manager web application.
    - Enter 1 for Oracle Identity Manager Default Authentication.
    - Enter 2 for SSO Authentication.
    - Enter 0 when you are finished.
    - If you select SSO authentication, 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 appears.

12. Specify your application server type.
    - Enter **4** for JBoss.
    - Enter 0 when you are finished.
    - Enter 1 to move to the next panel.

    The Cluster Information panel appears.
13. Provide the following information regarding deploying in a cluster:
    - Enter 1 for Yes (clustered) and enter the unique partition name at the prompt.
    - Enter 2 for No (non-clustered).
    - Enter 0 when you are finished.
    - Enter 1 to move to the next section.

    The Application Server Information panel appears.

    Important: If you are deploying in a clustered environment, select Yes and see Chapter 9, "Deploying in a Clustered JBoss Configuration" on page 9-1 for more information.
14. In the Application Server Information panel:
    - Provide the location where the application server is installed
    - Provide the location where the JDK is installed
    - Enter 1 to move to the next section.
15. When you receive a message about backing up the application server installation, enter 1 to move to the next section. The Summary panel appears.
16. On the Summary panel, enter 1 to begin installation.
17. After the installation is finished, the Completed panel appears. Enter 3 finish and exit.

After installing the Oracle Identity Manager server, perform the steps in Chapter 7, "Post-Install Configuration for Oracle Identity Manager Server and JBoss" on page 7-1 to continue the installation process.

Removing the Oracle Identity Manager Server Installation

To remove the Oracle Identity Manager server installation:

1. Stop the Oracle Identity Manager server if it is running and stop all Oracle Identity Manager processes.
2. Delete the <*XL_HOME*> directory where you installed the Oracle Identity Manager server.

7

Post-Install Configuration for Oracle Identity Manager Server and JBoss

After installing Oracle Identity Manager, you should considering performing the post-installation tasks documented in this chapter before using the application. Depending on your Oracle Identity Manager deployment, you may choose not to perform some of these tasks. The following is a list of the post-installation tasks documented in this chapter:

- Reserving JBoss Ports on Windows Installations
- Changing Keystore Passwords
- Setting Log Levels
- Enabling Single Sign-On (SSO) for Oracle Identity Manager
- Configuring Multiple JBoss Installations to Use a Single Database

Note: The examples in this chapter are Windows-based, however the post-installation tasks apply to UNIX and Linux as well.

Reserving JBoss Ports on Windows Installations

Perform the following steps to reserve the necessary ports for JBoss on Windows installations:

1. Select **Run** from the Windows **Start** menu. The Run dialog box displays.
2. Enter `regedt32` in the Run dialog box and click the **OK** button. The Registry Editor window appears.
3. Navigate to the following registry key:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`

4. If it does not already exist, create a ReservedPorts value, as follows:
   a. Point to **New** on the **Edit** menu and click **Multi-String Value**.
   b. Enter `ReservedPorts` as the value name and press the Enter key.
5. Double-click the **ReservedPorts** value. The Edit Multi-String dialog box appears.
6. In the Edit Multi-String dialog box, enter `1098-1434` in the **Value data** box.
7. Click the **OK** button to close the Edit Multi-String dialog box, and then close the Registry Editor window.

Changing Keystore Passwords

Oracle Identity Manager has two keystores: one for the Oracle Identity Manager server and one for the database. During installation, the passwords for both are set to *xellerate*. Oracle recommends changing the keystore passwords for all production installations. You can use the keytool to change the keystore password for either keystore.

To change the keystore password:

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

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

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

Table 7–1 Command Options for keytool

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 the Oracle Identity Manager server or .xldatabasekey for the database)
`-storetype` <*option*>	JKS for .xlkeystore and JCEKS for .xldatabasekey

4. Launch a plain-text editor and open <*XL_HOME*>\xellerate\config\xlconfig.xml
5. Edit the `<xl-configuration>.<Security>.<XLPKIProvider>.<KeyStore>` section to specify the keystore password.

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 (in the clear). For example, change the following block:

```
<Security>
<XLPKIProvider>
<KeyStore>
<Location>.xlkeystore</Location>
<Password encrypted="true">xYr5V2FfkRYHxKXHeT9dDg==</Password>
<Type>JKS</Type>
<Provider>sun.security.provider.Sun</Provider>
</KeyStore>
```

to the following:

```
<Security>
<XLPKIProvider>
<KeyStore>
```

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

6. Restart your application server.

   When you stop and start the application server, 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.

7. If all of the preceding steps have succeeded, you can delete the backup file.

Setting Log Levels

Oracle Identity Manager uses log4j for logging. For JBoss-based installations, logging is configured in the log4j.xml file.

By default, Oracle Identity Manager is configured to output at the Warning level. You can change the log level universally for all components or for an individual component. For normal operation of Oracle Identity Manager, this post-installation configuration step is not required.

Oracle Identity Manager Component Logging

The components are listed in the *<XL_HOME>*\xellerate\config\log.properties file in the XELLERATE section. They are:

```
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
```

Setting Log Levels for JBoss

The log4j.xml file is used for all logging with JBoss; therefore, Oracle Identity Manager components use an Xellerate tag. The log4j.xml file contains a general setting for Xellerate:

```
<category name="XELLERATE">
  <priority value="WARN" />
</category>
```

You can change the log level for all components by editing the `priority value` of the general setting, or for a specific component by adding a new logging category element.

The available categories are listed in the log.properties file in the XELLERATE section. See Oracle Identity Manager Component Logging on page 7-3 for more information.

For example, to change the level for the Oracle Identity Manager server, add the following element to the log4j.xml file:

```
<category name="XELLERATE.SERVER">
  <priority value="WARN" />
  <appender-ref ref="FILE"/>
</category>
```

To set Oracle Identity Manager log levels in JBoss:

1. Open the file *<JBOSS_HOME>*\server\default\conf\log4j.xml in a text editor.
2. Insert an element for the desired component.
3. Set the `priority value` to the appropriate level for the desired components.

   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
4. Save your changes.

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

The following procedure describes how to enable Single Sign-On for Oracle Identity Manager with ASCII character logins. To enable Single Sign-On with non-ASCII character logins, use the following procedure—but include the additional configuration setting described in step 4.

> **See Also:** Oracle*MetaLink* Note 394670.1 for additional information about configuring Single Sign-On for Oracle Identity Manager with Oracle Access Manager. You can access the Oracle*MetaLink* Web site at:
>
> https://metalink.oracle.com/

Note: Header names comprised only of alphabetic characters are certified. Oracle recommends not using special characters or numeric characters in header names.

To enable Single Sign-On for Oracle Identity Manager:

1. Stop the application server gracefully.
2. Launch a plain-text editor and open the following file:

   <*XL_HOME*>\xellerate\config\xlconfig.xml

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 your application server and web server configuration to enable Single Sign-On by referring to your application and web server vendor documentation.
6. Restart the application server.

Configuring Multiple JBoss Installations to Use a Single Database

When two or more non-clustered JBoss installations connected to a load balancer point to a single database, you must configure the individual JBoss instances to use different JMS tables.

Complete the following procedure on the second and all other JBoss instances using the same Oracle Identity Manager database so they use different JMS tables:

1. Launch a plain-text editor, navigate to the directory <*JBOSS_HOME*>\server\default\deploy\jms, then open the file <*database_name*>-jdbc2-service.xml.

Note that <*database_name*> refers to the common database used by multiple JBoss instances.

2. In all the queries and statements in the sqlProperties section of the <*database_name*>-jdbc2-service.xml, change the names of the tables represented by JMS_MESSAGES and JMS_TRANSACTIONS to new, unique, and valid values.

3. Add the following statements to the end of the file:

```
DELETE_TEMPORARY_MESSAGES = DELETE FROM <NEW_JMS_MESSAGES_NAME>
    WHERE TXOP='T'
CREATE_IDX_MESSAGE_TXOP_TXID = CREATE INDEX
    <NEW_JMS_MESSAGES_NAME>_TXOP_TXID ON <NEW_JMS_MESSAGES_NAME> (TXOP, TXID)
CREATE_IDX_MESSAGE_DESTINATION = CREATE INDEX
    <NEW_JMS_MESSAGES_NAME>_DESTINATION ON <NEW_JMS_MESSAGES_NAME>(DESTINATION)
```

Note: <*NEW_JMS_MESSAGES_NAME*> represents the new name of the JMS_MESSAGES tables you changed in step 2.

4. Save and close the file.

8

Starting and Stopping the Oracle Identity Manager Server

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

Important: You must complete all post-installation steps in Chapter 7, "Post-Install Configuration for Oracle Identity Manager Server and JBoss" on page 7-1 before starting the Oracle Identity Manager Server.

Removing Backup xlconfig.xml Files After Starting or Restarting

After starting any Oracle Identity Manager component either the first time, or after changing any passwords in xlconfig.xml, passwords are encrypted and saved. However, Oracle Identity Manager also keeps a backup copy of xlconfig.xml (named xlconfig.xml.<x>) before saving. This backup xlconfig.xml.<x> file contains the passwords in plain text.

Important: Be sure to remove these files after starting any Oracle Identity Manager component either the first time, or after restarting after changing any passwords in xlconfig.xml once you have established that the new password is working properly. The backup file is named xlconfig.xml.<x>, where x is the latest available number, for example xlconfig.xml.0, xlconfig.xml.1, and so on.

Starting the Oracle Identity Manager Server

This section describes how to start the Oracle Identity Manager server on Windows, UNIX, or Linux.

To start the Oracle Identity Manager server:

1. Verify that your database is up and running.
2. Start the Oracle Identity Manager server by running one of the following scripts appropriate for your operating system. Running the Oracle Identity Manager server start script also starts the JBoss application server.

   On Windows

   `<XL_HOME>\xellerate\bin\xlStartServer.bat`

   On UNIX or Linux

   `<XL_HOME>/xellerate/bin/xlStartServer.sh`

Stopping the Oracle Identity Manager Server

This section describes how to stop the Oracle Identity Manager server gracefully on Windows, UNIX, or Linux. To stop the Oracle Identity Manager server gracefully, you stop the JBoss application server by running one of the following scripts appropriate for your operating system.

On Windows

`<JBOSS_HOME>\bin\shutdown.bat -S`

On UNIX or Linux

`<JBOSS_HOME>/bin/shutdown.sh -S`

Accessing the Administrative and User Console

After staring the JBoss application server and Oracle Identity Manager you can access the Administrative and User Console.

To access the Administrative and User Console:

1. Launch your web browser, then point it to the following URL:

   `http://<hostname>:<port>xlWebApp`

   Where *<hostname>* represents the name of the machine hosting the application server and *<port>* refers to the port on which the server is listening. The port number for JBoss is 8080.

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

   For example:

   `http://localhost:8080/xlWebApp`

2. After the Oracle Identity Manager login screen appears, login with your user name and password.

   Note: The default administrator user name and password are xelsysadm.

Using Diagnostic Dashboard to Verify Installation

The Diagnostic Dashboard verifies each component in your post-installation 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.

Note: See "Using the Diagnostic Dashboard" on page 2-6 for more information.

9

Deploying in a Clustered JBoss Configuration

This chapter describes how to deploy Oracle Identity Manager in a clustered JBoss application server environment.

This chapter discusses the following topics:

> **Caution:** Deploying an application in a clustered environment is a complex procedure. This document assumes that you have expertise in installing and using applications in a JBoss cluster. These instructions provide the Oracle Identity Manager-specific details only. They are not complete instructions for setting up a JBoss cluster. For more information on clustering, refer to your JBoss documentation.

Overview: Installing Oracle Identity Manager on a JBoss Cluster

To install Oracle Identity Manager on a JBoss cluster, you must complete the following general tasks:

1. Install Oracle Identity Manager on the first node in your JBoss cluster.

   Refer to "Installing Oracle Identity Manager on the First Node" on page 9-2 for more information.

2. Copy the JBoss and Oracle Identity Manager installation directories from the first node in your JBoss cluster to all other nodes, making sure to maintain the original directory structure during throughout this process.

   Refer to "Copying Oracle Identity Manager to Additional JBoss Nodes" on page 9-2 for more information.

3. Locate the JDBC driver files (mssqlserver.jar, msbase.jar, and msutil.jar) and copy them to the <*JBOSS_HOME*>\server\all\lib directory.

Refer to "Configuring JBoss for SQL Server" on page 4-5 for more information.

4. Set up the load balancer for your JBoss cluster.

   Refer to "Setting up the Load Balancer for JBoss" on page 9-2 for more information.

5. Perform post-installation configuration of Oracle Identity Manager on the JBoss cluster.

   Refer to "Configuring Oracle Identity Manager on the JBoss Cluster" on page 9-5 for more information.

6. Start the cluster.

   Refer to "Starting the JBoss Cluster" on page 9-8 for more information.

Installing Oracle Identity Manager on the First Node

Follow the installation steps for the Oracle Identity Manager server in "Installing the Oracle Identity Manager Server on Windows" on page 5-1 or "Installing the Oracle Identity Manager Server on UNIX or Linux" on page 6-2 to install Oracle Identity Manager on the initial node in your JBoss cluster.

Copying Oracle Identity Manager to Additional JBoss Nodes

For each additional node in your JBoss cluster, copy the JBoss and Oracle Identity Manager installation directories from the first node to all other nodes, making sure to maintain the original directory structure and hierarchy throughout this process.

Setting up the Load Balancer for JBoss

The procedure for installing a load balancer for your JBoss cluster varies according to the operating system running on the host machines where your JBoss nodes are installed:

Setting Up a Load Balancer for JBoss on Windows

To set up a load balancer on Windows:

1. Download the latest distribution package for the Apache2 web server from Apache.org, then install the Apache server in a directory that this document henceforth refers to as <*APACHE_HOME*>.
2. Download the latest distribution package mod_jk 1.2.x from the Tomcat connector section page at the following URL:
   `http://tomcat.apache.org/download-connectors.cgi`.
3. Copy the library named mod_jk.so to the <*APACHE_HOME*>/modules directory.
4. Setup Apache to use modjk by adding the following line (and the accompanying comment line) as the last line of the <*APACHE_HOME*>\conf\httpd.conf file:

   ```
   # Include mod_jk configuration file

   Include conf/mod_jk.conf
   ```

5. In the directory <*APACHE_HOME*>/conf, create a configuration file to forward requests to JBoss instances.

   Name this file mod-jk.conf and populate with the following lines:

   ```
   # Load mod_jk module
   ```

```
# Specify the filename of the mod_jk lib
LoadModule jk_module modules/mod_jk.so
# Where to find workers.properties
JkWorkersFile conf/workers.properties
# Where to put jk logs
JkLogFile logs/mod_jk.log

# Set the jk log level [debug/error/info]
JkLogLevel info
# Select the log format
JkLogStampFormat  "[%a %b %d %H:%M:%S %Y]"
# JkOptions indicates to send SSK KEY SIZE
JkOptions +ForwardKeySize +ForwardURICompat -ForwardDirectories
# JkRequestLogFormat
JkRequestLogFormat "%w %V %T"
# Mount your applications
JkMount /application/* loadbalancer
# You can use external file for mount points.
# It will be checked for updates each 60 seconds.
# The format of the file is: /url=worker
# /examples/*=loadbalancer
JkMountFile conf/uriworkermap.properties
# Add shared memory.
# This directive is present with 1.2.10 and
# later versions of mod_jk, and is needed for
# for load balancing to work properly
JkShmFile logs/jk.shm
# Add jkstatus for managing runtime data
<Location /jkstatus/>
JkMount status
Order deny,allow
Deny from all
Allow from all
</Location>
```

6. Review the directive descriptions at the following URL:

   http://jakarta.apache.org/tomcat/connectors-doc/config/workers.html

   Make sure to observe the guidelines concerning Apache cache size.

   In the directory *<APACHE_HOME>*/conf, create a file named workers.properties and populate it with the following lines:

```
# Define list of workers that will be used
     # for mapping requests
       worker.list=loadbalancer,status
     # Define Node1
     # modify the host as your host IP or DNS name.
       worker.node1.port=8009
       worker.node1.host=<IP of node1>
       worker.node1.type=ajp13
       worker.node1.lbfactor=1
     # worker.node1.local_worker=1 (1)
       worker.node1.cachesize=10
     # Define Node2
     # modify the host as your host IP or DNS name.
       worker.node2.port=8009
       worker.node2.host= <IP of node2>
       worker.node2.type=ajp13
       worker.node2.lbfactor=1
```

```
# worker.node2.local_worker=1 (1)
  worker.node2.cachesize=10
# Load-balancing behavior
  worker.loadbalancer.type=lb
  worker.loadbalancer.balance_workers=node1,node2
  worker.loadbalancer.sticky_session=1
# worker.loadbalancer.local_worker_only=1
# worker.list=loadbalancer
```

7. If your JBoss cluster contains more than two nodes, you need to add extra lines to the workers.properties file in the directory <*APACHE_HOME*>/conf.

   For example, if you have three nodes, you need to add the following lines.

```
# modify the host as your host IP or DNS name.
     worker.node3.port=8009
     worker.node3.host= <IP of node3>
     worker.node3.type=ajp13
     worker.node3.lbfactor=1
   # worker.node3.local_worker=1 (1)
 worker.node3.cachesize=10
```

   For each subsequent node, you need to add the preceding group of lines again, except you must change all references to node3 to node4, node5, or node 6, and so on as appropriate.

8. In the <*APACHE_HOME*>/conf directory, create the file uriworkermap.properties, which will hold the URL mappings Apache forwards to Tomcat.

   Specifically, it enables mod_jk to forward to Tomcat requests from /mx-console, /web-console, /xlWebApp, /xlScheduler as well as /Nexaweb. The syntax for each line is `/url=worker_name`. Paste this example into the file you created:

```
# Simple worker configuration file
     # Mount the Servlet context to the ajp13 worker
     /jmx-console=loadbalancer
     /jmx-console/*=loadbalancer
     /web-console=loadbalancer
     /web-console/*=loadbalancer
     /xlWebApp=loadbalancer
     /xlWebApp/*=loadbalancer
     /xlScheduler=loadbalancer
     /xlScheduler/*=loadbalancer
     /Nexaweb=loadbalancer
     /Nexaweb/*=loadbalancer
```

9. Start Apache by launching Windows Explorer, navigating to the directory <*APACHE_HOME*>/bin, then double clicking Apache.exe.

Setting Up a Load Balancer for JBoss on UNIX or Linux

To set up the load balancer on UNIX or Linux:

1. Download the binary file for Apache 2.0 for UNIX or Linux from the following URL:

   http://httpd.apache.org/download.cgi

2. Run the following commands to install Apache:

   a. `tar xvfz httpd-2.0.54.tar.gz`

   b. `cd httpd-2.0.54`

c. `./configure --prefix=/opt/apache2 --enable-module=so`

d. `make`

e. `make install`

3. Download the file `jakarta-tomcat-connectors-1.2.14-src.tar.gz` from the following URL:
`http://www.apache.org/dist/jakarta/tomcat-connectors/jk/source/jk-1.2.14/`

4. Run the following commands to install the connector:

a. `tar xzvf jakarta-tomcat-connectors-1.2.14-src.tar.gz`

b. `cd jakarta-tomcat-connectors-1.2.14-src/jk/native`

c. `chmod 755 buildconf.sh`

d. `./buildconf.sh`

e. `./configure --with-apxs=/opt/apache2/bin/apxs`

f. `make`

g. `make install`

h. `cd / jakarta-tomcat-connectors-jk1.2.14-src/jk/native/apache-2.0/`

i. `cp mod_jk.so /opt/apache2/modules/`

5. Complete steps 4 to 8 in the procedure "Setting Up a Load Balancer for JBoss on Windows" on page 9-2 as they are the same steps for Windows and UNIX or Linux.

6. Navigate to the <*APACHE_HOME*>\bin\ directory, then run the following command:

```
./apachectl start
```

Configuring Oracle Identity Manager on the JBoss Cluster

After you install Oracle Identity Manager on your JBoss cluster, you must perform certain configuration steps on each node in the cluster.

To configure Oracle Identity Manager on your JBoss cluster:

1. For each successive node in the cluster, navigate to the directory <*JBOSS_HOME*>/server/all/deploy/jbossweb-tomcat55.sar/, open server.xml in a text editor, and perform the following steps:

a. Locate the following string:

```
<Engine name="jboss.web" defaultHost="localhost" jvmRoute
```

b. Change the value of `jvmRoute` to the name of the node associated with the machine on which you are currently working. (The name of the node should be node1, node2, or node3, and so on as listed in the file workers.properties associated with the machine on which you are currently working).

For Example:

```
<Engine name="jboss.web" defaultHost="localhost"
jvmRoute="node1">
```

2. For each successive node in your cluster, navigate to the directory <*JBOSS_HOME*>/ server/all/deploy, then open the following files:

   cluster-service.xml

   tc5-cluster-service.xml

   a. Comment out the following block in both of the preceding files:

```
<!--
<Config>
            <UDP mcast_addr="228.1.2.3" mcast_port="45566" ip_ttl="8" ip_
mcast="true" mcast_send_buf_size="800000" mcast_recv_buf_size="150000"
ucast_send_buf_size="800000" ucast_recv_buf_size="150000"
loopback="false"/>
            <PING timeout="2000" num_initial_members="3" up_thread="true"
down_thread="true"/>
            <MERGE2 min_interval="10000" max_interval="20000"/>
            <FD shun="true" up_thread="true" down_thread="true"
timeout="2500" max_tries="5"/>
            <VERIFY_SUSPECT timeout="3000" num_msgs="3" up_thread="true"
down_thread="true"/>
            <pbcast.NAKACK gc_lag="50" retransmit_
timeout="300,600,1200,2400,4800" max_xmit_size="8192" up_thread="true"
down_thread="true"/>
            <UNICAST timeout="300,600,1200,2400,4800"
window_size="100" min_threshold="10" down_thread="true"/>
            <pbcast.STABLE desired_avg_gossip="20000"
               up_thread="true" down_thread="true"/>
            <FRAG frag_size="8192" down_thread="true" up_thread="true"/>
            <pbcast.GMS join_timeout="5000" join_retry_timeout="2000"
               shun="true" print_local_addr="true"/>
            <pbcast.STATE_TRANSFER up_thread="true" down_thread="true"/>
         </Config>
 -->
```

   b. Uncomment the following block in both files:

```
 <Config>
            <TCP bind_addr="thishost" start_port="7800" loopback="true"/>
            <TCPPING initial_hosts="thishost[7800],otherhost[7800]" port_
range="3" timeout="3500" num_initial_members="3" up_thread="true"
down_thread="true"/>
            <MERGE2 min_interval="5000" max_interval="10000"/>
            <FD shun="true" timeout="2500" max_tries="5" up_thread="true"
              down_thread="true" />
            <VERIFY_SUSPECT timeout="1500" down_thread="false" up_
thread="false" />
           <pbcast.NAKACK down_thread="true" up_thread="true"
gc_lag="100" retransmit_timeout="3000"/>
            <pbcast.STABLE desired_avg_gossip="20000" down_thread="false"
              up_thread="false" />
            <pbcast.GMS join_timeout="5000" join_retry_timeout="2000"
              shun="false"  print_local_addr="true" down_thread="true"
              up_thread="true"/>
            <pbcast.STATE_TRANSFER up_thread="true" down_thread="true"/>
         </Config>
```

   c. Within the block listed in Step b, replace `thishost` with the IP of the machine on which you are currently working.

The entire IP list must be surrounded by double quotes. For example: `TCPbind_addr="192.168.161.20"`.

d. Within the block listed in Step b, replace `otherhost` with the IP of the other machine in the cluster, or, if the cluster contains more than two nodes, replace `otherhost` with a comma-delimited list of all the IPs.

The IP must be surrounded by double quotes.

3. For each successive node in the cluster, modify the <*XL_HOME*>/xellerate/config/xlconfig.xml file.

Locate the setting for the `java.naming.provider.url` in the `<Discovery>` section and insert a comma-delimited list of URLs corresponding to all the nodes in cluster.

For example, you would change a string something like the following:

```
<java.naming.provider.url>
    jnp://localhost:1100
  </java.naming.provider.url>
to the following string:
 <java.naming.provider.url>
    jnp://<IP of node1>:1100,<IP of node 2>:1100
  </java.naming.provider.url>
```

Configuring the JBoss Cluster to Use a Common Database

Perform the following steps on the second and remaining cluster members to configure the cluster to use a common database:

1. Launch a plain-text editor, navigate to the directory <*JBOSS_HOME*>\server\all\deploy-hasingleton\jms\, then open the file <*database_name*>-jdbc2-service.xml.

Note that <*database_name*> refers to the common database used by the cluster.

2. In all the queries and statements in the sqlProperties section of the <*database_name*>-jdbc2-service.xml, change the names of the tables represented by JMS_MESSAGES and JMS_TRANSACTIONS to new, unique, and valid values.

3. Add the following statements to the end of the file:

```
DELETE_TEMPORARY_MESSAGES = DELETE FROM <NEW_JMS_MESSAGES_NAME>
    WHERE TXOP='T'
CREATE_IDX_MESSAGE_TXOP_TXID = CREATE INDEX
    <NEW_JMS_MESSAGES_NAME>_TXOP_TXID ON <NEW_JMS_MESSAGES_NAME> (TXOP, TXID)
CREATE_IDX_MESSAGE_DESTINATION = CREATE INDEX
    <NEW_JMS_MESSAGES_NAME>_DESTINATION ON <NEW_JMS_MESSAGES_NAME>(DESTINATION)
```

Note: <*NEW_JMS_MESSAGES_NAME*> represents the new name of the JMS_MESSAGES tables you changed in step 2.

4. Save and close the file.

Starting the JBoss Cluster

To start the JBoss cluster on which you have installed and configured Oracle Identity Manager:

1. Initially, start only one node in the cluster (commonly referred to as the master node).

   Navigate to the directory <*XL_HOME*>/xellerate/bin, then run one of the following commands, as appropriate for the operating system on the machine hosting the JBoss application server and Oracle Identity Manager:

   On Windows:

   `xlStartServer.bat`

   On UNIX or Linux:

   `xlStartServer.sh`

2. On each remaining machine in the cluster, navigate to the directory <*XL_HOME*>/xellerate/bin, then run one of the following commands, as appropriate for the operating system on the machine hosting the JBoss application server and Oracle Identity Manager:

   On Windows:

   `xlStartServer.bat`

   On UNIX or Linux:

   `xlStartServer.sh`

3. Access the Administration console by launching a browser and pointing it to the following URL

   http://<*IP of machine where apache server is running*>/xlWebApp

10

Installing and Configuring the Oracle Identity Manager Design Console

This chapter explains how to install the Oracle Identity Manager Design Console, which is a Java client. You have the option to install the Design Console on the same computer as your Oracle Identity Manager server or on a separate computer.

This chapter discusses the following topics:

Requirements

Verify that your environment meets the following requirements for 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, you need to 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 using both IP and hostname.
- 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 hostname of the application server, then try adding the hostname and IP address in the hosts file in the directory C:\winnt \system32\drivers\etc\.

Installing the Design Console

The following procedure describes how to install the Design Console.

Important: All Oracle Identity Manager components must be installed in different home directories. If you are installing the Design Console on a machine that is hosting another Oracle Identity Manager component, such as the Oracle Identity Manager server or the Remote Manager, you must specify a different install directory for the Design Console.

To install the Design Console on a Windows host:

1. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.
2. Launch Windows Explorer, then navigate to the installServer directory on the installation CD.
3. Double-click the setup_client.exe file.
4. Choose a language from the list on the Installer screen. The Welcome page appears.
5. On the Welcome page, click **Next**.
6. On the Target directory screen, complete one of the following sub-steps:
   a. The default directory for the Design Console is C:\oracle. To install the Design Console into this directory, click **Next**.
   b. To install the Design Console into another directory, enter the path in the **Directory** field, then click **Next**.

      or

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

      Note: If the directory path that you does not exist, the Base Directory settings text box appears: Click **OK**. Oracle Identity Manager creates this directory for the Oracle Identity Manager server. If you do not have write permission to create the default directory for the Oracle Identity Manager server, a message appears informing you that the installer could not create the directory, Click **OK** to dismiss the message, then contact your System Administrator to obtain the appropriate permissions.
7. On the Application Server page, select JBoss, then click **Next**. The next screen prompts you to specify the JRE to use with Design Console.
8. Select either the JRE that is installed with Oracle Identity manager or specify an existing JRE. Click **Next**. The Application Server configuration screen appears.
9. On the Application Server Host Information page, enter the information appropriate for the application server hosting your Oracle Identity Manager server:
   a. Enter the host name or IP address in the upper field.

      Note: The host name is case-sensitive.

   b. Enter the naming port for the application server on which Oracle Identity Manager is deployed in the lower field.

c. Click **Next**.

10. On the Graphical Workflow Rendering Information page, enter the Application server configuration information:
    a. Enter the Oracle Identity Manager server host IP address.
    b. Enter the port number.
    c. Select **Yes** or **No** to specify whether the Design Console should use SSL.
    d. Click **Next**.
11. On the Shortcut page, select (or deselect) the check boxes for the shortcut options according to your preferences:
    a. Choose to create a shortcut to the Design Console on the Start Menu.
    b. Choose to create a shortcut to the Design Console on the desktop.
    c. Click **Next** when you are satisfied with the check box settings.
12. On the Summary page, click **Install** to initiate Design Console installation.
13. The final installation page displays a reminder to copy certain application server-specific files to your Oracle Identity Manager server installation. Follow these instructions and then click OK.
14. Click **Finish** to complete the installation process.

Removing the Design Console Installation

To remove the Design Console installation:

1. Stop the Oracle Identity Manager server and the Design Console if they are running.
2. Stop all Oracle Identity Manager processes.
3. Delete the <*XL_DC_HOME*> directory where you installed the Design Console.

Post-Installation Requirements for the Design Console

For both clustered and non-clustered installations, copy the <*JBOSS_HOME*>\client\jbossall-client.jar file from the machine hosting your Oracle Identity Manager server to the directory <XL_DC_HOME>\xlclient\ext on the machine where you are installing the Design Console instance.

To complete installation for clustered installations:

1. Change the <Discovery> settings in the <XL_DC_HOME>/xlclient/Config/xlconfig.xml file for all Design Console installations.

   For example, you would change a string like the following:

   ```
   <java.naming.provider.url>
     jnp://localhost:1100
   </java.naming.provider.url>
   ```

   to the following string:

   ```
   <java.naming.provider.url>
     jnp://<IP of node1>:1100,<IP of node 2>:1100
   </java.naming.provider.url>
   ```
2. Add the following tag to Discovery.CoreServer section of the <XL_DC_HOME>/xlclient/Config/xlconfig.xml file:

```
<jnp.partitionName>MyPartition</jnp.partitionName>
```

MyPartition represents the partition name you specified during Oracle Identity Manager on JBoss clusters.

3. To configure Workflow Visualization to access all available nodes in the cluster:
   a. Open the <XL_DC_HOME>/xlclient/Config/xlconfig.xml and locate the following statement:

      ```
      <ApplicationURL>...</ApplicationURL>
      ```

   b. Replace the application server URL with the IP address and port of the Web server, as follows:

      ```
      <ApplicationURL>http://<webserverIP>/xlWebApp/LoginWorkflowRenderer.do
      </ApplicationURL>
      ```

Configuring SSL Communication With the Design Console (optional)

After installing the Oracle Identity Manager Design Console, you may want to configure it to communicate to your Oracle Identity Manager Server over SSL. Use the following procedure to configure communication from your Design Console to the Oracle Identity Manager Server over SSL.

To configure communication from your Design Console to the Oracle Identity Manager Server over SSL:

1. Back up your jboss-<version#> folder.
2. Export the Oracle Identity Manager Server certificate using the following commands:
   a. `cd <XL_HOME>\config`
   b. `%JAVA_HOME%\bin\keytool -export -file xlserver.cer(-keystore .xlkeystore -storepass xellerate -alias xell`

      A file named xlserver.cer is created in the config folder.
3. Open the <*XL_HOME*>\config\xljbossssl-service.xml file:
   a. Find the following line:

      ```
      <attribute name="KeyStorePass"><XDtConfig:configParameter
      ValueparamName="KeyStorePass"/></attribute>
      ```

   b. Change the line to the following:

      ```
      <attribute name="KeyStorePass">xellerate</attribute>
      ```

4. Change the installation profile using the following commands:
   a. `cd <XL_HOME>\profiles`
   b. Open the jboss.profile file and set the following properties:
      - `configure.ssl.invoker=true`
      - `jboss.ssl.invocation=true`
      - `jboss.ssl.port=10443`
      - `jboss.ssl.clustered.port=10444`
      - `jboss.stateful.invoker=xl-stateful-rmi-invoker`

- `jboss.stateless.invoker=xl-stateless-rmi-invoker`

5. Run the setup command by using the following commands:
   a. `cd <XL_HOME>\setup`
   b. `setup_jboss.cmd`
6. Edit the login-config.xml file by using the following commands:
   a. `cd <JBOSS_DIR>\server\default\conf`
   b. Open the login-config.xml file and find the XML tags toward the end in the file that look like the following:

```
<policy>
...
...
...
       <application-policy name= "xellerate">
              <authentication>
              ....
              ....
             </authentication>
       </application-policy>
</policy>
```

   c. You will see two application-policy entries. Remove the last entry.

Note: Be sure to remove the lines starting with <application-policy name="xellerate"> and ending through </application-policy>. Do not remove the last line ending with </policy>.

7. Copy the <*XL_HOME*>\config\xlserver.cer file to <*XL_DC_HOME*>\java\lib\security on all Design Console systems that will communicate with the Oracle Identity Manager server.

   Use the following command to copy the xlserver.cer file:

```
..\..\bin\keytool -import -file xlserver.cer -keystore
cacerts -storepass changeit -trustcacerts -alias xell
```

   When prompted, enter yes to trust the certificate.

8. Copy the <*XL_HOME*>\config\.xlkeystore file to the <*JBOSS_HOME*>\server\default\conf\ directory.
9. Copy the cacerts from the <XL_DC_HOME>\java\lib\security directory to the <*JBOSS_HOME*>\server\default\conf\ directory.
10. Open the <*JBOSS_HOME*>\server\default\deploy\jbossweb-tomcat50.sar\server.xml file:
    a. Find the line that starts with:

```
<!-- SSL/TLS Connector configuration using the admin devl
guide keystore -->
```

    b. Edit the lines in this entry so that it appears as follows:

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore
-->
        <Connector port="8443" address="${jboss.bind.address}"
              maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
              scheme="https" secure="true" clientAuth="false"
```

```
                keystoreFile="${jboss.server.home.dir}/conf/.xlkeystore"
                keystorePass="xellerate"
                truststoreFile="${jboss.server.home.dir}/conf/cacerts"
                truststorePass="changeit"
               sslProtocol = "TLS" />
```

c. Uncomment the entry.

d. Save and close the updated server.xml file.

Starting the Design Console

Double-click <*XL_DC_HOME*>\xlclient\xlclient.cmd or select Design Console from the Windows Start menu or desktop.

11

Installing and Configuring the Oracle Identity Manager Remote Manager

This chapter explains how to install Oracle Identity Manager Remote Manager. It contains the following sections:

Installing the Remote Manager on Windows

The following procedure describes how to install the Remote Manager on Windows.

> **Important:** All Oracle Identity Manager components must be installed in different home directories. If you are installing the Remote Manager on a machine that is hosting another Oracle Identity Manager component (the server or the Design Console), specify an install directory that hasn't been used yet.

To install the Remote Manager on a Windows host:

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

   The Welcome page appears.
5. On the Welcome page, click **Next**.
6. On the Target directory page, complete one of the following sub-steps:
   a. The default directory for Oracle Identity Manager products is C:\oracle. To install Remote Manager into this directory, click **Next**.
   b. To install Remote Manager into another directory, enter the path in the **Directory name** field, and click **Next**.

or

Navigate to the desired location, then click **Next**.

Note: If the directory path that you specified does not exist, the Base Directory settings text box appears: Click **OK**. Oracle Identity Manager creates this directory for the Oracle Identity Manager server. If you do not have write permission to create the default directory for the Oracle Identity Manager server, a message appears informing you that the installer could not create the directory. Click **OK** to dismiss the message, then contact your System Administrator to obtain the appropriate permissions.

---

7. Select either the JRE that is installed with Oracle Identity Manager or specify an existing JRE.

   Click **Next**. The Remote Manager Configuration screen appears.

8. On the Remote Manager Configuration page, enter the appropriate information for the Remote Manager:
   a. Enter the Service Name.
   b. Enter the Remote Manager binding port.
   c. Enter the Remote Manager SSL port.
   d. Click **Next**.
9. On the Shortcut page, select (or deselect) the check boxes for the shortcut options according to your preferences:
   a. Choose to create a shortcut for the Remote Manager on the desktop.
   b. Choose to create a shortcut for the Remote Manager on the Start Menu.
   c. Click **Next** when you are satisfied with the check box settings.
10. On the Summary page, review the configuration details, and then click **Install** to initiate installation.
11. After the installation has completed, click **Finish** on the Completed page to exit.

Installing the Remote Manager on UNIX or Linux

The following procedure describes how to install the Remote Manager on UNIX or Linux.

Note: Before installing the Remote Manager you must set the JAVA_Home variable to Sun JDK 1.4.2_08 or higher. Oracle Identity Manager Release 9.0 supports JDK 1.4.2_08 or higher, for example 1.4.2_xx—but not versions 1.5 or higher.

To install the Remote Manager on UNIX or Linux:

1. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.
2. From the File Manager, access the installServer directory on the installation CD.
3. Run the install_rm.sh file.

The command-line installer starts.

4. Choose a language from the list by entering a number and then entering **0** to apply the language.

   The Welcome panel appears.

5. On the Welcome panel, enter **1** to move to the next panel.

   The Target directory panel appears.

6. On the Target directory panel, enter the path to the directory where 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, you are asked to create it. Enter **y**, for yes.

   Important: All Oracle Identity Manager components must be installed in different home directories. If you are installing the Remote Manager on a machine that is hosting an Oracle Identity Manager server, you must specify a unique install directory.

7. Specify the JRE to use with Remote Manager:

   - Enter 1 to install the JRE bundled with Oracle Identity Manager.
   - Enter **2** to use an existing JRE at a specified location.
   - Enter **0** to accept your selections
   - Enter 1 to move to the next panel.

   The Remote Manager Configuration panel appears.

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

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

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

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

   d. Enter 1 to move to the next panel.

      The Remote Manager installation summary panel appears.

9. Check the information.

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

     Oracle Remote Manager installs and the Post Install Summary panel appears.

10. Enter **3** to finish the installation.

Configuring the Remote Manager

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

Oracle Identity Manager server and the Remote Manager. (The server must trust the Remote Manager certificate).

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

Trusting the Remote Manager Certificate

To configure the Remote Manager:

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

   Note: The server certificate in <*XL_HOME*>\ is also named xlserver.cert, so make sure you do not overwrite that certificate.

2. Open a command prompt on the server computer.
3. To import the certificate using the keytool, use the following command:

   ```
   <JAVA_HOME>\jre\bin\keytool -import -alias rm_trusted_cert -file <RM_cert_
   location>\xlserver.cert -trustcacerts -keystore <XL_
   HOME>\xellerate\config\.xlkeystore -storepass xellerate
   ```

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

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

4. Enter **Y** at the prompt to trust the certificate.
5. Launch a plain-text editor, then open the <*XL_HOME*>\xellerate\config\xlconfig.xml file.
6. Locate the `<RMIOverSSL>` property and set it to `true`, for example:

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

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

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

   or

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

8. Save the file.
9. Restart your application server.

Using Your Own Certificate

Complete the following procedures to use your own certificate.

To configure the Remote Manager Server System to use your own certificate:

1. Import your custom key in a new keystore (new_keystore_name) other than .xlkeystore.

   Be sure to remember the password (new_keystore_pwd) you used for the new keystore.

2. Copy this new keystore to the following directory:

   <*XL_RM_HOME*>\xlremote\config\

3. Open the following file in a text editor:

   <*XL_RM_HOME*>\xlremote\config\xlconfig.xml

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

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

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

   - For all other JREs, change the values to:

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

5. Restart the Remote Manager Server and open xlconfig.xml to make sure the password for the new keystore was encrypted.

To configure the Oracle Identity Manager Server System to use your own certificate:

1. Import the same certificate key used in the Remote Manager system to a new keystore (new_svrkeystore_name) other than .xlkeystore.

   Be sure to remember the password (new_svrkeystor_pwd) you used for the new keystore.

2. Copy this new keystore to the following directory:

   <*XL_HOME*>\xellerate\config

3. Open the following file in a text editor:

   <*XL_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 the Oracle Identity Manager Server and open xlconfig.xml to make sure the password for the new keystore was encrypted.

Enabling Client-side Authentication for Remote Manager

To enable client-side authentication:

1. On the machine hosting the Remote Manager, launch a plain-text editor and open <*XL_RM_HOME*>\xlremote\config\xlconfig.xml
2. Set the `<ClientAuth>` property to `true`, for example:

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

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

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

4. Locate the `<KeyManagerFactory>` property.

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

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

   or

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

5. Save the file.
6. Copy the server certificate to the Remote Manager computer.

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

   Note: The Remote Manager certificate is also named xlserver.cert, so make sure you do not overwrite that certificate.

7. Open a command prompt on the Remote Manager computer.
8. Import the certificate using the keytool, use the following command:

   ```
   <JAVA_HOME>\jre\bin\keytool -import -alias trusted_server_cert -file <server_
   cert_location>\xlserver.cert -trustcacerts -keystore <XL_RM_
   HOME>\xlremote\config\.xlkeystore -storepass xellerate
   ```

   <*JAVA_HOME*> is the location of the Java directory for your Remote Manager, the value of `alias` is an arbitrary name for the certificate in the store, <*XL_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, substitute that value for xellerate, which is the default value of the storepass variable.

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

Starting Remote Manager

Use the following to start the Remote Manager:

- **Windows**: run the following script:

  `<XL_RM_HOME>\xlremote\remotemanager.bat`

- **UNIX or Linux**: run the following script:

  `<XL_RM_HOME>/xlremote/remotemanager.sh`

Removing the Remote Manager Installation

To remove the Remote Manager installation:

1. Stop the Oracle Identity Manager server and the Remote Manager if they are running.
2. Stop all Oracle Identity Manager processes.
3. Delete the <*XL_RM_HOME*> directory where you installed the Remote Manager.

12

Troubleshooting Your Oracle Identity Manager Installation

This section describes problems that can occur during the Oracle Identity Manager Installation and contains the following topics:

- Task Scheduler fails in a Clustered Environment
- Default Login Not Working

> **Tip:** You can use the Diagnostic Dashboard tool to assist when you troubleshoot your Oracle Identity Manager Installation. Refer to the *Oracle Identity Manager Administrative and User Console* for detailed information.

Task Scheduler fails in a Clustered Environment

The Task Scheduler fails to work properly when the cluster members (machines that are part of the cluster) have different settings on their system clocks. Oracle highly recommends that the system clocks for all cluster members be synchronized within a second of each other.

Default Login Not Working

If the default login is not working for the Design Console or Administrative and User Console:

- Make sure that you have copied Jbossall-client.jar to the Design Console computer. (JBoss only)
- Make sure that the Distributed Transaction Coordinator is running (it should have been set as a default). (SQL Server only)

Index

K

L

N

O

P

R

S

T

X