Oracle® Identity Manager

Installation and Upgrade Guide for JBoss

Release 9.0

B25938-01

May 2006

ORACLE®

Oracle Identity Manager Installation and Upgrade Guide for JBoss Release 9.0

B25938-01

Primary Author: Don Biasotti

Contents

5 Database Setup

6 Installing Oracle Identity Manager Server on Windows

7 Installing Oracle Identity Manager Server on Linux

8 Post-Install Configuration for Oracle Identity Manager Server and JBoss

9 Starting the Oracle Identity Manager Server

10 Deploying in a Clustered JBoss Configuration

11 Installing and Configuring Oracle Identity Manager Design Console

12 Installing and Configuring the Oracle Identity Manager Remote Manager

13 Upgrading to Oracle Identity Manager 9.0.1 from Versions 8.5.2 or 8.5.3

Preface

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.

Oracle Identity Manager has formerly been known as both Oracle Xellerate Identity Provisioning and also 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
- upgrade to Oracle Identity Manager 9.0.1 from Oracle Xellerate Identity Provisioning versions 8.5.2, 8.5.3 or 9.0.0

Note: The information in this guide applies generally to all Oracle Identity Manager 9.0.x versions. However, the Upgrade chapters ("Upgrading to Oracle Identity Manager 9.0.1 from Versions 8.5.2 or 8.5.3" and "Upgrading to Oracle Identity Manager 9.0.1 from Version 9.0.0") and Appendix A, "Supplementary Upgrade Information" contain version specific information about Oracle Identity Manager.

Audience

The *Oracle Identity Manager Installation and Upgrade Guide* is intended for System Administrators who plan to install Oracle Identity Manager 9.0 on a JBoss application server, or upgrade from Oracle Xellerate Identity Provisioning versions 8.5.2, 8.5.3, or 9.0.0 running on JBoss to Oracle Identity Manager 9.0.1.

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 Release Notes*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Best Practices 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. Where needed to distinguish between Oracle Identity Manager versions, you may see 85x or 900 included in the directory convention. For example <XL_85x_HOME>, which refers to directory where Oracle Identity Manager version 8.5.2 or 8.5.3 is installed, and <XL_900_DC_HOME>, which refers to the directory where the Oracle Identity Manager Design Console version 9.0.0 is installed. Examples of this convention include the following: <JBOSS_HOME>, <XL_HOME>, <XL_DC_HOME>, <XL_RM_HOME>, <XL_85x_HOME>, <XL_85x_DC_HOME>, <XL_85x_RM_HOME>, <XL_900_HOME>, <XL_900_DC_HOME>, and <XL_900_RM_HOME>.

<xml_tag_level1>.<xml_tag_level2>.
.<xml_tag_level3>.<xml_tag_level4>.
	In the XML file, the embedded tag levels (multiple levels) are depicted as single line because the size of some xml mark-up is too big to display as it is in the file. For example:
	
	`<xml_1>wwwwwwwww</xml_1>`
	`<xml_2>xxxxxxxxx</xml_2>`
	`<xml_3>yyyyyyyyy</xml_3>`
	`<xml_4>zzzzzzzzz</xml_4>`
	
	Is shown in this document as:
	
	`<xml_1>.<xml_2>.<xml_3>.<xml_4>`

1
Introduction

This chapter provides a brief introduction to the Oracle Identity Manager product and its architecture.

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.

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

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:

- Custom Client applications
- Design Console
- Administrative and User Console

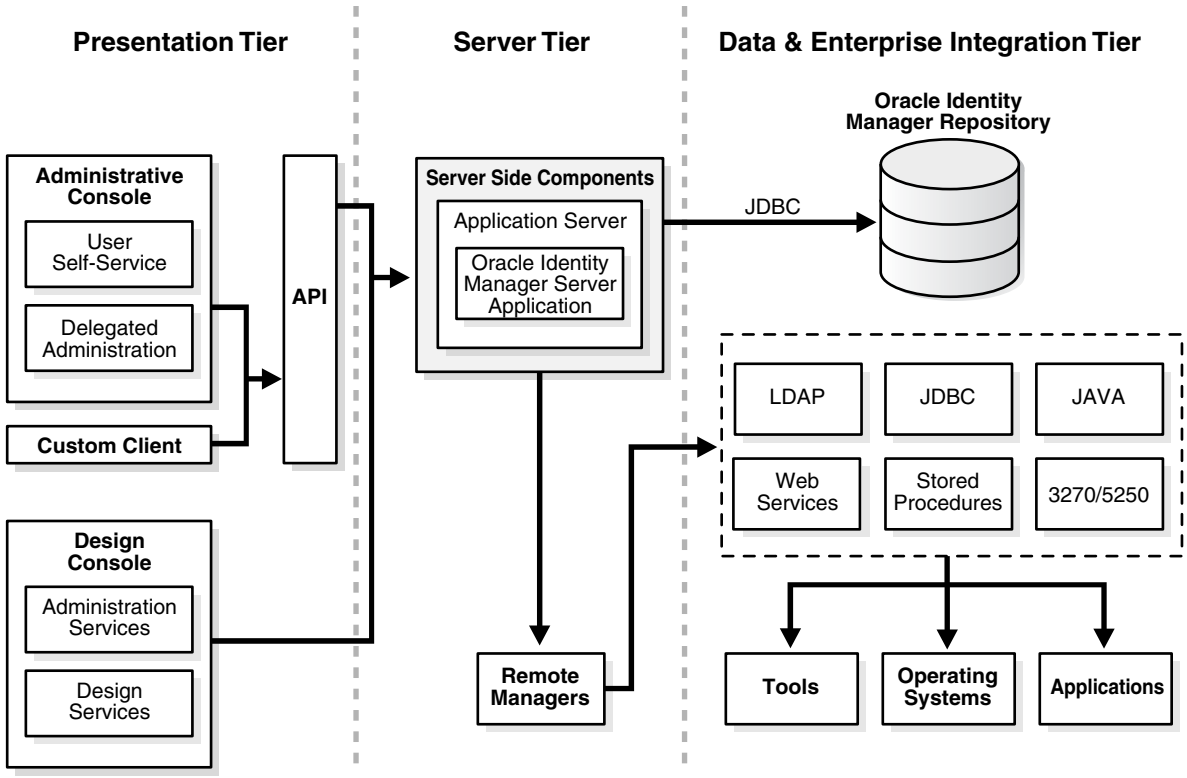
The Server tier contains the Oracle Identity Manager Server component, which serves as a bridge between the Presentation and Data and Enterprise Integration tiers. All requests between the clients and the database are processed through the Server tier.

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



Software

The Oracle Identity Manager system consists of Oracle Identity Manager software deployed in combination with certain external software. These software components can be deployed on one or more host machines that meet the supported requirements. See "Hardware and Software Requirements" on page 2-1 for more information.

2

Planning the Installation or Upgrade to 9.0.1

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 2-7 for more information.

Installation Components

A typical Oracle Identity Manager deployment consists of the following:

- Oracle Identity Manager software
- An application server
- A database

The following sections describe the hardware and software needed for a basic Oracle Identity Manager installation, which 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)

Hardware and Software Requirements

Important: The information in this guide applies generally to all Oracle Identity Manager 9.0.x versions. 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 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: There is a possibility that the Oracle Identity Manager installation program may conflict with previously installed applications, utilities, or drivers. Therefore, try to remove all non-essential software and drivers from the installation machine before loading Oracle Identity Manager. The same practice should be followed to ensure that the database host can create the database schema.

Supported JBoss Application Servers

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

Important: The JBoss installer requires JDK version 1.4.2_08 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
- RedHat Linux AS 4.1

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
- Microsoft SQL Server 2000 with Service Pack 3a

Note: Certain limitations have been identified in Microsoft SQL Server 2000 Service Pack 4. For details, check the Microsoft Web site.

Host System Requirements for Oracle Identity Manager Components

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

Oracle Identity Manager Server Host Requirements

Table 2–1 lists the host requirements for Oracle Identity Manager Server:

Table 2–1 Oracle Identity Manager Server Host Requirements

Server Platform	Item
Windows	■ **Processor Type**: Intel Xeon or Pentium IV ■ **Processor Speed**: 2.4 GHz or higher, 400 MHz FSB or higher ■ **Number of Processors**: 1 (or more, if needed) ■ **Memory**: Use whichever is greater: 2 GB (or more, if needed) or 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
Linux	■ **Processor Type**: Intel Xeon or Pentium IV ■ **Processor Speed**: 2.4 GHz or higher, 400 MHz FSB or higher ■ **Number of Processors**: 1 (or more, if needed) ■ **Memory**: Use whichever is greater: 2 GB (or more, if needed) or 2 GB for each Oracle Identity Manager Server instance ■ **Hard Disk Space**: 20 GB (initial size) ■ **Operating System**: RedHat Linux AS 4.1

Database Server Host Requirements

Table 2–2 provides sample database host requirements for selective supported operating systems and should be considered only as guidelines. 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	■ **Processor Type**: Intel Xeon ■ **Processor Speed**: 2.4 GHz or higher, 400 MHz FSB or higher ■ **Number of Processors**: 2 (or more, if needed) ■ **Memory**: 2 GB for each CPU (or more, if needed) ■ **Hard Disk Space**: 40 GB (initial size) ■ **Operating System**: Microsoft Windows 2000 (Server, Advanced Server, Professional), Windows 2003 Server SP1 and Windows XP

Table 2–2 (Continued)Sample Database Server Host Requirement

Database Server	
Platform	**Item**
Linux	■ **Processor Type**: Intel Xeon ■ **Processor Speed**: 2.4 GHz or higher, 400 MHz FSB or higher ■ **Number of Processors**: 2 (or more, if needed) ■ **Memory**: 2 GB for each CPU (or more, if needed) ■ **Hard Disk Space**: 20 GB (initial size) ■ **Number of Hard Disks**: 1 Disk (or more, as data grows and if needed) ■ **Operating System**: RedHat Linux AS 4.1

Design Console Host Requirements

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

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 host requirements for the Oracle Identity Manager Remote Manager:

Table 2–4 Remote Manager Host Requirements

Remote Manager	
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**: Microsoft Windows 2003 Server SP1
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**: RedHat Linux AS 4.1

Table 2–4 (Continued)Remote Manager Host Requirements

Remote Manager Platform	Item
Solaris	▪ **Sun Fire V100 Server** ▪ **Number of Processors**: 1 (or more, if needed) ▪ **Memory**: 512 MB (or more, if needed) ▪ **Hard Disk Space**: 10 - 20 GB (or more, if needed) ▪ **Software**: IBM WebSphere Application Server ▪ **Operating System**: Solaris 10
AIX	▪ **Processor Type**: PowerPC ▪ **Number of Processors**: 1 (or more, if needed) ▪ **Memory**: 512 MB (or more, if needed) ▪ **Hard Disk Space**: 10 - 20 GB (or more, if needed) ▪ **Software**: IBM WebSphere Application Server ▪ **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, include clustering
Oracle 10g Release 2	10.2.0.1.0
Oracle9i	9.2.0.7
SQL Server	2000, with SP3a
Microsoft Windows Server	2003 Enterprise Edition SP1
RedHat Linux	AS 4.1
Sun JDK	1.4.2_08 or higher
Microsoft Internet Explorer	6.x

Before You Start

Before installing Oracle Identity Manager, you should read "Hardware and Software Requirements" on page 2-1 and "Installation Worksheet" on page 2-6 to help plan your installation.

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
IT Developer	■ Planning Your Installation (this section) ■ Oracle Identity Manager Installation ■ Installing the Design Console

Installation Worksheet

The Installation Worksheet table 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

Check Box	Item	Default	User Selection
	The base directory for installing Oracle Identity Manager.	Windows: C:\Oracle 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*> Linux: /opt/j2sdk<*version*>	
	The JBoss install directory	Windows: C:\jboss-<*version*> 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*.

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 Java Virtual Machine (JVM)
- A supported Database
- Database Encryption Key Generation

3

Installation Overview

To deploy the Oracle Identity Manager system, you must install and configure certain third-party software, including a database and an application server. You must also install the Oracle Identity Manager software, including the following components:

- Oracle Identity Manager Server
- Oracle Identity Manager Design Console
- Oracle Identity Manager Remote Manager

To install and configure Oracle Identity Manager for JBoss:

1. Install the Java JDK—see "Installing the Java JDK" on page 4-1 for more information.
2. Install JBoss—see "Installing JBoss" on page 4-1 for more information.
3. Set memory parameters—see "Setting Memory Parameters" on page 4-2 for more information.
4. If desired, set up and use the Diagnostic Dashboard—see "Using the Diagnostic Dashboard" on page 2-7 for more information.
5. Install and setup your database:

   Oracle

   a. Install Oracle—see "Installing Oracle" on page 5-1 for more information.

   b. Create your Oracle database—see "Creating an Oracle Database" on page 5-1 for more information.

   c. Prepare the Oracle database—see "Preparing the Oracle Database" on page 5-2 for more information.

   SQL Server

   a. Install the SQL Server—see "Installing and Configuring SQL Server" on page 5-4 for more information.

   b. Copy the Microsoft JDBC driver for SQL Server—see "Setting Up JBoss with SQL Server" on page 5-5 for more information.

   c. Register the SQL Server—see "Registering SQL Server" on page 5-5 for more information.

   d. Create an SQL Server database—see "Creating an SQL Server Database" on page 5-6 for more information.

   e. Create an SQL Server database account—see "Creating an SQL Server Database Account" on page 5-7 for more information.

6. Install Oracle Identity Manager components:

   Windows

   a. Install the Oracle Identity Manager Server—see "Installing the Oracle Identity Manager Server on Windows" on page 6-2 for more information.

   b. Install the Oracle Identity Manager Design Console—see "Installing the Design Console" on page 11-1 for more information.

   c. Install the Oracle Identity Manager Remote Manager—see "Installing the Remote Manager for Windows" on page 12-1 for more information.

   Linux

   a. Install the Oracle Identity Manager Server—see "Installing the Oracle Identity Manager Server on Linux" on page 7-2 for more information.

   b. Install the Oracle Identity Manager Remote Manager—see "Installing the Remote Manager for Linux" on page 12-2 for more information.

7. (Optional) Change keystore passwords—see "Changing Keystore Passwords (optional)" on page 8-1 for more information.

8. Configure the Remote Manager—see "Configuring the Remote Manager" on page 8-1 for more information.

9. Copy the appropriate JBoss jar files to the Design Console—see "Post-Installation Requirements for the Design Console" on page 11-3 for more information.

10. (Optional) Set log levels—see "Setting Log Levels (optional)" on page 8-2 for more information.

11. Configure multiple JBoss installations to use a single database—see "Configuring Multiple JBoss Installations to Use a Single Database" on page 8-4 for more information.

12. Enable Single Sign-On—see "Enabling Single Sign-On (SSO)" on page 8-4 for more information.

13. Start Oracle Identity Manager—As appropriate to the machine hosting your Oracle Identity Manager installation, complete the steps in one of the sub-sections that follow:

    Windows

    a. Start the Oracle Identity Manager Server—see"Starting Oracle Identity Manager on Windows" on page 9-1 for more information.

    b. Start the Design Console—see "Starting the Design Console" on page 11-5 for more information.

    c. Start the Administrative and User Console—see "Starting the Administrative and User Console on Windows" on page 9-2 for more information.

    Linux

    a. Start the Oracle Identity Manager Server—see "Starting Oracle Identity Manager on Linux" on page 9-2 for more information.

    b. Start the Administrative and User Console—see "Starting the Administrative and User Console on Linux" on page 9-2 for more information.

4

Installing and Configuring JBoss for Oracle Identity Manager

This chapter explains how to set up JBoss before for Oracle Identity Manager. You must perform the following tasks:

1. Install the Java JDK—see "Installing the Java JDK" on page 4-1 for more information.
2. Install JBoss—see "Installing JBoss" on page 4-1 for more information.
3. Set memory parameters—see "Setting Memory Parameters" on page 4-2 for more information.

> **Note:** See Chapter 10, "Deploying in a Clustered JBoss Configuration" on page 10-1 for information about preparing to deploy Oracle Identity Manager in a JBoss cluster.

Installing the Java JDK

To use JBoss with Oracle Identity Manager, you must have **j2sdk1.4.2_08 or higher** already installed on your computer.

To verify that the correct version of the Java JDK has been installed on your machine, complete the following steps:

1. Open a console window.
2. Type **java -version**

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

```
C:\>java -version
java version "1.4.2_08"
Java(TM) 2 Runtime Environment, Standard Edition (build 1.4.
Java HotSpot(TM) Client VM (build 1.4.2_08-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 a copy of JBoss 4.0.2 from: http://www.sourceforge.net

Setting Environment Variables

After you have verified that j2sdk1.4.2_08 or higher is installed on your computer, complete the following steps to set your environment variables:

Note: The following instructions are for Windows. For Linux, use the equivalent shell variable commands and settings.

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

   In the text box labelled **Variable Value**, add **the location of your JDK** to the end of the existing path.

   For example, if your existing path is something like the following:

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

   You change it to something like the following:

   ```
   c:\j2sdk1.4.2_08\bin;%SystemRoot%\system32;%SystemRoot%;C:\Program Files
   ```

   Click **OK** to commit your change.

2. In the scroll box labelled **System Variables**, search for **JAVA_HOME**. If it does not exist, complete Step **a**. If JAVA_HOME does exist, complete Step **b**.

   a. Click **New**. In the text box labelled **Variable Name**, type **JAVA_HOME**, In the text box labelled **Variable Value**, type the **path to your JDK**. Click **OK** to commit your entry, then click **OK** twice more to close the Environment Variables and System Properties dialogs, respectively.

   b. Click **Edit**. Verify that the **path to your JDK** exists in the text box labelled **Variable Value**. If it does not, set **Variable Value** to the **path for your JDK**. Click **OK** to commit your entry, then click **OK** twice more to close the Environment Variables and System Properties dialogs, respectively.

   Note: A pop-up window may appear displaying a message asking if you want to update the JDK. Close this window without updating the JDK, since you previously verified that **j2sdk1.4.2_08 or higher** is installed on your computer.

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 Windows or Linux.

Setting Memory Allocation for Windows

To set JBoss memory on a Windows host, complete the following steps:

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 Linux

To set the memory allocation for JBoss on Linux, complete the following steps:

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

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

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

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

4. Save and close the run.sh file.

5

Database Setup

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:

Setting Up the Oracle Database

To use Oracle for your database, you must:

1. Install Oracle—see "Installing Oracle" on page 5-1 for more information.
2. Create your Oracle database—see "Creating an Oracle Database" on page 5-1 for more information.
3. Prepare the Oracle database—see "Preparing the Oracle Database" on page 5-2 for more information.

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 **Typical** 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" screen of the DBCA.

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

Preparing the Oracle Database

Once 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:

- prepare_xl_db.sh (for Linux)
- prepare_xl_db.bat (for Windows)

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

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 Linux typically holds these privileges).
- The script must be run on the machine where the database resides.

To prepare your Oracle database for Oracle Identity Manager, complete the steps associated with the operating system on the machine hosting your Oracle database:

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 execute permission for the script:

   ```
   $ chmod 755 prepare_xl_db.sh
   ```

3. Run the script **prepare_xl_db.sh** 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.

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 type 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
```

where, “XELL” is the database name, “C:\oracle\ora92” is ORACLE_HOME, “xladm” is the name of the Oracle Identity Manager user to be created, “xladm” is the password for the Oracle Identity Manager user, “xeltbs” is the name of the tablespace to be created, “C:\oracle\oradata” is the directory where the datafiles will be placed, “xeltbs_01” is the name of the datafile (you do not need to give .dbf extension), “TEMP” is the name of the temporary tablespace that already exists in your database, and “manager” is the 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.

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.

Setting Up the SQL Server

To use SQL Server for your database, you must:

1. Install the SQL Server—see "Installing and Configuring SQL Server" on page 5-4 for more information.

2. Copy the Microsoft JDBC driver for SQL Server—see "Setting Up JBoss with SQL Server" on page 5-5 for more information.
3. Register the SQL Server—see "Registering SQL Server" on page 5-5 for more information.
4. Create an SQL Server database—see "Creating an SQL Server Database" on page 5-6 for more information.
5. Create an SQL Server database account—see "Creating an SQL Server Database Account" on page 5-7 for more information.

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, complete the following steps:

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 something like the following:

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

   <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.

Setting Up JBoss with 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**

where <*JBOSS_HOME*> is the home directory of your JBoss installation.

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

Registering SQL Server

Use the following steps 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 on 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. Type 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 text box labelled **Login name**, type **the account name used to connect to your SQL server**. Typically, this is **sa**.

b. In the **Password** text box, type 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 drop-down list labelled **Group name**, then click **Next**.

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

Creating an SQL Server Database

Complete the following steps to create a new database for Oracle Identity Manager:

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 type **XELL** in the text box labelled **Name**.

> **Note:** 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.

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 5–1.

> **Note:** Table 5–1 lists initial sizes for a production environment. For non-production installations, you can use the default initial sizes provided for the filegroups.

Table 5–1 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: To ensure successful installation of Oracle Identity Manager, filegroup names must be entered exactly as they appear in Table 5–1. 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 type **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 an SQL Server Database Account

Complete the following procedure 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.

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 type **xladm** (or whatever account name you prefer).
5. Select **SQL Server Authentication**, then type the **password** associated with the account you specified in the Password text box.
6. In the Database combo box within the Defaults section, select **XELL** from the drop-down list. Leave the Language text 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.

6

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.

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

Oracle Identity Manager Components

Oracle Identity Manager for Windows includes the following components:

- Oracle Identity Manager Server—see "Installing the Oracle Identity Manager Server on Windows" on page 6-2 for more information.
- Oracle Identity Manager Design Console—see Chapter 11, "Installing and Configuring Oracle Identity Manager Design Console" on page 11-1 for more information.
- Oracle Identity Manager Remote Manager—see "Installing the Remote Manager for Windows" on page 6-2 for more information.

All components use a single database schema. Oracle Identity Manager documentation is also installed with each component.

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.

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. On the Welcome Message screen, click **Next**.
5. On the Oracle Identity Manager Application Options screen, select to install one of the following applications, and then click **Next**:
   - Oracle Identity Manager
   - Oracle Identity Manager with Audit and Compliance Module

   ---

   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 backup 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.

   ---

6. 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 popup appears informing you that the installer could not create the directory. Click **OK** to dismiss the popup, then contact your System Administrator to obtain the appropriate permissions.

---

7. 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**.
8. 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 this version of Oracle Identity Manager supports your existing database version.

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 **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 "Setting Up the Oracle Database" on page 5-1 or "Setting Up the SQL Server" on page 5-3 to be sure you set consistent information.

The installer checks for database connectivity as well as the existence of a database schema. A success or failure page appears, depending on the results of the test.

- Select the appropriate database options:
  - If a database exists, and the connectivity is good, proceed to Step 9.
  - 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.

9. On the Authentication Information page, select either the **Oracle Identity Manager Default Authentication** or **SSO** (Single Sign On) **Authentication** option. If you select SSO authentication, you must provide the header value in the field. Click **Next** after providing the header value.
10. On the Application Server Selection page, select **JBoss**, then click **Next**.
11. On the Cluster Information page, specify the server configuration (clustered or non-clustered). Select **No** (non-clustered) and click **Next**.

    Important: If you are deploying in a clustered environment, select **Yes**, enter the unique partition name, and see Chapter 10, "Deploying in a Clustered JBoss Configuration" on page 6-1 for more information.

12. On the Application Server Information page, enter the information pertaining to your application server and Java installation:
    a. Type the **path to your application server** installation

       or

       Navigate to your application server installation

    b. Type the **path to your JDK directory**

       or

       Navigate to your JDK directory

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

    c. Click **Next**.
13. Backup your application server when the Application Server Configuration Backup screen appears, then click **Next** to initiate server installation.
14. 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**.
15. The Summary screen appears. Click **Install** to install the application.
16. The Completed screen appears. Click **Finish** to exit the installer.

After installing the Oracle Identity Manager server, perform the steps in Chapter 8, "Post-Install Configuration for Oracle Identity Manager Server and JBoss" on page 8-1 to continue the installation process.

7

Installing Oracle Identity Manager Server on Linux

This chapter explains how to install Oracle Identity Manager on Linux. 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.

Note: Oracle Identity Manager is certified for RedHat Linux 4.1.

Oracle Identity Manager Components

Oracle Identity Manager for Linux includes the following components:

- Install the Oracle Identity Manager Server—see "Installing the Oracle Identity Manager Server on Linux" on page 7-2 for more information.
- Install the Oracle Identity Manager Remote Manager—see "Installing the Remote Manager for Linux" on page 12-2 for more information.

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 Linux

Note: Before installing Oracle Identity Manager server, be sure to copy the three Microsoft SQL Server JDBC driver .jar files to the Linux server and add the files to the CLASSPATH.

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

- Choose from among list of options

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

- Enter information at a prompt

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

The installer contains logical sections (panels).

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

Note: Before installing Oracle Identity Manager you must set the JAVA_HOME variable to Sun JDK 1.4.2 or higher.

To install Oracle Identity Manager server for 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
   ```

4. The installer starts in console mode, and the product Welcome Message panel appears.

a. Type **1** to display the next panel. The Oracle Identity Manager Application Options panel appears.

b. Type **1** to display the next panel. The Application Selection panel appears.

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
```

---

5. Select the application to install:

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

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

6. On the Target directory panel, complete one of the sub-steps that follow:

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 backup 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.

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

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

   The Database Server Selection panel appears.

Note: To install against an existing database, make sure that this version of Oracle Identity Manager supports your existing database version.

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.

---

7. On the Database Server Selection panel, specify the type of database you are using.

- Type **1** for **Oracle**.
- Type **2** for **SQL Server**.
- Type **0** when you are finished.
- Type **1** to move to the next panel.

8. Enter your database information:
   a. Enter the database **host name** or **IP address**.
   b. Enter (or accept the default) **port number**.
   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. Type **1** to move to the next panel.

   The Authentication Information panel appears.
9. Select the authentication mode for the Oracle Identity Manager web application.
   - Type **1** for Oracle Identity Manager **Default Authentication**.
   - Type **2** for **SSO** Authentication.
   - Type **0** when you are finished.
   - If you selected SSO mode, provide the **header value** at the prompt.
   - Type **1** to move to the next panel.

   The Application Server Selection panel appears.
10. Specify your application server type.
    - Type **4** for **JBoss**.
    - Type **0** when you are finished.
    - Type **1** to move to the next panel.

    The Cluster Information panel appears.
11. Provide the following information regarding deploying in a cluster:
    - Type **1** for **Yes** (clustered) and enter the unique **partition name** at the prompt.
    - Type **2** for **No** (non-clustered).
    - Type **0** when you are finished.
    - Type **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 10, "Deploying in a Clustered JBoss Configuration" on page 10-1 for more information.

12. In the Application Server Information panel:
    - Provide the location where the application server is installed

- Provide the location where the JDK is installed
- Type **1** to move to the next section.

13. When you receive a message about backing up the application server installation, type **1** to move to the next section. The Summary panel appears.
14. On the Summary panel, type **1** to begin installation.
15. After the installation is finished, the Completed panel appears. Type **3** finish and exit.

After installing the Oracle Identity Manager server, perform the steps in Chapter 8, "Post-Install Configuration for Oracle Identity Manager Server and JBoss" on page 8-1 to continue the installation process.

8

Post-Install Configuration for Oracle Identity Manager Server and JBoss

After you have installed Oracle Identity Manager, you must complete some post-installation tasks before you can use the application. Some of these tasks are common to all types of Oracle Identity Manager component installations; others are application server-specific tasks. This chapter describes:

- "General Post-installation Tasks" on page 8-1 for all Oracle Identity Manager installations
- "Post-installation Tasks for JBoss" on page 8-4

General Post-installation Tasks

For any Oracle Identity Manager installation, you must change the keystore passwords from their defaults. If you are using a Remote Manager, you must enable a trust relationship between the Remote Manager and the Oracle Identity Manager server. Several of these tasks are optional and not required for system operation.

Changing Keystore Passwords (optional)

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*. You can use the keytool to change the keystore password for either keystore. Oracle recommends changing the keystore passwords for all production installations.

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
   ```

   Where <JAVA_HOME> is the location of the Java directory associated with your application server, <new_password> is the new password for the keystore, the keystore option is the keystore whose password you are changing the (.xlkeystore for the Oracle Identity Manager server, or .xldatabasekey for the database), and and the storetype option is JKS for .xlkeystore and JCEKS for .xldatabasekey.
4. Launch a plain-text editor, then open the file **xlconfig.xml**, which is located in the directory **<XL_HOME>\xellerate\config**.

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 (optional)

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 8-2 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.

Post-installation Tasks for JBoss

If you are using JBoss for your application server, you must configure Oracle Identity Manager specifically for JBoss.

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. To accomplish this, complete the following steps for the second and all other JBoss instances using the same Oracle Identity Manager database:

1. Launch a plain-text editor, navigate to the directory <**JBoss_Home**>/**server**/<**config**>/**deploy**/**jms**, then open the file <**database_name**>**-jdbc2-service.xml**, where <JBoss_Home> is the root installation directory for a given JBoss instance, and <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 file you just opened, change to new, unique, and valid values the names of the tables represented by **JMS_NAMES** and **JMS_TRANSACTIONS**.
3. Add the following statements to the end of the file:

```
DELETE_TEMPORARY_MESSAGES = DELETE FROM TABLE
     WHERE TXOP='T'
CREATE_IDX_MESSAGE_TXOP_TXID = CREATE INDEX
     TABLE_TXOP_TXID ON TABLE (TXOP, TXID)
CREATE_IDX_MESSAGE_DESTINATION = CREATE INDEX
     TABLE_DESTINATION ON TABLE(DESTINATION)
```

4. Save and close the file.
5. Repeat the preceding steps for all remaining JBoss instances that point to the same database.

Enabling Single Sign-On (SSO)

Use the following steps to enable SSO for Oracle Identity Manager:

1. Stop the application server gracefully.
2. Launch a plain-text editor and open the <**XL_HOME**>**xellerate****config****xlconfig.xml** file.
3. Locate the following SSO configuration (these are the default settings without SSO):

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

4. Edit the SSO configuration to be the following:

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

   Replace <**SSO_HEADER_NAME**> with the appropriate header configured in your SSO system.

5. Change your application server and web server configuration to enable SSO. Refer to your application and web server vendor documentation for detailed instructions.
6. Restart the application server.

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

9

Starting the Oracle Identity Manager Server

This chapter, describes how to start the Oracle Identity Manager server for Windows and Linux.

> **Important:** You must complete all post-installation steps in Chapter 8, "Post-Install Configuration for Oracle Identity Manager Server and JBoss" on page 8-1 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 Oracle Identity Manager on Windows

This section describes how to start Oracle Identity Manager on Windows. Start up consists of the following basic steps:

1. Verify that your database is up and running
2. Start your application server
3. Start at least one of the Oracle Identity Manager client components.

Starting the Oracle Identity Manager Server

Run the **<XL_HOME>\xellerate\bin\xlStartServer.bat** command script.

Starting the Administrative and User Console on Windows

Once your application server is up and running, you can start your Administrative and User Console.

To start 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**.

Starting Oracle Identity Manager on Linux

This section describes how to start Oracle Identity Manager on Linux. The process consists of the following steps:

1. Verify that your database is up and running
2. Start your application server
3. Start one or more Oracle Identity Manager components

Starting the Oracle Identity Manager Server

Run the **<XL_HOME>/xellerate/bin/xlStartServer.sh** shell script.

Starting the Administrative and User Console on Linux

Once your application server is up and running, you can start your Administrative and User Console.

To start the Administrative and User Console:

1. Open your web browser, and enter the following URL:

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

   where <hostname> is the name of the machine hosting the application server, and <port> is 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 is **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 2-7 for more information.

10

Deploying in a Clustered JBoss Configuration

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

> **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.
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.
3. Locate the JDBC driver files (mssqlserver.jar, msbase.jar, and msutil.jar) and copy them to the <JBOSS_HOME>\server\all\lib directory.
4. Set up the load balancer for your JBoss cluster.
5. Perform post-installation configuration of Oracle Identity Manager on the JBoss cluster
6. Start the cluster.

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 6-2 or "Installing the Oracle Identity Manager Server on Linux" on page 7-2 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

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: 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 (as well as the accompanying comment line) as the last line of the **httpd.conf** file, which is located in the <APACHE_HOME>\conf directory:

   ```
   # 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 Linux

1. Download the binary file for Apache 2.0 for Linux from: http://httpd.apache.org/download.cgi
2. Execute 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. Execute 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/apache/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 5-7 in the procedure "Setting Up a Load Balancer for JBoss on Windows" on page 10-2 as they are the same steps for Windows and Linux.

6. Navigate to the directory <APACHE_HOME>\bin, then execute 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.

1. For each successive node in the cluster, navigate to the directory <**JBOSS_HOME**>/ **jboss-4.0.2/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 file **xlConfig.xml**, which resides in the directory `<XL_HOME>/xellerate/config`

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>
```

Starting the JBoss Cluster

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

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 execute one of the following commands, as appropriate for to the operating system on the machine hosting the JBoss application server and Oracle Identity Manager:
   - **xlStartServer.bat** (for Windows)
   - **xlStartServer.sh** (for non-Windows systems)
2. On each remaining machine in the cluster, navigate to the directory <**XL_HOME**>/**xellerate**/**bin**, then execute one of the following commands, as appropriate for to the operating system on the machine hosting the JBoss application server and Oracle Identity Manager:
   - **xlStartServer.bat** (for Windows)
   - **xlStartServer.sh** (for non-Windows systems)
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
   ```

11

Installing and Configuring Oracle Identity Manager Design Console

This section 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.

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

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. On the Welcome page, click **Next**.
5. On the Target directory screen, complete one of the following sub-steps:

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), specify an install directory that hasn't been used yet.

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, type 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 popup appears informing you that the installer could not create the directory, Click **OK** to dismiss the popup, then contact your System Administrator to obtain the appropriate permissions.

6. On the Application Server page, select JBoss, then click **Next**. The next screen prompts you to specify the JRE to use with Design Console.
7. Select either the JRE that is installed with Oracle Identity manager or specify an existing JRE. Click **Next**. The Application Server configuration screen appears.
8. On the Application Server Host Information page, enter the information appropriate for the application server hosting your Oracle Identity Manager server:
   a. Type the **host name** or **IP address** in the upper text box.
   b. Type the **naming port** for the application server on which Oracle Identity Manager is deployed in the lower text box.

   Note: The host name is case-sensitive.

   c. Click **Next**.
9. 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**.
10. 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.

11. On the Summary page, click **Install** to initiate Design Console installation.

12. 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.

13. Click **Finish** to complete the installation process.

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.

Perform the following steps for clustered installations:

1. Change the <Discovery> settings in the **<XL_DC_HOME>/xellerate/config/xlconfig.xml** file for all Design Console installations.

   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>
   ```

2. Add the following tag to Discovery.CoreServer section of the Design Console's xlconfig.xml file, located in the <XL_DC_HOME>/xellerate/config directory:

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

   where "MyPartition" is 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.com</Ap
   plicationURL>
   ```

Configuring Design Console Communication to the Oracle Identity Manager Server Over SSL (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 steps to configure communication from your Design Console to the Oracle Identity Manager Server over SSL:

1. Backup 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.

12

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 for Windows

Complete the following steps 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. On the Welcome page, click **Next**.
5. On the Target directory page, complete one of the following sub-steps:

   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.

   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 popup appears informing you that the installer could not create the directory. Click **OK** to dismiss the popup, then contact your System Administrator to obtain the appropriate permissions.

6. Select either the JRE that is installed with Oracle Identity Manager or specify an existing JRE. Click **Next**. The Remote Manager Configuration screen appears.
7. On the Remote Manager Configuration page, enter the appropriate information for the Remote Manager:
   a. Type the **Service Name**.
   b. Type the Remote Manager **binding port**.
   c. Type the Remote Manager **SSL port**.
   d. Click **Yes** to specify that the Remote Manager uses SSL to communicate with the server.

   Note: The **No** option for using non-SSL communication between the Remote Manager and the server is not supported and is displayed by the installer only for backward compatibility. Do not select the No option.

   e. Click **Next**.
8. 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.
9. On the Summary page, review the configuration details, and then click **Install** to initiate installation.
10. After the installation has completed, click **Finish** on the Completed page to exit.

Installing the Remote Manager for Linux

To install the Remote Manager on Linux:

Note: Before installing the Remote Manager you must set the JAVA_Home variable to Sun JDK 1.4.2 or higher.

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.

4. The command-line installer starts, and the Welcome panel appears. Type 1, to move to the next panel.

   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.

5. 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.
   - Type **1**, to move to the next panel.
   - If the directory does not exist, you are asked to create it. Type **y**, for yes.
6. Specify the JRE to use with Remote Manager:
   - Type **1** to install the JRE bundled with Oracle Identity Manager.
   - Type **2** to use an existing JRE at a specified location.
   - Type **0** to accept your selections
   - Type **1** to move to the next panel.

   The Remote Manager Configuration panel appears.
7. On the Remote Manager Configuration panel, enter the Remote Manager configuration information:
   a. Enter the Service Name, or press **Enter** to accept the default.
   b. Enter the Remote Manager binding port, or press **Enter** to accept the default.
   c. Enter the Remote Manager SSL port, or press **Enter** to accept the default.
   d. Type **1** to select yes and enable RMI over SSL.

      Note: The No option for using non-SSL communication between the Remote Manager and the server is not supported and is displayed by the installer only for backward compatibility. Do not select the **No** option.

   e. Type **0** to accept your selections.
   f. Type **1**, to move to the next panel.

      The Remote Manager installation summary panel appears.
8. Check the information.
   - Type **2** to go back and make changes.
   - Type **1** to start the installation.

     Oracle Remote Manager installs and the Post Install Summary panel appears.
9. Type **3** to finish

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**>**config** 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
   ```

   where <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. Type **Y** at the prompt to trust the certificate.
5. Launch a plain-text editor, then open the file **xlconfig.xml**, which resides in the directory <**XL_HOME**>**xellerate\config**\.
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 steps if you want to use your own certificate:

On the Remote Manager Server System:

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 <**XL_RM_HOME**>**xlremote****config**\ directory.
3. Open <**XL_RM_HOME**>**xlremote****config****xlconfig.xml** using a text editor.
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.

On the Oracle Identity Manager Server System:

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 <**XL_HOME**>**xellerate****config** directory.
3. Open <**XL_HOME**>**xellerate****config****xlconfig.xml** using a text editor.
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
   ```

   where <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. Type **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**: execute the <XL_RM_HOME>\xlremote\remotemanager.bat script.
- **Linux**: execute the <XL_RM_HOME>/xlremote/remotemanager.sh script.

13

Upgrading to Oracle Identity Manager 9.0.1 from Versions 8.5.2 or 8.5.3

You Oracle Identity Manager has formerly been known as both Oracle Xellerate Identity Provisioning and also 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.

Upgrade Overview

Both Oracle Identity Manager and the Oracle Identity Manager Audit and Compliance module run on the JBoss application server version 4.0.2. Therefore, upgrade from Oracle Xellerate Identity Provisioning version 8.5.2 or 8.5.3 (henceforth referred to collectively as version 8.5.x) to Oracle Identity Manager version 9.0.1 involves upgrade to both the JBoss application server (from version 3.2.7 to version 4.0.2) and the Oracle Identity Manager application.

You can upgrade a non-clustered JBoss 3.2.7-based version of Oracle Xellerate Identity Provisioning 8.5.x to either a clustered or non-clustered JBoss 4.0.2-based configuration of Oracle Identity Manager 9.0.1. The new JBoss 4.0.2 application servers (in either clustered or non-clustered configuration) associated with your Oracle Identity Manager 9.0.1 installation can run on either Windows or Linux hosts.

The JBoss application server does not support an in-place upgrade; therefore, you must perform the following sequence of tasks to install Oracle Identity Manager version 9.0.1 and, if you desire, the optional Oracle Identity Manager Audit and Compliance module as well.

The following is an overview of the process to upgrade from Oracle Xellerate Identity Provisioning version 8.5.x to Oracle Identity Manager version 9.0.1:

1. Upgrade the database you used for Oracle Xellerate Identity Provisioning 8.5.x. Refer to "Upgrading Your Database" on page 13-2 for more information.
2. Install a fresh instance of the JBoss 4.0.2 application server on the machine that will host your Oracle Identity Manager 9.0.1 server. Refer to "Installing the JBoss 4.0.2 Application Server" on page 13-8 for more information.
3. Install a fresh instance of Oracle Identity Manager 9.0.1 on the host running your JBoss 4.0.2 application server. Depending on your operating system, refer to the following:
    a. Chapter 6, "Installing Oracle Identity Manager Server on Windows" on page 6-1 or Chapter 7, "Installing Oracle Identity Manager Server on Linux" on page 7-1

b. Chapter 11, "Installing and Configuring Oracle Identity Manager Design Console" on page 11-1

c. Chapter 12, "Installing and Configuring the Oracle Identity Manager Remote Manager" on page 12-1

4. Migrate your legacy Oracle Xellerate Identity Provisioning 8.5.x configuration settings to your new Oracle Identity Manager 9.0.1 environment. Refer to "Migrating and Updating Component Settings" on page 13-9 for more information.

5. Migrate any Oracle Xellerate Identity Provisioning 8.5.x custom code, including custom clients, scheduled tasks, event handlers, and libraries bound to adapters to your new Oracle Identity Manager 9.0.1 environment. Refer to "Migrating Custom Code to 9.0.1" on page 13-13 for more information.

6. Perform post-installation configuration of your Oracle Identity Manager environment. Refer to "Post-Installation Configuration" on page 13-14 for more information.

Note: This chapter describes upgrading from Oracle Xellerate Identity Provisioning 8.5.2 or 8.5.3 to Oracle Identity Manager version 9.0.1, with optional addition of the Oracle Identity Manager Audit and Compliance.

The Oracle Identity Manager 9.0.1 upgrade package is contained in upg_852_853_to_901.zip. Extract the contents of this package to a temporary directory on the machine where you plan to install Oracle Identity Manager 9.0.1. Henceforth, this document refers to this temporary directory as <**Patch**>.

If you are running an earlier version of Oracle Xellerate Identity Provisioning, contact Oracle Technical Support for the appropriate upgrade patch.

Note: This chapter only covers upgrading to Oracle Identity Manager 9.0.1 from an Oracle Xellerate Identity Provisioning 8.5.x installation deployed on JBoss application server.

Upgrading Your Database

Upgrade the database used by your Oracle Xellerate Identity Provisioning 8.5.x installation. You can choose among the following upgrade methods:

- Perform an in-place upgrade of the existing database configured for Oracle Xellerate Identity Provisioning 8.5.x.
- Create a new instance of the database, then import the data used by your Oracle Xellerate Identity Provisioning 8.5.x installation into that new database.

Upgrading an Existing Database Instance

This approach upgrades your existing database instance by upgrading the database schema while your database remains in-place.

1. Extract the contents of the Oracle Identity Manager 9.0.1 upgrade package (upg_852_853_to_901.zip) to a temporary directory on the machine where you plan to

install Oracle Identity Manager 9.0.1. Henceforth, this document refers to this temporary directory as <**Patch**>.

2. Backup your existing database. As appropriate to your particular database, use the **export/backup** utilities provided with the Oracle database or SQL Server to perform a complete backup of your production database.

   Production database backup includes, but is not limited to, complete export or backup of the Oracle Xellerate Identity Provisioning 8.5.x database instance to ensure that no data is lost during the upgrade process. If the upgrade fails, this backup can be used to restore the database to its original state.

3. Verify your database configuration. Make sure that your existing database is properly configured. As appropriate for your database, consult the following documentation:

   Oracle

   "Setting Up the Oracle Database" on page 5-1

   SQL Server

   "Setting Up the SQL Server" on page 5-3

4. If you plan to install the optional Oracle Identity Manager Audit and Compliance module, you should create a separate file group for your SQL Server or a separate tablespace for Oracle databases to facilitate the new user profile auditing feature in version 9.0.1 of the Oracle Identity Manager Audit and Compliance module. If your database is SQL Server, you must create a new file group. If your database is Oracle, the new separate tablespace is not mandatory, but it is highly recommended for performance reasons.

   Note: Refer to "Creating a User Profile Audit File Group in SQL Server" on page A-1 for details on how to create a new file group in SQL Server. Refer to Oracle database documentation for details on setting up a tablespace for Oracle databases.

   ---

5. Upgrade your database schema from Oracle Xellerate Identity Provisioning 8.5.x to Oracle Identity Manager 9.0.1 by using the one of the following scripts appropriate for your database and operating system. Be sure to run the script on the machine where the database resides.

   Oracle

   Note: The **xl_db_upg_852_853_to_901** script also upgrades the required stored procedures for Oracle.

   For Oracle on Linux:

   a. Enable execute permissions on the **xl_db_upg_852_853_to_901.sh** script:

      ```
      chmod 755 xl_db_upg_852_853_to_901.sh
      ```

   b. Run the following script on the drive where you want to upgrade your database schema:

      <Patch>/Database/Oracle/Scripts/xl_db_upg_852_853_to_901.sh

c. Enter the appropriate information for the Oracle database when prompted by the **xl_db_upg_852_853_to_901.sh** script.

For Oracle on Windows:

a. Run the following batch script on the drive where you want to upgrade your database schema:

<Patch>\Database\Oracle\Scripts\xl_db_upg_852_853_to_901.bat

The following is the command line usage for the Oracle **xl_db_upg_852_853_to_901.bat** script:

```
xl_db_upg_852_853_to_901.bat <ORACLE_SID>
<ORACLE_HOME> <ORACLE_XELL_USER>
<ORACLE_XELL_USER_PWD> <PATCH>
```

SQL Server

a. Run the **<Patch>\Database\SQLServer\Scripts\upg_852_853_to_901.bat** batch file.

Note: Refer to "Executing the SQL Server Upgrade Script" on page A-1 for more information on executing this script on an SQL Server database.

---

6. New stored procedures have been introduced in Oracle Identity Manager 9.0.1. Perform the following steps to create the requisite stored procedures for your database:

Note: If you are using an Oracle database, you can skip this step as running the **xl_db_upg_852_853_to_901** script already created the required stored procedures for Oracle.

SQL Server

a. Launch a plain-text editor, then open the file compile_all_XL_SP.bat, which resides in the directory **<Patch>/Database/SQLServer/StoredProcedures/**.

b. For every stored procedure listed in the **Sequential Lists** section of **compile_all_XL_SP.bat**, replace the string **@sysuser** with the **database user name**. This is necessary because SQL Server requires functions invoked from a stored procedure to be qualified by the database user name (owner). Be sure you replace the entire **@sysuser** string, including the @ character.

c. Navigate to the directory **<Patch>/Database/SQLServer/StoredProcedures/**, then run the batch file **compile_all_XL_SP.bat**.

Note: Refer to "Executing the SQL Server Upgrade Script" on page A-1 for more information on executing this script on an SQL Server database.

---

7. To upgrade and enable the optional Oracle Identity Manager Audit and Compliance module, perform the following steps appropriate for your database:

Note: This step is necessary only if you are upgrading from Oracle Xellerate Identity Provisioning 8.5.x to the 9.0.1 version of the Oracle Identity Manager Auditing and Compliance module.

Oracle

a. Log in to SQL *Plus with the credentials of the Oracle Xellerate Identity Provisioning 8.5.x database schema owner.

b. Run the following script:

<Patch>\Database\Oracle\Scripts\Oracle_Enable_XACM.sql

SQL Server

a. Run the **<Patch>/Database/SQLServer/Scripts/SQLServer_Enable_XACM.bat** batch file.

Note: Refer to "Executing the SQL Server Upgrade Script" on page A-1 for more information on executing this script on an SQL Server database.

8. The user profile auditing feature and the reports feature introduced in Oracle Identity Manager 9.0.1 require that certain metadata be loaded into the database. As appropriate for the operating system on the machine hosting your Oracle Identity Manager server, load Oracle Identity Manager metadata into your database by executing one of the following commands:

Windows

Run the batch file **LoadXML.bat**, which resides in the **<Patch>\Database\Utilities** directory.

Linux

Run the script **LoadXML.sh**, which resides in the directory **<Patch>/Database/Utilities/**.

Note: Refer to "Loading Metadata into the Database" on page A-2 before executing this script.

Creating a New, Upgraded Database Instance

This approach creates a new database instance, then upgrades it with the database schema for Oracle Identity Manager 9.0.1. This method ensures that your current working database remains available if a rollback is required. Use the following steps for creating a new, upgraded database instance:

1. Use the **export/backup** utility provided by SQL Server or Oracle database to perform a complete export of all the data in your existing database.
2. Create a new database. See either of the following: "Setting Up the Oracle Database" on page 5-1 or "Setting Up the SQL Server" on page 5-3 for more information.

Important: If you create a new Oracle database, make sure to specify the username and password used by your original database instance as the credentials for your new database.

3. Using the **import** utility provided by your particular database, import the data you exported from your original database in **Step 1** into your newly created database you made in **Step 2**. This creates an exact copy of your original database instance.
4. If you plan to install the optional Oracle Identity Manager Audit and Compliance module, you should create a separate file group for your SQL Server or a separate tablespace for Oracle databases to facilitate the new user profile auditing feature in version 9.0.1 of the Oracle Identity Manager Audit and Compliance module. If your database is SQL Server, you must create a new file group. If your database is Oracle, the new separate tablespace is not mandatory, but it is highly recommended for performance reasons.

   Note: Refer to "Creating a User Profile Audit File Group in SQL Server" on page A-1 for details on how to create a new file group in SQL Server. Refer to Oracle database documentation for details on setting up a tablespace for Oracle databases.

5. Upgrade your database schema from Oracle Xellerate Identity Provisioning 8.5.x to Oracle Identity Manager 9.0.1 by using one of the following scripts appropriate for your database and operating system. Be sure to run the script on the machine where the database resides.

   Oracle

   Note: The **xl_db_upg_852_853_to_901** script also upgrades the required stored procedures for Oracle.

   For Oracle on Linux:

   a. Enable execute permissions on the **xl_db_upg_852_853_to_901.sh** script:

      ```
      chmod 755 xl_db_upg_852_853_to_901.sh
      ```

   b. Run the following script on the drive where you want to upgrade your database schema:

      <Patch>/Database/Oracle/Scripts/xl_db_upg_852_853_to_901.sh

   c. Enter the appropriate information for the Oracle database when prompted by the **xl_db_upg_852_853_to_901.sh** script.

   For Oracle on Windows:

   a. Run the following batch script on the drive where you want to upgrade your database schema:

      <Patch>\Database\Oracle\Scripts\xl_db_upg_852_853_to_901.bat

      The following is the command line usage for the Oracle **xl_db_upg_852_853_to_901.bat** script:

      ```
      xl_db_upg_852_853_to_901.bat <ORACLE_SID>
      ```

```
<ORACLE_HOME> <ORACLE_XELL_USER>
<ORACLE_XELL_USER_PWD> <PATCH>
```

SQL Server

a. Run the **<Patch>\Database\SQLServer\Scripts\upg_852_853_to_901.bat** batch file.

Note: Refer to "Executing the SQL Server Upgrade Script" on page A-1 for more information on executing this script on an SQL Server database.

---

6. New stored procedures have been introduced in Oracle Identity Manager 9.0.1. Perform the following steps to create the requisite stored procedures for your database:

Note: If you are using an Oracle database, you can skip this step as running the **xl_db_upg_852_853_to_901** script already created the required stored procedures for Oracle.

SQL Server

a. Launch a plain-text editor and open the **<Patch>/Database/SQLServer/StoredProcedures/compile_all_XL_SP.bat** batch file.

b. For every stored procedure listed in the **Sequential Lists** section of **compile_all_XL_SP.bat**, replace the **@sysuser** string with the **database user name**. This is necessary because SQL Server requires functions invoked from a stored procedure to be qualified by the database user name (owner). Be sure you replace the entire **@sysuser** string, including the @ character.

c. Run the **<Patch>/Database/SQLServer/StoredProcedures/compile_all_XL_SP.bat** batch file.

Note: Refer to "Executing the SQL Server Upgrade Script" on page A-1 for more information on executing this script on an SQL Server database.

---

7. To upgrade and enable the optional Oracle Identity Manager Audit and Compliance module, perform the following steps appropriate for your database:

Note: This step is necessary only if you are upgrading the 8.5.x version of the Audit and Compliance module to the 9.0.1 version of the Audit and Compliance module.

Oracle

a. Log in to SQL *Plus with the credentials of the Oracle Xellerate Identity Provisioning 8.5.x database schema owner.

b. Run the following script:

<Patch>\Database\Oracle\Scripts\Oracle_Enable_XACM.sql

SQL Server

a. Run the **<Patch>/Database/SQLServer/Scripts/SQLServer_Enable_XACM.bat** batch file.

Note: Refer to "Executing the SQL Server Upgrade Script" on page A-1 for more information on executing this script on an SQL Server database.

---

8. The user profile auditing and reports features introduced in Oracle Identity Manager 9.0.1 require that certain metadata be loaded into the database. As appropriate for the operating system on the machine hosting your Oracle Identity Manager server, load Oracle Identity Manager metadata into your database by executing one of the following:

   Windows

   a. Run the **<Patch>\Database\Utilities\LoadXML.bat** batch file.

   Linux

   a. Run the **<Patch>/Database/Utilities/LoadXML.sh** script.

Note: Refer to "Loading Metadata into the Database" on page A-2 before executing this script.

Installing the JBoss 4.0.2 Application Server

Upgrading JBoss from version 3.2.7 to version 4.0.2 requires installation of a new instance of the application server, because JBoss does not provide an in-place upgrade mechanism for the versions involved. This new instance can be installed on the same machine that hosts the 3.2.7 instance or on a different machine.

Tip: Installing multiple versions of an application server on the same machine can possibly reduce the downtime caused by the upgrade; however, you must ensure that the two instances do not contend for the same set of ports. Configuration of your new JBoss 4.0.2 instance to use a nondefault ports is a manual process. Refer to your JBoss documentation for details.

Caution: Oracle Identity Manager 9.0.1 supports JBoss clustering. Make sure to guard against port contention whenever you upgrade a non-clustered machine running Oracle Xellerate Identity Provisioning 8.5.x so that it can run in a clustered, Oracle Identity Manager 9.0.1 environment.

Refer to Chapter 4, "Installing and Configuring JBoss for Oracle Identity Manager" on page 4-1 for more information on setting up, installing, and configuring a new instance of your JBoss application server. Relevant sections in this chapter detail the configuration requirements you must perform before and during application server installation.

To upgrade an existing Oracle Identity Manager installation from a non-clustered to a clustered environment, see Chapter 10, "Deploying in a Clustered JBoss Configuration" on page 10-1 for more information.

Caution: Do not overwrite your existing application server installation. Instead, make sure to install the new application server instance in a directory other than the one used by your existing application server instance.

Caution: Make sure to shut down your existing JBoss application server instance before you begin Oracle Identity Manager 9.0.1 installation.

Note: During Oracle Identity Manager installation, the installer recognizes that the specified database credentials belong to an existing encrypted database. Therefore it prompts you to copy the file .xldatabasekey from the old installation directory (8.5.x) to the installation directory (9.0.1) so that the same key can be used to decrypt the data read from the database. You should ignore this prompt because post-installation steps in these upgrade instructions require you to copy .xldatabasekey and other files from your 8.5.x installation directory to your 9.0.1 installation directory. (See Step 2 in "Migrating Oracle Identity Manager Server Settings" for more information.)

Migrating and Updating Component Settings

After you install the Oracle Identity Manager 9.0.1 components (Oracle Identity Manager Server, Design Console, and Remote Manager), you must migrate certain settings from your version Oracle Xellerate Identity Provisioning 8.5.x environment to your version 9.0.1 components and update other various settings as described in this section.

Migrating Oracle Identity Manager Server Settings

To migrate and otherwise update the settings on your newly installed Oracle Identity Manager 9.0.1 servers, complete the following steps:

1. Backup the contents of your Oracle Identity Manager 9.0.1 server configuration directory **<XL_HOME>/xellerate/config**
2. Copy the following configuration files from your version Oracle Xellerate Identity Provisioning 8.5.x installation directory (<XL_85x_HOME>) to the corresponding version 9.0.1 installation directory (<XL_HOME>), overwriting files, as necessary.

```
xellerate/config/.xldatabasekey
xellerate/config/.xlkeystore
xellerate/config/configkey.key
xellerate/config/FormMetaData.xml
xellerate/config/xell.csr
xellerate/config/xlconfig.xml
xellerate/config/xlserver.cert
```

3. If you are *not* upgrading to a clustered environment, launch a plain-text editor, open the file **log4j.xml**, which resides in the directory **<JBOSS_3.2.7_HOME>/server/default/conf/**, then copy all tags that were added to this file as part of Oracle Xellerate Identity Provisioning 8.5.x setup to the file log4j.xml that resides in the directory **<JBOSS_4.0.2_HOME>/server/default /conf/**.

   Alternatively, if you are upgrading from a non-clustered environment to a clustered environment, copy all the tags that were added as part of Oracle Xellerate Identity Provisioning 8.5.x setup from the file **log4j.xml**, which resides in the directory **<JBOSS_3.2.7_HOME>/server/default/conf/** to the file **log4j.xml**, which resides in **<JBOSS_4.0.2_HOME>/server/all/conf/**. To identify added tags, look for entries that resemble the following:

```
<category name="XELLERATE.DDM">
     <priority value="DEBUG"/>
</category>
<category name="XELLERATE">
     <priority value="WARN"/>
</category>
<category name="com.nexaweb.server">
     <priority value="WARN"/>
</category>
```

   In all of these tags “priority value” is set to one of the permissible log4j levels, such as DEBUG or WARN.

   By copying these relevant tags, you migrate the existing log categories and their current log-level settings from your JBoss 3.2.7/Oracle Xellerate Identity Provisioning 8.5.x environment to your new JBoss 4.0.2/ Oracle Identity Manager 9.0.1 environment.

4. Update the file **xlconfig.xml**, which resides in the directory **<XL_HOME>/xellerate/config/**. See "Upgrading the Server Configuration File" on page A-4 for more information.

5. Update the file **FormMetaData.xml**, which resides in the directory **<XL_HOME>/xellerate/config/**. See "Upgrading the Metadata File" on page A-6 for more information.

6. Copy the contents of the directory **<XL_85x_HOME>/xellerate/adapters** to the directory **<XL_HOME>/xellerate/adapters**.

> **Important:** If you are upgrading from a non-clustered environment to a clustered environment, make sure to repeat steps 1 through 6 on all cluster members.

Migrating Remote Manager Settings

The Remote Manager installation wizard performs most Remote Manager configuration tasks. However, when you are upgrading, you must manually migrate certain version 8.5.x configuration files to your new Remote Manager installation directory. In some cases, you must also modify these files. Complete the following steps to complete configuration of your version 9.0.1 Remote Manager.

1. Backup the contents of your version 9.0.1 Remote Manager configuration directory, which is **<XL_RM_HOME>/xlremote/config**

2. Copy the following configuration files from your version 8.5.x Remote Manager installation directory (<XL_85x_RM_HOME>) to the corresponding version 9.0.1

Remote Manager installation directory (<XL_RM_HOME>), overwriting files, as necessary.

```
xlremote/config/.xlkeystore
xlremote/config/configkey.key
xlremote/config/xell.csr
xlremote/config/xlconfig.xml
xlremote/config/xlserver.cert
```

3. As of version 9.0.1, and for all future releases, the log.properties file replaces the log.conf file as the Remote Manager configuration file. Complete the following steps to migrate all the Remote Manager logging settings:

   a. Copy the **<XL_HOME>/xellerate/config/log.properties** file from the version 9.0.1 server installation directory to the version 9.0.1 Remote Manager **<XL_RM_HOME>/xlremote/config/** installation directory.

   b. Copy any version 8.5.x custom logging-related settings that may exist in the file log.conf, which resides in the directory **<XL_85x_RM_HOME>/xlremote/config/**, to the file **log.properties**, which resides in the directory **<XL_RM_HOME>/xlremote/config/**.

   Note: Copy only the custom logging-related settings in the log.conf file, not the syntax of the 8.5.x log.conf file.

   c. You must convert the formatting of the log-level settings in log.conf to new formatting in the log.properties file. For example, a logging-related entry in log.conf might look similar to the following:

   ```
   Logger.module.RemoteManager=WARN
   ```

   The corresponding entry in log.properties might look like the following:

   ```
   # log4j.logger.XELLERATE.RemoteManager=DEBUG
   ```

   You need to uncomment the line, then set the parameter to the value already set in the log.conf entry, so that the log.properties entry looks something like the following:

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

   Repeat this for all logging-related entries, then save and close the file.

4. Update the file xlconfig.xml in the directory **<XL_RM_HOME>/xlremote/config/**. See "Upgrading the Remote Manager Configuration File" on page A-7 for more information.

Updating the Oracle Identity Manager Server

You must update the bootstrap information in the configuration file for your Oracle Identity Manager server by completing the following steps:

1. Launch a plain-text editor, then open the file xlconfig.xml, which resides in the directory <XL_HOME>/xellerate/config/, of the machine hosting your Oracle Identity Manager server. Ensure that the bootstrap address and port in the configuration file point to your version 9.0.1 server or servers. The following configuration parameters, which contain the bootstrap information, must be updated:

   ```
   <xl-configuration>.<Discovery>.<CoreServer>.<java.naming.provider.url>
   ```

```
<xl-configuration>.<Discovery>.<BackOffice>.<java.naming.provider.url>
<xl-configuration>.<Discovery>.<Scheduler>.<java.naming.provider.url>
<xl-configuration>.<Discovery>.<JMSServer>.<java.naming.provider.url>
```

For example, you might change a parameter setting for an un-upgraded, non-clustered configuration such as this:

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

To something like the following for an upgraded, clustered configuration:

```
<java.naming.provider.url>
      jnp://192.168.20.5:1100,192.168.20.6:1100
</java.naming.provider.url>
```

2. As necessary, update the other external components used in deployment (like IIS) with the new port information. For detailed procedures, consult the documentation for each external component.

Note: Restart the application server after completing the upgrade process.

Updating Design Console Settings

When you upgrade a non-clustered Oracle Xellerate Identity Provisioning 8.5.x environment to a clustered Oracle Identity Manager 9.0.1 environment, you must update the version 9.0.1 Design Console so that the bootstrap address and port in the configuration file point to your version 9.0.1 Oracle Identity Manager server.

Complete the following steps:

1. Launch a plain text editor, open the file **xlconfig.xml**, which resides in the directory **<XL_DC_HOME>/xlclient/config/**, then locate the following configuration parameter:

   ```
   <xl-configuration>.<Discovery>.<CoreServer>.<java.naming.provider.url>
   ```

2. Within the tag **<java.naming.provider.url></java.naming.provider.url>**, add a comma-delimited list of some of the bootstrap addresses and ports in your configuration, using the following format:

   ```
   jnp://<ip-addr-or-host-name1>:<port1>,<ip-addr-or-host-name2>:<port2>,...<ip-addr-or-host-namen>:<portn>
   ```

   The completed string for a clustered installation might look something like the following:

   ```
   <java.naming.provider.url>jnp://192.168.20.5:1100,192.168.20.6:1100</java.naming.provider.url>
   ```

3. Add to the discovery/CoreServer section a partition information statement similar to the following:

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

4. Locate the **<ApplicationURL>** tag and changes its value to the URL of the Web server that is hosting the clustered environment.

Migrating Custom Code to 9.0.1

In a version 9.0.1 environment, you can recycle custom code (including custom clients, scheduled tasks, event handlers and libraries bound to adapters) originally used in your version 8.5.x environment.

Important: Before migrating custom code from the 8.5.x environment, the custom code must first be rebuilt using the Oracle Identity Manager 9.0.1 libraries.

Recompiling Custom Code

Custom code written for Oracle Xellerate Identity Provisioning 8.5.x needs to be rebuilt using the Oracle Identity Manager 9.0.1 libraries, which are located in **<XL_HOME>/xellerate/lib**.

Using the integrated development environment (that is, Eclipse, JDeveloper, WASD or command line javac) that originally compiled the version 8.5.x custom code, recompile all custom java code using Oracle Identity Manager 9.0.1 libraries instead of Oracle Xellerate Identity Provisioning 8.5.x libraries.

Migrating Adapters

Custom java libraries bound to functional Oracle Xellerate Identity Provisioning 8.5.x adapters can be reused in a Oracle Identity Manager 9.0.1 environment after they have been recompiled using Oracle Identity Manager 9.0.1 libraries.

The recompiled custom java libraries that were originally in the directory **<XL_85x_HOME>/xellerate/JavaTasks** must be copied to the directory **<XL_HOME>/xellerate/JavaTasks**.

The recompiled custom java libraries that were originally in the directory **<XL_85x_RM_HOME>/xlremote/JavaTasks** must be copied to the directory **<XL_RM_HOME>/xlremote/JavaTasks**.

Important: If you are upgrading from a non-clustered to a clustered environment, you must repeat this step on all cluster members.

Note: You do not need to recompile the adapters themselves.

Migrating Scheduled Tasks

Custom scheduled tasks that were functional in Oracle Xellerate Identity Provisioning 8.5.x can be reused in your Oracle Identity Manager 9.0.1 environment after you have recompiled them using Oracle Identity Manager 9.0.1 libraries.

The recompiled custom scheduled tasks need to be copied to the directory **<XL_HOME>/xellerate/ScheduleTask**.

Note: If you are upgrading from a non-clustered to a clustered environment, you must repeat this step on all cluster members.

Migrating Event Handlers

Custom event handlers that were functional in Oracle Xellerate Identity Provisioning 8.5.x can be reused in your version 9.0.1 environment after you have recompiled them using Oracle Identity Manager 9.0.1 libraries.

The recompiled custom event handlers must be copied to the directory **<XL_HOME>/xellerate/EventHandlers**.

Note: If upgrading from a non-clustered environment to a clustered environment then repeat this step on all cluster members.

Migrating xlWebApp Customizations

You must reapply any customizations (for example, JSP customizations) made to the Oracle Xellerate Identity Provisioning 8.5.x web application to the 9.0.1 Oracle Identity Manager environment.

Migrate any customizations previously applied to your version 8.5.x web application to the out-of-box version 9.0.1 web application **xlWebApp.war**, which resides in the directory **<XL_HOME>/xellerate/webapp**.

After migrating the 8.5.x web application customizations, you must patch your version 9.0.1 web application. See Appendix B, "Patching an Existing Oracle Identity Manager Installation" on page B-1 for more information.

Migrating Custom Clients

Any custom clients that were built using Oracle Xellerate Identity Provisioning 8.5.x APIs must be updated and recompiled to make them compatible with the Oracle Identity Manager 9.0.1 APIs. For example, certain APIs might have been deprecated or replaced by new APIs. Refer to the *Oracle Identity Manager Release Notes* for a comprehensive list of API calls that have changed between Oracle Xellerate Identity Provisioning 8.5.x and Oracle Identity Manager 9.0.1.

Post-Installation Configuration

The following post-installation configurations are necessary to complete the upgrade process.

Post-Installation Configuration for the Oracle Identity Manager Auditing and Compliance Module

The following post-installation configuration procedures might be necessary if you have installed the Oracle Identity Manager Audit and Compliance module (previously named Oracle Xellerate Auditing and Compliance Manager in 8.5.x). The following is an overview of the process:

1. Set the user profile audit level
2. Generate user snapshots
3. Execute the Generate Snapshot script

Setting the User Profile Audit Level

1. Define a secondary data source for reporting, if necessary. Refer to the *Oracle Identity Manager Audit Report Developer's Guide* for more information on defining a secondary data source.
2. Start the application server hosting your Oracle Identity Manager server.
3. Set the **audit level**. The permissible values, in descending order are:
   - Process Task
   - Resource Form
   - Resource
   - Membership
   - Core
   - None

   Specify an audit level by completing the following sub-steps:
   a. Log into the **Design Console** as an administrator
   b. Navigate to the **System Configuration** page
   c. Locate **XL.UserProfileAuditDataCollection** and sets its value to **Resource Form** or the appropriate audit level.
4. To collect user profile audit data in the secondary reporting data store, complete the following sub-steps:
   a. Log into the **Design Console** as an administrator
   b. Navigate to the **System Configuration** page
   c. Locate **XL.UserProfileAuditInSecondaryDS** and set its value to **TRUE**.

Generating User Snapshots

If you installed the Oracle Identity Manager Audit and Compliance module, you must generate new snapshots for all existing users in the system when either of the following two situations occur:

- You upgrade from version 8.5.x to version 9.0.1 with the Oracle Identity Manager Audit and Compliance module
- You elevate the audit level for an existing Oracle Identity Manager Audit and Compliance module environment

To generate new snapshots, complete the following steps:

1. Launch a plain-text editor and open the file **GenerateSnapshot** script located in the **<XL_HOME>/xellerate/bin/** directory. If you are running on Windows, open **GenerateSnapshot.bat**. If you are running on Linux, open **GenerateSnapshot.sh**.
2. Edit the following variables in the GenerateSnapshot script:
   a. Modify the set `XEL_HOME=`variable to point to the directory where you installed Oracle Identity Manager.
   b. Modify the set `APP_SERVER=@appserver` variable to be:

      ```
      set APP_SERVER=jboss
      ```

   c. Modify the set `APP_SERVER_HOME=@app_server_home` variable to point to the directory where you installed JBoss.

d. Modify the set `JAVA_HOME=@jdk_loc` variable to point to the directory containing the JDK.

e. Modify the SQL_SERVER_DRIVER_DIR variable to point to the directory containing the SQL Server JDBC drivers. For example:

Windows

In **GenerateSnapshot.bat**, change the following line:

```
REM set SQL_SERVER_DRIVER_DIR=C:\Program Files\Microsoft SQL Server 2000
Driver for JDBC\lib
```

to the following:

```
set SQL_SERVER_DRIVER_DIR=<Set appropriate value here>
```

Linux

In **GenerateSnapshot.sh**, change the following line:

```
# SQL_SERVER_DRIVER_DIR=/msdrivers/lib
# export SQL_SERVER_DRIVER_DIR
```

to the following:

```
SQL_SERVER_DRIVER_DIR=<Set appropriate value here>
export SQL_SERVER_DRIVER_DIR
```

3. Execute one of the following GenerateSnapshot scripts as appropriate for the operating system on the machine hosting the Design Console:

Windows

- Run the batch file **GenerateSnapshot.bat**, which resides in the directory **<XL_HOME>/xellerate/bin/**.

Linux

- Run the batch file **GenerateSnapshot.sh**, which resides in the directory **<XL_HOME>/xellerate/bin/**.

Post-Installation Configuration Tasks for Oracle Identity Manager

The following tasks apply to the various Oracle Identity Manager components:

- You must apply to all new application server instances all performance tuning settings previously applied to the application servers you used for Oracle Xellerate Identity Provisioning 8.5.x.
- Verify that your upgrade process has succeeded by confirming that all version 8.5.x data is accessible in your version 9.0.1 environment, for example, that you can access all users, organizations, groups, resources, process definitions, rule definitions, forms, and adapter definitions that were part of your version 8.5.x installation.

  Once you are confident that your entire 8.5.x environment is accessible in 9.0.1, back up, then remove the application servers you used for your 8.5.x environment.
- If necessary, you must update your new application server so that it uses default ports. If you update your new application server so that it uses default ports, be sure to update the bootstrap addresses in the Oracle Identity Manager Server's configuration file, <XL_HOME>xellerate/config/xlconfig.xml. See"Updating the Oracle Identity Manager Server" on page 13-11 for more information.

14

Upgrading to Oracle Identity Manager 9.0.1 from Version 9.0.0

Oracle Identity Manager has formerly been known as both Oracle Xellerate Identity Provisioning and also 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 chapter describes upgrading from Oracle Xellerate Identity Provisioning 9.0.0 to Oracle Identity Manager version 9.0.1, with optional addition of the Oracle Identity Manager Audit and Compliance.

The Oracle Identity Manager 9.0.0 upgrade package is contained in upg_900_to_901.zip. Extract the contents of this package to a temporary directory on the machine where you plan to install Oracle Identity Manager 9.0.1. Henceforth, this document refers to this temporary directory as **<Patch>**.

Important: The Oracle Identity Manager 9.0.0 to 9.0.1 upgrade for JBoss is supported only for environments using SQL Server as a database.

Upgrade Overview

The following is an overview of the process for upgrading to Oracle Identity Manager version 9.0.1 from Oracle Xellerate Identity Provisioning 9.0.0:

1. Upgrade the database you used for Oracle Xellerate Identity Provisioning 9.0.0. Refer to "Upgrading Your 9.0.0 Database to 9.0.1" on page 14-2 for more information.
2. Perform the pre-upgrade configuration tasks. Refer to"Pre-Upgrade Configuration" on page 14-3 for more information.
3. Perform the upgrade to Oracle Identity Manager 9.0.1. Refer to "Performing the Upgrade to 9.0.1" on page 14-7 for more information.
4. Migrate any Oracle Xellerate Identity Provisioning 9.0.0 custom code, including custom clients, scheduled tasks, event handlers, and libraries bound to adapters to your new Oracle Identity Manager 9.0.1 environment. Refer to "Migrating Custom Code to 9.0.1" on page 14-8 for more information.

Upgrading Your 9.0.0 Database to 9.0.1

Perform the following steps to upgrade your existing SQL Server database used for Oracle Xellerate Identity Provisioning 9.0.0:

1. Extract the contents of the Oracle Identity Manager 9.0.1 upgrade package (upg_900_to_901.zip) to a temporary directory on the machine where you plan to install Oracle Identity Manager 9.0.1. Henceforth, this document refers to this temporary directory as **<Patch>**.
2. Backup your existing SQL Server database. Use the utilities provided with your SQL Server database to perform a complete backup of your production database. Production database backup includes, but is not limited to, complete export or backup of the Oracle Xellerate Identity Provisioning 9.0.0 database instance to ensure that no data is lost during the upgrade process. If the upgrade fails, this backup can be used to restore the database to its original state.
3. Verify your existing SQL Server database configuration is properly configured. Consult "Setting Up the SQL Server" on page 5-3 or your SQL Server documentation for more information if needed.
4. Upgrade your database schema from Oracle Xellerate Identity Provisioning 9.0.0 to Oracle Identity Manager 9.0.1 by using the **upg_900_to_901.bat** script. Be sure to run the script on the machine where the database resides.
   a. Run the **<Patch>\Database\SQLServer\Scripts\upg_900_to_901.bat** batch file.

   Note: Refer to "Executing the SQL Server Upgrade Script" on page A-1 for more information on executing this script on an SQL Server database.

5. New stored procedures have been introduced in Oracle Identity Manager 9.0.1. Perform the following steps to create the required stored procedures for your SQL Server database:
   a. Launch a plain-text editor and open the **<Patch>/Database/SQLServer/StoredProcedures/compile_all_XL_SP.bat** file.
   b. For every stored procedure listed in the **Sequential Lists** section of **compile_all_XL_SP.bat**, replace the **@sysuser** string with the **database user name**. This is necessary because SQL Server requires functions invoked from a stored procedure to be qualified by the database user name (owner).
   c. Go to the **<Patch>/Database/SQLServer/StoredProcedures/** directory and run the **compile_all_XL_SP.bat** batch file.

   Note: Refer to "Executing the SQL Server Upgrade Script" on page A-1 for more information on executing this script on an SQL Server database.

6. To upgrade and enable the optional Oracle Identity Manager Audit and Compliance module, perform the following steps:

Note: This step is necessary only if you are upgrading the 9.0.0 version of the Audit and Compliance module to the 9.0.1 version of the Audit and Compliance module.

a. Run the **<Patch>/Database/SQLServer/Scripts/SQLServer_Enable_XACM.bat** batch file.

Note: Refer to "Executing the SQL Server Upgrade Script" on page A-1 for more information on executing this script on an SQL Server database.

7. The user profile auditing feature and the reports feature introduced in Oracle Identity Manager 9.0.1 require that certain metadata be loaded into the database. As appropriate for the operating system on the machine hosting your Oracle Identity Manager server, load Oracle Identity Manager metadata into your database by executing one of the following:

   Windows

   a. Run the **<Patch>\Database\Utilities\LoadXML.bat** batch file.

   Linux

   a. Run the **<Patch>/Database/Utilities/LoadXML.sh** batch file.

   Note: Refer to "Loading Metadata into the Database" on page A-2 before executing this script.

Pre-Upgrade Configuration

Before you upgrade to the Oracle Identity Manager 9.0.1, you must prepare for the upgrade by performing pre-upgrade configuration tasks to the following components:

- Oracle Identity Manager Server
- Remote Manager
- Design Console

Pre-Upgrade Configuration for the Oracle Identity Manager Server

Prepare the Oracle Identity Manager Server for upgrade to 9.0.1 by updating 9.0.0 libraries, scripts, and configuration files using the following steps:

Important: If upgrading from a clustered JBoss environment, perform the following steps on all cluster members, including the model node.

1. Backup the following directories.
   - <XL_900_HOME>\xellerate\ext
   - <XL_900_HOME>\xellerate\config
   - <XL_900_HOME>\xellerate\DDTemplates

- <XL_900_HOME>\xellerate\lib
- <XL_900_HOME>\xellerate\setup
- <XL_900_HOME>\xellerate\webapp
- <XL_900_HOME>\xellerate\bin
- <XL_900_HOME>\documentation

2. Copy the directories and files listed in the location of the **From** column in the following table to the location listed in the **To** column in the following table. Overwrite the existing files in the **To** location if necessary.

Table 14–1 Oracle Identity Manager Server Pre-Upgrade Files to Copy

Copy From....	To
Patch\xellerate\DDTemplates	<XL_HOME>\xellerate\DDTemplates
Patch\xellerate\lib	<XL_HOME>\xellerate\lib
Patch\xellerate\webapp	<XL_HOME>\xellerate\webapp
Patch\xellerate\bin	<XL_HOME>\xellerate\bin
Patch\xellerate\config	<XL_HOME>\xellerate\config
Patch\documentation	<XL_HOME>\documentation
Patch\xellerate\ext\nexaweb-common.jar	<XL_HOME>\xellerate\ext
Patch\xellerate\readme.htm	<XL_HOME>

3. Copy the following files from Patch\xellerate\setup to <XL_HOME>\xellerate\setup:
   - setup.xml
   - patch_jboss.cmd
   - patch_jboss.sh
   - jboss-setup.xml
4. Modify the **<XL_HOME >/xellerate/config/xlconfig.xml** file as follows:
   a. Locate the parameter **<xl-configuration>.<Offlining>. .<MessageHandlerMDB>.<message-handler-task>**.

> **Note:** Refer to "Conventions" on page -viii for more information on identifying and locating xml tags.

Insert the following block of lines:

```
<ProcessOfflineMessage>com.thortech.xl.schedule.jms.processOfflineProcesses
.processOfflinedProvisioningProcesses</ProcessOfflineMessage>
<ProcessTaskOfflineMessage>com.thortech.xl.schedule.jms.processTaskOffline.
processOfflinedProcessTask</ProcessTaskOfflineMessage>
```

after the string:

<xl-configuration>.<Offlining>.<MessageHandlerMDB>.<message-handler -task>.<ReconOfflineMessage>

but before the string:

<xl-configuration>.<Offlining>.<MessageHandlerMDB>.<message-handler-task>.<TestMessage>

b. Locate the configuration parameter **<xl-configuration>.<Offlining>**.

Note: Refer to "Conventions" on page -viii for more information on identifying and locating xml tags.

Insert the following block of lines:

```
<process_offline_queue>
       <queueName>queue/xlQueue</queueName>
       <autoAcknowledge>true</autoAcknowledge>
       <replyTo></replyTo>
       <persistentFlag>true</persistentFlag>
       <disableMessageId>true</disableMessageId>
       <disableTimeStampe>false</disableTimeStampe>
        <messageEncrypt>false</messageEncrypt>
</process_offline_queue>
<process_task_offline_queue>
    <queueName>queue/xlQueue</queueName>
     <autoAcknowledge>true</autoAcknowledge>
     <replyTo></replyTo>
     <persistentFlag>true</persistentFlag>
     <disableMessageId>true</disableMessageId>
     <disableTimeStampe>false</disableTimeStampe>
     <messageEncrypt>false</messageEncrypt>
</process_task_offline_queue>
```

after the string:

<xl-configuration>.<Offlining>.</attestation_workflow_task_queue>

but before the string:

<xl-configuration>.<Offlining>.<test_queue>

5. Edit the <XL_HOME>/xellerate/setup/patch_jboss script as follows:

Windows

Edit patch_jboss.cmd and replace the following:

- replace @java_loc with the path to the Java installation directory
- replace @loc with the path to the Oracle Identity Manager server 9.0.1 installation directory

Linux

Edit patch_jboss.sh and replace the following:

- replace @loc with the path to the Oracle Identity Manager server 9.0.1 installation directory

Pre-Upgrade Configuration for the Design Console

Prepare the Oracle Identity Manager Design Console for upgrade to 9.0.1 by updating 9.0.0 libraries, scripts, and configuration files using the following steps:

1. Backup the following files and directories:

- <XL_900_DC_HOME>\xlclient\XLDesktopClient.ear<XL_900_DC_HOME>\xlclient\CustomClient.zip

- <XL_900_DC_HOME>\xlclient\xlFvcUtil.ear
- <XL_900_DC_HOME>\xlclient\lib
- <XL_900_DC_HOME>\xlclient\ext
- <XL_900_DC_HOME>\documentation

2. Copy the following files from Patch\xlclient\ to <XL_DC_HOME>\xlclient, overwriting existing files if necessary:
   - Patch\xlclient\XLDesktopClient.ear
   - Patch\xlclient\CustomClient.zip
   - Patch\xlclient\xlFvcUtil.ear
3. Copy Patch\xellerate\ext\nexaweb-common.jar to XL_DC_HOME>\xellerate\ext, overwriting the existing file if necessary.
4. Copy the contents of the Patch\xlclient\lib directory to <XL_DC_HOME>\xlclient\lib, overwriting files if necessary.
5. Copy the contents of the Patch\documentation directory to <XL_DC_HOME>\documentation, overwriting files if necessary.
6. Copy Patch\xellerate\readme.htm to <XL_DC_HOME>\xlclient\, overwriting the existing file if necessary.

Pre-Upgrade Configuration for the Remote Manager

Prepare the Oracle Identity Manager Remote Manager for upgrade to 9.0.1 by updating 9.0.0 libraries, scripts, and configuration files using the following steps:

1. Backup the content of the following directories:
   - <XL_900_RM_HOME>\xlremote\lib
   - <XL_900_RM_HOME>\xlremote\config
2. Copy the contents of the Patch\xlremote\lib directory to the <XL_RM_HOME>\xlremote\lib directory, overwriting files if necessary.
3. Edit the xlconfig.xml file in the <XL_RM_HOME>/xlremote/config/ directory as follows:
   a. Locate the parameter **<xl-configuration>.<Offlining>.<MessageHandlerMDB>.<message-handler-task>**.

      Note: Refer to "Conventions" on page -viii for more information on identifying and locating xml tags.

Insert the following block of lines:

```
<ProcessOfflineMessage>com.thortech.xl.schedule.jms.processOfflineProcesses
.processOfflinedProvisioningProcesses</ProcessOfflineMessage>
<ProcessTaskOfflineMessage>com.thortech.xl.schedule.jms.processTaskOffline.
processOfflinedProcessTask</ProcessTaskOfflineMessage>
```

after the string:

<xl-configuration>.<Offlining>.<MessageHandlerMDB>.<message-handler-task>.<ReconOfflineMessage>

but before the string:

<xl-configuration>.<Offlining>.<MessageHandlerMDB>.<message-handler-task>.<TestMessage>

b. Locate the configuration parameter **<xl-configuration>.<Offlining>**.

Note: Refer to "Conventions" on page -viii for more information on identifying and locating xml tags.

Insert the following block of lines:

```
<process_offline_queue>
        <queueName>queue/xlQueue</queueName>
        <autoAcknowledge>true</autoAcknowledge>
        <replyTo></replyTo>
        <persistentFlag>true</persistentFlag>
        <disableMessageId>true</disableMessageId>
        <disableTimeStampe>false</disableTimeStampe>
         <messageEncrypt>false</messageEncrypt>
</process_offline_queue>
<process_task_offline_queue>
    <queueName>queue/xlQueue</queueName>
     <autoAcknowledge>true</autoAcknowledge>
     <replyTo></replyTo>
     <persistentFlag>true</persistentFlag>
     <disableMessageId>true</disableMessageId>
     <disableTimeStampe>false</disableTimeStampe>
     <messageEncrypt>false</messageEncrypt>
</process_task_offline_queue>
```

after the string:

<xl-configuration>.<Offlining>.</recon_offline_queue>

but before the string:

<xl-configuration>.<Offlining>.<test_queue>

Performing the Upgrade to 9.0.1

Upgrading from an existing Oracle Xellerate Identity Provisioning 9.0.0 deployment to Oracle Identity Manager 9.0.1 involves assembling a new enterprise application archive (EAR) file from the latest libraries, then redeploying the EAR.

Perform the following steps after completing all the pre-upgrade tasks to upgrade an existing Oracle Xellerate Identity Provisioning 9.0.0 deployment to Oracle Identity Manager 9.0.1:

1. Make sure the JBoss application server is not running.
2. Run the patch_jboss script:

   Windows

   - Run <XL_HOME>\xellerate\setup\patch_jboss.cmd

   Linux

   - Run <XL_HOME>/xellerate/setup/patch_jboss.sh

Note: If you are upgrading from a non-clustered version 9.0.0 Oracle Xellerate Identity Provisioning environment to a clustered version 9.0.1 Oracle Identity Manager environment, you must repeat these steps on each node in the cluster.

Migrating Custom Code to 9.0.1

In a version 9.0.1 environment, you can recycle custom code (including custom clients, scheduled tasks, event handlers and libraries bound to adapters) originally used in your version 9.0.0 environment.

Important: Before migrating custom code from the 9.0.0 environment, the custom code must first be rebuilt using the Oracle Identity Manager 9.0.1 libraries.

Recompiling Custom Code

Custom code written for Oracle Xellerate Identity Provisioning 9.0.0 needs to be rebuilt using the Oracle Identity Manager 9.0.1 libraries, which are located in **<XL_HOME>/xellerate/lib**.

Using the integrated development environment (that is, Eclipse, JDeveloper, WASD or command line javac) that originally compiled the version 9.0.0 custom code, recompile all custom java code using Oracle Identity Manager 9.0.1 libraries instead of Oracle Xellerate Identity Provisioning 9.0.0 libraries.

Migrating Adapters

Custom java libraries bound to functional Oracle Xellerate Identity Provisioning 9.0.0 adapters can be reused in a Oracle Identity Manager 9.0.1 environment after they have been recompiled using Oracle Identity Manager 9.0.1 libraries.

The recompiled custom java libraries that were originally in the directory **<XL_900_HOME>/xellerate/JavaTasks** must be copied to the directory **<XL_HOME>/xellerate/JavaTasks**.

The recompiled custom java libraries that were originally in the directory **<XL_900_RM_HOME> /xlremote/JavaTasks** must be copied to the directory **<XL_RM_HOME>/xlremote/JavaTasks**.

Important: If you are upgrading from a non-clustered to a clustered environment, you must repeat this step on all cluster members.

Note: You do not need to recompile the adapters themselves.

Migrating Scheduled Tasks

Custom scheduled tasks that were functional in Oracle Xellerate Identity Provisioning 9.0.0 can be reused in your Oracle Identity Manager 9.0.1 environment after you have recompiled them using Oracle Identity Manager 9.0.1 libraries.

The recompiled custom scheduled tasks need to be copied to the directory **<XL_HOME>/xellerate/ScheduleTask**.

Note: If you are upgrading from a non-clustered to a clustered environment, you must repeat this step on all cluster members.

Migrating Event Handlers

Custom event handlers that were functional in Oracle Xellerate Identity Provisioning 9.0.0 can be reused in your version 9.0.1 environment after you have recompiled them using Oracle Identity Manager 9.0.1 libraries.

The recompiled custom event handlers must be copied to the directory **<XL_HOME>/xellerate/EventHandlers**.

Note: If upgrading from a non-clustered environment to a clustered environment then repeat this step on all cluster members.

Migrating xlWebApp Customizations

You must reapply any customizations (for example, JSP customizations) made to the Oracle Xellerate Identity Provisioning 9.0.0 web application to the 9.0.1 Oracle Identity Manager environment.

Migrate any customizations previously applied to your version 9.0.0 web application to the out-of-box version 9.0.1 web application **xlWebApp.war**, which resides in the directory **<XL_HOME>/xellerate/webapp**.

After migrating the 9.0.0 web application customizations, you must patch your version 9.0.1 web application. See Appendix B, "Patching an Existing Oracle Identity Manager Installation" on page B-1 for more information.

Migrating Custom Clients

Any custom clients that were built using Oracle Xellerate Identity Provisioning 9.0.0 APIs must be updated to make them compatible with the Oracle Identity Manager 9.0.1 APIs. For example, certain APIs might have been deprecated and replaced by new APIs. Refer to the *Oracle Identity Manager Release Notes* for a comprehensive list of API calls that have changed between Oracle Xellerate Identity Provisioning 9.0.0 and Oracle Identity Manager 9.0.1.

Upgrading the Diagnostic Dashboard

To upgrade your existing 9.0.0 Diagnostic Dashboard to version 9.0.1, you must install a new instance of the Diagnostic Dashboard. Use the following steps to upgrade to the 9.0.1 Diagnostic Dashboard:

1. Install a new instance of the XIMDD application using the new, version 9.0.1 XIMDD.war file in the Patch\DiagnosticDashboard directory
2. Refer to "Installing the Diagnostic Dashboard" on page 2-7 for more information.

15

Troubleshooting Your Oracle Identity Manager Installation

This section describes problems that can occur during the Oracle Identity Manager Installation.

> **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)

A

Supplementary Upgrade Information

Use the additional information in this Appendix as a supplement to Chapter 13, "Upgrading to Oracle Identity Manager 9.0.1 from Versions 8.5.2 or 8.5.3" on page 13-1 and Chapter 14, "Upgrading to Oracle Identity Manager 9.0.1 from Version 9.0.0" on page 14-1 to assist you in the upgrade process.

Creating a User Profile Audit File Group in SQL Server

User Profile Audit is one of the new features introduced in Oracle Identity Manager 9.0.1. For performance reasons, UPA tables are placed in a separate file group called **XELL_UPA**, which must be created by your database administrator before you upgrade Oracle Identity Manager. Complete the following steps to create the new file group.

1. 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 the **server on which your database is running**.
3. Double-click **Databases**, right-click the database that needs to be upgraded, then click **Properties**.
4. Click the **Data Files** tab, specify the filename and location of the .NDF file as well as the amount of space allocated for this file.
5. Add a new **filegroup** named **XELL_UPA**.
6. Click **OK**.

Executing the SQL Server Upgrade Script

The upgrade package includes command line scripts that will upgrade the Oracle Xellerate Identity Provisioning 8.5.x or 9.0.0 SQL Server database and associated stored procedures to Oracle Identity Manager 9.0.1. These command line scripts execute a set of SQL Server scripts through the OSQL interface on the SQL Server database. All the command line scripts take the following five parameters.

Table A–1 Parameters for Command Line Scripts

Arguments	Description
<server-name[\instance-name]>	The name of the server under the "SQL Server Group" in Enterprise Manager. **\instance-name** represents the instance running under the server.
<db-user>	The database user ID
<password>	The password of db-user
<db-name>	The name of the database
<script-location>	The absolute path to the command line script

For example:

1. To upgrade the database, run the batch file **<Patch>/Database/SQLServer/Scripts/upg_852_853_to_901.bat**, with the following command-line arguments:

   ```
   <Patch>/Database/SQLServer/Scripts/upg_852_853_to_901.bat
   <server-name[\instance-name]> <db-user> <password> <db-name>
   <Patch>/Database/SQLServer/Scripts
   ```

   Note: If you are upgrading to Oracle Identity Manager 9.0.1 from Oracle Xellerate Identity Provisioning 9.0.0, you will be using **upg_900_to_901.bat** in the preceding example.

2. To compile the new stored procedures, run **<Patch>/Database/SQLServer/StoredProcedures/compile_all_XL_SP.bat** with the following command-line arguments:

   ```
   <Patch>/Database/SQLServer/StoredProcedures/compile_all_XL_SP.bat
   <server-name[\instance-name]> <db-user> <password> <db-name>
   <Patch>/Database/SQLServer/StoredProcedures
   ```

3. To enable the Oracle Identity Manager Audit and Compliance module, run the batch file **<Patch>/Database /SQLServer/Scripts/SQLServer_Enable_XACM.bat**, with the following command-line arguments:

   ```
   SQLServer_Enable_XACM.bat <server-name[\instance-name]> <db-user> <password>
   <db-name> <Patch>/Database/SQLServer/Scripts
   ```

Loading Metadata into the Database

You must load certain metadata into your database by completing the following steps:

1. As appropriate for the operating system of the machine hosting your Oracle Identity Manager server, edit either **LoadXML.bat** or **LoadXML.sh** located in **<Patch>/Database/Utilities/** and update the value for the variable **JAVA_HOME**.
2. As appropriate for your database and operating system of the machine hosting your Oracle Identity Manager server, complete one of the following sub-steps:

   SQL Server and Windows

   a. Launch a plain-text editor, open the file **LoadXML.bat**, and uncomment the following line:

```
REM SET SQL_SERVER_DRIVER_DIR=
```

b. Assign the path to the SQL Server driver directory that contains the msbase.jar, msutil.jar and mssqlserver.jar files:

```
SET SQL_SERVER_DRIVER_DIR=<PATH_TO_SQL_DRIVER>
```

SQL Server and Linux

a. Launch a plain-text editor, open the file **LoadXML.sh**, and uncomment the following line:

```
#SQL_SERVER_DRIVER_DIR=
#export SQL_SERVER_DRIVER_DIR
```

b. Assign the path to the JDBC driver for SQL Server, so that the line reads something like the following:

```
SQL_SERVER_DRIVER_DIR=<PATH_TO_SQL_DRIVER>
export SQL_SERVER_DRIVER_DIR
```

Oracle and Windows

a. Launch a plain-text editor, open the file **LoadXML.bat**, and uncomment the following line:

```
REM SET ORACLE_DRIVER_DIR=
```

b. Assign the path to the Oracle driver directory containing the Oracle JDBC drivers:

```
SET ORACLE_DRIVER_DIR=<PATH_TO_ORACLE_DRIVER>
```

Oracle and Linux

a. Launch a plain-text editor, open the file **LoadXML.sh**, and uncomment the following line:

```
#ORACLE_DRIVER_DIR=
#export ORACLE_DRIVER_DIR
```

b. Assign the path to the JDBC driver for Oracle, so that the line reads something like the following:

```
ORACLE_DRIVER_DIR=<PATH_TO_ORACLE_DRIVER>
export ORACLE_DRIVER_DIR
```

3. Open a command prompt or console and run the **<Patch>/Database/Utilities/LoadXML.bat** or **LoadXML.sh** script with the following command line parameters in the specified order for the type of database you are using:

Oracle

a. JDBC URL (example: jdbc:oracle:thin:@<db_host_ip>:<port>:<SID>)

b. Database user name

c. Password

SQL Server

a. JDBC URL (example: jdbc:microsoft:sqlserver://<ipaddress>:<port>)

b. Database name

c. Database user name

d. Password

Upgrading the Server Configuration File

The primary configuration file for Oracle Identity Manager, which is named xlconfig.xml, has been updated for the 9.0.1 release. If you are upgrading from Oracle Xellerate Identity Provisioning version 8.5.x to Oracle Identity Manager 9.0.1, you must add or modify parameters in this file, as detailed in the following sub-sections.

Adding New Configuration Parameters

Add the following configuration parameters to your version 9.0.1 configuration file:

1. Launch a plain-text editor, then open xlconfig.xml, which resides in the directory **<XL_HOME>/xellerate/config/**.
2. Locate the parameter **<xl-configuration>.<Offlining>. .<MessageHandlerMDB>.<message-handler-task>**.

> **Note:** Refer to "Conventions" on page -viii for more information on identifying and locating xml tags.

Insert the following block of lines:

```
<AuditorOfflineMessage>com.thortech.xl.audit.engine.jms.XLAuditMessageHandler</
AuditorOfflineMessage>
<AttestationRequestMessage>com.thortech.xl.schedule.jms.attestation.processOffl
inedAttestationRequests</AttestationRequestMessage>
<AttestationTaskMessage>com.thortech.xl.schedule.jms.attestation.processOffline
dAttestationTasks</AttestationTaskMessage>
<AttestationWorkflowTaskMessage>com.thortech.xl.schedule.jms.attestation.proces
sOfflinedAttestationWorkflowTasks</AttestationWorkflowTaskMessage>
<ProcessOfflineMessage>com.thortech.xl.schedule.jms.processOfflineProcesses.pro
cessOfflinedProvisioningProcesses</ProcessOfflineMessage>
<ProcessTaskOfflineMessage>com.thortech.xl.schedule.jms.processTaskOffline.proc
essOfflinedProcessTask</ProcessTaskOfflineMessage>
```

after the string:

<xl-configuration>.<Offlining>.<MessageHandlerMDB>.<message-handler-task>.<ReconOfflineMessage>

but before the string:

<xl-configuration>.<Offlining>.<MessageHandlerMDB>.<message-handler-task>.<TestMessage>

3. Locate the configuration parameter <xl-configuration>.<Offlining>, then navigate to the space that starts after the following string:

```
<xl-configuration>.<Offlining>.</recon_offline_queue>
```

and before the following string:

```
<xl-configuration>.<Offlining>.<test_queue>
```

> **Note:** Refer to "Conventions" on page -viii for more information on identifying and locating xml tags.

Insert the following block of lines into the space between the preceding two strings:

```
<auditor_offline_queue>
   <queueName>queue/xlQueue</queueName>
   <autoAcknowledge>true</autoAcknowledge>
   <replyTo></replyTo>
   <persistentFlag>true</persistentFlag>
   <disableMessageId>true</disableMessageId>
   <disableTimeStampe>false</disableTimeStampe>
   <messageEncrypt>false</messageEncrypt>
</auditor_offline_queue>
<attestation_request_queue>
   <queueName>queue/xlQueue</queueName>
   <autoAcknowledge>true</autoAcknowledge>
   <replyTo></replyTo>
   <persistentFlag>true</persistentFlag>
   <disableMessageId>true</disableMessageId>
   <disableTimeStampe>false</disableTimeStampe>
   <messageEncrypt>false</messageEncrypt>
</attestation_request_queue>
<attestation_task_queue>
   <queueName>queue/xlQueue</queueName>
   <autoAcknowledge>true</autoAcknowledge>
   <replyTo></replyTo>
   <persistentFlag>true</persistentFlag>
   <disableMessageId>true</disableMessageId>
   <disableTimeStampe>false</disableTimeStampe>
   <messageEncrypt>false</messageEncrypt>
</attestation_task_queue>
<attestation_workflow_task_queue>
   <queueName>queue/xlQueue</queueName>
   <autoAcknowledge>true</autoAcknowledge>
   <replyTo></replyTo>
   <persistentFlag>true</persistentFlag>
   <disableMessageId>true</disableMessageId>
   <disableTimeStampe>false</disableTimeStampe>
   <messageEncrypt>false</messageEncrypt>
</attestation_workflow_task_queue>
<process_offline_queue>
       <queueName>queue/xlQueue</queueName>
       <autoAcknowledge>true</autoAcknowledge>
       <replyTo></replyTo>
       <persistentFlag>true</persistentFlag>
       <disableMessageId>true</disableMessageId>
       <disableTimeStampe>false</disableTimeStampe>
        <messageEncrypt>false</messageEncrypt>
</process_offline_queue>
<process_task_offline_queue>
    <queueName>queue/xlQueue</queueName>
     <autoAcknowledge>true</autoAcknowledge>
     <replyTo></replyTo>
     <persistentFlag>true</persistentFlag>
     <disableMessageId>true</disableMessageId>
     <disableTimeStampe>false</disableTimeStampe>
     <messageEncrypt>false</messageEncrypt>
</process_task_offline_queue>
```

4. Add the XML snippet <BlockMode>ECB</BlockMode> under the following two locations:

   - <xl-configration>.<Security>.<XLSymmetricProvider>.<Keys>.<DBSecretKey>

- <xl-configration>.<Security>.<XLSymmetricProvider>.<Keys>.<JMSKey>

5. Save and close the file.

Updating Existing Configuration Parameters

Complete the following steps to update existing configuration parameters:

1. Change the value of the following tag from ConnectionFactory to java:/JmsXA:

   ```
   <xl-configuration>.<Discovery>.<JMSServer>.<connectionFactory>
   ```

2. If you are upgrading an existing, non-clustered 8.5.x environment to a clustered, version 9.0.1 environment, change the value of the following tag from false to true on all cluster members:

   ```
   <xl-configuration>.<Scheduler>.<Clustering>
   ```

3. Locate the tag:

   ```
   <xl-configuration>.<RMSecurity>.<LoggerConfigFilePath>
   ```

   change it to the following value:

   ```
   <XL_RM_HOME>/xlremote/config/log.properties
   ```

Upgrading the Metadata File

The metadata file containing information related to user interface forms has been updated for Oracle Identity Manager 9.0.1. Complete the following steps to configure this metadata file:

1. Launch a plain-text editor, then open the file FormMetaData.xml, which resides in the directory **<XL_HOME>/xellerate/config/**.
2. Locate the XML element **<FormManagementMetaData>.<Attribute name="-30">**.
3. Change the value of **dataLength** from **256** to **30**. For example, change something like the following string:

   ```
   <Attribute name="-30" label="Group Name" displayComponentType="TextField"
   variantType="String" dataLength="256" map="Groups.Group Name" />
   ```

   to something like the following string:

   ```
   <Attribute name="-30" label="Group Name" displayComponentType="TextField"
   variantType="String" dataLength="30" map="Groups.Group Name" />
   ```

4. Navigate to the end of the file, then locate the following line:

   ```
   </FormManagementMetaData>
   ```

   Insert the following block just preceding the line **</FormManagementMetaData>**. (In other words, the inserted block should become the last XML elements under the document root **<FormManagementMetaData>**)

   This is the block to insert:

   ```
   <!-- List of attributes that will be displayed in the "Attestation Wizard" -->
   <Attribute name="-31" label="Groups" displayComponentType="LookupField"
   variantType="long" dataLength="50" map="Groups.Group Name">

   <ValidValues lookupMethod="findGroups"
   ```

```
operationClass="Thor.API.Operations.tcGroupOperationsIntf"
displayColumns="Groups.Group Name" selectionColumn="Groups.Group Name"
permission="write"/>
</Attribute>

<Attribute name="-32" label="Groups1" displayComponentType="LookupField"
variantType="long" dataLength="50" map="Groups.Group Name">

<ValidValues lookupMethod="findGroups"
operationClass="Thor.API.Operations.tcGroupOperationsIntf"
displayColumns="Groups.Group Name" selectionColumn="Groups.Group Name"/>
</Attribute>

<Attribute name="-33" label="Resources" displayComponentType="LookupField"
variantType="long" dataLength="50" map="Objects.Name">

<ValidValues lookupMethod="findObjects"
operationClass="Thor.API.Operations.tcObjectOperationsIntf"
displayColumns="Objects.Name" selectionColumn="Objects.Name"/>
</Attribute>

<Attribute name="-34" label="Users" displayComponentType="LookupField"
variantType="long" dataLength="50" map="Users.User Name">

<ValidValues lookupMethod="getActiveUsers"
operationClass="Thor.API.Operations.tcUserOperationsIntf"
displayColumns="Users.User ID,Users.Last Name,Users.First Name"
selectionColumn="Users.User ID" permission="write"/>
</Attribute>
```

Upgrading the Remote Manager Configuration File

The primary configuration file for the Remote Manager has been updated for the 9.0.1 release. If you are upgrading from Oracle Xellerate Identity Provisioning version 8.5.x to Oracle Identity Manager 9.0.1, you must add or modify parameters in the file **xlconfig.xml**, as detailed in the following sub-sections.

Adding New Configuration Parameters

Complete the following steps to add JMS-related parameters to the Remote Manager configuration file:

1. Launch a plain-text editor, then open xlconfig.xml, which resides in the directory **<XL_RM_HOME>/xlremote/config**.
2. Locate the parameter **<xl-configuration>.<Offlining>**, then find the line:

   ```
   Locate the parameter <xl-configuration>.<Offlining>, then find the line:
   ```

3. Insert the following block:

   ```
   <AuditorOfflineMessage>com.thortech.xl.audit.engine.jms.XLAuditMessageHandler</
   AuditorOfflineMessage>
   <AttestationRequestMessage>com.thortech.xl.schedule.jms.attestation.processOffl
   inedAttestationRequests</AttestationRequestMessage>
   <AttestationTaskMessage>com.thortech.xl.schedule.jms.attestation.processOffline
   dAttestationTasks</AttestationTaskMessage>
   <AttestationWorkflowTaskMessage>com.thortech.xl.schedule.jms.attestation.proces
   sOfflinedAttestationWorkflowTasks</AttestationWorkflowTaskMessage>
   ```

```
<ProcessOfflineMessage>com.thortech.xl.schedule.jms.processOfflineProcesses.pro
cessOfflinedProvisioningProcesses</ProcessOfflineMessage>
<ProcessTaskOfflineMessage>com.thortech.xl.schedule.jms.processTaskOffline.proc
essOfflinedProcessTask</ProcessTaskOfflineMessage>
```

after the following line:

```
<xl-configuration>.<Offlining>.<MessageHandlerMDB>.<message-handler-task>.<Recon
OfflineMessage>
```

and preceding the following line:

```
<xl-configuration>.<Offlining>.<MessageHandlerMDB>.<message-handler-task>.<Test
Message>
```

4. Locate the following parameter:

```
<xl-configuration>.<Offlining>
```

5. Insert the following block:

```
<auditor_offline_queue>
   <queueName>queue/xlQueue</queueName>
   <autoAcknowledge>true</autoAcknowledge>
   <replyTo></replyTo>
   <persistentFlag>true</persistentFlag>
   <disableMessageId>true</disableMessageId>
   <disableTimeStampe>false</disableTimeStampe>
   <messageEncrypt>false</messageEncrypt>
</auditor_offline_queue>
<attestation_request_queue>
   <queueName>queue/xlQueue</queueName>
   <autoAcknowledge>true</autoAcknowledge>
   <replyTo></replyTo>
   <persistentFlag>true</persistentFlag>
   <disableMessageId>true</disableMessageId>
   <disableTimeStampe>false</disableTimeStampe>
   <messageEncrypt>false</messageEncrypt>
</attestation_request_queue>
<attestation_task_queue>
   <queueName>queue/xlQueue</queueName>
   <autoAcknowledge>true</autoAcknowledge>
   <replyTo></replyTo>
   <persistentFlag>true</persistentFlag>
   <disableMessageId>true</disableMessageId>
   <disableTimeStampe>false</disableTimeStampe>
   <messageEncrypt>false</messageEncrypt>
</attestation_task_queue>
<attestation_workflow_task_queue>
   <queueName>queue/xlQueue</queueName>
   <autoAcknowledge>true</autoAcknowledge>
   <replyTo></replyTo>
   <persistentFlag>true</persistentFlag>
   <disableMessageId>true</disableMessageId>
   <disableTimeStampe>false</disableTimeStampe>
   <messageEncrypt>false</messageEncrypt>
</attestation_workflow_task_queue>
<process_offline_queue>
       <queueName>queue/xlQueue</queueName>
       <autoAcknowledge>true</autoAcknowledge>
       <replyTo></replyTo>
       <persistentFlag>true</persistentFlag>
```

```
        <disableMessageId>true</disableMessageId>
        <disableTimeStampe>false</disableTimeStampe>
         <messageEncrypt>false</messageEncrypt>
</process_offline_queue>
<process_task_offline_queue>
    <queueName>queue/xlQueue</queueName>
     <autoAcknowledge>true</autoAcknowledge>
     <replyTo></replyTo>
     <persistentFlag>true</persistentFlag>
     <disableMessageId>true</disableMessageId>
     <disableTimeStampe>false</disableTimeStampe>
     <messageEncrypt>false</messageEncrypt>
</process_task_offline_queue>
```

after the following line:

```
<xl-configuration>.<Offlining>.</recon_offline_queue>
```

and preceding the following line:

```
<xl-configuration>.<Offlining>.<test_queue>
```

> **Note:** Refer to "Conventions" on page -viii for more information on identifying and locating xml tags.

6. Save and close the file.

Updating Existing Configuration Parameters

To update Remote Manager-related configuration parameters.

1. Launch a plain-text editor, then open xlconfig.xml, which resides in the directory <XL_RM_HOME>/xlremote/config.
2. Locate the <xl-configuration>.<RMSecurity>.<LoggerConfigFilePath> tag and change it to the following value:

```
<XL_RM_HOME>/xlremote/config/log.properties
```

B

Patching an Existing Oracle Identity Manager Installation

Patching an existing Oracle Identity Manager installation involves assembling a new enterprise application archive (EAR) file from the latest libraries, then redeploying the EAR. To patch a JBoss installation, complete the following steps:

1. Stop your JBoss application server gracefully. Typically, you do this by running one of the following commands, as appropriate for the operating system on the machine hosting your Oracle Identity Manager server:

   Windows

   ```
   <JBoss-install-dir>/bin/shutdown.bat -S
   ```

   Linux

   ```
   <JBoss-install-dir>/bin/shutdown.sh -S
   ```

2. Run the following patch command:

   ```
   <XL_HOME>\xellerate\setup\patch_jboss.cmd
   ```

> **Note:** If you are upgrading from a non-clustered version 8.5.x or 9.0.0 Oracle Xellerate Identity Provisioning environment to a clustered version 9.0.1 Oracle Identity Manager environment, you must repeat these steps on each node in the cluster.