Oracle® Identity Manager

Installation and Upgrade Guide for WebLogic

Release 9.0

B28761-01

May 2006

ORACLE®

Oracle Identity Manager Installation and Upgrade Guide for WebLogic Release 9.0

B28761-01

Primary Author: Don Biasotti

Contents

10 Deploying in a Clustered WebLogic Configuration

11 Installing and Configuring Oracle Identity Manager Design Console

12 Installing and Configuring Oracle Identity Manager Remote Manager

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

14 Troubleshooting Your Oracle Identity Manager Installation

A Supplementary Upgrade Information

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 WebLogic application server
- upgrade to Oracle Identity Manager 9.0.1 from Oracle Xellerate Identity Provisioning versions 8.5.2 or 8.5.3

Note: The information in this guide applies generally to all Oracle Identity Manager 9.0.x versions. However, the Upgrade chapter (Chapter 13, "Upgrading to Oracle Identity Manager 9.0.1 from Versions 8.5.2 or 8.5.3") and Appendix A, "Supplementary Upgrade Information" contain version specific information about Oracle Identity Manager.

Audience

The *Oracle Identity Manager Installation and Upgrade Guide for WebLogic* is intended for System Administrators who plan to install Oracle Identity Manager 9.0 on a WebLogic application server, or upgrade from Oracle Xellerate Identity Provisioning versions 8.5.2 or 8.5.3 running on WebLogic 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 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. Additional examples of this convention include the following: <WEBLOGIC_HOME>, <XL_HOME>, <XL_DC_HOME>, <XL_RM_HOME>, <XL_85x_HOME>, <XL_85x_DC_HOME>, and <XL_85x_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

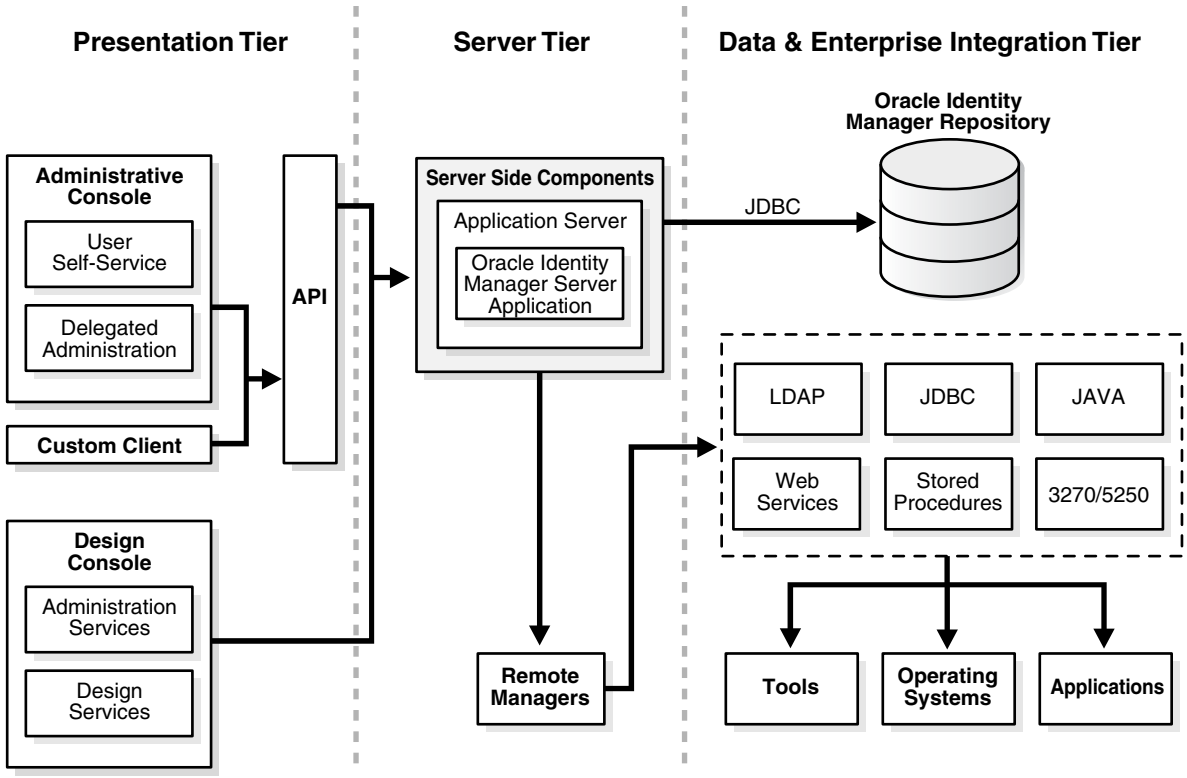
The Server tier contains the Oracle Identity Manager Server component, which serves as a bridge between the Presentation and Data and Enterprise Integration tiers. All requests between the clients and the database are processed through the Server tier.

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 WebLogic 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 hardware and software 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 2-6 for more information.

Installation Components

Oracle Identity Manager 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 database requirements 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 WebLogic Application Servers

Oracle Identity Manager Release 9.0 is certified on the BEA WebLogic Server 8.1 with Service Pack 4 application server.

WebLogic requires a JMS server running in each application server instance (clustered or non-clustered mode), so there is no need for a separate JMS server instance running on a host that is not running any Oracle Identity Manager component.

Supported Operating Systems

Oracle Identity Manager Release 9.0 for the BEA WebLogic 8.1 application server with Service Pack 4 is supported on the following operating systems:

- Microsoft Windows Server 2003 Enterprise Edition with SP1
- Solaris 10

Supported Databases

Select one database for your Oracle Identity Manager installation. Oracle Identity Manager 9.0 supports the following databases:

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

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, " Host requirements for Oracle Identity Manager Server" lists the host requirements for Oracle Identity Manager Server:

Table 2–1 Host requirements for Oracle Identity Manager Server

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
Solaris	■ Sun Fire 210 Server ■ 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: Solaris 10

Database Server Host Requirements

Table 2–2, " Sample Database Server Host Requirements" 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 Requirements

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 and 2003 Server
Solaris	■ Sun Fire 250 Server ■ 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) ■ Number of Hard Disks: 1 Disk (or more, as data grows and if needed) ■ Operating System: Solaris 10

Design Console Host Requirements

Table 2–1, " Host requirements for Oracle Identity Manager Server" 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, " Remote Manager Host Requirements" 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
Solaris	▪ Sun Fire 210 Server Memory: 1 GB (or more, if needed) ▪ Number of Processors: 1 (or more, if needed) ▪ Hard Disk Space: 10 GB (initial size) ▪ Operating System: Solaris 10
Solaris	▪ 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
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 Version Details

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

Table 2–5 Supported Version Details

Item	Version Details
BEA WebLogic	8.1 SP4, 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
Sun Solaris	10
JDK	See your WebLogic application server documentation for details about which specific JDK version.
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 2-5 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 UNIX: /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.	1521 for Oracle 1433 for SQL Server	
	The name of the database for your installation.	N/A[1]	
	The name and password of the database account Oracle Identity Manager uses to access the database.	N/A[1]	
	The JDK install directory	Windows: C:\j2sdk<version> UNIX: /opt/j2sdk<version>	
	The WebLogic install directory	Windows: C:\bea UNIX: /opt/bea	

[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

Note: Follow the instructions in Chapter 10, "Deploying in a Clustered WebLogic Configuration" if you are deploying in a clustered WebLogic environment.

To install and configure Oracle Identity Manager for WebLogic:

1. Install WebLogic—see "Installing WebLogic" on page 4-1 for more information.
2. Create a WebLogic domain, user, and group for Oracle Identity Manager—see "Creating a WebLogic Domain, User, and Group for Oracle Identity Manager" on page 4-1 for more information.
3. (Optional and for Solaris only) Set permissions to facilitate installing Oracle Identity Manager as a non-root user—see "Preparing to Install Oracle Identity Manager as a Non-Root User on Solaris" on page 4-3 for more information.
4. (Optional) Set up and use the Diagnostic Dashboard—see "Using the Diagnostic Dashboard" on page 2-6 for more information.
5. Install and setup your database—see Chapter 5, "Database Setup".

   Oracle

   a. Install Oracle—see "Installing Oracle" on page 5-1 for more information.
   b. Create the Oracle database —"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 SQL Server— see "Installing and Configuring SQL Server" on page 5-4 for more information.
   b. Register SQL Server—see "Registering SQL Server" on page 5-5 for more information.
   c. Create the SQL Server database—see "Creating an SQL Server Database" on page 5-5 for more information.
   d. Create the SQL Server database account—see "Creating an SQL Server Database Account" on page 5-7 for more information.
6. Install the Oracle Identity Manager software:

   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 on Windows" on page 12-1 for more information.

Solaris

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

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

7. Configure the Oracle Identity Manager Server and the WebLogic application server after installing the Oracle Identity Manager software—see Chapter 8, "Post-Install Configuration for Oracle Identity Manager and WebLogic" for more information.

8. Configure the Oracle Identity Manager Design Console—see"Post-install Requirements for the Design Console" on page 11-3 for more information.

9. Configure the Oracle Identity Manager Remote Manager—see "Configuring the Remote Manager" on page 12-4 for more information.

10. Start the Oracle Identity manager components:

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 Oracle Identity manager Design Console—see "Starting the Design Console" on page 11-3 for more information.

c. Start the Oracle Identity Manager Remote Manager—see "Starting Remote Manager" on page 12-6 for more information.

Solaris

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

b. Start the Oracle Identity Manager Remote Manager—see "Starting Remote Manager" on page 12-6 for more information.

4

Installing and Configuring WebLogic for Oracle Identity Manager

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

1. "Installing WebLogic" on page 4-1
2. "Creating a WebLogic Domain, User, and Group for Oracle Identity Manager" on page 4-1
3. (Optional and for Solaris only) "Preparing to Install Oracle Identity Manager as a Non-Root User on Solaris" on page 4-3

> **Note:** Follow the instructions in Chapter 10, "Deploying in a Clustered WebLogic Configuration" if you are deploying WebLogic in an application server cluster with managed servers.

After completing the tasks in this chapter, you must install and configure a database by following the steps in Chapter 5, "Database Setup" on page 21 before installing Oracle Identity Manager.

Installing WebLogic

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

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

Before you install Oracle Identity Manager on WebLogic, you must create a WebLogic domain, user, and group for Oracle Identity Manager. Use the following procedure to create a WebLogic domain, user, and group for Oracle Identity Manager by performing the steps specific to your operating system:

1. Launch the WebLogic Configuration Wizard:

   Windows:

   a. Start the Configuration Wizard from the Start menu by selecting **BEA WebLogic Platform 8.1>Configuration Wizard**.

   UNIX

a. Go to the WebLogic **bin** directory:

```
cd <WEBLOGIC_HOME>/weblogic81/common/bin
```

b. Start the Configuration Wizard using the following command:

```
sh config.sh
```

2. Perform the following steps from the Configuration Wizard:

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

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

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

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

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

---

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

f. Select the **Sun SDK**.

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

h. Exit the Configuration Wizard after the domain is created

3. Start the WebLogic Admin server:

Windows:

a. Start the WebLogic Admin server from the **Start** menu by selecting **BEA WebLogic Platform 8.1**>**User Projects**><**domain name**>>**Start Server**.

UNIX:

a. Go to the WebLogic **user_projects/domains** directory. For example:

```
cd <WEBLOGIC_HOME>/user_projects/domains/
```

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

```
cd <domain name>
```

c. Start the WebLogic Admin server using the following command:

```
sh startWebLogic.sh
```

4. Log in to the WebLogic Admin Server Console using your new account by pointing a web browser to the following url:
`http://<hostname>:7001/console`

a. Select **Security**>**Realms**>**myrealm**>**Groups** from the navigation panel on the left.

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

c. Enter **User** for the group name in the Name field under the General tab and optionally enter a description for the group. Click **Apply**.

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

---

d. Select **Security**>**Realms**>**myrealm**>**Users** from the navigation panel on the left.

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

f. Enter **Internal** for the user name in the Name field under the General tab and optionally enter a description for the user.

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

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

h. Select the **Groups** tab.

i. Add the **User** group to the list of Current Groups for the **Internal** user by selecting **User** from the list of Possible Groups and clicking the **--> right arrow button**. Click **Apply**.

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

Installing Oracle Identity Manager as a non-root user on a WebLogic application server running on Solaris requires certain permissions. Verify the following before attempting to install Oracle Identity Manager as a non-root user on a WebLogic application server running on Solaris:

- Verify the operating system user account installing Oracle Identity Manager has the following:
  - Write and execute permissions on the specific WebLogic Domain directory
  - (optional) Write permission on the WebLogic lib and lib/mbeantypes directories

5

Database Setup

Oracle Identity Manager requires a database. You must have your database set up and installed 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 an Oracle database—see "Creating an Oracle Database" on page 5-1 for more information.
3. Prepare the Database—see "Preparing the Oracle Database" on page 5-2 for more information.

Installing Oracle

Install Oracle9i or 10g Release 2 (see "Supported Databases" on page 2-2 for the specific supported databases). Oracle recommends using the **Typical** installation.

> **Note:** If you choose a **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 Unix)
- 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 Unix 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:

Unix:

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

2. Register your SQL Server—see"Registering SQL Server" on page 5-5 for more information.
3. Create a database for Oracle Identity Manager—see "Creating an SQL Server Database" on page 5-5 for more information.
4. Create a database account for Oracle Identity Manager—see "Creating an SQL Server Database Account" on page 5-7 for more information.

After you have completed these tasks, proceed to install Oracle Identity Manager.

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 the following Web site:

   `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. (See 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
   ```

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

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

Registering 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

Important: 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.

   c. Select Automatically Grow File.

   d. Select By Percent, then type 10 in the associated text box.

   e. 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 trigger 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 all of 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.

Note: Make sure the WebLogic server is running during Oracle Identity Manager installation.

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 "Installing the Design Console" on page 11-1for more information.
- Oracle Identity Manager Remote Manager—see"Installing the Remote Manager on Windows" on page 12-1 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 the particulars of your database.

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

> **Important:** If WebLogic is installed in nondefault directory (other than weblogic81), the Oracle Identity Manager installer will fail unless you create a symbolic link of weblogic81 for the nondefault directory where WebLogic is installed. You can create a symbolic link in Windows by using additional Microsoft or 3rd-party tools.

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 <**WEBLOGIC_HOME>\weblogic81\server\lib** directory and add the driver location to the system CLASSPATH environment variable:
   - mssqlserver.jar
   - msbase.jar
   - msutil.jar
2. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.

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

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 the type of database you are using with Oracle Identity Manager (either Oracle or SQL Server), then click Next.
8. On the Database Information page, provide all database connectivity information that is required to install the database schema. You install this schema just once, as part of your initial Oracle Identity Manager installation. Thereafter, you configure all the other Oracle Identity Manager components to point to this common schema.

   Note: To install against an existing database, verify that 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 verify your settings.

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. After you do that, click Next.

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 and click Next.
10. On the Application Server Selection page, select BEA WebLogic, and click Next.
11. On the Cluster Information page, specify the server configuration (clustered or non-clustered).
    - Select No for non-clustered and click Next.
    - Select Yes for clustered, enter the cluster name, and click Next.

Important: Refer to Chapter 10, "Deploying in a Clustered WebLogic Configuration" if you are deploying in a clustered environment.

---

12. On the WebLogic Directory page, enter the application server and Java information.
    a. Type the path to the root directory for your application server

       or

       Navigate to the root directory for your application server

    b. Type the path to the JDK directory associated with your application server

       or

       Navigate to the JDK directory associated with your application server.

c. Click Next.

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

Note: The information you enter differs for clustered and non-clustered installations.

WebLogic server information for a non-clustered installation

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

Note: The host name is case-sensitive.

---

b. Type the WebLogic Server Name (default is myserver).

c. Type the Admin Port (default is 7001).

d. Type the WebLogic Server Port (default is 7001).

e. Type the Login Name for the WebLogic domain administrator. (This is the administrator account you configured through the WebLogic configuration wizard).

f. Enter and confirm the domain administrator Password.

g. Click Next to commit your settings.

WebLogic server information for a clustered installation

a. Type the host name or IP address of the machine hosting the application server.

b. Type the Managed Server Name (for example, XL_MANAGED_SERVER_1).

Note: The host name is case-sensitive.

---

c. Type the Admin Port (default is 7001).

d. Type the Managed Server Port (for example, 7051).

e. Type the Login Name for the WebLogic domain administrator (the administrator account you configured using the WebLogic configuration wizard).

f. Type and confirm the administrator Password.

g. Click Next.

14. On the WebLogic Domain Information page, type the appropriate WebLogic domain information.

a. Type the path to the WebLogic domains folder.

or

Navigate to the location.

b. Type the configuration directory name (generally this is the same as the domain name).

c. Type the configuration directory name (generally this is the same as the domain name).

d. Click Next.

15. Backup your application server when the Application Server Configuration Backup screen appears, then click Next.

16. On the Installation Summary page, click Install to initiate the server software installation. Depending on the speed of your machine, the installation script may require a few minutes to load the base database schema script and generate the corresponding log file.

17. If the installer detects an existing encrypted database, it will display a pop-up message to copy the .xldatabasekey file to the new installation location. Click OK to proceed. If the existing database is not encrypted, you are prompted to encrypt it. Click OK to proceed.

18. On the Completed screen, click Finish to exit the installer.

Once you have finished installing the Oracle Identity Manager Server, follow the instructions in Chapter 8, "Post-Install Configuration for Oracle Identity Manager and WebLogic" to continue the installation.

7

Installing Oracle Identity Manager Server on UNIX

This chapter describes how to install Oracle Identity Manager on a computer running UNIX. Refer to "Supported Operating Systems" on page 2-2 for more information on the supported UNIX platforms. You must install the Oracle Identity Manager server on systems running the application server. Oracle Identity Manager components such as the Remote Manager can be installed on separate systems. Each component has its own installer.

Note: Make sure the WebLogic server is running during Oracle Identity Manager installation.

Oracle Identity Manager Components

Oracle Identity Manager on UNIX includes the following components:

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

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

Installing Documentation

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

Installing the Oracle Identity Manager Server on UNIX

Oracle Identity Manager for UNIX 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 **2**.
- To cancel the installation, type the number **3**.
- To redisplay the current panel, type the number **5**.

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

Note: If WebLogic is installed in nondefault directory (other than weblogic81), the Oracle Identity Manager installer will fail unless you create a symbolic link of weblogic81 for the nondefault directory where WebLogic is installed. You can create a symbolic link in UNIX by using the internal ln command.

To install Oracle Identity Manager server for UNIX:

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 <WEBLOGIC_HOME>/weblogic81/server/lib/ directory and add the driver location to the system CLASSPATH environment variable:
   - mssqlserver.jar
   - msbase.jar
   - msutil.jar
2. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.
3. From the console, change directory (cd) to the installServer directory on the installation CD and perform the following:
   a. Set the JAVA_HOME variable to the Sun JRE 1.4.2 or higher, for example:

      ```
      export JAVA_HOME=/opt/bea/jdk142_05
      ```

   b. Prepend the PATH variable with the /jre/bin directory, for example:

```
export PATH=/opt/bea/jdk142_05/jre/bin:$PATH
```

4. Run the install_server.sh file using the following command:

   ```
   $ sh install_server.sh
   ```

5. 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 panel appears.

   b. Type 1 to move 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 chmod -R u+x *.sh command.

6. Select the application to install:

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

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

7. 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 then backup your previous Oracle Identity Manager home by renaming the original directory.

   Furthermore, 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. In some cases (such as a new installation), the config directory is not created. This does not indicate a failure in the installer. You must then create the config directory and copy the .xldatabasekey file into it.

8. Specify the type of database you are using.
   - Type 1 to select Oracle.
   - Type 2 to select SQL Server.
   - Type 0 to finish.
   - Type 1, to move to the next panel.

   The Database Information panel appears.
9. 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.
10. 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.
11. Specify your application server type.
   - Type 3 for BEA WebLogic
   - Type 0 when you are finished
   - Type 1 to move to the next panel

   The Cluster Information panel appears.
12. Specify if the application server is clustered or not, provide the information specific to your cluster, then perform the following sub-steps:

- Type 1 for Yes.
- Type 2 for No.
- Type 0 when you are finished
- If you selected Yes, enter the cluster name at the prompt
- Type 1 to move to the next section.

The Application Server Information panel appears.

13. Enter the application server information at the prompts.
    - Enter the path to the application server or press Enter to accept the default.
    - Enter the path to the application server's JDK directory or press Enter to accept the default.
    - Type 1 to move to the next panel.

    The application server information panel appears.
14. Enter the login information for the application server:

    Note: The information you enter differs for clustered and non-clustered installations.

    WebLogic server information for a non-clustered installation

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

    Note: The host name is case-sensitive.

    b. Enter the WebLogic Server Name (default is myserver).
    c. Enter the Admin Port (default is 7001).
    d. Enter the WebLogic Server Port (default is 7001).
    e. Enter the Login Name for the WebLogic domain administrator. (This is the administrator account you configured through the WebLogic configuration wizard).
    f. Enter and confirm the domain administrator Password.
    g. Enter 1 to move to the next section.

    WebLogic server information for a clustered installation

    a. Enter the host name or IP address of the machine hosting the application server.
    b. Enter the Managed Server Name (for example, XL_MANAGED_SERVER_1).

    Note: The host name is case-sensitive.

    c. Enter the Admin Port (default is 7001).
    d. Enter the Managed Server Port (for example, 7051).

e. Enter the Login Name for the WebLogic domain administrator (the administrator account you configured using the WebLogic configuration wizard).

f. Enter and confirm the administrator Password.

g. Enter 1 to move to the next section.

   The second application server information panel appears.

15. Enter the domain information:

    a. Enter the domain location. This is the WebLogic directory that contains domain directories (sometimes called the configuration or target location in WebLogic).

    b. Enter the configuration directory name. This is the directory that contains the specific domain that you are installing Oracle Identity Manager in (sometimes called the configuration or domain name).

    c. Enter the domain name. This is the name of the domain that you are installing Oracle Identity Manager in.

    d. Type 1 to move to the next section.

16. When a message warning you to back up your application server installation appears, proceed to back up your installation, then type 1 to move to the next section.

17. After the Information Summary page appears, verify the information displayed, then do one of the following:

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

    Oracle Identity Manager installs and the Completed panel appears.

18. Type **3** to finish.

Once you have finished installing the Oracle Identity Manager Server, follow the instructions in Chapter 8, "Post-Install Configuration for Oracle Identity Manager and WebLogic" to continue the installation.

8

Post-Install Configuration for Oracle Identity Manager and WebLogic

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 for all Oracle Identity Manager installations—see "General Post-installation Tasks" on page 8-1 for more information.
- Post-installation tasks for a WebLogic configuration—see "Post-Installation Steps for WebLogic" on page 8-4 for more information.

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 WebLogic-based Oracle Identity Manager installations, logging is configured in the logging properties file, <**XL_HOME>/xellerate/config/log.properties**.

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.ACCOUNTMANAGEMENT

log4j.logger.XELLERATE.SERVER

log4j.logger.XELLERATE.RESOURCEMANAGEMENT

log4j.logger.XELLERATE.REQUESTS

log4j.logger.XELLERATE.WORKFLOW

log4j.logger.XELLERATE.WEBAPP

log4j.logger.XELLERATE.SCHEDULER

log4j.logger.XELLERATE.SCHEDULER.Task

log4j.logger.XELLERATE.ADAPTERS

log4j.logger.XELLERATE.JAVACLIENT

log4j.logger.XELLERATE.POLICIES

log4j.logger.XELLERATE.RULES

log4j.logger.XELLERATE.DATABASE

log4j.logger.XELLERATE.APIS

log4j.logger.XELLERATE.OBJECTMANAGEMENT

log4j.logger.XELLERATE.JMS

log4j.logger.XELLERATE.REMOTEMANAGER

log4j.logger.XELLERATE.CACHEMANAGEMENT

log4j.logger.XELLERATE.ATTESTATION

log4j.logger.XELLERATE.AUDITOR
```

Setting Log Levels for WebLogic

To set Oracle Identity Manager log levels in Oracle Identity Manager running on WebLogic, edit the logging properties file (log.properties).

Complete the following steps to set log levels:

1. Open the <XL_HOME>\xellerate\config\log.properties file in a text editor. This file contains a general setting for Oracle Identity Manager and specific settings for the components and modules that comprise Oracle Identity Manager.

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

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

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

2. Set the general value to the desired log level. 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
3. Set other component log levels as desired. Individual components or modules can have different log levels. For example, the following values set the log level for the Account Management module to INFO, while the server is at DEBUG and the rest of Oracle Identity Manager is at the WARN level.

   ```
   log4j.logger.XELLERATE=WARN

   log4j.logger.XELLERATE.ACCOUNTMANAGEMENT=INFO

   log4j.logger.XELLERATE.SERVER=DEBUG
   ```
4. Save your changes.
5. Restart your application server so that the changes take effect.

Post-Installation Steps for WebLogic

After you install the Oracle Identity Manager software, perform the tasks in this section:

Configuring WebLogic for Oracle Identity Manager

Once you install Oracle Identity Manager, you must set the memory size, set up the authentication information for Oracle Identity Manager, then create and configure an XML registry.

To configure WebLogic for Oracle Identity Manager:

1. Use the WebLogic administration console to shutdown the application server gracefully.
2. Navigate to <**WEBLOGIC_HOME>\user_projects\domains\<domain_name**> (for example, C:\bea\user_projects\domains\mydomain).
3. Open the WebLogic start script file in a text editor. The start script is:
   - startWebLogic.cmd for Windows.
   - startWebLogic.sh for Solaris.
4. Edit the script to specify memory options:

   For Windows:

   Locate the line that starts with:

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

and add the following line preceding it:

```
MEM_ARGS="-Xmx1024m"

export MEM_ARGS
```

5. Save and close the file.
6. Restart the WebLogic server by navigating to the directory

   <XL_HOME>\xellerate\bin\ and running xlStartServer.bat (for Windows) or xlStartServer.sh (for UNIX).
7. Login to the WebLogic administration console.
8. In the left frame, select Security, select Realms, select myrealms, select Providers, then select Authentication.
9. Click Configure a new **Xellerate Authenticator.**
   a. Leave Name as the default.
   b. Set the **Control Flag** to **Sufficient**, then click **Create**.
10. In the left frame, click **Authentication** and select **DefaultAuthenticator**.
    a. Set the **Control Flag** to **Sufficient**, then click **Apply**.
11. In the left frame, click Services.
12. Right-click XML, then select Configure a new XMLRegistry from the short-cut menu.
13. Enter the registry information:
    a. Enter a unique name, such as Oracle Identity Manager XML registry.
    b. Use default values for the other fields, then click Create.
14. Click the **Target and Deploy** tab.
    a. Click the server check box to select it (myserver is the default server name).
    b. Click Apply.

    Note: For clustered environments, be sure perform this step on all cluster members.

15. In the left-hand frame, click **XML**, then click your new XML registry entry to expand it.
16. Right-click Parser Select Entries, then select Configure a New XMLPareserSelectRegistryEntry from the short-cut menu.
17. Enter the configuration information:
    a. Make sure the Public ID field is blank.
    b. Make sure the System ID field is blank.
    c. In the Root Element Tag field, enter database.
    d. In the Document Builder Factory field, enter the following string:

       `org.apache.crimson.jaxp.DocumentBuilderFactoryImpl`
    e. Make sure the Parser Class Name field is blank.
    f. In the SAX Parser Factory field, enter the following string:

       `org.apache.xerces.jaxp.SAXParserFactoryImpl`.
    g. Click Create.

18. Stop the WebLogic application server gracefully.
19. If you are using an Oracle database, copy the ojdbc14.jar file from `<XL_HOME>\xellerate\ext\` to `<WEBLOGIC_HOME>\weblogic81\server\lib\`. For clustered environments, copy the ojdbc14.jar file to `<WEBLOGIC_HOME>\weblogic81\server\lib\` on each of the `XLMANAGED_SERVER_HOST` nodes in the cluster.
20. Restart the WebLogic Server in order for the new configuration to become active.

Configuring XA Connection Settings

After you install Oracle Identity Manager on WebLogic, you must set up an XA connection by completing the following steps:

1. Log in to the WebLogic administrative console, and select Services.
2. Select JDBC on the Services page.
3. Select Connection Pools on the JDBC page.
4. Select xlXAConnectionPool on the Connection Pools page.
5. Select the Connections tab.
6. Select Show under Advanced Options.
7. Select Keep XA Connection Till Transaction Complete.
8. Click Apply to commit your changes.
9. Restart your WebLogic application server.

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>
```

9

Starting Oracle Identity Manager

This chapter, describes how to start the various Oracle Identity Manager components for Windows and UNIX.

> **Note:** You must complete all relevant post-installation steps described in Chapter 8, "Post-Install Configuration for Oracle Identity Manager and WebLogic" before starting Oracle Identity Manager.

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

There are two command scripts for starting your WebLogic application server:

- xlStartServer.bat for an administrative server, which resides in the <XL_HOME>\xellerate\bin directory.

- xlStartManagedServer.cmd for a managed server, which resides in the directory <WEBLOGIC_HOME>\user_projects\domains\<domain_name>\, where <domain_name> is the name of your WebLogic domain.

Starting the Administrative and User Console

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 default port number for WebLogic is 7001.

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

For example:

`http://localhost:7001/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 UNIX

This section describes how to start Oracle Identity Manager on Solaris. 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 Administrative and User Console

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 default port for WebLogic is 7001.

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

For example:

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

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

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

Using Diagnostic Dashboard to Verify Installation

The Diagnostic Dashboard verifies each component in your post-installation environment by testing for:

- A trusted Store
- Single Sign-On Configuration
- Messaging capability
- A task scheduler
- A Remote Manager

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

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

10

Deploying in a Clustered WebLogic Configuration

This chapter explains how to deploy Oracle Identity Manager in a clustered WebLogic 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 running applications on a WebLogic cluster. These instructions only provide details specific to Oracle Identity Manager. They are not complete instructions for setting up a WebLogic cluster. For more information on clustering, consult your WebLogic documentation.

A clustered environment requires multiple host computers. These instructions involve a deployment of 3+n machines. Your configuration may vary.

Table 10-1 describes the entities needed for a cluster, the computers that they run on, and the software required for the entities. Host computers and entities are labeled descriptively.

Table 10–1 WebLogic-based Oracle Identity Manager Cluster Host Computers

Host Computers	Entities	Software	Description
ADMIN_SERVER_HOST	Administrative Server	WebLogic	The Administrative Server is the WebLogic Server instance that configures and manages the WebLogic Server instances in its domain.
XLMANAGED_SERVER_HOST_n	xlManagedServer_n node manager	WebLogic Oracle Identity Manager Server	Managed Servers are WebLogic Server instances that are the cluster members. Members are controlled by the Administration Server. Each application server in your cluster runs Oracle Identity Manager. The managed servers run on one or more host computers (replace n with a number, such as xlManagedServer_1). You can have more than one application server for each host computer.
NA	xlCluster		The name of the WebLogic cluster for Oracle Identity Manager.

Table 10–1 (Cont.) WebLogic-based Oracle Identity Manager Cluster Host Computers

Host Computers	Entities	Software	Description
IIS_HOST	IIS server	IIS WebLogic IIS plug-in	The IIS web server acts as the front end to the WebLogic cluster, and handles load balancing.

Setting Up a WebLogic Oracle Identity Manager Cluster

The basic procedure for deploying Oracle Identity Manager in a WebLogic cluster is to install and configure an administrative server and a single managed server, and then clone the managed server for the other cluster members.

Note: This chapter assumes that you are running a dedicated administrative server host which is not running Oracle Identity Manager.

To set up a WebLogic Oracle Identity Manager cluster:

1. Install WebLogic on the ADMIN_SERVER_HOST.
2. Install WebLogic on all managed hosts (XLMANAGED_SERVER_HOST_1...n).
3. Configure the XLMANAGED_SERVER_HOST_1 to listen to the administrative server—see "Configuring a Node Manager for a Managed Server" on page 10-3 for more information.
4. Create a WebLogic configuration—see"Creating a WebLogic Configuration" on page 10-3 for more information.
5. Configure the Remote Start options for xlManagedServer1 and start the cluster—see "Configuring Remote Start Options" on page 10-7 for more information.
6. Install Oracle Identity Manager on the ADMIN_SERVER_HOST—see "Installing Oracle Identity Manager" on page 10-8 for more information.
7. Configure WebLogic—see"Configuring WebLogic Post-Oracle Identity Manager Installation" on page 10-8 for more information.
8. Add new servers to your cluster—see "Adding New Servers to Your WebLogic Cluster" on page 10-10 for more information.
9. (Optional) Configure the IIS Proxy Plug-Ins—see "Configuring IIS Proxy Plug-ins" on page 10-12 for more information.
10. (Optional) Configure database-based HTTP session failover—see "Configuring Database-based HTTP Session Failover" on page 10-12 for more information.

Installing WebLogic

Install WebLogic on the administrative server and XLMANAGED_SERVER_HOST_1 and any other XLMANAGED_SERVER_HOST_n machines. Configure the node manager on all MANAGED_SERVER_HOST machines so they can be controlled by the administrative server. See "Configuring a Node Manager for a Managed Server" on page 10-3 for more information.

Configuring a Node Manager for a Managed Server

To control your remote servers from the administrative server, once you install WebLogic on a host machine, you must edit the nodemanager.hosts file. For each machine on which you have installed WebLogic, Edit the file to specify the IP address of your administrative host. The default location of the nodemanager.hosts is:

Windows:

```
<WEBLOGIC_HOME>\weblogic81\common\nodemanager
```

UNIX:

```
<WEBLOGIC_HOME>/weblogic81/common/nodemanager
```

Creating a WebLogic Configuration

Before installing Oracle Identity Manager, prepare your administrative server host (ADMIN_HOST). Use the WebLogic Configuration Wizard to create a configuration. The configuration includes a domain for Oracle Identity Manager, a cluster, and settings for your managed server (xlManagedServer_1) and its host machine (XLMANAGED_SERVER_HOST_1).

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

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

To create a WebLogic Oracle Identity Manager cluster configuration:

1. Start the **Configuration** Wizard:

   Windows:

   Click **Start**, select **Programs**, select **BEA WebLogic Platform 8.1**, then select **Configuration Wizard**.

   UNIX:

   Run **<WEBLOGIC_HOME>/weblogic81/common/bin/config.sh**.

2. On the Create or Extend a Configuration page, create a new configuration:

   a. Click the **Create a new WebLogic configuration** radio button to select it.

b. Click **Next**.

3. On the Select a Configuration Template page, select the basic template:
   a. Select the **Basic WebLogic Server Domain** template.
   b. Click **Next**.
4. On the Choose Express or Custom Configuration page, choose a custom configuration:
   a. Click the **Custom** radio button to create a custom configuration.
   b. Click **Next**.
5. On the Configure the Administration Server page, enter your administration server information:
   a. Enter a name for the Administrative server (such as **AdminServer**).
   b. Accept the defaults for the other fields.
   c. Click **Next**.
6. On the Managed Servers, Clusters, and Machine Options page, set up your cluster:
   a. Click the Yes radio button to create the cluster.
   b. Click **Next**.
7. On the Configure Managed Servers page, configure your managed server:
   a. Click the **Add** button to create a Managed Sever entry.
   b. Click **Next**.
8. On the Configure Cluster page, configure your cluster:
   a. Click the **Add** button to create a cluster entry.
   b. Specify a name for the cluster (such as **xlCluster**).
   c. Provide a unique multicast address and port number.

      At this time, the Cluster Address is not required.
   d. Click **Next**.
9. On the Assign Servers to Cluster page, assign the managed server to your cluster:
   a. Highlight the managed server name from the **Server** pane.
   b. Use the right arrow to assign it to the cluster.
   c. Click **Next**.
10. On the Configure Machines page, configure your managed server host machine:

    For a Windows host:
    a. Click the **Machine** tab.
    b. Click the **Add** button.
    c. Enter the name of the managed server host (such as **XLMANAGED_SERVER_HOST_1**).
    d. Enter the **host address**.
    e. Enter the **listen port**.
    f. Click **Next**.

For a UNIX host:

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

   The *Configure Machines* page UNIX machine tab appears.

b. Click the **Add** button.

c. Enter the name of the managed server host (such as **XLMANAGED_SERVER_HOST_1**).

d. Select if you want to enable GID binding.

e. Enter the GID to bind as.

f. Select if you want to enable UID binding.

g. Enter the UID to bind as.

h. Enter the host address.

i. Enter the listen port.

j. Click **Next**.

11. On the Assign Servers to Machines page, assign the managed server to the managed server host machine:

    a. Select the server.

    b. Select the host machine.

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

    d. Click **Next**.

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

    a. Click **No**.

    b. Click **Next**.

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

    a. Click **No**.

    b. Click **Next**.

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

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

    b. Enter a password and confirm it.

    c. If desired, enter a description for the user. (Optional)

    d. Click the **Yes** radio button to create an additional user and group which are required by Oracle Identity Manager (so the *Internal* user can be created for Oracle Identity Manager).

    e. Click **Next**.

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

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

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

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

c. Enter a **password** and confirm it.

d. Enter a **description** for this user.

e. Click the **Group** tab.

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

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

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

> **Note:** The User group name is case-sensitive.

    c. Enter a description for the group.

    d. Click **Next**.

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

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

    b. Click the Internal user check box in the **User** list to select it.

    c. Click **Next**.

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

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

    If you are running the Wizard on a Windows machine, the Configure Windows Options page appears. Otherwise, the The Configure Server Start Mode and Java SDK page appears. In this case, skip this step and continue with Step 21.

20. Configure your Windows Options. You can choose to create a start menu shortcut for the administrative server, and to run the administrative server as a Windows service.

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

    b. Click **Next**.

> **Note:** If you add a shortcut to the Start Menu, the Build Start Menu Entries screen appears. Select or decline the options, then click **Next**.

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

    a. Select the desired **mode** for WebLogic.

    b. Select the **Sun SDK**.

    c. Click **Next**.

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

    - Enter the **name of your domain** in the **Configuration Name** field.

- If desired, change the **Configuration Location**.
- Review other configuration details. If desired, go back to make any changes.
- Click **Create**.

23. On the Creating Configuration page, complete your configuration and start the administrative server.
    - Click the **Start Admin Server** check box (Note that this applies to Windows only. To start the admin server on UNIX, see "Starting the Administration Server on UNIX" on page 10-7 for more information.)
    - Click **Done**.

The wizard exits and the server starts.

Starting the Administration Server on UNIX

To start the admin server on a UNIX machine, use the following commands:

cd <WEBLOGIC_HOME>/user_projects/domains/<domain_name>

sh startWebLogic.sh.

The server starts.

Configuring Remote Start Options

To allow the managed servers to be controlled remotely by the administration console, set the server classpath and the memory parameters. Use the WebLogic administration console to configure the server.

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

To configure the server remote start options:

1. To open the WebLogic administration console, point your browser to the following URL:

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

2. Click the server name (for example **xlManagedServer_1**) under **<domain name>/Servers**.
3. Click the **Remote Start** tab.
4. For UNIX, skip to the next step. For Windows, locate the **Class Path** field and enter the path to the **weblogic.jar**, for example:

   ```
   c:\bea\weblogic81\server\lib\weblogic.jar;
   ```

5. Set the arguments to **–Xmx512m** to increase the memory.
6. Make sure the Node Manager is running on the remote host (for example XLMANAGED_SERVER_HOST_1). If not, start the node manager on the host.
7. Start the server (for example xlManagedServer_1) from the administration console.
   a. Click **<domain>**, select **Clusters**, select **xlCluster**, then select **<xlManagedServer_n>** in the navigation bar on the left side of the screen.
   b. Select the **Control** tab in the main pane.

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

Note: If you have a problem starting the server because of Host Name validation, go to **server**, select **Key Stores & SSL** under the **Configuration** tab and change **None** to **Hostname Verification** under the **Advanced Options** and start the server again.

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

Installing Oracle Identity Manager

Install Oracle Identity Manager on ADMIN_HOST. See either Chapter 6, "Installing Oracle Identity Manager Server on Windows" or Chapter 7, "Installing Oracle Identity Manager Server on UNIX" for more information.

Configuring WebLogic Post-Oracle Identity Manager Installation

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

Perform the following post-installation steps:

1. Stop the managed server and administration server.

   Restart the administration server using **xlStartServer.bat** for Windows, or **xlStartServer.sh** for UNIX. See Chapter 9, "Starting Oracle Identity Manager" for more information on starting the administration server.

2. Complete the post-installation tasks to configure Oracle Identity Manager for WebLogic, including creating the Xellerate authenticator and setting the control flags to **sufficient** for both the Default authenticator and Xellerate Authenticator. See "Configuring WebLogic for Oracle Identity Manager" on page 8-4 for more information.

3. Copy the complete Oracle Identity Manager directory from ADMIN_HOST to XLMANAGED_SERVER_HOST_1 maintaining the identical directory hierarchy structure. If the XLMANAGED_SERVER_HOST_1 is located on the same machine as ADMIN_HOST, you do not need to copy the Oracle Identity Manager directory.

4. Each server in the cluster needs to know the location of the others. See for more information. See "Specifying Cluster Members" on page 10-9 for more information.

5. If XLMANAGED_SERVER_HOST_1 is a different machine than ADMIN_HOST, copy the following Oracle Identity Manager files to the WebLogic installation directory on the XLMANAGED_SERVER_HOST_1:

   - copy **<XL_HOME>\ext\nexaweb-common.jar to the <WEBLOGIC_HOME>\weblogic81\server\lib** directory
   - copy **<XL_HOME>\xellerate\lib\wlXLSecurityProviders.jar to the <WEBLOGIC_HOME>\weblogic81\server\lib\mbeantypes** directory

6. Start the cluster.

Specifying Cluster Members

To specify the location of all the cluster members, edit the xlconfig.xml file (located in the <XL_HOME>\xellerate\config directory) for each Oracle Identity Manager component. Modify the Discovery section to specify the cluster members.

You can accomplish this one of two ways:

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

  If you use this approach, the port number has to be same on all the machines.

- Specify a list of server URLs (including port), for each of the servers in the cluster.

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

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

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

Adding New Servers to Your WebLogic Cluster

Once you have set up your cluster, you can add more servers by cloning your first managed server (*xlManagedServer1*).

> **Note:** If you install WebLogic in a different location on a new managed server host, additional configuration is necessary.

To add a server to your cluster:

1. Install WebLogic on XLMANAGED_SERVER_HOST_n. See "Installing WebLogic" on page 10-2 for more information.

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

2. Configure the Node Manager for xlManagedServer_n. See "Configuring a Node Manager for a Managed Server" on page 10-3 for more information.
3. Set up the Oracle Identity Manager Server on XLMANAGED_SERVER_HOST_n. See "Installing the Oracle Identity Manager Server on New Hosts" on page 10-10 for more information.
4. Configure the XLMANAGED_SERVER_HOST_n machine. See "Configuring New Host Machines" on page 10-10 for more information.
5. Add the new host machine to the list of cluster members. See "Specifying Cluster Members" on page 10-9 for more information.
6. Configure new JMS servers corresponding to the new cluster member managed servers. See "Creating JMS Entries for New Cluster Members" on page 10-11 for more information.

Installing the Oracle Identity Manager Server on New Hosts

To install Oracle Identity Manager onto a new host in your WebLogic Cluster:

1. Copy the **<XL_HOME>** directory (where Oracle Identity Manager is installed in the cluster) to the new host, maintaining the identical directory hierarchy structure.
2. Copy the **wlXLSecurityProviders.jar from <XL_HOME>\Xellerate\lib** directory into the **<WEBLOGIC_HOME>\weblogic81\server\lib\mbeantypes** directory.
3. Copy the **<XL_HOME>\ext\nexaweb-common.jar** file to the **<WEBLOGIC_HOME>\weblogic81\server\lib** directory.

Configuring New Host Machines

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

To add a new host to your WebLogic cluster:

1. Open the WebLogic administration console (*http://localhost:7001/console*).
2. Click **<domain_name>**.
3. Click **Machines**. (Navigate using the directory tree on the left pane).

4. Click **Configure a new Machine**.
   - Enter a name for this machine (for example **XLMANAGED_SERVER_HOST_2**).
   - Click **Create**.
5. Click the **Node Manager** tab open it.
   - Enter the Listen Address (IP address) for this machine.
   - Accept the default for the Listen Port.
   - Do not check the **Debug Enabled** box.
   - Click **Apply**.
6. Right-click the existing manager server name (for example **xlManagedServer_1**) and select **Clone <server_name>** from the shortcut menu.
   - Enter a name for the new server (for example **xlManagedServer2**).
   - Select the host computer from the **Machine** drop-down menu. (for example **XLMANAGED_SERVER_HOST_2**)
   - Make sure your cluster (for example **xlCluster**) is selected in the **Cluster** drop-down menu.
   - Scroll down and click **Clone**.
7. If WebLogic is installed in a different directory than xlManagedServer1, then change the remote start configuration to include the directory location. See "Configuring Remote Start Options" on page 10-7 for more information.
8. Go to the host machine and start the node manager.
9. Use the administration console to start the new cluster member.

Creating JMS Entries for New Cluster Members

1. On the administration server host, run the setup_wl_server script to configure a new JMS server corresponding to the new managed server and configure the distributed queue.

   To run the **setup_wl_server** script:

   a. Change directories (cd) to the **<XL_HOME>/xellerate/setup** directory.

   b. Run **setup_wl_server.cmd** for Windows and **setup_wl_server.sh** for UNIX, making sure to append the following parameters:

   <WEBLOGIC_HOME> <ADMIN_SERVER_HOST> <ADMIN_SERVER_HOST_port> <WEBLOGIC_admin_login> <WEBLOGIC_admin_password> <XLMANAGED_SERVER_HOST_n>

   The following sub-sections show what the complete command-line string looks like, depending on the operating system of the machine hosting your Oracle Identity Manager server.

   Unix

   ./setup_wl_server.sh /opt/bea814 t3://192.168.50.172 8001 wladmin wladmin XLMANAGED_SERVER_HOST_2

   Windows

   setup_wl_server.cmd c:\bea814 t3://192.168.50.172 8001 wladmin wladmin XLMANAGED_SERVER_HOST_2

Configuring IIS Proxy Plug-ins

To configure the Microsoft IIS proxy plug-ins:

1. For the web clients to failover properly, either:
   a. Place the Load Balancer before the WebLogic Server cluster and configure it for session affinity.

      or

   b. Configure a WebLogic Proxy Plug-in into the application server.
2. To configure IIS proxy plug-in, use the **iisproxy.dll** and **iisforward.dll** extension and filters. Follow the WebLogic documentation to perform this activity:
   a. Use the documentation at:

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

   b. You will be using Request Forwarding based on a context name **xlWebApp** and **Nexaweb**, while deploying the whole application. The following is a sample **iisproxy.ini** file.

      WlForwardPath=/xlWebApp*,/NexaWeb*

      Debug=ON

      WebLogicCluster=192.168.50.28:7051,192.168.50.184:7051

Configuring Database-based HTTP Session Failover

The WebLogic cluster is by default, configured to provide memory-to-memory session replication and failover. However, it is possible to use database-based replication.

To enable database-based replication:

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

   Note: The database tables required to hold the sessions must be created manually. Refer to http://e-docs.bea.com/wls/docs60/adminguide/config_web_app.html#jdbc_persistence for more information.

   It is possible to use other types of failover mechanisms in WebLogic. To use them, change the descriptor template (**weblogic.xml**) in the **<XL_HOME>/DDTemplates/xlWebApp** directory, then insert the proper settings for the web application descriptor. After the change, run **patch_weblogic** to fix the existing application. Be aware, however, that if the DDTemplate is changed (for example, when upgraded), the same changes must be performed to the template again.

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

Note: 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 name** field, then click **Next**.

   or

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

   Tip: 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. On the Application Server page, select **BEA WebLogic**, then click **Next**. The Application Client Location page appears.
7. Specify the JRE to use with the Design Console, choosing between the JRE bundled with Oracle Identity Manager, or point to an existing and compatible JRE on the system. Click **Next**.
8. On the Application Server configuration 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. Perform these steps and click **OK**.

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

Post-install Requirements for the Design Console

Perform the following steps after installing the Design Console:

1. Copy **<WEBLOGIC_HOME>\weblogic81\server\lib\weblogic.jar** on the machine hosting the Oracle Identity Manager Server to the **<XL_DC_HOME>\xlclient\ext** directory on the machine where the Design Console is installed.

2. If you are pointing the Design Console to a clustered server installation, edit the **<XL_DC_HOME>\xlclient\config\xlconfig.xml** file and add the cluster members in the URL under the <Discovery> section and point the Application URL for Workflow Visualization to the webserver to access the cluster. For example:

   - <ApplicationURL>http://<webserver>/xlWebApp/

     LoginWorkflowRenderer.do</ApplicationURL>

   - <Discovery>.<CoreServer>.<java.naming.provider.url>t3://

     192.168.50.31:7005, 192.168.50.32:7005</java.naming.provider.url>

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 Oracle Identity Manager Remote Manager

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

Installing the Remote Manager on Windows

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:

> **Note:** 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. Specify the JRE to use with the Remote Manager, choosing between the JRE bundled with Oracle Identity Manager, or point to an existing and compatible JRE on the system. Click **Next**.
7. On the Remote Manager Configuration page, enter the appropriate information for the Remote Manager:
   a. Type the **Service Name** (default is RManager).
   b. Type the Remote Manager **binding port** (default is 12346).
   c. Type the Remote Manager **SSL port** (default is 12345).
   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 Installation page, review the configuration details, and then click Install to initiate installation.
10. Click **Finish** to complete the installation.

Installing the Remote Manager for UNIX

To install the Remote Manager on UNIX (Solaris):

> **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.

Note: If the autostart routine is enabled for your machine, proceed to Step 6.

2. From the console, change directories (cd) to the installServer directory on the installation CD and run the install_rm.sh file.
3. The console mode installer starts, and the Welcome panel appears. Type 1, to move to the next panel.

   Tip: 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.

4. On the Target Directory Information 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.
5. Specify the JRE to use with the Remote Manager and Design Console:
   - Type **1** to select Install JRE bundled with Oracle Identity Manager
   - Type **2** to select use your existing JRE at the location specified

     After specifying the JRE to use, type **0** to accept your selection then type **1** to move to next panel.
6. 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 communication between the Remote Manager and 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.

   After entering the Remote Manager configuration information, type 0 to accept your selections then type 1, to move to the next panel.

   The Remote Manager installation summary panel appears.
7. Check the information.
   - Type **2** to go back and make changes.
   - Type **1** to start the installation.
8. 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, use that value instead of 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 property <RMIOverSSL> 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 Server

To enable client-side authentication:

1. On the machine hosting the Remote Manager, launch a plain-text editor, then open the file xlconfig.xml, which resides in the directory **<XL_RM_HOME>\xlremote\config**.
2. Locate the property <ClientAuth> and set it to **true**, for example:

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

3. Locate the property <RMIOverSSL> and make sure it 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 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

To start Remote Manager on Windows, execute the <XL_RM_HOME>\xlremote\remotemanager.bat script.

To start Remote Manager on Unix, 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

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 WebLogic application server version 8.1 with Service Pack 4. Upgrading 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, and upgrading from the Oracle Xellerate Audit and Compliance Manager 8.5.x to Oracle Identity Manager Audit and Compliance module 9.0.1 requires upgrading with the Oracle Identity Manager version 9.0.1 application.

The following is a list of the steps required in the upgrade process:

1. Upgrade the database you used for Oracle Xellerate Identity Provisioning 8.5.x—see "Upgrading Your Database" on page 13-1 for more information.
2. Prepare for the upgrade to Oracle Identity Manager 9.0.1 by performing the pre-upgrade configuration tasks—see "Pre-Upgrade Configuration" on page 13-7 for more information.
3. Migrating any version 8.5.x custom code to your new Oracle Identity Manager 9.0.1 deployment—see "Migrating Custom Code to 9.0.1" on page 13-11 for more information.
4. Upgrade your legacy Oracle Xellerate Identity Provisioning 8.5.x deployment to Oracle Identity Manager 9.0.1—see "Performing the Upgrade to 9.0.1" on page 13-13 for more information.
5. Perform the post-upgrade configuration tasks—see "Post-Upgrade Configuration" on page 13-13 for more information.

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 that 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 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 UNIX:

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 these scripts 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:

   <Patch>\Database\SQLServer\StoredProcedures\compile_all_XL_SP.bat

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).

c. Run the script:

   <Patch>\Database\SQLServer\StoredProcedures\compile_all_XL_SP.bat

Note: Refer to "Executing the SQL Server Upgrade Script" on page A-1 for more information on executing these scripts 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. run the batch file.

b. Run the following script:

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

SQL Server

a. Run the following script:

<Patch>\Database\SQLServer\Scripts\SQLServer_Enable_XACM.bat

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

8. The user profile auditing feature and the reports feature 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 **<Patch>\Database\Utilities\LoadXML.bat** batch file.

UNIX

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

Note: Refer to "Loading Metadata into the Database" on page A-2 for more information on 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. 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.

2. Export the existing database data using the export/backup utilities for your Oracle or SQL Server database.
3. Create a new database by following the steps outlined in either of the following:
   - "Setting Up the Oracle Database" on page 5-1
   - "Setting Up the SQL Server" on page 5-3

   Note: 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.

4. Using the **import** utility provided by your particular database, import the data you exported from your original database in **Step 2** into your newly created database you made in **Step 3**. This creates an exact copy of your original database instance.
5. 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.

6. Upgrade your database schema from Oracle Xellerate Identity Provisioning 8.5.x to Oracle Identity Manager 9.0.1 by using one of the 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 UNIX

   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 these scripts on an SQL Server database.

---

7. 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:

<Patch>\Database\SQLServer\StoredProcedures\compile_all_XL_SP.bat

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. Run the script:

<Patch>\Database\SQLServer\StoredProcedures\compile_all_XL_SP.bat

---

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

---

8. 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.

   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

   Oracle

   a. Run the following script:

      <Patch>\Database\SQLServer\Scripts\SQLServer_Enable_XACM.bat

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

9. The user profile auditing and the reports feature 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

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

   UNIX

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

   Note: Refer to "Loading Metadata into the Database" on page A-2 for more information on 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 8.5.x libraries, scripts, and configuration files using the following steps:

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

1. Backup the following directories:
   - <XL_85x_HOME>\xellerate\config
   - <XL_85x_HOME>\xellerate\DDTemplates
   - <XL_85x_HOME>\xellerate\ext
   - <XL_85x_HOME>\xellerate\lib
   - <XL_85x_HOME>\xellerate\setup
   - <XL_85x_HOME>\xellerate\webapp
   - <XL_85x_HOME>\xellerate\bin
   - <XL_85x_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 13–1 Oracle Identity Manager Server Pre-Upgrade Files to Copy

Copy From....	To
Patch\xellerate\DDTemplates	<XL_HOME>\xellerate\DDTemplates
Patch\xellerate\ext	<XL_HOME>\xellerate\ext
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\readme.htm	<XL_HOME>

3. Copy the following files from Patch\xellerate\setup to <XL_HOME>\xellerate\setup:
   - setup.xml
   - weblogic-setup.xml
   - patch_weblogic.cmd
   - patch_weblogic.sh
4. Remove the following libraries from the <XL_HOME>\xellerate\ext directory:
   - classes12.zip
   - csv-1.0.jar
   - oscache-2.0.2-22Jan04.jar
   - sax.jar
   - dom.jar
   - jaxp-api.jar

5. Upgrade the <XL_HOME>/xellerate/config/xlconfig.xml file. See "Upgrading the Server Configuration File" on page A-3 for more information.
6. Upgrade the <XL_HOME>/xellerate/config/FormMetaData.xml. See "Upgrading the Metadata File" on page A-6 for more information.
7. Edit the <XL_HOME>/xellerate/setup/patch_weblogic script. For Windows, the script is named patch_weblogic.cmd. For UNIX, the script is named patch_weblogic.sh. Replace the following in the patch_weblogic script:
   - replace @bea_home with the path to the WebLogic installation directory
   - replace @loc with the path to the Oracle Identity Manager server installation directory
8. Edit the <XL_HOME>\xellerate\Profiles\weblogic.profile file as follows:
   a. Locate the Reporting data source property and modify it to be the following:

      ```
      # Reporting data source

      datasource.report=jdbc/xlXADS
      ```

   b. Set the following parameter values:

      ```
      weblogic.max-beans-in-free-pool = 100

      weblogic.transaction.timeout = 1200
      ```

9. Use a text editor to edit the PurgeCache script in the <XL_HOME>\xellerate\bin\ directory. For Windows, edit the PurgeCache.bat file. For UNIX, edit the PurgeCache.sh file.
   - Replace oscache-2.0.2-22Jan04.jar with oscache.jar in the definition of the CLASSPATH environment variable.
10. As of version 9.0.1, and for all future releases, the log.properties file replaces the log.conf file as the Oracle Identity Manager server configuration log file. Complete the following steps to migrate all the version 8.5.x logging settings:
    a. Copy any version 8.5.x custom logging-related settings that exist in the log.conf file, which resides in the backup directory **<XL_85x_HOME>/xellerate/config/**, to the **log.properties** file, which resides in the directory **<XL_HOME>/xellerate/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.

    b. 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.ADAPTERS=WARN
       ```

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

       ```
       # log4j.logger.XELLERATE.ADAPTERS=WARN
       ```

       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.ADAPTERS=WARN
       ```

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

11. Copy the ojdbc14.jar file from Patch\xellerate\ext to <WEBLOGIC_HOME>\weblogic81\server\lib\. For clustered environments, copy the ojdbc14.jar file to <WEBLOGIC_HOME>\weblogic81\server\lib\ on each of the XLMANAGED_SERVER_HOST nodes in the cluster.

Pre-Upgrade Configuration for the Design Console

Prepare the Oracle Identity Manager Design Console for upgrade to 9.0.1 by updating 8.5.x libraries, scripts, and configuration files using the following steps:

1. Backup the following files and directories:
   - <XL_85x_DC_HOME>\xlclient\XLDesktopClient.ear
   - <XL_85x_DC_HOME>\xlclient\CustomClient.zip
   - <XL_85x_DC_HOME>\xlclient\lib
   - <XL_85x_DC_HOME>\xlclient\ext
   - <XL_85x_DC_HOME>\documentation
2. Copy the following files from Patch\xlclient\ to the <XL_DC_HOME>\xlclient directory, overwriting existing files if necessary:
   - Patch\xlclient\fvc.properties
   - Patch\xlclient\fvcutil.cmd
   - Patch\xlclient\XLDesktopClient.ear
   - Patch\xlclient\CustomClient.zip
   - Patch\xlclient\xlFvcUtil.ear
3. Open the <XL_DC_HOME>\xlclient\fvcutil.cmd file. Set the following environment variable values:
   - Set @java_loc to the path of the java directory
   - Set @auth_config to the path of the authwl.conf file
4. Copy the contents of the Patch\documentation directory to <XL_DC_HOME>\documentation, overwriting files if necessary.
5. Copy Patch\xellerate\readme.htm to <XL_DC_HOME>\xlclient\, overwriting the existing file if necessary.
6. Copy the contents of the Patch\xlclient\lib directory to <XL_DC_HOME>\xlclient\lib, overwriting files if necessary.
7. Copy the contents of the Patch\xlclient\ext directory to <XL_DC_HOME>\xlclient\ext, overwriting files if necessary.
8. Remove the following from the <XL_DC_HOME>\xlclient\ext\ directory:
   - classes12.zip
   - csv-1.0.jar
   - oscache-2.0.2-22Jan04.jar

Pre-Upgrade Configuration for the Remote Manager

Prepare the Oracle Identity Manager Remote Manager for upgrade to 9.0.1 by updating 8.5.x libraries, scripts, and configuration files using the following steps:

1. Backup the content of the following directories:
   - <XL_85x_RM_HOME>\xlremote\lib
   - <XL_85x_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. 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 log 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. Upgrade the <XL_RM_HOME>/xlremote/config/xlconfig.xml file. See "Upgrading the Remote Manager Configuration File" on page A-7 for more information.

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.

Note: Before migrating custom code from the 8.5.x environment, you must first rebuild it 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**.

Note: In 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 in **<XL_85x_HOME>/xellerate/ScheduleTask** need to be copied to **<XL_HOME>/xellerate/ScheduleTask**.

Note: In a clustered environment you must repeat this step on all cluster members.

Migrating xlWebApp Customizations

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

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**.

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.

Performing the Upgrade to 9.0.1

Upgrading from an existing Oracle Xellerate Identity Provisioning 8.5.x 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 8.5.x deployment to Oracle Identity Manager 9.0.1 in a WebLogic environment:

1. Make sure the WebLogic application server is running. If it is not running, start it.
2. Run the patch_weblogic script:

   Windows

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

   UNIX

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

Post-Upgrade Configuration

The following post-upgrade configurations are required to complete the upgrade.

Post-Upgrade Configuration for the Audit and Compliance Module

The following post-upgrade 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 set 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 (previously named Oracle Xellerate Auditing and Compliance Manager in 8.5.x), 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 Xellerate Auditing and Compliance Manager module
- You elevate the audit level for Audit and Compliance module

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 UNIX, 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=weblogic

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

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

   e. If you are running on Windows and using SQL Server as your database, set the **SQL_SERVER_DRIVER_DIR** variable in **GenerateSnapshot.bat** to point to the directory containing the SQL Server JDBC drivers and remove the comment for the line. For example, change:

      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>

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/**.

   UNIX

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

Upgrading the Diagnostic Dashboard

To upgrade your existing 8.5.x 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. Remove the existing XIMDD application
2. Install a new instance of the XIMDD application using the new, version 9.0.1 XIMDD.war file in the Patch\DiagnosticDashboard directory
3. See "Using the Diagnostic Dashboard" on page 2-6 for more information.

14

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.

Oracle Identity Manager Installation Fails with a WebLogic Clustered Environment

The Oracle Identity Manager installation may fail within a WebLogic clustered environment when the wrong values are defined for the target server and server port number. You **should not** define the Admin Server as a target during the installation process, since the setup script needs to create the JMS Server on a cluster member.

Work Around Example

Use the following steps as an example to clean up the WebLogic services so that you can continue with the installation:

1. Open the WebLogic administration console to clean up the services that have been created for your cluster.
2. Select the JDBC tab and delete:
   a. the connection pools
   b. both data sources
3. Select the JMS tab and delete:
   a. the xleConnectionFactory
   b. every xlJDBCStore
   c. every xlJMSServer
4. Open the file **weblogic.profile**, which resides in the directory **<XL_HOME>\Profile**, then change the following:
   a. The WebLogic Server **target name** from **myserver** to **<cluster_member1>**
   b. The WebLogic Server **target port** from **7001** to **7051**.

5. Run the script **setup_weblogic.cmd**.
6. Review the log file to see that it runs successfully
7. Once the setup script runs successfully, you must restart the WebLogic Server.

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

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 and you are using an SQL Server, make sure that the Distributed Transaction Coordinator is running (it should have been set as a default).

A

Supplementary Upgrade Information

Use the additional information in this Appendix as a supplement the information in Chapter 13, "Upgrading to Oracle Identity Manager 9.0.1 from Versions 8.5.2 or 8.5.3" when performing the upgrade.

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, User Profile Audit 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 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.

Table A–1 (Cont.) Parameters for Command Line Scripts

Arguments	Description
<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

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 **JAVA_HOME** variable.
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>

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 UNIX

a. Launch a plain-text editor, open the file LoadXML.sh, then uncomment the following lines:

#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 follows:

1. Launch a plain-text editor, then open **xlconfig.xml**, which resides in the directory **<XL_HOME>/xellerate/config/**.

2. Locate the tag **<xl-configuration>.<Offlining>. .<MessageHandlerMDB>.<message-handler-task>**

Note: Refer to Table 1-1, "Formatting Conventions," on page 2 for more information on identifying and locating xml tags.

- Insert the following block of lines:

```
<AuditorOfflineMessage>com.thortech.xl.audit.engine.jms.XLAuditMessageHandl
er</AuditorOfflineMessage>

<AttestationRequestMessage>com.thortech.xl.schedule.jms.attestation.process
OfflinedAttestationRequests</AttestationRequestMessage>

<AttestationTaskMessage>com.thortech.xl.schedule.jms.attestation.processOff
linedAttestationTasks</AttestationTaskMessage>

<AttestationWorkflowTaskMessage>com.thortech.xl.schedule.jms.attestation.pr
ocessOfflinedAttestationWorkflowTasks</AttestationWorkflowTaskMessage>

<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>.
```

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 Table 1-1, "Formatting Conventions," on page 2 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 tag `<BlockMode> ECB </BlockMode>` under the following two locations:
   - <xl-configration>.<Security>.<XLSymmetricProvider>.<Keys>.<DBSecretKey>
   - <xl-configration>.<Security>.<XLSymmetricProvider>.<Keys>.<JMSKey>
5. Locate the following XML tag:

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

   Change it to the following value:

   <XL_RM_HOME>/xlremote/config/log.properties
6. Save and close the file.

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:

   <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 preceding the </FormManagementMetaData> line. (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:

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

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>.<
     ReconOfflineMessage>
     ```

   - and preceding the following line:

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

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 Table 1-1, "Formatting Conventions," on page 2 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 tag:

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

   and change it to the following value:

   <XL_RM_HOME>/xlremote/config/log.properties