Oracle® Identity Manager

Installation Guide for WebLogic

Release 9.0.3.1

B32461-03

May 2007

Oracle Identity Manager Installation Guide for WebLogic Release 9.0.3.1

B32461-03

Primary Author: Don Biasotti

Contents

8 Starting the Oracle Identity Manager Server

9 Deploying in a Clustered WebLogic Configuration

10 Installing and Configuring the Oracle Identity Manager Design Console

11 Installing and Configuring Oracle Identity Manager Remote Manager

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 Thor Xellerate Identity Manager. The Oracle Identity Manager Audit and Compliance module was formerly known as Oracle Xellerate Audit and Compliance Manager.

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

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

Audience

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

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

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

- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager API Usage Guide*
- *Oracle Identity Manager Audit Report Developer's Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Globalization Guide*
- *Oracle Identity Manager Glossary of Terms*
- *Oracle Identity Manager Integration Guide for Crystal Reports*
- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Upgrade 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 the WebLogic application server is referred to as <*BEA_HOME*>. The directory where you install the 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.

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

1

Introduction

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

- Product Overview
- Oracle Identity Manager Components
- Product Architecture
- Installation Overview

Product Overview

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

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

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

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

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

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

Oracle Identity Manager Components

Oracle Identity Manager includes the following components:

- Oracle Identity Manager Server
- Oracle Identity Manager Remote Manager

- Oracle Identity Manager Design Console (for Windows only)

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

Product Architecture

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

The presentation tier contains the following components:

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

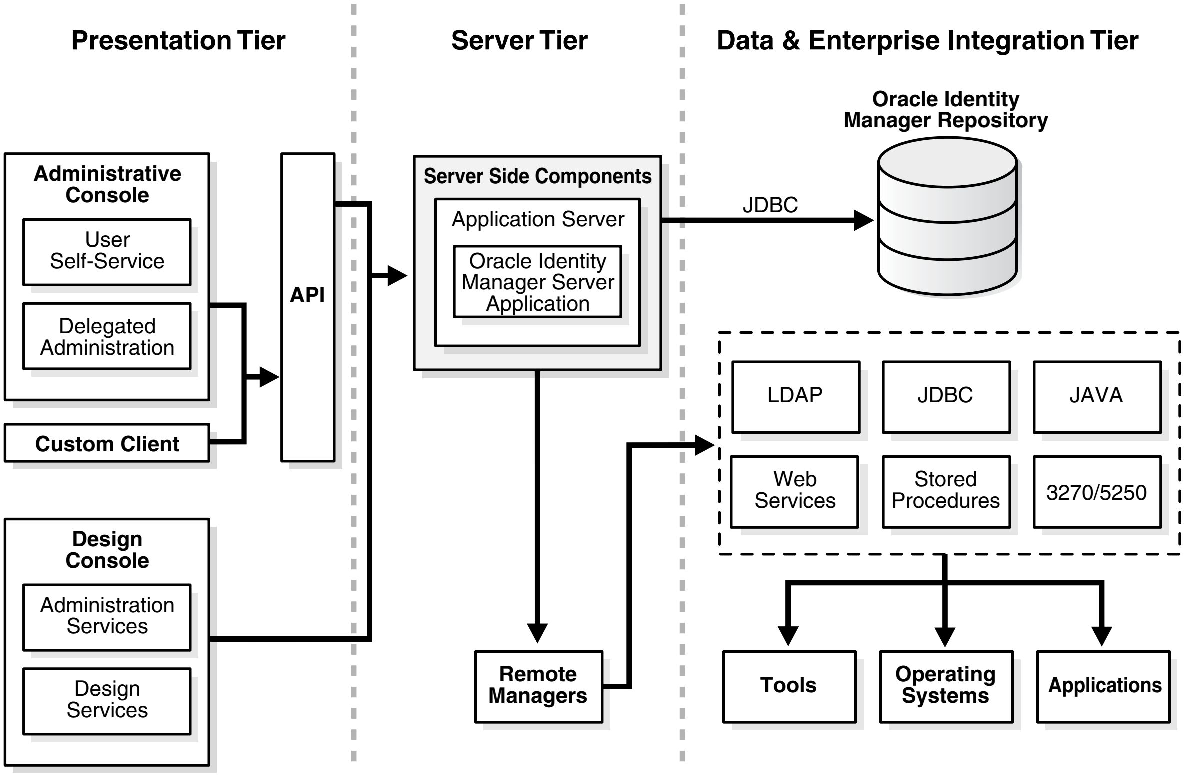
The server tier contains the Oracle Identity Manager Server component, which serves as a bridge between the presentation tier and the data and enterprise integration tier. All requests between the clients and the database are processed through the server tier.

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

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



Installation Overview

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

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

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

2

Planning the Installation

Oracle strongly recommends that you familiarize yourself with the components required for your deployment before starting to install Oracle Identity Manager. Oracle also recommends that you install and use the included Diagnostic Dashboard to ensure that your system is ready for installation. See "Using the Diagnostic Dashboard" on page 2-5 for more information.

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)

This chapter discusses the following topics:

- Host System Requirements for Oracle Identity Manager Components
- Planning for Non-English Oracle Identity Manager Environments
- Before You Start
- Using the Diagnostic Dashboard

Host System Requirements for Oracle Identity Manager Components

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

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

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

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

Oracle Identity Manager Server Host Requirements

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

Table 2–1 Host Requirements for Oracle Identity Manager Server

Server Platform	Item
Windows and Linux	■ Processor Type: Intel Xeon or Pentium IV ■ Processor Speed: 2.4 GHz or higher, 400 MHz FSB or higher ■ Number of Processors: 1 ■ Memory: 2 GB for each Oracle Identity Manager Server instance ■ Hard Disk Space: 20 GB (initial size)
Solaris	■ Server: Sun Fire V210 ■ Number of Processors: 1 ■ Memory: 2 GB for each Oracle Identity Manager Server instance ■ Hard Disk Space: 20 GB (initial size)

Database Server Host Requirements

Table 2–2 provides sample database host requirements for selective supported operating systems and should be considered only as guidelines. Increase each measurement if more size is needed for your deployment. Consult your SQL Server or Oracle database documentation for the specific database host requirements.

Table 2–2 Sample Database Server Host Requirements

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

Design Console Host Requirements

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

Table 2–3 Design Console Host Requirements

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

Remote Manager Host Requirements

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

Table 2–4 Remote Manager Host Requirements

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

Planning for Non-English Oracle Identity Manager Environments

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

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

Before You Start

Before installing Oracle Identity Manager, you should read "Host System Requirements for Oracle Identity Manager Components" on page 2-1 and "Installation Worksheet" on page 2-4 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 2–5 indicates the document sections each installation team member should read.

Table 2–5 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 in Table 2–6 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 2–6 Installation Worksheet

Item	Default	User Selection
The base directory for installing Oracle Identity Manager.	Windows: C:\oracle UNIX or Linux: /opt/oracle	
The name or IP address of the machine where the Oracle Identity Manager database is installed.	N/A[1]	
The TCP port number on which the database listens for connections.	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:\bea\j2sdk<version> UNIX or Linux: /opt/bea/j2sdk<version>	

Table 2–6 (Cont.) Installation Worksheet

Item	Default	User Selection
The WebLogic install directory	Windows: C:\bea UNIX or Linux: /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 supported Java Virtual Machine (JVM)
- A supported Database
- Microsoft SQL Server JDBC Libraries Test

3

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

After completing the tasks in this chapter, you must install and configure a database by following the steps in Chapter 4, "Installing and Configuring a Database for Oracle Identity Manager" on page 21 before installing Oracle Identity Manager.

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

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.

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

1. Launch the WebLogic Configuration Wizard:

   Windows:

   a. Start the Configuration Wizard from the **Start** menu by selecting **BEA WebLogic Platform**, and then **Configuration Wizard**.

   UNIX or Linux:

   a. Go to the WebLogic bin directory:

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

b. Start the Configuration Wizard using the following command:

```
sh config.sh
```

2. 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 1.4.2_11**.

   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 application server:

   Windows:

   a. Start the WebLogic application server from the **Start** menu by selecting **BEA WebLogic Platform**, then **User Projects**, then <**domain name**>, and then **Start Server**.

   UNIX or Linux:

   a. Go to the WebLogic user_projects/domains directory.

   For example:

   ```
   cd <BEA_HOME>/user_projects/domains/
   ```

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

   ```
   cd <domain name>
   ```

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

   ```
   sh startWebLogic.sh
   ```

4. Log in to the WebLogic Admin Console using your new account by pointing a web browser to the following url:

   ```
   http://<hostname>:7001/console
   ```

   a. Select **Security**, then **Realms**, then **myrealm**, and then **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**, then **Realms**, then **myrealm**, and then **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

4

Installing and Configuring a Database for Oracle Identity Manager

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 database:

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

Using an Oracle Database for Oracle Identity Manager

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

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

Installing Oracle

Install Oracle9i or 10g Release 2. Refer to the *Oracle Identity Manager Release Notes* for the specific supported databases. Oracle recommends using the Basic 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** field of the DBCA.

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

Configuring the Database for Globalization Support

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

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

See Also: *Oracle Identity Manager Globalization Guide*

Preparing the Oracle Database

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

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

> **Note:** The Java JVM is required to enable XA transaction support. If you did not install the JVM during your Oracle installation, you must install it now. Consult Oracle documentation for specific instructions.

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

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

- On UNIX or Linux, run the following:

  ```
  prepare_xl_db.sh
  ```

- On Windows, run the following:

  ```
  prepare_xl_db.bat
  ```

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

You must observe the following prerequisites when using these scripts:

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

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

Preparing the Database on UNIX or Linux

To prepare the database on UNIX or Linux:

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

   ```
   chmod 755 prepare_xl_db.sh
   ```

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

   ```
   ./prepare_xl_db.sh
   ```

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

> **Note:** If you encounter errors after running the prepare_xl_db.sh script, run the following command to ensure the prepare_xl_db.sh is executable on UNIX and then run the prepare_xl_db.sh script again.
>
> ```
> $ dos2unix prepare_xl_db.sh
> ```

Preparing the Database on Windows

To prepare the database on Windows:

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

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

   For example, the string you enter on the command line might look something like the following:

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

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

Table 4–1 Options for the prepare_xl_db.bat Script

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

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

Evaluating Script Results

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

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

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

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

Removing Oracle Identity Manager Entries from an Oracle Database

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

Using Oracle RAC Databases for Oracle Identity Manager

This section explains how to deploy Oracle RAC databases for Oracle Identity Manager and contains the following sections:

- Installing Oracle Identity Manager for Oracle RAC
- Oracle RAC Net Services
- JDBC and Oracle RAC
- Configuring WebLogic Application Servers for Oracle RAC

Installing Oracle Identity Manager for Oracle RAC

Oracle RAC is a cluster database with a shared cache architecture that provides highly scalable and available database solutions. A RAC consists of multiple database instances on different machines and acting in tandem to provide these features.

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

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

1. Ensure the RAC is properly set up and configured with the Oracle Identity Manager schema owner.
2. Start the Oracle Identity Manager installer program.
3. Enter the host name, port number, and database name of a single database instance in the RAC on the Database Parameters screen of the Oracle Identity Manager installer program.
4. Complete the Oracle Identity Manager installation by finishing the steps in the installer program.
5. Configure your application server for RAC by referring to Configuring WebLogic Application Servers for Oracle RAC.

Oracle RAC Net Services

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

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

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

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

Parameter	Description
LOAD_BALANCE	Specifies whether client load balancing is enabled (on) or disabled (off). The default setting is on.
FAILOVER	Specifies whether failover is enabled (on) or disabled (off). The default setting is on.

Table 4–2 (Cont.) Parameters for Oracle RAC Database Net Services Name Entries

Parameter	Description
ADDRESS_LIST	Specifies the list of all the nodes in the RAC, including their host names and the ports they listen on.

JDBC and Oracle RAC

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

The following is sample code that demonstrates an example JDBC URL used to connect to a RAC database:

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

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

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

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

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

Configuring WebLogic Application Servers for Oracle RAC

This section explains how to configure both non-clustered and clustered WebLogic application servers for Oracle RAC by ensuring the data sources and connection pools are configured to use the RAC JDBC connection string.

Note: Before configuring WebLogic application servers for Oracle RAC, you must:

- Get the RAC net services name from the tnsnames.ora file.
- Construct the RAC JDBC URL by referring to JDBC and Oracle RAC.

Perform the following steps to configure both non-clustered and clustered WebLogic application servers for Oracle RAC:

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

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

3. Save and close the <*XL_HOME*>/xellerate/config/xlconfig.xml file.
4. Start the WebLogic application server and open the WebLogic Administrative Console using a web browser.
5. Log in to the WebLogic Administrative Console by using the administrator account.
6. Select **Services**, then select **JDBC**, then select **Connection Pools**, and then select **xlConnectionPool**.
7. Select the **General** tab for xlConnectionPool.
8. Enter the RAC JDBC URL described in step 2 in the **URL** field and save the settings.
9. Select the **Connections** tab for xlConnectionPool.
10. Select **Advanced Options** and set the following:
    - Enable the **Test Reserved Connections** option
    - Set the **Test Table Name** value to `dual`

    Save the settings.
11. Select **Services**, then select **JDBC**, then select **Connection Pools**, and then select **xlXAConnectionPool**.
12. Select the **General** tab for xlXAConnectionPool.
13. Enter the RAC JDBC URL described in step 2 in the **URL** field and save the settings.
14. Select the **Connections** tab for xlXAConnectionPool.
15. Select **Advanced Options** and set the following:
    - Enable the **Test Reserved Connections** option
    - Set the **Test Table Name** value to `dual`
    - Enable the **Keep XA Connection Till Transaction Complete** option

    Save the settings.
16. Restart the Admin Server and the Managed Server (if one exists). For WebLogic clusters, restart all nodes in the cluster.

Using a SQL Server Database for Oracle Identity Manager

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

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

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

Installing and Configuring SQL Server

To install and configure SQL Server for Oracle Identity Manager:

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

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

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

   `http://www.microsoft.com`

3. On the machine hosting the application server, 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 (step 4). If your classpath is more than 256 characters, the installer does not work properly.

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

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

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

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

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

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

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

6. Run the script instjdbc.sql.

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

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

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

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

Registering SQL Server

To register the SQL server:

1. Start the Microsoft SQL Server Enterprise Manager application.

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

2. In the left pane of the SQL Server Enterprise Manager application window, select **Console Root**, then select **Microsoft SQL Servers**.
3. Right-click **SQL Server Group** and select **New SQL Server Registration**.
4. In the Register SQL Server Wizard dialog, click **Next**.
5. On the Select a SQL Server page, perform one of the three following sub-steps:
   a. Select your server from the list in the right pane, click Add, then click **Next**.
   b. Select LOCAL, then click Add, then click **Next**.
   c. Enter the host name of your server in the text entry box, click **Add**, then click **Next**.
6. On the Select an Authentication Mode page, select The SQL Server login information that was assigned to me by the administrator [SQL Server Authentication], then click **Next**.
7. On the Register Connection Option page, select **Login automatically using my SQL server account information**, then complete the following sub-steps
   a. In the text box labelled **Login name**, enter the account name used to connect to your SQL server. Typically, this is **sa**.
   b. In the **Password** text box, enter the password associated with the account name you specified, then click **Next**.
8. On the Select SQL Server Group page, select **Add the SQL Server(s) to an existing SQL Server Group**, select a group from the list labelled **Group name**, then click **Next**.
9. On the Completing the Register SQL Server Wizard page, click **Finish**, then click **Done**.

Creating a SQL Server Database

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

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

To create a new database for Oracle Identity Manager:

1. Start the Microsoft SQL Server Enterprise Manager application.

   From the Windows **Start** menu, select **Programs**, select **Microsoft SQL Server**, then select **Enterprise Manager**.
2. In the left pane of the SQL Server Enterprise Manager application window, select **Console Root**, select **Microsoft SQL Servers**, select the server group to which your server belongs, then double-click the icon representing your server.
3. Right-click Databases, then select **New Database**.
4. In the Database Properties dialog, select the General tab, then enter **XELL** in the text box labelled **Name**.

5. Select the **Data Files** tab, then, for the **Initial Size** and **Filegroup** columns in the Database files matrix, enter the information from the corresponding columns in Table 4–3.

Table 4–3 Database Files

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

Note: Table 4–3 lists initial sizes for a production environment. For non-production installations, you can use the default initial sizes provided for the filegroups.

Important: To ensure successful installation of Oracle Identity Manager, filegroup names must be entered exactly as they appear in Table 4–3. You can vary the File Name and Location strings to match the database name and the location of your SQL Server installation.

c. Select **Automatically Grow File**.

d. Select **By Percent**, then enter **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 a SQL Server Database Account

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

Note: The following procedure assumes the account name xladm. If you want an account name other than xladm, make sure to specify that login instead of xladm throughout the following procedure and also when installing Oracle Identity Manager.

To create a SQL Server database account and permissions:

1. Launch the Microsoft SQL Server Enterprise Manager application.

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

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

3. Select Security, right-click **Logins**, then select **New Login**.

4. In the SQL Server Login Properties dialog, select the **General** tab. In the **Name** field, enter **xladm** (or whatever account name you prefer).

5. Select **SQL Server Authentication**, then enter the password associated with the account you specified in the **Password** text box.

6. In the **Database** list in the **Defaults** section, select **XELL** from the 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.

Removing Oracle Identity Manager Entries from a SQL Server Database

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

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

5

Installing the Oracle Identity Manager Server on Windows

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

This chapter contains the following topics:

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

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

Setting Environment Variables Before Installing the Oracle Identity Manager Server

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

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

```
set JAVA_HOME=<BEA_HOME>\jdk142_11
```

Note: Refer to the *Oracle Identity Manager Release Notes* to learn the certified JDK versions.

- Verify the Sun JVM bundled with WebLogic server is being used when a Java command is executed. To do this, include the WebLogic server directory jdk142_11\bin in the PATH ahead of all other path entries, for example:

  ```
  set PATH=<BEA_HOME>\jdk142_11\bin;%PATH%
  ```

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

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

Important: 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.

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.

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

   Note: If the autostart routine is enabled for your 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. Select a language on the Installer screen and click **OK**. The Welcome screen appears.
5. Click **Next** on the Welcome screen. The Admin User Information screen appears.
6. Enter a password you want to use for the Oracle Identity Manager Administrator, confirm the password by entering it again, and then click **Next**. The OIM Application Options screen appears.
7. Select one of the following applications to install and click **Next**:
   - Oracle Identity Manager
   - Oracle Identity Manager with Audit and Compliance Module
8. After the Target directory screen appears, complete one of the following bulleted actions:
   - The default directory for the Oracle Identity Manager server is C:\oracle. To install the Oracle Identity Manager server into this directory, click **Next**.
   - To install the Oracle Identity Manager server into another directory, enter the path in the Directory field, then click **Next**.

     or

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

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

9. On the Database Server Selection page, specify the type of database you are using with Oracle Identity Manager (either **Oracle** or **SQL Server**), then click **Next**.

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

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

    > **Note:** To install against an existing database, verify that the version of Oracle Identity Manager you are installing is certified with your existing database version. Refer to the *Oracle Identity Manager Release Notes* to confirm the certified configurations.
    >
    > When Oracle Identity Manager is installed against an existing database, a warning message will appear indicating the database schema already exists and instructing you to copy the .xldatabasekey file from the existing Oracle Identity Manager installation to the new <*XL_HOME*>\xellerate\config\ directory after you complete the installation process.
    >
    > 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 "Using an Oracle Database for Oracle Identity Manager" on page 4-1 or "Using a SQL Server Database for Oracle Identity Manager" on page 4-7 to verify your settings.

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

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

11. On the Authentication Information page, select either the **Oracle Identity Manager Default Authentication** or **SSO** (Single Sign-On) **Authentication** option. If you select Single Sign-On authentication, you must provide the header variable

used in the Single Sign-On system in the **Enter the header value for SSO Authentication** field. Click **Next**.

12. On the Application Server Selection page, select **BEA WebLogic**, and click Next.
13. 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 9, "Deploying in a Clustered WebLogic Configuration" if you are deploying in a clustered environment.

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

    a. Enter the path to the root directory for your application server

    or

    Click **Browse** and navigate to the root directory for your application server

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

    or

    Click **Browse** and navigate to the JDK directory associated with your application server.

    c. Click **Next**.

15. 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.

    To provide 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. Click **Next** to commit your settings.

    To provide WebLogic server information for a clustered installation:

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

      Note: The host name is case-sensitive.

   b. Enter the **WebLogic Server Name**.

   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 (the administrator account you configured using the WebLogic configuration wizard).

   f. Enter and confirm the administrator **Password**.

   g. Click **Next**.

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

   a. Enter the path to the WebLogic domains folder.

      or

      Navigate to the location.

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

   c. Enter the domain name.

   d. Click **Next**.

17. Back up your application server when the Application Server Configuration Backup screen appears, then click **Next**.

18. 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.

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

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

20. After the Oracle Identity Manager server installs, a message appears listing the location of the installer log file and the next steps you should perform.

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

21. 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 7, "Post-Installation Configuration for Oracle Identity Manager and WebLogic" to continue the installation.

Removing the Oracle Identity Manager Server Installation

To remove the Oracle Identity Manager server installation:

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

6

Installing the Oracle Identity Manager Server on UNIX or Linux

This chapter describes how to install Oracle Identity Manager on a computer running UNIX or Linux. Refer to *Oracle Identity Manager Release Notes* for more information on the supported UNIX or Linux platforms. You must install the Oracle Identity Manager server on systems running the application server. Oracle Identity Manager components such as the Remote Manager can be installed on separate systems. Each component has its own installer.

This chapter discusses the following topics:

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

Setting Environment Variables Before Installing the Oracle Identity Manager Server

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

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

  ```
  export JAVA_HOME=<BEA_HOME>jdk142_11
  ```

  > **Note:** Refer to the *Oracle Identity Manager Release Notes* to learn the certified JDK versions.

- Verify the Sun JVM bundled with WebLogic server is being used when a Java command is executed. To do this, include the WebLogic server directory jdk142_11/bin in the PATH ahead of all other path entries, for example:

  ```
  export PATH=<BEA_HOME>/jdk142_11/bin:$PATH
  ```

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 or Linux

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 or Linux by using the internal `ln` command.

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

- Choose from among list of options

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

- Enter information at a prompt

  To enter information at the prompt, enter the information and press **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, enter the number zero (0) to indicate that the desired item has been selected.
- To move to the next installation panel, enter the number one (1).
- To go back to the previous panel, enter the number two (2).
- To cancel the installation, enter the number three (3).
- To redisplay the current panel, enter the number five (5).

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

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

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

To install Oracle Identity Manager server for UNIX or Linux:

1. If you are using SQL Server as your database, before installing the Oracle Identity Manager server be sure the following three files are in the <*BEA_HOME*>/weblogic81/server/lib/ directory and add the driver location to the 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.
4. Run the install_server.sh file using the following command:

   ```
   sh install_server.sh
   ```

   The installer starts in console mode.

   Note: If you are not installing Oracle Identity Manager from distributed media (a CD), you must set the execute bit of all shell scripts in the installServer directory. To set the execute bit for all shell scripts recursively, navigate to the installServer directory and run the `chmod -R u+x *.sh` command.

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

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

   The Admin User Information panel appears.
7. Enter a password you want to use for the Oracle Identity Manager Administrator, confirm the password by entering it again, and then enter **1** to move to the next panel.

   The OIM Application Options panel appears.
8. Enter **1** on the OIM Application Options panel to display the next panel.

   The Select the Oracle Identity Manager application to install panel appears.
9. Select the application to install:

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

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

The Target directory panel appears.

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

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

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

The Database Server Selection panel appears.

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

11. Specify the type of database you are using.

– Enter **1** to select Oracle.

– Enter **2** to select SQL Server.

– Enter **0** to finish.

– Enter 1 to move to the next panel.

The Database Information panel appears.

12. 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. Enter 1 to move to the next panel

The Authentication Information panel appears.

13. Select the authentication mode for the Oracle Identity Manager web application.

- Enter 1 for Oracle Identity Manager Default Authentication.
- Enter **2** for SSO Authentication.
- Enter **0** when you are finished.
- If you select SSO authentication, you must provide the header variable used in the Single Sign-On system when prompted.
- Enter 1 to move to the next panel.

The Application Server Selection panel appears.

14. Specify your application server type.
    - Enter **3** for BEA WebLogic
    - Enter 0 when you are finished
    - Enter 1 to move to the next panel

    The Cluster Information panel appears.

15. Specify if the application server is clustered or not, provide the information specific to your cluster, then perform the following sub-steps:
    - Enter 1 for Yes.
    - Enter **2** for No.
    - Enter 0 when you are finished
    - If you selected Yes, enter the cluster name at the prompt
    - Enter 1 to move to the next section.

    The Application Server Information panel appears.

16. 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.
    - Enter 1 to move to the next panel.

    The application server information panel appears.

17. Enter the login information for the application server:

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

    To specify 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.

To specify WebLogic server information for a clustered installation:

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

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

b. Enter the **WebLogic Server Name**.

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 (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.

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

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

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

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

Oracle Identity Manager installs and the Completed panel appears.

21. Enter **3** to finish.

Once you have finished installing the Oracle Identity Manager Server, follow the instructions in Chapter 7, "Post-Installation Configuration for Oracle Identity Manager and WebLogic" to continue the installation.

Removing the Oracle Identity Manager Server Installation

To remove the Oracle Identity Manager server installation, perform the following steps:

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

7

Post-Installation 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 the post-installation tasks are optional, depending on your deployment, before using the applications.

This chapter discusses the following topics:

- Required Post-Installation Tasks for WebLogic
- Optional Post-installation Tasks

Required Post-Installation Tasks for WebLogic

After you install the Oracle Identity Manager software on WebLogic, you *must* perform the tasks in this section for Oracle Identity Manager to operate properly.

Configuring WebLogic for Oracle Identity Manager

After 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.

> **Note:** If you are configuring WebLogic for Oracle Identity manager in a clustered environment, start the following procedure on step 7.

To configure WebLogic for Oracle Identity Manager:

1. Use the WebLogic administration console to shut down the application server gracefully.
2. Navigate to <*BEA_HOME*>\user_projects\domains\<*domain_name*> (for example, C:\bea\user_projects\domains\mydomain).
3. Open the WebLogic start script file in a text editor. The start script is:
   - **For Windows**:

     ```
     startWebLogic.cmd
     ```

   - **For UNIX or Linux**:

     ```
     startWebLogic.sh
     ```

4. Edit the script to specify memory options:

For Windows:

Locate the line that starts with the following:

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

Add the following line just before it:

```
set MEM_ARGS=-Xmx1024m -XX:PermSize=128m
```

For UNIX or Linux:

Locate the line that starts with the following:

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

Add the following lines just before it:

```
MEM_ARGS="-Xmx1024m -XX:PermSize=128m"
export MEM_ARGS
```

5. Save and close the file.
6. Stop the application server using Admin Console and then start the WebLogic server by navigating to the following directory:

   <*XL_HOME*>\xellerate\bin\

   Run the following command on Windows:

   ```
   xlStartServer.bat
   ```

   Run the following command on UNIX or Linux:

   ```
   xlStartServer.sh
   ```

7. Log in 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 OIM 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, for example, **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 the word "database" without quotation marks.
    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. Restart the WebLogic Server for the new configuration to become active.

Note: If you are using SQL Server as your database and the Oracle Identity Manager server log shows traces of exceptions related to MS JDBC classes, you must add three MS JDBC files to the beginning of CLASSPATH in the startWebLogic script located in the domain directory and restart the server.

Add the following three files, located in the /weblogic81/server/lib/ directory, to the beginning of CLASSPATH in the startWebLogic script and restart the server:

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

In a clustered environment, add these three .jar files in the **Class Path** field in the **Remote Start** tab of all Managed Servers.

Configuring XA Connection Settings

After you install Oracle Identity Manager on WebLogic, you must set up an XA connection.

To set up an XA connection:

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.

Verifying WebLogic Configuration Settings for Production Environments

Before deploying Oracle Identity Manager into production environments on WebLogic application servers, you should verify certain WebLogic configuration settings. While Oracle Identity Manager will operate properly on WebLogic application servers if the following settings are not enabled, you should verify the following for production environments to ensure you realize the proper performance typically not encountered in simulated test or development environments. Use the WebLogic Administrative Console to verify the following settings:

- Connection Pool settings for both the Oracle Identity Manager JDBC Connection pools, xlConnectionPool and xlXAConnectionPool, are set as follows:
  - Initial Capacity: 30
  - Maximum Capacity: 50
  - Capacity Increment: 5
- **Test Reserved Connections** is enabled for both xlConnectionPool and xlXAConnectionPool and the test table name is `XSD`.
- **Keep XA Connection Till Transaction Complete** is enabled for xlXAConnectionPool.
- The JMS server affinity of the JMS Connection Factory, xlConnectionFactory, is disabled.
- The Redelivery Limit for JMS Queue (xlQueue) is set to `1`.

  > **Note:** In a WebLogic cluster, verify this setting for all physical queues that are part of the queue/xlqueue distributed queue.

- The **Error Destination** for JMS Queue (xlQueue) is set to the proper error queues. For the default queue (xlQueue), the error queue name is queue/xlErrorQueue.

  > **Note:** In a WebLogic cluster, verify this setting for all physical queues that are part of the queue/xlqueue distributed queue. The Error Destination will be different for the different physical queues participating in the distributed queue.

- The **Replicate JNDI Name In Cluster** setting for JMS Queues (xlQueue and xlErrorQueue) are enabled.

> **Note:** In a WebLogic cluster, verify this setting for all physical queues that are part of the queue/xlqueue and queue/xlErrorQueue distributed queue.

Optional Post-installation Tasks

After installing Oracle Identity Manager, you should considering performing the optional post-installation tasks documented in this section before using the application. Depending on your Oracle Identity Manager deployment, you may choose not to perform some of these tasks.

Changing Keystore Passwords

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

To change the keystore password:

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

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

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

Table 7–1 Command Options for keytool

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

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

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

   - Change the password tag to `encrypted="false"`.

- Enter the password (in the clear). For example, you could 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.

Note: On UNIX or Linux, you may also want to clear the shell's command history by using the following command:

```
history -c
```

Setting Log Levels

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

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

- DEBUG
- INFO
- WARN
- ERROR
- FATAL

By default, Oracle Identity Manager is configured to output at the Warning level—except for DDM, which is configured to output at the Debug level by default. You can change the log level universally for all components or for an individual component.

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

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

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

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.
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.

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

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

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

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

To enable Single Sign-On for Oracle Identity Manager:

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

   <*XL_HOME*>\xellerate\config\xlconfig.xml
3. Locate the following Single Sign-On configuration (the following are the default settings without Single Sign-On):

   ```
   <web-client>
   <Authentication>Default</Authentication>
   <AuthHeader>REMOTE_USER</AuthHeader>
   </web-client>
   ```
4. Edit the Single Sign-On configuration to be the following and replace <*SSO_HEADER_NAME*> with the appropriate header configured in your Single Sign-On system:

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

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

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

   Replace <*SSO_HEADER_NAME*> with the appropriate header configured in your Single Sign-On system
5. Change your application server and web server configuration to enable Single Sign-On by referring to your application and web server vendor documentation.
6. Restart the application server.

Configuring Custom Authentication

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

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

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

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

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

To specify a custom authentication provider for WebLogic:

1. Start the **WebLogic Server Console** and open the **Authentication Providers** page from *domain*/Security/Realms/*realm name*/Providers/Authentication.
2. On the Authentication Providers page, select **Oracle Identity Manager Authenticator** from the table at the bottom of the page. The Oracle Identity Manager Authenticator page appears.
3. On the Oracle Identity Manager Authenticator page, select the **Allow Custom Authentication** check box on the **Details** tab, and then click **Apply**.
4. On the Authentication Providers page, configure a new authentication provider by clicking the **Configure a new ...** link for the custom authentication provider you want to add.
5. When you are finished configuring the new authentication provider, be sure that it is listed after Oracle Identity Manager Authenticator (which is the Oracle Identity Manager JAAS module) in the list of authentication providers. If the Oracle Identity Manager Authenticator is not listed above your custom authentication provider, click **Re-order the Configured Authentication Providers**.
6. Restart the WebLogic application server.

Protecting the JNDI Namespace

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

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

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

   ```
   <java.naming.security.principal>
   <java.naming.security.credentials>
   ```

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

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

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

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

4. Restart the server.

Troubleshooting the JNDI Namespace Configuration If you created a user that is the only user that can perform lookups, you may see the following exception when attempting to start the Oracle Identity Manager server where *<user_name>* represents the user you created to perform lookups:

```
[XELLERATE.ACCOUNTMANAGEMENT],Class/Method: Authenticate/connect User with ID: <user_name>
was not found in Xellerate.
[XELLERATE.ACCOUNTMANAGEMENT],Class/Method: Authenticate/connect User with ID: <user_name>
was not found in Xellerate.
[XELLERATE.ACCOUNTMANAGEMENT],Class/Method: XellerateLoginModuleImpl/login encounter some
problems:
com.thortech.xl.security.tcLoginException:
  at com.thortech.xl.security.tcLoginExceptionUtil.createException(Unknown Source)
  at com.thortech.xl.security.tcLoginExceptionUtil.createException(Unknown Source)
  at com.thortech.xl.security.Authenticate.connect(Unknown Source)
  at com.thortech.xl.security.wl.XellerateLoginModuleImpl.login(Unknown Source)
  at weblogic.security.service.DelegateLoginModuleImpl.login(DelegateLoginModuleImpl.java:71)
```

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

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

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

8

Starting the Oracle Identity Manager Server

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

> **Note:** You must complete all relevant post-installation steps described in Chapter 7, "Post-Installation 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>, where x is the latest available number, for example xlconfig.xml.0, xlconfig.xml.1, and so on) 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 for the first time, or after restarting after changing passwords in xlconfig.xml once you have established that the new password is working properly.

Starting the Oracle Identity Manager Server

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

To start the Oracle Identity Manager server:

1. Verify that your database is up and running.

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

   Windows

   To start an administrative server on Windows, run the <*XL_HOME*>\xellerate\bin\xlStartServer.bat script.

   UNIX or Linux

   To start an administrative server on UNIX or Linux, run the <*XL_HOME*>/xellerate/bin/xlStartServer.sh script.

Stopping the Oracle Identity Manager Server

This section describes how to stop the Oracle Identity Manager server on Windows and UNIX or Linux. To stop an administrative server or managed server:

1. Log in to the WebLogic Admin Server Console by pointing a web browser to the following url:

   ```
   http://<hostname>:7001/console
   ```

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

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

Accessing the Administrative and User Console

After starting the WebLogic application server and Oracle Identity Manager you can access the Administrative and User Console.

To access the Administrative and User Console:

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

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

   Where <*hostname*> represents the name of the machine hosting the application server and <*port*> refers to the port on which the server is listening. The 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, log in with your user name and password.

Using the 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 2-5 for information on installing and using the Diagnostic Dashboard.

9 Deploying in a Clustered WebLogic Configuration

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

This chapter discusses the following topics:

About WebLogic Clusters

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

Table 9–1 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.

Table 9–1 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.

Table 9–1 (Cont.) WebLogic-based Oracle Identity Manager Cluster Host Computers

Host Computers	Entities	Software	Description
NA	xlCluster		The name of the WebLogic cluster for Oracle Identity Manager.
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.

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.

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 9-3 for more information.
4. Create a WebLogic configuration.

   See"Creating a WebLogic Configuration" on page 9-3 for more information.
5. Configure the Remote Start options for xlManagedServer1 and start the cluster.

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

   See "Installing Oracle Identity Manager" on page 9-9 for more information.
7. Configure WebLogic.

   See"Configuring WebLogic Post-Oracle Identity Manager Installation" on page 9-9 for more information.
8. Add new servers to your cluster.

See "Adding New Servers to Your WebLogic Cluster" on page 9-10 for more information.

9. (Optional) Configure the IIS Proxy Plug-Ins.

   See "Configuring IIS Proxy Plug-ins" on page 9-13 for more information.

10. (Optional) Configure database-based HTTP session failover.

    See "Configuring Database-based HTTP Session Failover" on page 9-13 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 9-3 for more information.

Configuring a Node Manager for a Managed Server

To control your remote servers from the Administrative Server after you install WebLogic on a host machine, you must edit the nodemanager.hosts file. On each machine where WebLogic is installed, edit the nodemanager.hosts file and specify the IP address of your administrative host.

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

The default location of the nodemanager.hosts file is:

Windows:

```
<BEA_HOME>\weblogic81\common\nodemanager
```

UNIX or Linux:

```
<BEA_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.

Overview

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

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 Internal user and the User group.
9. Add the Internal user to the User group.
10. Set start up mode and choose the SDK.
11. Save your configuration.

Procedure

Perform the following steps to create a WebLogic Oracle Identity Manager cluster configuration:

1. Start the Configuration Wizard:

   Windows:

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

   UNIX or Linux:

   Run <*BEA_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** option 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** option 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. Select the IP address from the **Listen Address** list.
   c. Enter the listening port, for example 7051.
   d. Accept the default values for all other fields.
   e. Click **Next**.

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** section.
   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 Node Manager listen address.
    e. Accept the default value of 5555 for the listening port.
    f. Click **Next**.

    For a UNIX or Linux host:

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

       The *Configure Machines* page UNIX or Linux 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** option 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** options 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.

    - On Windows, click the **Start Admin Server** check box.

      To start the admin server on UNIX or Linux, see "Starting the Administration Server on UNIX or Linux" on page 9-8.

    - Click **Done**.

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

Starting the Administration Server on UNIX or Linux

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

```
cd <BEA_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. Open the WebLogic administration console by pointing 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.
   a. Set the **Java Home** field to the Sun JDK that is included with WebLogic. For example, if WebLogic is installed on the C drive, you set the **Java Home** field to `C:\bea\jdk142_11`
   b. Set the **BEA Home** field. For example, if WebLogic is installed on the C drive, you set the **BEA Home** field to `C:\bea\`
   c. Increase the memory by setting the **Arguments** field to `-Xmx1024m`
   d. For deployments on Windows, locate the **Class Path** field and enter the path to the weblogic.jar. If you are using SQL Server as your database, you must also add the mssqlserver.jar, msbase.jar, and msutil.jar MS JDBC files to the **Class Path** field. For example:

      ```
      C:\sqljars\msbase.jar;C:\sqljars\msutil.jar;C:\sqljars\mssqlserver.jar;
      ```

      Note: Be sure to perform this step on all Managed Servers.

   e. Click **Apply** to save the setting on the **Remote Start** tab.
4. Make sure the Node Manager is running on the remote host, for example XLMANAGED_SERVER_HOST_1. If the Node Manager is not running, start it by running the *<BEA_HOME>*\weblogic81\server\bin\startNodeManager script.

5. Start the server, 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** for both Admin and Managed servers, 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 5, "Installing the Oracle Identity Manager Server on Windows" or Chapter 6, "Installing the Oracle Identity Manager Server on UNIX or Linux" for more information.

Configuring WebLogic Post-Oracle Identity Manager Installation

After 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.

To perform post-installation configuration of WebLogic:

1. Stop the managed server and administration server.

2. Restart the administration server using xlStartServer.bat for Windows, or xlStartServer.sh for UNIX or Linux.

   See Chapter 8, "Starting the Oracle Identity Manager Server" for more information on starting the administration server.

3. Complete the post-installation tasks to configure Oracle Identity Manager for WebLogic, including creating the OIMAuthenticator and setting the control flags to sufficient for both the Default authenticator and OIMAuthenticator. See "Configuring WebLogic for Oracle Identity Manager" on page 7-1 for more information.

4. 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.

5. Each server in the cluster needs to know the location of the others. See "Specifying Cluster Members" on page 9-12 for more information.

6. 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 <*BEA_HOME*>\weblogic81\server\lib directory
- copy <*XL_HOME*>\xellerate\lib\wlXLSecurityProviders.jar to the <*BEA_HOME*>\weblogic81\server\lib\mbeantypes directory

7. Start the cluster.

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 3-1 for more information.

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

2. Configure the Node Manager for xlManagedServer_n.

   See "Configuring a Node Manager for a Managed Server" on page 9-3 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 9-10 for more information.

4. Configure the XLMANAGED_SERVER_HOST_n machine.

   See "Configuring New Host Machines" on page 9-11 for more information.

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

   See "Specifying Cluster Members" on page 9-12 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 9-11 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 <*BEA_HOME*>\weblogic81\server\lib\mbeantypes directory.

3. Copy the <XL_HOME>\ext\nexaweb-common.jar file to the *<BEA_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** on 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.
   - 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** menu, for example, XLMANAGED_SERVER_HOST_2.
   - Make sure your cluster, for example xlCluster, is selected in the **Cluster** menu.
   - Enter the listen address in the **Listen Address** field.
   - Enter the listen port in the **Listen Port** field.
   - Scroll down and click **Clone**.
7. If WebLogic is installed in a different directory than xlManagedServer1, then change the remote start configuration to include the directory location. Remove the -Xmx350m entry from the **Arguments** field in the **Remote Start** tab.
8. Go to the host machine and start the node manager.

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 or Linux, making sure to append the following parameters:

```
<BEA_HOME> <ADMIN_SERVER_HOST> <ADMIN_SERVER_HOST_port>
<WEBLOGIC_admin_login> <WEBLOGIC_admin_password> <XLMANAGED_SERVER_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 or Linux

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

Windows

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

c. Stop all Managed Servers gracefully using the Admin Console and then gracefully stop the Admin Server.

d. Start the Admin Server by running the <*XL_HOME*>\xellerate\bin\xlStartServer script.

Specifying Cluster Members

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

1. Edit the <*XL_HOME*>\xellerate\config\xlconfig.xml file on each node in the cluster. Modify the Discovery section to specify the cluster members. You can accomplish this one of 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.

   - In the xlconfig.xml file on each server in the cluster, specify all the URLs (including port) for all 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 all servers 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
.naming.provider.url>
<java.naming.factory.initial>weblogic.jndi.WLInitialContextFactory</java.na
ming.factory.initial
>
</CoreServer>
<BackOffice>
<java.naming.provider.url>t3://192.168.50.28:7051,192.168.50.184:7051</java
.naming.provider.url>
```

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

2. Start all cluster members using the Admin Console.

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.

10

Installing and Configuring the 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.

This chapter discusses the following topics:

- Requirements
- Installing the Design Console
- Post-install Requirements for the Design Console
- Starting the Design Console

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 following directory:
>
> C:\winnt\system32\drivers\etc\

Installing the Design Console

The following procedure describes how to install the Design Console.

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

To install the Design Console on a Windows host:

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

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

   a. The default directory for the Design Console is C:\oracle. To install the Design Console into this directory, click **Next**.

   b. To install the Design Console into another directory, enter the path in the **Directory 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 dialog appears informing you that the installer could not create the directory. Click **OK** to dismiss the dialog, then contact your System Administrator to obtain the appropriate permissions.

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

   The Application Client Location page appears.
8. 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**.
9. On the Application Server configuration page, enter the information appropriate for the application server hosting your Oracle Identity Manager server:

   a. Enter the host name or IP address.

      Note: The host name is case-sensitive.

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

   c. Click **Next**.

10. On the Graphical Workflow Rendering Information page, enter the Application server configuration information.

    a. Enter the Oracle Identity Manager server host IP address.

    b. Enter the port number.

    c. Select **Yes** or **No** to specify whether the Design Console should use SSL.

    d. Click **Next**.

11. On the **Shortcut** page, select or deselect the check boxes for the shortcut options according to your preferences:

    a. Choose to create a shortcut to the Design Console on the Start Menu.

    b. Choose to create a shortcut to the Design Console on the desktop.

    c. Click **Next** when you are satisfied with the check box settings.

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

13. The final installation page displays a reminder to copy certain application server-specific files to your Oracle Identity Manager server installation.

    Perform these steps and click **OK**.

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

Removing the Design Console Installation

To remove the Design Console installation:

1. Stop the Oracle Identity Manager server and the Design Console if they are running.

2. Stop all Oracle Identity Manager processes.

3. Delete the <*XL_DC_HOME*> directory where you installed the Design Console.

Post-install Requirements for the Design Console

Perform the following steps after installing the Design Console:

1. Copy <*BEA_HOME*>\weblogic81\server\lib\weblogic.jar on the 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.

11

Installing and Configuring Oracle Identity Manager Remote Manager

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

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

Installing the Remote Manager on Windows

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

> **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.

To install the Remote Manager on a Windows host:

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

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

or

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

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

7. 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**.

8. On the Remote Manager Configuration page, enter the appropriate information for the Remote Manager:

   a. Enter the Service Name (default is RManager).

   b. Enter the Remote Manager binding port (default is 12346).

   c. Enter the Remote Manager SSL port (default is 12345).

   d. Click **Next**.

9. On the **Shortcut** page, select (or deselect) the check boxes for the shortcut options according to your preferences:

   a. Choose to create a shortcut for the Remote Manager on the desktop.

   b. Choose to create a shortcut for the Remote Manager on the Start Menu.

   c. Click **Next** when you are satisfied with the check box settings.

10. On the Installation page, review the configuration details, and then click Install to initiate installation.

11. Click **Finish** to complete the installation.

Installing the Remote Manager on UNIX or Linux

To install the Remote Manager on UNIX or Linux:

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

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

> **Note:** If the autostart routine is enabled for your machine, proceed to step 3.

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

   The command-line installer starts.

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

   The Welcome panel appears.

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

5. On the Target directory panel, enter the path to the directory where you want to install the Oracle Identity manager Remote Manager. The default directory is /opt/oracle.

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

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

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

   - Enter **1** to select Install JRE bundled with Oracle Identity Manager
   - Enter **2** to select use your existing JRE at the location specified

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

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

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

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

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

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

      The Remote Manager installation summary panel appears.

8. Check the information.

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

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

Configuring the Remote Manager

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

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

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

Trusting the Remote Manager Certificate

To configure the Remote Manager:

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

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

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

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

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

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

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

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

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

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

   or

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

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

Using Your Own Certificate

Complete the following procedures to use your own certificate.

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

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

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

2. Copy this new keystore to the following directory:

   `<XL_RM_HOME>\xlremote\config\`

3. Open the following file in a text editor:

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

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

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

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

   - For all other JREs, change the values to:

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

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

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

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

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

2. Copy this new keystore to the following directory:

   `<XL_HOME>\xellerate\config`

3. Open the following file in a text editor:

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

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

   ```
   <TrustStore>
      <Location>new_svrkeystore_name</Location>
      <Password encrypted="false">new_svrkeystor_pwd</Password>
      <Type>JKS</Type>
   ```

```
    <Provider>sun.security.provider.Sun</Provider>
</TrustStore>
```

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

Enabling Client-side Authentication for Remote Manager

To enable client-side authentication:

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

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

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

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

4. Locate the `<KeyManagerFactory>` property.

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

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

   or

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

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

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

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

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

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

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

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

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

Starting Remote Manager

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

To start Remote Manager on UNIX or Linux, execute the <*XL_RM_HOME*>/xlremote/remotemanager.sh script.

Removing the Remote Manager Installation

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

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

12

Troubleshooting Your Oracle Identity Manager Installation

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

- Oracle Identity Manager Installation Fails with a WebLogic Clustered Environment
- Task Scheduler fails in a Clustered Environment
- Default Login Not Working

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

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 <*XL_HOME*>\Profile\weblogic.profile file, 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).

Index