Oracle® Identity Manager

Installation Guide for Oracle Application Server

Release 9.0.3

B32459-02

March 2007

Oracle Identity Manager Installation Guide for Oracle Application Server Release 9.0.3

B32459-02

Primary Author: Don Biasotti

Contents

10 Installing and Configuring the Oracle Identity Manager Design Console

11 Installing and Configuring the Oracle Identity Manager Remote Manager

12 Troubleshooting Your Oracle Identity Manager Installation

Index

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 Release 9.0.3 on Oracle Application Server.

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

Audience

The *Installation Guide for Oracle Application Server* is intended for system administrators who plan to install Oracle Identity Manager Release 9.0.3 on Oracle 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 documentation set, visit Oracle Technology Network at:

`http://www.oracle.com/technology/documentation`

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.

Convention	Meaning
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.
<*_HOME>	The directory where an application is installed. The directory where you install Oracle Identity Manager server is referred to as <*XL_HOME*>. Each Oracle Identity Manager component includes an abbreviation: <*XL_DC_HOME*> for the Design Console and <*XL_RM_HOME*> for the Remote Manager. <*ORACLE_HOME*> represents the directory where Oracle Application Server is installed.
OC4J	Oracle Containers for J2EE

<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, and contains the following sections:

- 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

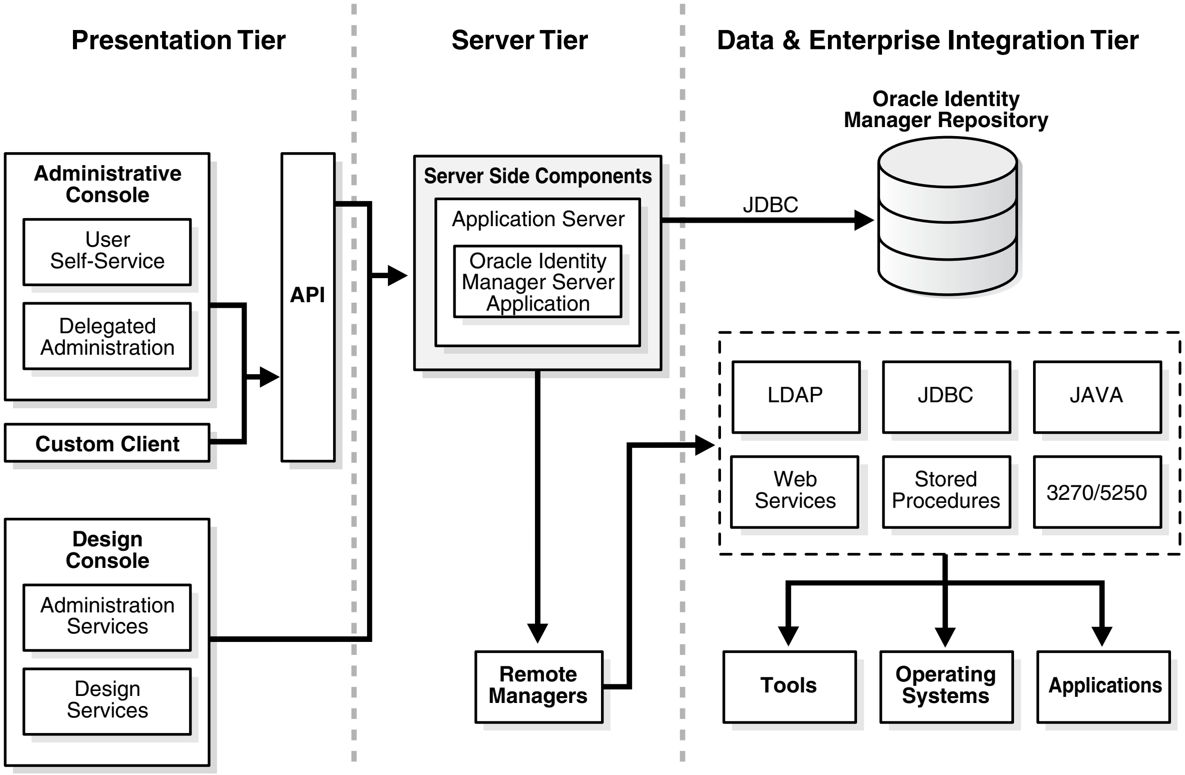
The server tier contains the Oracle Identity Manager Server component, which serves as a bridge between the presentation tier and the data and enterprise integration tier. All requests between the clients and the database are processed through the server tier.

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 Oracle 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 Oracle Application Server:

1. Use Chapter 2, "Planning the Installation" on page 2-1 to prepare for the installation.

2. Use Chapter 3, "Installing and Configuring Oracle Application Server for Oracle Identity Manager" on page 3-1 to set up Oracle Application Server 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 Oracle Identity Manager Server on Windows" on page 5-1
    - Chapter 6, "Installing Oracle Identity Manager Server on UNIX or Linux" on page 6-1

5. Use Chapter 7, "Post-Install Configuration for Oracle Identity Manager Server and Oracle Application Server" on page 7-1 to perform basic Oracle Identity Manager Server and Oracle Application Server 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 Oracle Application Server Configuration" on page 9-1 to install and configure Oracle Identity Manager in a clustered Oracle Application Server environment.
8. Use Chapter 10, "Installing and Configuring the Oracle Identity Manager Design Console" on page 10-1 to install, configure, and start the Oracle Identity Manager Design Console.
9. Use Chapter 11, "Installing and Configuring the Oracle Identity Manager Remote Manager" on page 11-1 to install, configure, and start the Oracle Identity Manager Remote Manager.
10. Use Chapter 12, "Troubleshooting Your Oracle Identity Manager Installation" on page 12-1 to 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 contains 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 the minimum 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 Oracle Identity Manager Server Host Requirements

Server Platform	Item
Windows and Linux	■ Processor Type: Intel Xeon or Pentium IV ■ Processor Speed: 2.4 GHz or higher, 400 MHz FSB or higher ■ Number of Processors: 1 ■ Memory: 2 GB for each Oracle Identity Manager Server instance ■ Hard Disk Space: 20 GB (initial size)
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 database vendor's documentation for the specific database host requirements.

Table 2–2 Sample Database Server Host Requirement

Database Server Platform	Item
Windows and Linux	■ Processor Type: Intel Xeon ■ Processor Speed: 2.4 GHz or higher, 400 MHz FSB or higher ■ Number of Processors: 2 ■ Memory: 4 GB total or 2 GB for each CPU ■ Hard Disk Space: 40 GB (initial size) for Windows, 20 GB (initial size) for Linux
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	■ Sun Fire V100 Server ■ Number of Processors: 1 ■ Memory: 512 MB ■ Hard Disk Space: 10 GB
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 table enables you to identify configuration attributes you need before starting the Oracle Identity Manager installation. Print this worksheet and use it to take notes as you go through your installation. Use the *User Selection* column to fill-in information specific to your installation:

Table 2–6 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	
The name of the database for your installation.	N/A	
The name and password of the database account Oracle Identity Manager uses to access the database.	N/A	

Table 2–6 (Cont.) Installation Worksheet

Item	Default	User Selection
The JDK install directory	Windows: <*ORACLE_HOME*>\jdk UNIX or Linux: <*ORACLE_HOME*>/jdk	
The Oracle Application Server install directory	Windows: C:\product\10.1.3.1\OracleAS_1 UNIX or Linux: /opt/product/10.1.3.1/OracleAS_1	

[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

3

Installing and Configuring Oracle Application Server for Oracle Identity Manager

This chapter explains how to set up Oracle Application Server before installing Oracle Identity Manager and contains the following topics: You must perform the following tasks:

- Installing Oracle Application Server
- Setting the RMI Port Number Range
- Setting Environment Variables
- Verifying the Java JDK Version

Installing Oracle Application Server

When you run the Oracle SOA Suite installer program you must choose the **Advanced Install** option and choose only the **J2EE Server and Web Server** option on the Select Installation Type screen. No other installation type will support Oracle Identity Manager Release 9.0.3—you must choose the **J2EE Server and Web Server option**. After the installer finishes, the OC4J instance within your Oracle Application Server instance starts automatically.

Setting the RMI Port Number Range

The Oracle Process Manager and Notification server (OPMN) dynamically assigns port numbers to each OC4J instance within your Oracle Application Server instance. To ensure you can access the Oracle Identity Manager Design Console and Administrative and User Console on Oracle Application Server, you must set the RMI port number range to be unique in the <*ORACLE_HOME*>/opmn/conf/opmn.xml file. Perform the following steps to set a unique RMI port number range:

1. Open the <*ORACLE_HOME*>/opmn/conf/opmn.xml file with a text editor.
2. Locate the `<port id="rmi" range="12401-12500"/>` entry for the instance you will install Oracle identity Manager on.
3. Set the port number in the range to be a port within the OC4J range, for example:

```
<port id="rmi" range="12408"/>
```

> **Note:** When you install Oracle Identity Manager, on the installer's Application Server Information page, you must enter this RMI port number you set in the opmn.xml file in the **RMI Port No** field.

4. Save and close the opmn.xml file.

For Oracle Application Server clusters, repeat these steps on each node in the cluster so that each opmn.xml file contains the same unique port number.

Setting Environment Variables

After you have verified that Oracle Identity Manager is using the JDK included with Oracle Application Server (refer to "Verifying the Java JDK Version" for more information), complete the following steps to set your environment variables:

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

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

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

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

   Change it to the following:

   ```
   <ORACLE_HOME>\jdk\bin;%SystemRoot%\system32;%SystemRoot%;C:\Program Files
   ```

   Click **OK** to commit your change.

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

   a. Click **New**. In the text box labelled **Variable Name**, enter `JAVA_HOME`. In the text box labelled **Variable Value**, enter the path to your JDK, for example: <*ORACLE_HOME*>\jdk.

      Click **OK** to commit your entry, then click **OK** twice more to close the **Environment Variables** and **System Properties** dialogs, respectively.

   b. Click **Edit**. Verify that the path to your JDK exists in the text box labelled **Variable Value**. If it does not exist, set **Variable Value** to the path for your JDK, for example: <*ORACLE_HOME*>\jdk.

      Click **OK** to commit your entry, then click **OK** twice more to close the **Environment Variables** and **System Properties** dialogs, respectively.

   > **Note:** A message may appear displaying a message asking if you want to update the JDK. Close this window without updating the JDK, as Oracle Identity Manager Release 9.0.3 for Oracle Application Server requires that you use the JDK included with Oracle Application Server.

Verifying the Java JDK Version

Oracle Identity Manager for Oracle Application Server requires that you use the JDK included with Oracle Application Server. Remove any other JDK versions from your system.

The following procedure explains how to verify that the correct version of the Java JDK will be used by Oracle Identity Manager. To verify on a Windows system:

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

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

   ```
   C:\>java -version
   java version "1.5.0_06"
   Java(TM) 2 Runtime Environment, Standard Edition (build 1.5.0_06-b05)
   Java HotSpot(TM) Client VM (build 1.5.0_06-b05, mixed mode)
   ```

4

Installing and Configuring a Database for Oracle Identity Manager

Oracle Identity Manager requires a database. You must install and configure your database before you begin the Oracle Identity Manager installation. This chapter contains the following topics:

- Using an Oracle Database for Oracle Identity Manager
- Using Oracle RAC Databases for Oracle Identity Manager

Using an Oracle Database for Oracle Identity Manager

To use Oracle for your database, you must:

1. Install Oracle—see "Installing Oracle" on page 4-1 for more information.
2. Create your Oracle database—see "Creating an Oracle Database" on page 4-1 for more information.
3. Prepare the Oracle database—see "Preparing the Oracle Database" on page 4-2 for more information.

Installing Oracle

Install the Oracle9i or 10g Release 2 database by referring to the documentation delivered with the Oracle database. Refer to the *Oracle Identity Manager Release Notes* for the specific supported versions. Oracle recommends using the Basic installation.

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

Creating an Oracle Database

You need to create a new Oracle database instance for Oracle Identity Manager. When creating the database, make sure to configure the Oracle JVM feature and enable query rewrite.

You can use the Database Configuration Assistant (DBCA) tool to create the database. To configure the Oracle JVM feature, select the Oracle JVM feature on the Standard Database Features page of the DBCA.

To enable the database for query rewrite, set the init.ora parameters `QUERY_REWRITE_ENABLED` to `TRUE` and `QUERY_REWRITE_INTEGRITY` to `TRUSTED` in the **All Initialization Parameters** field of the DBCA.

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

Configuring the Database for Globalization Support

For globalization support for Oracle Identity Manager, 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 latest version of 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

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

- Verify that query 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:

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

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

You must observe the following prerequisites when using the prepare_xl_db 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.

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

UNIX 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 execute permission for the script:

   ```
   chmod 755 prepare_xl_db.sh
   ```

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

   ```
   ./prepare_xl_db.sh
   ```

4. Provide information appropriate for your database and host machine when the script prompts you for the following items:

   a. The location of your Oracle home (ORACLE_HOME)

   b. The name of your database (ORACLE_SID)

   c. The name of the Oracle Identity Manager database user to be created

   d. The password for the Oracle Identity Manager database user

   e. The name of the tablespace to be created for storing Oracle Identity Manager data

   f. The directory in which to store the data file for the Oracle Identity Manager tablespace

   g. The name of the data file (you do not need to append the .dbf extension)

   h. The name of the temporary tablespace.

5. Check the prepare_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 Linux and then run the prepare_xl_db.sh script again.
>
> ```
> $ dos2unix prepare_xl_db.sh
> ```

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

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

Argument	Description
`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.

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

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

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

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

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 Oracle Application Server 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 Oracle Application Server 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.
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 Oracle Application Server for Oracle RAC

This section explains how to configure both non-clustered and clustered Oracle 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 Oracle Application Server 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 Oracle Application Servers for Oracle RAC:

Note: If you are configuring an Oracle Application Server cluster for Oracle RAC, perform each of the following steps on all nodes in the cluster.

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. Log in to the Oracle Application Server Administrative Console using a web browser.
5. Select the application server where Oracle Identity Manager is installed and then select the OC4J instance within the Oracle Application Server instance you are configuring for Oracle RAC .
6. Select the **Administration** tab, then select **Services**, and then select **JDBC Resources**.
7. Locate the **Connection Pools** section and select **xlConnectionPool**.
8. Set the **URL** property value to the RAC JDBC URL described in step 2.
9. Save the settings.
10. Select **xlXAConnectionPool**.
11. Set the **URL** property value to the RAC JDBC URL described in step 2.
12. Save the settings.
13. For a clustered Oracle Application Server environment, repeat steps 5–12 for each node in the cluster.
14. Restart the Oracle Application Server. If you are configuring an Oracle Application Server cluster for Oracle RAC, restart all nodes in the cluster.

5

Installing Oracle Identity Manager Server on Windows

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

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

This chapter contains the following topics:

- Installing the Database Schema
- Installing Documentation
- Installing the Oracle Identity Manager Server on Windows

Installing the Database Schema

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

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

Installing Documentation

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

Installing the Oracle Identity Manager Server on Windows

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

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

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

1. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.
2. From Windows Explorer, access the installServer directory on the installation CD and double-click the setup_server.exe file.
3. Select a language on the Installer screen and click **OK**. The Welcome screen appears.
4. Click **Next** on the Welcome screen. The Admin User Information screen appears.
5. 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.
6. Select one of the following applications to install and then click **Next**:
   - Oracle Identity Manager
   - Oracle Identity Manager with Audit and Compliance Module

   > **Important:** Do not install Oracle Identity Manager on top of an existing Oracle Identity Manager installation. For each new installation, use a different home directory. If you want to reuse the same name of an existing Oracle Identity Manager home directory, then backup your original Oracle Identity Manager home by renaming that directory.
   >
   > Remember at all times that all Oracle Identity Manager components must be installed in different home directories. For example, you cannot install the Remote Manager in the same directory as the Oracle Identity Manager server.

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

8. On the Database Server Selection page, specify **Oracle** as the database you are using with Oracle Identity Manager and click **Next**.
9. On the Database Information page, provide all database connectivity information required to install the database schema. You install this schema just once, as part of your initial Oracle Identity Manager installation. Thereafter, you configure all the other Oracle Identity Manager components to point to this common schema.

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

When Oracle Identity Manager is installed against an existing database, 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.
- 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 to be sure you set consistent information.

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

- Select the appropriate database options:
  - If a database exists, and the connectivity is good, proceed to step 10.
  - If no connectivity is detected, you are prompted to enter new information or to fix the connection. Click **Next** after entering new information or fixing the connection.

10. 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**.
11. On the Application Server Selection page, select **Oracle Application Server**, then click **Next**.
12. Specify the server configuration by selecting **No** on the Application Server is Clustered screen and click **Next**. Refer to Chapter 9, "Deploying in a Clustered Oracle Application Server Configuration" if you are deploying Oracle Identity Manager for an Oracle Application Server cluster.
13. On the Application Server Information page, enter the information pertaining to your application server and Java installation:

    a. Enter the path to your application server installation

    or

    Click Browse and navigate to your application server installation

    b. Enter the path to the Oracle Application Server JDK directory

    or

    Click Browse and navigate to your Oracle Application Server JDK directory

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

    c. Click **Next**.

    d. Enter the OC4J administrator user name, oc4jadmin, in the **User Name** field.

    e. Enter the password for the OC4J administrator in the **Password** field.

    f. Enter the OC4J instance name in the **OC4J Instance Name** field.

    g. Enter the RMI port number in the **RMI Port No** field. You can identify the RMI port number by executing the following command from the <*ORACLE_HOME*>\opmn\bin\ directory:

    ```
    opmnctl status -l
    ```

    h. Enter 6003 in the **Oracle Process Manager and Notification (OPMN) Port No** field.

    i. Click **Next**.
14. Backup your application server when the Application Server Configuration Backup screen appears, then click **Next** to initiate server installation.

15. If the installer detects an existing database, you can choose to use that database. Select **Yes**, then click **Next**. If the existing database is not encrypted, you are prompted to encrypt it. Select **Yes**, then click **Next**.
16. The Summary screen appears. Click **Install** to install the application.
17. The Completed screen appears. Click **Finish** to exit the installer.

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

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 by stopping Oracle Application Server.
2. Delete the <*XL_HOME*> directory where you installed the Oracle Identity Manager server.

6

Installing Oracle Identity Manager Server on UNIX or Linux

This chapter explains how to install Oracle Identity Manager on UNIX or Linux. Refer to the *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.

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

This chapter contains the following topics:

- Installing the Database Schema
- Installing Documentation
- Installing the Oracle Identity Manager Server on UNIX or Linux

Installing the Database Schema

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

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

Installing Documentation

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

Installing the Oracle Identity Manager Server on UNIX or Linux

To install Oracle Identity Manager on the Oracle Application Server running on UNIX or Linux, you must install as the same non-root user that installed the Oracle Application Server. Do not attempt to install Oracle Identity Manager on the Oracle Application Server running on UNIX or Linux as the root user.

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 the Enter key. To accept a default value—default values are enclosed in brackets after a prompt—simply press the **Enter** key to accept them.

The installer contains logical sections (panels).

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

Note: Before installing Oracle Identity Manager you must set the JAVA_HOME variable to <*ORACLE_HOME*>/jdk/bin.

To install Oracle Identity Manager server on UNIX or Linux:

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.

1. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.
2. From the console, change directory (cd) to the installServer directory on the installation CD and run the install_server.sh file using the following command:

   ```
   sh install_server.sh
   ```

   The installer starts in console mode.

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

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

---

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

   Enter **0** to apply the language selection. The Welcome Message panel appears.

4. Enter **1** on the Welcome Message panel to display the next panel.

   The Admin User Information panel appears.

5. 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.

6. Enter **1** on the OIM Application Options panel to display the next panel.

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

7. Select the application to install:

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

   Enter 0 when you are finished to apply the application selection. The Target directory panel appears.

8. On the Target directory panel, 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.

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

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

   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.

9. On the Database Server Selection panel, specify the type of database you are using.
   - Enter 1 for Oracle.
   - Enter 0 when you are finished.
   - Enter 1 to move to the next panel.
10. Enter your database information:
    a. Enter the database host name or IP address.
    b. Enter (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.
11. Select the authentication mode for the Oracle Identity Manager web application:
    - Enter 1 for Oracle Identity Manager Default Authentication.
    - Enter 2 for SSO Authentication.
    - Enter 0 when you are finished.
    - If you select SSO authentication, you must provide the header variable used in the Single Sign-On system when prompted.
    - Enter 1 to move to the next panel.

    The Application Server Selection panel appears.
12. Specify your application server type.
    - Enter 1 for Oracle Application Server.
    - Enter 0 when you are finished.
    - Enter 1 to move to the next panel.

    The Cluster Information panel appears.

13. Enter 2 for No (non-clustered). Refer to Chapter 9, "Deploying in a Clustered Oracle Application Server Configuration" if you are deploying Oracle Identity Manager for an Oracle Application Server cluster. Enter 0 to proceed to the next panel.

    The Application Server Information panel appears.

14. In the Application Server Information panel:

    - Enter the path to where the application server is installed
    - Enter the path to where the Oracle Application Server JDK is installed
    - Enter 1 to move to the next section.

    The Oracle Application Server Information panel appears.

15. On the Oracle Application Server Information panel:

    - Enter the user name for the Oracle Application Server administrator
    - Enter the password for the Oracle Application Server administrator
    - Enter the Oracle Application Server Instance Name
    - Enter the RMI port number. You can identify the RMI port number by executing the following command from the <*ORACLE_HOME*>/opmn/bin/ directory:

      ```
      opmnctl status -l
      ```

    - Enter the Oracle Process Manager and Notification (OPMN) Port Number. The default port number is 6003.
    - Enter 1 to move to the next panel.

16. When you receive a message about backing up the application server installation, enter 1 to move to the next section. The Summary panel appears.

17. On the Summary panel, enter 1 to begin installation.

18. After the installation finishes, the Completed panel appears. Enter 3 to finish and exit.

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

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 by stopping Oracle Application Server.

2. Delete the <*XL_HOME*> directory where you installed the Oracle Identity Manager server.

7

Post-Install Configuration for Oracle Identity Manager Server and Oracle Application Server

After you have installed Oracle Identity Manager, you must complete some post-installation tasks before you can use the application. Additionally, there are several optional post-installation tasks you may choose to complete, depending on your deployment, before using the application. The following is a list of the sections in this chapter:

- Required Post-Installation Tasks for Oracle Application Server
- Optional Post-installation Tasks

Required Post-Installation Tasks for Oracle Application Server

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

Increasing the Oracle Application Server Heap Size

After installing Oracle Identity Manager on Oracle Application Server, you must increase the Oracle Application Server heap size before using Oracle Identity Manager. Perform the following steps to increase the Oracle Application Server heap size:

1. Open the <*ORACLE_HOME*>\opmn\conf\opmn.xml file in a text editor.
2. Search for the following string:

   ```
   -XX:MaxPermSize=128M
   ```

   Change this string to the following:

   ```
   -XX:MaxPermSize=512M
   ```

3. Save and close the <*ORACLE_HOME*>\opmn\conf\opmn.xml file.
4. Restart the Oracle Application Server after increasing the heap size.

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 file.
5. Edit the <xl-configuration>.<Security>.<XLPKIProvider>.<KeyStore> section to specify the keystore password.

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

   - Change the password tag to `encrypted="false"`.
   - Enter the password (in the clear). For example, change the following block:

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

to the following:

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

6. Restart your application server.

   When you stop and start the application server, a backup of the configuration file is created. The configuration file (with the new password) is read in, and the password is encrypted in the file.

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

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

   - DEBUG
   - INFO
   - WARN
   - ERROR
   - FATAL

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

   ```
   log4j.logger.XELLERATE=WARN
   log4j.logger.XELLERATE.ACCOUNTMANAGEMENT=INFO
   log4j.logger.XELLERATE.SERVER=DEBUG
   ```

4. Save your changes.

5. Restart your application server so that the changes take effect.

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.

8

Starting the Oracle Identity Manager Server

This chapter explains 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:

- Removing Backup xlconfig.xml Files After Starting or Restarting
- Starting the Oracle Identity Manager Server
- Stopping the Oracle Identity Manager Server
- Accessing the Administrative and User Console
- Using Diagnostic Dashboard to Verify Installation

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

Removing Backup xlconfig.xml Files After Starting or Restarting

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

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

Starting the Oracle Identity Manager Server

This section describes how to start the Oracle Identity Manager server on Windows, UNIX, or Linux. To start the Oracle Identity Manager server you start the Oracle Application Server. Use the following steps to start the Oracle Application Server and Oracle Identity Manager:

1. Verify that your database is up and running

2. Start the Oracle Application Server as follows:

   Windows

   From the **Start** menu, select **Oracle - <*Oracle Application Server Instance Name*>**, then select Oracle **Process Manager**, then select **Start Oracle Process Manager**.

   UNIX or Linux

   a. Go to the <*ORACLE_HOME*>/opmn/bin directory

   b. Run the following command:

   ```
   ./opmnctl startall
   ```

Stopping the Oracle Identity Manager Server

This section describes how to stop the Oracle Identity Manager server gracefully on Windows, UNIX, or Linux. To stop the Oracle Identity Manager server gracefully, you stop the Oracle Application Server using the following steps:

Windows

From the **Start** menu, select **Oracle - <*Oracle Application Server Instance Name*>**, then select Oracle **Process Manager**, then select **Stop Oracle Process Manager**.

UNIX or Linux

1. Go to the <*ORACLE_HOME*>/opmn/bin/ directory.
2. Run the following command:

   ```
   ./opmnctl stopall
   ```

Accessing the Administrative and User Console

After starting the Oracle Application Server and the Oracle Identity Manager server you can access the Administrative and User Console. Perform the following steps to access the Administrative and User Console:

1. Add the fully-qualified domain name of the host with your OC4J instance to your system's hosts file. This fully-qualified domain name can be found from URL that appears after you log into Enterprise Manager for Oracle Application Server. Use this fully-qualified domain name when accessing Oracle Identity Manager to avoid session time out issues.
2. Launch your web browser, then point it to the following URL:

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

   <*hostname*> represents the name of the machine hosting the application server and <*port*> refers to the port on which the Oracle Application Server is listening. The default port number for Oracle Application Server is 7777. To learn which port Oracle Application Server is listening on, open <*ORACLE_HOME*>/install/readme.txt on UNIX or Linux, and <*ORACLE_HOME*>\install\readme.txt on Windows.

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

   For example:

```
http://localhost:7777/xlWebApp
```

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

Using Diagnostic Dashboard to Verify Installation

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

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

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

Note: See "Using the Diagnostic Dashboard" on page 2-5 for more information.

9

Deploying in a Clustered Oracle Application Server Configuration

This chapter describes how to deploy Oracle Identity Manager in a clustered Oracle Application Server environment and contains the following sections:

Overview

This chapter describes the steps to deploy Oracle Identity Manager in a Oracle Application Server clustered configuration using three example clusters members as follows:

- Cluster Node A and Cluster Node B are Oracle Application Servers running Oracle Identity Manager.
- Cluster Node C is an Oracle HTTP Web Server.

Installing Oracle Application Server on Cluster Members

The first step in deploying Oracle Identity Manager in a clustered Oracle Application Server configuration is to install Oracle Application Server on the cluster members, for example, on Cluster Node A, Cluster Node B, and Cluster Node C.

Perform the following steps on the Oracle Universal Installer to install Oracle Application Server on the cluster members:

- On Cluster Node A:
  - Install the Oracle Application Server by selecting the **J2EE Server** option on the Select Installation Type screen.
  - Select the **Configure this as an Administrator OC4J instance** option on the Administration Settings screen.

  - Select the **Configure this OC4J instance to be part of an Oracle Application Server cluster topology** option and specify the host name and Port for the discovery address on the Cluster Topology Configuration screen.

- On Cluster Node B:

  - Install the Oracle Application Server by selecting the **J2EE Server** option on the Select Installation Type screen.
  - *Do not* select the **Configure this as an Administrator OC4J instance** option on the Administration Settings screen.
  - Select the **Configure this OC4J instance to be part of an Oracle Application Server cluster topology** option and specify the host name and Port for the discovery address on the Cluster Topology Configuration screen.

- On Cluster Node C:

  - Install the Web Server by selecting the **Web Server** option on the Select Installation Type screen.
  - Select the **Configure this Oracle HTTP Server instance to be part of an Oracle Application Server cluster** option and specify the host name and Port for the discovery address on the Cluster Topology Configuration screen.

Creating OC4J Instances

After installing Oracle Application Server on the cluster members, create OC4J instances named xlClusterMember on Cluster Node A and on Cluster Node B by using the following steps:

1. Log in to the Oracle Enterprise Manager 10g Application Server Control.
2. Click the name of the Cluster Node you want to create the OC4J instance on.
3. Click **Create OC4J Instance**.
4. Enter `xlClusterMember` as the instance name and leave all other instance parameters as their default value.
5. Click Create to create and start the xlClusterMember instance.
6. Start the OC4J instances you created on each Cluster Node.

Repeat these steps until you create xlClusterMember instances on both Cluster Node A and on Cluster Node B.

Installing Oracle Identity Manager on Cluster Members

After creating OC4J instances, install Oracle Identity Manager on both Cluster Node A and Cluster Node B with the same database schema information.

Refer to Chapter 5, "Installing Oracle Identity Manager Server on Windows" or Chapter 6, "Installing Oracle Identity Manager Server on UNIX or Linux" to install Oracle Identity Manager on both Cluster Node A and Cluster Node B.

Important: When installing Oracle Identity Manager on both Cluster Node A and Cluster Node B, be sure to set the following information when prompted by the Oracle Identity Manager Server Installer:

- Select **Yes** when prompted as to whether the application server is clustered.
- Enter `xlClusterMember` as the OC4J instance name.
- Enter xlClusterMember's RMI port number as the RMI port. You can identify the RMI port number by executing the following command from the <*ORACLE_HOME*>/opmn/bin/ directory:

  ```
  opmnctl status -l
  ```

Configuring Oracle Identity Manager for the Oracle Application Server Cluster

After installing Oracle Identity Manager, perform the following steps to configure it for the Oracle Application Server cluster:

1. Copy the Oracle Identity Manager log4j-1.2.8.jar log file from the <*XL_HOME*>\xellerate\ext\ directory to the <*ORACLE_HOME*>\jdk\jre\lib\ext\ directory on both Cluster Node A and Cluster Node B.
2. Increase the Oracle Application Server heap size on both Cluster Node A and Cluster Node B by performing the following steps:
   a. Open the <*ORACLE_HOME*>\opmn\conf\opmn.xml file in a text editor.
   b. Locate the `process-type id="<`*`Instance Name`*`>"` entry. If using the instance names in this chapter, *`Instance Name`* will be `xlClusterMember`.
   c. Change `-XX:MaxPermSize=128M` to be `-XX:MaxPermSize=512M`
   d. Save and close the <*ORACLE_HOME*>\opmn\conf\opmn.xml file.
3. Restart all the cluster members, including Cluster Node A, Cluster Node B, and Cluster Node C.

Accessing the Oracle Identity Manager Administrative and User Console for the Cluster

After restarting all the cluster members you can access the Oracle Identity Manager Administrative and User Console for the cluster by going to the following URL:

http://<*Node_C_host_name*>:<*web_server_port*>/xlWebApp

Note: *Node_C_host_name* represents the host name of the web server and *web_server_port* represents the port number of the web server on Node C, which is 7777 by default.

Installing and Configuring the Design Console for the Cluster

You can install the Oracle Identity Manager Design Console on any Windows node in the cluster. Refer to Chapter 10, "Installing and Configuring the Oracle Identity Manager Design Console" for Design Console requirements and installation steps.

Configuring the Design Console to be Cluster Aware

You must configure the Design Console to be cluster aware. Perform the following steps to configure the Design Console to be cluster aware:

1. Open <*XL_DC_HOME*>\xlclient\config\xlconfig.xml using a text editor.
2. Modify the java.naming.provider.url attribute to be cluster aware, for example:

   ```
   ormi://<host name>:12408/Xellerate,ormi://<host name>:12408/Xellerate
   ```

3. Save and close the xlconfig.xml file.

10

Installing and Configuring the Oracle Identity Manager Design Console

This section explains how to install the Oracle Identity Manager Design Console 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 contains the following topics:

Requirements

Verify that your environment meets the following requirements for Design Console installation:

- You must have an Oracle Identity Manager server installed and running.
- If you are installing on a computer other than the host for the application server, you need to know the host name and port number of the computer hosting that application server.
- The Design Console host must be able to ping the application server host using both IP and hostname.

Note: If you cannot resolve the hostname of the application server, then try adding the hostname and IP address in the hosts file in the directory C:\winnt \system32\drivers\etc\.

Installing the Design Console

To install the Design Console on a Windows host:

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

4. 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:

   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.

   a. The default directory for the Design Console is C:\oracle. To install the Design Console into this directory, click **Next**.
   b. To install the Design Console into another directory, enter the path in the **Directory** field, then click **Next**.

      or

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

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

7. On the Application Server page, select **Oracle**, then click **Next**. The next screen prompts you to specify the JRE to use with Design Console.
8. Select either the JRE that is installed with Oracle Identity Manager or specify an existing JRE. Click **Next**. The Application Server configuration screen appears.
9. On the Application Server Host Information page, enter the information appropriate for the application server hosting your Oracle Identity Manager server:

   a. Enter the host name or IP address in the upper text box.
   b. Use the default, pre-filled value of 12401 for the OC4J naming port.

   Note: The host name is case-sensitive.

   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 the Oracle Application Server is listening on—the default port is 7777. To learn which port Oracle Application Server is listening on, open <*ORACLE_HOME*>/install/readme.txt on UNIX or Linux, and <*ORACLE_HOME*>\install\readme.txt on Windows.

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

   d. Click **Next**.

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

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

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

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

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

13. The final installation page displays a reminder to copy certain application server-specific files to your Oracle Identity Manager server installation. Follow these instructions and then click OK.

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

Removing the Design Console Installation

To remove the Design Console installation, perform the following steps:

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

2. Stop all Oracle Identity Manager processes.

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

Post-Installation Requirements for the Design Console

After installing the Design Console, you must perform the following required steps before using it for Oracle Identity Manager on Oracle Application Server:

1. Copy the <*ORACLE_HOME*>\j2ee\home\lib\ejb.jar file on the Oracle Application Server system to the <*XL_DC_HOME*>\xlclient\ext directory on the Design Console system.

2. Copy the <*ORACLE_HOME*>\j2ee\home\oc4jclient.jar file on the Oracle Application Server system to the <*XL_DC_HOME*>\xlclient\ext directory on the Design Console system.

Starting the Design Console

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

11

Installing and Configuring the Oracle Identity Manager Remote Manager

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

Installing the Remote Manager on Windows

Complete the following steps to install the Remote Manager on a Windows host:

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

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

   a. The default directory for Oracle Identity Manager products is C:\oracle. To install Remote Manager into this directory, click **Next**.

   b. To install Remote Manager into another directory, enter the path in the **Directory name** field, and click **Next**.

   or

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

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

---

7. Select either the JRE that is installed with Oracle Identity Manager or specify an existing JRE. Click **Next**. The Remote Manager Configuration screen appears.
8. On the Remote Manager Configuration page, enter the appropriate information for the Remote Manager:
   a. Enter the Service Name.
   b. Use the default, pre-filled value of 12346 as the binding port.
   c. Use the default, pre-filled value of 12345 as the Remote Manager SSL port.
   d. Click **Next**.
9. On the Shortcut page, select (or deselect) the check boxes for the shortcut options according to your preferences:
   a. Choose to create a shortcut for the Remote Manager on the desktop.
   b. Choose to create a shortcut for the Remote Manager on the Start Menu.
   c. Click **Next** when you are satisfied with the check box settings.
10. On the Summary page, review the configuration details, and then click **Install** to initiate installation.
11. After the installation has completed, click **Finish** on the Completed page to exit.

Installing the Remote Manager on UNIX or Linux

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.
2. From the File Manager, access the installServer directory on the installation CD.
3. Run the install_rm.sh file. The command-line installer starts.
4. Choose a language from the list by entering a number and then entering 0 to apply the language. The Welcome panel appears.
5. On the Welcome panel, enter 1 to move to the next panel. The Target directory panel appears.

6. On the Target directory panel, enter the path to the directory where you want to install the Oracle Identity manager Remote Manager. The default directory is /opt/oracle.
   - Enter 1 to move to the next panel.
   - If the directory does not exist, you are asked to create it. Enter y for yes.

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

7. Specify the JRE to use with Remote Manager:
   - Enter 1 to install the JRE included with Oracle Identity Manager.
   - Enter 2 to use an existing JRE at a specified location.
   - Enter 0 to accept your selections
   - Enter 1 to move to the next panel.

   The Remote Manager Configuration panel appears.
8. On the Remote Manager Configuration panel, enter the Remote Manager configuration information:
   a. Enter the Service Name, or press the Enter key to accept the default.
   b. Enter 12346 as the Remote Manager binding port.
   c. Enter 12345 as the Remote Manager SSL port.
   d. Enter 1 to move to the next panel.

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

     Oracle Remote Manager installs and the Post Install Summary panel appears.
10. Enter 3 to finish the 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 certificates:

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

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

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

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

   <*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 and set the value to `SUNX509`. For example:

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

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

Using Your Own Certificate

Complete the following steps if you want to use your own certificate:

On the Remote Manager Server System:

1. Import your custom key in a new keystore (new_keystore_name) other than .xlkeystore. Be sure to remember the password (new_keystore_pwd) you used for the new keystore.
2. Copy this new keystore to the <*XL_RM_HOME*>\xlremote\config\ directory.
3. Open <*XL_RM_HOME*>\xlremote\config\xlconfig.xml using a text editor.

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

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

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

On the Oracle Identity Manager Server System:

1. Import the same certificate key used in the Remote Manager system to a new keystore (new_svrkeystore_name) other than .xlkeystore. Be sure to remember the password (new_svrkeystor_pwd) you used for the new keystore.
2. Copy this new keystore to the <*XL_HOME*>\xellerate\config directory.
3. Open <*XL_HOME*>\xellerate\config\xlconfig.xml using a text editor.
4. Locate the <RMSecurity> tag and change the value in the <Location> and <Password> tags as follows:

```
<TrustStore>
   <Location>new_svrkeystore_name</Location>
   <Password encrypted="false">new_svrkeystor_pwd</Password>
   <Type>JKS</Type>
   <Provider>sun.security.provider.Sun</Provider>
</TrustStore>
```

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

Enabling Client-side Authentication for Remote Manager

To enable client-side authentication:

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

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

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

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

4. Locate the <KeyManagerFactory> property and set the value to `SUNX509`. For example:

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

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

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

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

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

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

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

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

Starting Remote Manager

Use the following to start the Remote Manager:

- **Windows**: execute the *<XL_RM_HOME>*\xlremote\remotemanager.bat script.
- **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 chapter describes problems that can occur during the Oracle Identity Manager Installation and contains the following topics:

- Task Scheduler fails in a Clustered Environment

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

Task Scheduler fails in a Clustered Environment

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

Index