Oracle® Identity Manager

Installation Guide for WebSphere

Release 9.0

B32141-01

October 2006

ORACLE®

Oracle Identity Manager Installation Guide for WebSphere Release 9.0

B32141-01

Primary Author: Don Biasotti

Contents

8 Starting the Oracle Identity Manager Server

9 Deploying in a Clustered WebSphere Configuration

Preface

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

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

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

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

Audience

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

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

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

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

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0 documentation set, visit Oracle Technology Network at:

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

Conventions

The following text conventions are used in this document:

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

Convention	Meaning
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.
<*_HOME>	The directory where an application is installed. The directory where you install Oracle Identity Manager server is referred to as <*XL_HOME*>. Each Oracle Identity Manager component includes an abbreviation: <*XL_DC_HOME*> for the Design Console and <*XL_RM_HOME*> for the Remote Manager. The directory where the WebSphere application server is installed is referred to as <*WEBSPHERE_HOME*> and includes the /WebSphere/AppClient/ directories. The directory where the WebSphere Network Deployment Manager is installed is referred to as <*NDM_HOME*> and includes the /WebSphere/DeploymentManager/ directories. The directory where the WebSphere Client is installed is referred to as <*WEBSPHERE_CLIENT_HOME*> and includes the /WebSphere/AppClient/ directories.

1

Introduction

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

Product Overview

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

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

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

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

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

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

Oracle Identity Manager Components

Oracle Identity Manager for includes the following components:

- Oracle Identity Manager Server
- Oracle Identity Manager Remote Manager

- Oracle Identity Manager Design Console (for Windows only)

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

Product Architecture

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

The presentation tier contains the following components:

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

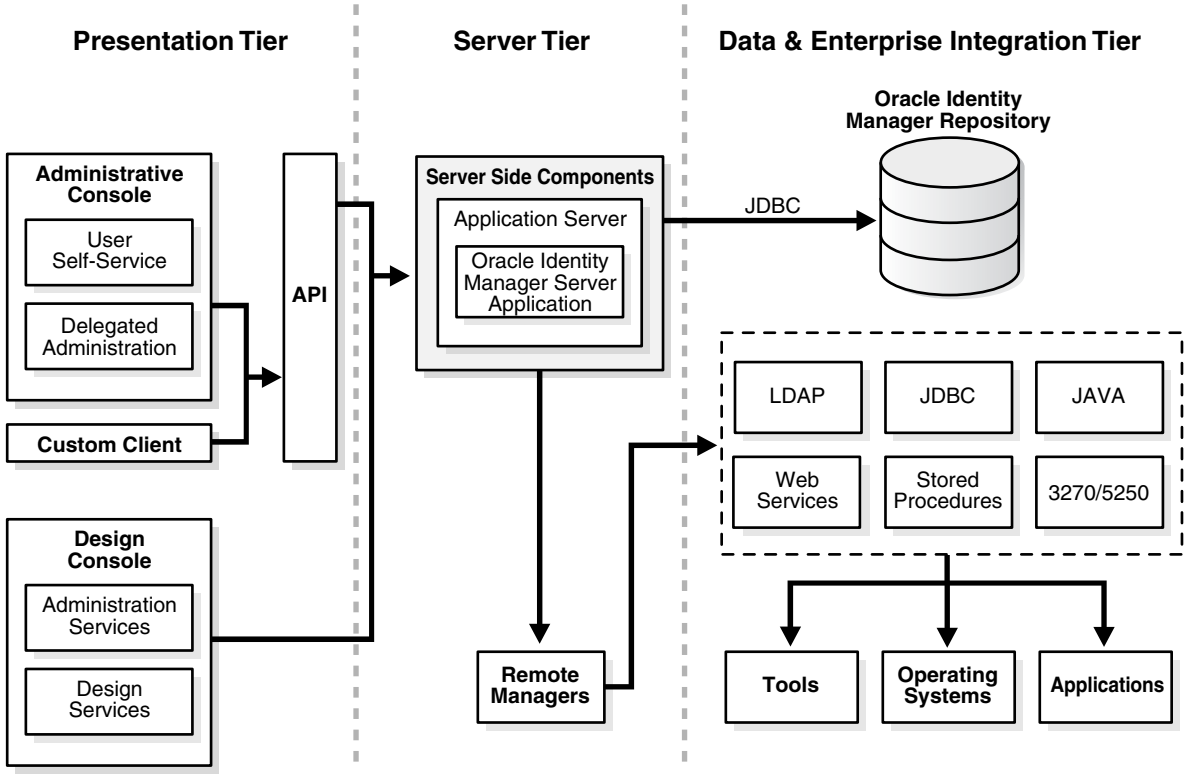
The server tier contains the Oracle Identity Manager Server component, which serves as a bridge between the presentation tier and the data and enterprise integration tier. All requests between the clients and the database are processed through the server tier.

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

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

1. Use Chapter 2, "Planning the Installation" on page 2-1 to prepare for the installation.
2. Use Chapter 3, "Installing and Configuring WebSphere for Oracle Identity Manager" on page 3-1 to set up WebSphere 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 and WebSphere" on page 7-1 to perform basic Oracle Identity Manager Server and WebSphere 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 WebSphere Configuration" on page 9-1 to deploy Oracle Identity Manager in a WebSphere cluster.
8. Use Chapter 10, "Installing and Configuring the Oracle Identity Manager Design Console" on page 10-1 to install, configure, and start the Oracle Identity Manager Design Console.
9. Use Chapter 11, "Installing and Configuring Oracle Identity Manager Remote Manager" on page 11-1 to install, configure, and start the Oracle Identity Manager Remote Manager.
10. Use Chapter 12, "Troubleshooting Your Oracle Identity Manager Installation" on page 12-1 to help troubleshoot your Oracle Identity Manager installation.

2

Planning the Installation

Oracle strongly recommends that you familiarize yourself with the components required for your deployment before starting to install Oracle Identity Manager. Oracle also recommends that you install and use the included Diagnostic Dashboard to ensure that your system is ready for installation. See "Using the Diagnostic Dashboard" on page 2-8 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 JMS server (WebSphere-based clustered installations only)
- A Design Console
- An Administrative and User Console (running in a web-browser)

This chapter discusses the following topics:

Release 9.0.2 for Initial Deployments Only

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

Hardware and Software Requirements

The following sections list the supported host computer, application server, and database requirements for installing Oracle Identity Manager and its components:

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

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

Caution: There is a possibility that the Oracle Identity Manager installation program may conflict with previously installed applications, utilities, or drivers. Therefore, try to remove all non-essential software and drivers from the installation machine before installing Oracle Identity Manager. The same practice should be followed to ensure that the database host can create the database schema.

Supported WebSphere Application Servers

Oracle Identity Manager Release 9.0 is certified on the IBM WebSphere 5.1.1.5 application server.

In a clustered deployment, WebSphere requires a JMS server instance on a machine that is not running any Oracle Identity Manager component. Normally, only one JMS server can exist on a cluster. However, if you desire a back-up JMS server, use a hot/cold disk mirror setup so that the embedded JMS instance can utilize its failover mechanism.

Supported Operating Systems

Oracle Identity Manager is supported on the following operating systems:

- Microsoft Windows Server 2003 Enterprise Edition with SP1 and 2003 R2 Enterprise Edition
- RedHat Linux AS 4.1 and 4.2
- Solaris 10
- AIX 5L 5.3

Supported Databases

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

- Oracle9i Enterprise Edition Release 9.2.0.7
- Oracle 10g Release 2 Enterprise Edition Release 10.2.0.1.0
- Microsoft SQL Server 2000 with Service Pack 3a

Host Requirements for Oracle Identity Manager Components

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

Oracle Identity Manager Server Host Requirements

Table 2–1 lists the minimum host requirements for Oracle Identity Manager Server 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	Requirement
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: Use whichever is greater	2 GB for each Oracle Identity Manager Server instance
	Hard Disk Space	20 GB (initial size)
	Operating System	Microsoft Windows Server 2003 Server with SP1 and 2003 R2 Enterprise Edition, or RedHat Linux AS 4.1 or 4.2
Solaris	Server	Sun Fire V210
	Number of Processors	1
	Memory: Use whichever is greater	2 GB for each Oracle Identity Manager Server instance
	Hard Disk Space	20 GB (initial size)
	Operating System	Solaris 10
AIX	Processor Type	PowerPC
	Number of Processors	1
	Memory: Use whichever is greater:	2 GB for each Oracle Identity Manager Server instance
	Hard Disk Space	20 GB (initial size)
	Operating System	AIX 5L 5.3

Database Server Host Requirements

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

Table 2–2 Sample Database Server Host Requirements

Database Server Platform	Item	Requirement
Windows and Linux	Processor Type	Intel Xeon
	Processor Speed	2.4 GHz or higher, 400 MHz FSB or higher
	Number of Processors	2
	Memory	2 GB for each CPU
	Hard Disk Space	40 GB (initial size)
	Operating System	Microsoft Windows 2000 and 2003 Server or RedHat Linux AS 4.1 or 4.2
Solaris	Server	Sun Fire V250
	Number of Processors	2
	Memory	2 GB for each CPU
	Hard Disk Space	40 GB (initial size)
	Number of Hard Disks	1 Disk
	Operating System	Solaris 10
AIX	Processor Type	PowerPC
	Number of Processors	2
	Memory	2 GB for each CPU
	Hard Disk Space	40 GB (initial size)
	Operating System	AIX 5L 5.3

Design Console Host Requirements

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

Table 2–3 Design Console Host Requirements

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

JMS Server Host Requirements

Table 2–4 lists the minimum host requirements for the JMS Server:

Table 2–4 JMS Server Host Requirements

JMS Sever Platform	Item	Requirement
Windows and Linux	Processor Type	Intel Pentium IV
	Processor Speed	2.4 GHz
	Number of Processors	1
	Memory	512 MB
	Hard Disk Space	10 GB
	Software	IBM WebSphere Application Server
	Operating System	Microsoft Windows 2003 Server with SP1 or RedHat Linux AS 4.1 or 4.2
Solaris	Server	Sun Fire V100
	Number of Processors	1
	Memory	512 MB
	Hard Disk Space	10 GB
	Software	IBM WebSphere Application Server
	Operating System	Solaris 10
AIX	Processor Type	PowerPC
	Number of Processors	1
	Memory	512 MB
	Hard Disk Space	10 GB
	Software	IBM WebSphere Application Server
	Operating System	AIX 5L 5.3

Remote Manager Host Requirements

Table 2–5 lists the minimum host requirements for the Oracle Identity Manager Remote Manager:

Table 2–5 Remote Manager Host Requirements

Remote Manager Platform	Item	Requirement
Windows and Linux	Processor Type	Intel Pentium IV
	Processor Speed	1.4 GHz or higher
	Number of Processors	1
	Memory	512 MB
	Hard Disk Space	1 GB
	Operating System	Microsoft Windows Server 2000, 2003 Enterprise Edition with SP1, and 2003 R2 Enterprise Edition, or RedHat Linux AS 4.1 or 4.2
Solaris	Server	Sun Fire V210

Table 2–5 (Cont.) Remote Manager Host Requirements

Remote Manager Platform	Item	Requirement
	Number of Processors	1
	Memory: Use whichever is greater	2 GB for each Oracle Identity Manager Server instance
	Hard Disk Space	20 GB (initial size)
	Operating System	Solaris 10
AIX	Processor Type	PowerPC
	Number of Processors	1
	Memory	512 MB
	Hard Disk Space	1 GB
	Operating System	AIX 5L 5.3

Supported Version Details

Table 2–6 lists version details for third-party components compatible with Oracle Identity Manager version 9.0:

Table 2–6 Support Details for Third-Party Components

Item	Version Details
WebSphere	5.1.1.5
Oracle9i	9.2.0.7
Oracle 10g Release 2	10.2.0.1.0
SQL Server	2000, with SP3a
Microsoft Windows Server	2003 Enterprise Edition with SP1 and 2003 R2 Enterprise Edition
RedHat Linux	AS 4.1 or 4.2
Sun Solaris	9
IBM AIX	5L 5.3
JDK	See your WebSphere application server documentation for details about which specific JDK version.
Microsoft Internet Explorer	6.x

Planning for Non-English Oracle Identity Manager Environments

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

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

- For Oracle database globalization support, you must configure the database for Unicode. Refer to "Creating an Oracle Database" on page 4-1 for more information.

Before You Start

Before installing Oracle Identity Manager, you should read "Hardware and Software Requirements" on page 2-1 and "Installation Worksheet" on page 2-7 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 2-7 indicates the document sections each installation team member should read.

Table 2–7 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 2–8 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.	NA*	
The TCP port number on which the database listens for connections.	1521 for Oracle 1433 for SQL Server	
The name of the database for your installation.	NA*	

Table 2–8 (Cont.) Installation Worksheet

Item	Default	User Selection
The name and password of the database account Oracle Identity Manager uses to access the database.	NA*	
The JDK install directory	Windows: C:\Program Files\WebSphere\AppServer\java UNIX or Linux: /opt/WebSphere/AppServer/java	
The WebSphere install directory, known as *<WEBSPHERE_HOME>* throughout this document.	Windows: C:\Program Files\WebSphere\AppServer UNIX or Linux: /opt/WebSphere/AppServer	

*NA = 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 Diagnostic Dashboard 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
- A supported version of the WebSphere application server
- Microsoft SQL Server JDBC Libraries Test
- For WebSphere clusters only, an embedded JMS server

Note: The Diagnostic Dashboard fails to return the JMS server status for WebSphere application servers on Windows systems that contain a space in the installation path.

3

Installing and Configuring WebSphere for Oracle Identity Manager

This chapter explains how to set up WebSphere before and after installing Oracle Identity Manager.

This chapter discusses the following topics:

Note: Refer to "Deploying in a Clustered WebSphere Configuration" on page 9-1 if you are using WebSphere in an application server cluster.

Overview of WebSphere Installation and Configuration

The following are high-level pre- and post-installation tasks. You must perform all of these tasks.

Task overview: WebSphere installation and configuration:

1. Install the WebSphere Application Server.

   See "Installing the WebSphere Application Server" on page 3-2 for more information.

2. Install WebSphere Application Client.

   See "Installing the WebSphere Application Client" on page 3-2 for more information.

3. Enable SOAP Communication to WebSphere.

See "Enabling SOAP Communication with WebSphere" on page 3-3 for more information.

4. Upgrade WebSphere server and client software.

   See "Upgrading the WebSphere Server and Client" on page 3-4 for more information.

5. Prepare the environment.

   See "Setting Environment Variables" on page 3-4 for more information.

6. Increase the memory setting for the Java Virtual Machine.

   See "Setting the Memory Size" on page 3-4 for more information.

7. Obtain the cell and node name of the WebSphere instance where you plan to install Oracle Identity Manager.

   See "Obtaining the WebSphere Cell and Node Name" on page 3-5 for more information.

8. Install Oracle Identity Manager.

   See "Installing Oracle Identity Manager with WebSphere" on page 3-5 for more information.

Installing the WebSphere Application Server

Install the 5.1.1.5 version of WebSphere using the full (default) installation option.

If you select instead a custom installation of WebSphere, pay attention to the following:

- Make sure that the path you specify for the application server location ends with `AppServer`. For example on Windows, a valid path might be the following:

  C:\IBM\WebSphere\AppServer

- Make sure that the following WebSphere components are installed during the WebSphere installation:
  - Admin scripting
  - Ant utilities
  - Assembly and deployment tools
  - Embedded Messaging Server and client
- By default, the WebSphere installation uses the application server name server1.

  You can use any server name for your Oracle Identity Manager installation. See "Configuring WebSphere on a Nondefault Server" on page 7-3 for detailed information on configuring WebSphere to use a nondefault server name.

Installing the WebSphere Application Client

The WebSphere Application Client is required to run the Oracle Identity Manager Design Console. Install the WebSphere Application Client 5.1 with the typical (default) installation. Consult your WebSphere documentation for detailed installation procedures.

Enabling SOAP Communication with WebSphere

The Oracle Identity Manager installer communicates with WebSphere as a SOAP client using JACL commands to create data sources, set up message queues, and perform other operations.

To enable SOAP communication with WebSphere:

1. Open the following file in a text editor:

   <*WEBSPHERE_HOME*>\properties\soap.client.props

   Edit the property lines as follows:

   ```
   com.ibm.SOAP.securityEnabled=true
   com.ibm.SOAP.loginUserid=xelsysadm
   com.ibm.SOAP.loginPassword=xelsysadm
   ```

2. Save and close the file.

> **Note:** If you used a user ID or password other than xelsysadm for WebSphere, enter those here.

Obtaining the Bootstrap Port

During WebSphere Application Client installation, you are prompted for the WebSphere Server hostname and port. The port is the WebSphere bootstrap port. You also must provide this port number during Design Console installation. Obtain the bootstrap port number using the WebSphere administrative console.

> **Note:** The WebSphere application server must be running to obtain the bootstrap port number.

To view the bootstrap port number on a non-clustered (singleton) installation:

1. Log in to the WebSphere administrative console.
2. Select **System Administration**, select **<Server1 Name>**, select **End Points**, then select **Bootstrap Address**.

   The bootstrap port is displayed.

To view the bootstrap port number on a clustered installation:

1. Log in to the WebSphere administrative console.
2. Select **System Administration**, select **Deployment Manager**, select **End Points**, then select **Bootstrap Address**.

   The bootstrap port is displayed.

> **Note:** If you are using a clustered WebSphere environment, manually edit the Oracle Identity Manager Design Console configuration file and provide a list of all the bootstrap ports in the cluster. See "Installing Oracle Identity Manager Cluster using a Shared Directory" on page 9-20 for more information.

Upgrading the WebSphere Server and Client

Both the WebSphere server and the client must be updated with the latest fix packs from IBM.

Perform these upgrades in the following order:

1. Upgrade your WebSphere server as follows:
   a. from 5.1 to 5.1.1
   b. from 5.1.1 to 5.1.1.5
2. Upgrade your WebSphere client as follows:
   a. from 5.1 to 5.1.1
   b. from 5.1.1 to 5.1.1.5

Setting Environment Variables

Setting environment variables involves the following:

- Be sure the JAVA_HOME system variable is set to the appropriate JDK. On Solaris or Linux, set JAVA_HOME to Sun JDK 1.4.2_08 or higher, for example 1.4.2_xx—but not versions 1.5 or higher. On AIX, set JAVA_HOME to the WebSphere JDK.
- Remove the ANT_HOME system variable if that variable is defined.
- Ensure that the IBM JVM bundled with WebSphere server is being used when a Java command is executed. To do this, include the WebSphere server directory java/jre/bin in the PATH ahead of all other path entries, for example:

  Windows

  ```
  set PATH=<WEBSPHERE_HOME>\java\jre\bin;%PATH%
  ```

  UNIX or Linux

  ```
  export PATH=<WEBSPHERE_HOME>/java/jre/bin:$PATH
  ```

Setting the Memory Size

Use the following steps to set the memory size. The WebSphere application server must be running to set the memory size.

To set the memory size:

1. Connect to the WebSphere administrative console using the following URL:

   ```
   http://<WebSphere Host>:<WebSphere Admin Port>/admin
   ```

2. Select **Servers**, then **Application Servers**.
3. Select the server name.
4. On the **Configuration** tab, scroll to the **Additional Properties** section.
5. Select **Process Definition**.
6. On the **Configuration** tab, scroll to the **Additional Properties** section.
7. Click **Java Virtual Machine**.

8. In the **General Properties** list, change the value for **Maximum Heap Size** to 1024 MB.
9. Select **OK**.
10. Select **Save** to commit the setting.

Obtaining the WebSphere Cell and Node Name

After installing and initially configuring WebSphere, use the following procedure to obtain the cell and node name of the WebSphere instance where you plan to install Oracle Identity Manager. The Oracle Identity Manager installer will prompt you for this information during installation.

To obtain the cell and node name:

1. Connect to the WebSphere administrative console using the following URL:

   `http://<WebSphere Host>:<WebSphere Admin Port>/admin`

2. Click **Servers** on the left section.
3. Click **Application Servers** under **Servers**.
4. Click the **server instance** (server1, default) on the right section.
5. Click the **Runtime** tab.
6. Note the values for **Cell Name** and **Node Name**.

Note: If the value of **State** is not `Started`, then restart the server instance.

Installing Oracle Identity Manager with WebSphere

The Oracle Identity Manager installer needs to communicate with your WebSphere server during installation, therefore you must verify that the application server is running before you start installation.

To start WebSphere on Windows, use the Windows Start Menu, or the <*WEBSPHERE_HOME*>\bin\startServer.bat script. For example, run:

```
<WEBSPHERE_HOME>\bin\startServer.bat <server name>
```

To start WebSphere on UNIX or Linux, use the <*WEBSPHERE_HOME*>/bin/startServer.sh script. For example, run:

```
<WEBSPHERE_HOME>/bin/startServer.sh <server name>
```

To install Oracle Identity Manager, follow the installation instructions in the chapter specific to your operating system. See "Installing Oracle Identity Manager Server on Windows" on page 5-1 or "Installing Oracle Identity Manager Server on UNIX or Linux" on page 6-1 for more information.

4

Installing and Configuring a Database for Oracle Identity Manager

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

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

Using an Oracle Database for Oracle Identity Manager

The following are the high-level tasks for using an Oracle database for Oracle Identity Manager.

Task overview: Using Oracle for your database:

1. Install Oracle.

   See "Installing Oracle" on page 4-1 for more information.

2. Create an Oracle Database.

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

3. Prepare the Database.

   See "Preparing the Oracle Database" on page 4-2 for more information.

Installing Oracle

Install Oracle9i or 10g release 2. See "Supported Databases" on page 2-2 for more information about specific supported database versions. Oracle recommends using the Basic installation.

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

Creating an Oracle Database

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

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

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

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

Configuring the Database for Globalization Support

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

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

See Also: *Oracle Identity Manager Globalization Guide*

Preparing the Oracle Database

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

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

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

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

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

- UNIX or Linux:

  `prepare_xl_db.sh`

- Windows:

  `prepare_xl_db.bat`

Both of these scripts ship with the Oracle Identity Manager installer and reside in the following directory:

\installServer\Xellerate\db\oracle\

You must observe the following prerequisites when using these scripts:

- The script must be run by the user holding dba privilege (for example, the oracle user on UNIX 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.

Preparing on UNIX or Linux

To prepare the scripts on UNIX or Linux:

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

   ```
   chmod 755 prepare_xl_db.sh
   ```

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

   ```
   ./prepare_xl_db.sh
   ```

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

Preparing on Windows

To prepare the scripts on Windows:

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

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

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

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

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

Table 4–1 Options for the prepare_xl_db.bat Script

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

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

Interpreting the Script Results

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

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

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

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

Using a SQL Server Database for Oracle Identity Manager

The following are high-level tasks for using a SQL Server database with Oracle Identity Manager.

Task overview: Using SQL Server for your database:

1. Install and configure SQL Server.

   See "Installing and Configuring SQL Server" on page 4-5 for more information.

2. Register your SQL server.

   See "Registering SQL Server" on page 4-5 for more information.

3. Create an SQL Server database.

   See "Creating a SQL Server Database" on page 4-6 for more information.

4. Create an SQL Server database account.

   See "Creating a SQL Server Database Account" on page 4-7 for more information.

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

Installing and Configuring SQL Server

To install and configure SQL Server for Oracle Identity Manager:

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

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

2. On the machine hosting the application server, download the SQL Server 2000 Driver for JDBC Service Pack 3 from `http://www.microsoft.com`

3. On the machine hosting the application server, install SQL Server 2000 Driver for JDBC Service Pack 3.

   Note: Make sure to specify a short path for the installation folder, such as C:\JDBCjars, so that you can easily add the path to your CLASSPATH (step 4). If your classpath is more than 256 characters, the installer does not work properly.

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

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

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

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

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

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

5. Enable distributed transactions by installing SQL Server JDBC XA procedures. This involves copying the sqljdbc.dll file in the *<SQLServer JDBC Driver>*\ SQLServer JTA\ directory to the following directory:

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

6. Run the script instjdbc.sql. Follow the instructions for installing stored procedures for Java Transaction APIs (JTA).

   These instructions are bundled with the SQL Server 2000 Driver for JDBC (see the help file jdbcsqlsrv9.html).

7. Make sure the Distributed Transaction Coordinator (MSDTC) service for your SQL Server is running. If necessary, use the SQL Server Service Manager to start it.

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

Registering SQL Server

To register the SQL server:

1. Start the Microsoft SQL Server Enterprise Manager application.

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

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

Creating a SQL Server Database

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

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

To create a new database for Oracle Identity Manager:

1. Start the Microsoft SQL Server Enterprise Manager application.

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

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

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

Table 4–2 Datafiles Files

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

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

   a. Select **Automatically Grow File**.

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

   c. Select **Unrestricted file growth**.

> **Tip:** The PRIMARY filegroup contains the system objects required for SQL Server to operate. The XELL_DATA filegroup stores the physical data and primary keys, XELL_INDEX filegroup stores indexes, XELL_TEXT stores large text fields and XELL_UPA stores physical data and primary keys of the User Profile Audit component.

6. Select the **Transaction Log** tab, then change the initial size to 500MB.

   Leave all the other options on the tab at their default values.

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

7. Click **OK** to trigger database creation.

Creating a SQL Server Database Account

Complete the following procedure to create a database account for Oracle Identity Manager and assign appropriate permissions to that account.

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

To create a SQL Server database account:

1. Launch the Microsoft SQL Server Enterprise Manager application.

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

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

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

4. In the SQL Server Login Properties dialog, select the **General** tab.

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

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

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

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

7. Select the **Database Access** tab.

   In the upper panel, select the check box associated with XELL.

8. In the lower panel, select the check-boxes associated with all of the following:

   - public
   - db_owner
   - db_accessadmin
   - db_securityadmin
   - db_ddladmin
   - db_datareader
   - db_datawriter

9. Click **OK** to commit your changes.

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

10. To check your database settings, right-click the icon representing your server, then select **Properties** from the shortcut menu.

11. On the SQL Server Properties page, select the **Security** tab, then verify that Authentication is set to SQL Server and Windows.

12. Click the **General** tab, then verify that the check boxes associated with **Autostart SQL Server** and **Autostart MSDTC** are selected.

    If **Autostart SQL Server Agent** is selected, do not change the existing setting, because that setting may be required by other applications.

    Click **OK** to close the **SQL Server Properties** page.

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

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

During the schema installation, a corresponding log file is created under the following directory:

<*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.

Caution: Do not install Oracle Identity Manager on top of an existing Oracle Identity Manager installation. For each new installation, use a different home directory. If you want to reuse the same name of an existing Oracle Identity Manager home directory, then back up your original Oracle Identity Manager home by renaming that directory.

Remember at all times that all Oracle Identity Manager components must be installed in different home directories. For example, you cannot install the Remote Manager in the same directory as the Oracle Identity Manager server.

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

1. If you are using SQL Server as your database, before installing the Oracle Identity Manager server be sure to copy the following three files located in C:\Program Files\<Microsoft SQL Server 2000 Driver for JDBC>\lib\ to the <WEBSPHERE_HOME>\lib\ directory and add the driver location to the system CLASSPATH environment variable:
   - mssqlserver.jar
   - msbase.jar
   - msutil.jar
2. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.

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

3. From Windows Explorer, access the installServer directory on the installation CD and double-click the setup_server.exe file.
4. Select a language on the Installer screen and click **OK**.

   The Welcome screen appears.
5. On the Welcome screen, click Next.
6. On the Oracle Identity Manager Application Options screen, select to install one of the following applications, and then click **Next**:
   - Oracle Identity Manager
   - Oracle Identity Manager with Audit and Compliance Module
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 dialog appears informing you that the installer could not create the directory. Click **OK** to dismiss the dialog, then contact your System Administrator to obtain the appropriate permissions.

---

8. On the Database Server Selection page, specify the type of database you are using with Oracle Identity Manager (either **Oracle** or **SQL Server**), then click **Next**.
9. On the Database Information page, provide all database connectivity information that is required to install the database schema.

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

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

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

   - In the **host** field, enter the host name or the IP address of the computer on which the database resides.
   - In the **PORT** field, enter the port number on which the database listens for connections. The default port is 1521 for Oracle and 1433 for SQL Server.
   - In **Database SID** field, enter the name of the database instance.
   - In the **User Name** field, enter the user name of the database account you created for Oracle Identity Manager.
   - In the **Password** field, enter the Oracle Identity Manager database user password.
   - Click **Next** to commit these settings.

Note: When setting the preceding items, refer to the configuration settings specified in "Using an Oracle Database for Oracle Identity Manager" on page 4-1 or "Using a SQL Server Database for Oracle Identity Manager" on page 4-4 to be sure you set consistent information.

The installer checks for database connectivity and if a database schema exists. If the check passes, the installer proceeds to the next step in the process. If the check fails, an error message 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. After you do that, click **Next**.

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 **WebSphere**, click **Next**.
12. On the Cluster Information page, specify whether the server configuration is clustered or non-clustered.

    For a non-clustered environment, select **No** (non-clustered) and click **Next**.

    If you are deploying in a clustered environment, select **Yes**, enter the cluster name, and see "Deploying in a Clustered WebSphere Configuration" on page 9-1 for more information.
13. On the WebSphere Directory Information page, enter the information appropriate for your application server and Java installation:
    a. Enter the full path to your WebSphere installation. Make sure to include `AppServer` in this path, for example: C:\Program Files\WebSphere \AppServer.

       or

       Click **Browse** and navigate to the location of your WebSphere installation.

    b. Enter the path to the JDK associated with your WebSphere application server. Do not include jre in this path. For example, a valid path might be: <*WEBSPHERE_HOME*>\java.

       or

       Click **Browse** and navigate to the location of your JDK installation.

    c. Click **Next**.
14. On the Application Server information page, enter the following application server information:

    WebSphere Server Information for a non-Clustered Installation

    a. Enter the host name or IP address for the machine on which your application server is running. You can enter `localhost` for a local installation.

b. Enter the cell name, which is the name of the folder under <*WEBSPHERE_HOME*>\config\cells.

c. Enter the node name, which is the your Oracle Identity Manager node name.

d. For the WebSphere server name, enter your Oracle Identity Manager server name. If you are using a server other than server1, see "Configuring WebSphere on a Nondefault Server" on page 7-3 for more information.

e. Click **Next**.

15. Back up your application server when the Application Server Configuration Backup screen appears, then click **Next** to initiate server installation.

16. On the Summary screen, click **Install** to initiate the server software installation.

17. 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**.

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

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

19. On the Completed screen, click **Finish** to exit the installer.

    Once you have finished installing an Oracle Identity Manager component, follow the instructions in "Post-Install Configuration for Oracle Identity Manager and WebSphere" on page 7-1 to continue with 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.

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

This chapter discusses the following topics:

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

Installing the Database Schema

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

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 Oracle Identity Manager on UNIX or Linux

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

- Choose from among list of options

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

- Enter information at a prompt

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

The installer contains logical sections (panels).

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

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

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

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

To install Oracle Identity Manager server for UNIX or Linux:

1. Before installing the Oracle Identity Manager server you must set the JAVA_HOME variable to the appropriate JDK.

   On Solaris or Linux, set JAVA_HOME to Sun JDK 1.4.2_08 or higher, for example 1.4.2_xx—but not versions 1.5 or higher.

On AIX, set JAVA_HOME to the WebSphere JDK. For example, use the following commands on AIX:

- `export JAVA_HOME=$<WEBSPHERE_HOME>/java`
- Add $JAVA_HOME/bin to the $PATH environment variable using the following command:

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

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

   `sh install_server.sh`

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

   The installer starts in console mode.
5. Choose a language by entering a number from the list of languages. Enter **0** to apply the language selection.

   The product Welcome Message panel appears.
6. Enter **1** on the Welcome Message panel to display the next panel.

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

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

      Enter **0** when you are finished and then enter 1 to move to the next section. The Target directory panel appears.
9. On the Target directory panel, complete one of the sub-steps that follow:
   - Enter the path to the directory where you want to install Oracle Identity Manager, for example, /opt/oracle/.
   - Enter 1 to move to the next panel.

If the directory does not exist, you are asked to create it. Enter **y**, for yes. The Database Server Selection panel appears.

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

When Oracle Identity Manager is installed against an existing database, the .xldatabasekey file from the earlier Oracle Identity Manager installation must be copied to the new <*XL_HOME*>/xellerate/config directory. In some cases (such as a new installation), the config directory is not created. This does not indicate a failure in the installer. You must then create the config directory and copy the .xldatabasekey file into it.

---

10. Specify the type of database you are using.
    - Enter **1** to select Oracle.
    - Enter **2** to select SQL Server.
    - Enter **0** to finish.
    - Enter **1** to move to the next panel.

    The Database Information panel appears.
11. 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.
12. 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.
13. Specify your application server type.
    - Enter 2 for IBM WebSphere.
    - Enter 0 when you are finished.

- Enter 1 to move to the next panel.

The Cluster Information panel appears.

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

    The Application Server Information panel appears.

    Note: The next steps in procedure are for non-clustered, WebSphere-based Oracle Identity Manager server installations only. Refer to "Deploying in a Clustered WebSphere Configuration" on page 9-1 for information on installing in a clustered WebSphere environment.

15. Enter the application server information at the prompts:
    a. Specify the path to the application server or press the Enter key to accept the default.
    b. Specify the path to the application server's JDK directory or press the Enter key to accept the default.
    c. Enter 1 to move to the next section.
16. Enter the login information for the WebSphere server:
    a. Enter the Application Server host name or IP address.
    b. Enter the WebSphere Cell Name.
    c. Enter the WebSphere Node Name.
    d. Enter the WebSphere Server Name.
    e. Enter 1 to move to the next section.
17. When a message appears warning you to back up your application server, proceed to back up your installation, then enter 1 to move to the next section.
18. On the Installation summary information page, verify the information displayed, then do one of the following:
    - Enter **2** to go back and make changes.
    - Enter 1 to start the installation.
19. After Oracle Identity Manager installs, the Completed panel appears. Enter 3 to finish and exit.

Before you can use Oracle Identity Manager, complete the steps in "Post-Install Configuration for Oracle Identity Manager and WebSphere" 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.
2. Delete the <*XL_HOME*> directory where you installed the Oracle Identity Manager server.

7

Post-Install Configuration for Oracle Identity Manager and WebSphere

After installing Oracle Identity Manager, perform the post-installation tasks documented in this chapter that are appropriate for your deployment before using the application. Depending on your Oracle Identity Manager deployment, you may choose not to perform some of these tasks.

The following are the post-installation tasks documented in this chapter:

Creating the Initial State of the JMS Server

To ensure that the Request Wizard in the Oracle Identity Manager Administrative and User Console (Web Client) works properly, verify that the JMS Server's initial state is set to START.

To check the initial state of the JMS server:

1. Open the server.xml file in the following directory:

   ```
   <WEBSPHERE_HOME>/config/cells/<cell name>/nodes/<node name>/servers/server1/
   ```

2. In the JMSServer section, if necessary, change the value of the initialState variable to START.

   The section should look something like the following:

   ```
   <components xmi:type="messagingserver:JMSServer" xmi:id="JMSServer_1"
   name="Internal JMS Server" description="Internal WebSphere JMS Server"
   numThreads="1">
   <stateManagement xmi:id="StateManageable_4" initialState="START"/>
   ```

3. Save and close the file.

Configuring WebSphere on Nondefault Ports

To run Oracle Identity Manager on WebSphere using nondefault ports (not 80, 443, or 9080), you must add the port mapping information for the server using the WebSphere administrative console. Add the port mapping for the HTTP transport for the nondefault server by using the WebSphere administrative console, as described in the following sections.

Configuring WebSphere on Nondefault HTTP Port

To use a nondefault HTTP port:

1. Select **Environment**, select **Virtual Host**, select **default_host**, then select **Host Alias**.
2. Click **New**.
3. Enter the Host Name and Port Number.

   Note: Setting the Virtual Host, by default, does not include the nonstandard ports for a WebSphere configuration. You must set the Virtual Host for nonstandard server installation and clustered environment installation.

4. Change the <ApplicationURL> tag in xlclient\config\xlconfig.xml to the correct HTTP port.
5. Restart the application server you used to install Oracle Identity Manager.

Configuring WebSphere on Nondefault Naming Service Port

To use a nondefault naming service port:

1. To find the naming service port, use the WebSphere Administrative Console.

   Click **Server**, select **Application Server**, select <**servername**>, select **End Points**, then select **Bootstrap_Address**.

   The screen displays the host name and port number.

   When installing on a nondefault port, the xlconfig.xml file must be modified even if the installation is on server1. In a clustered environment, the xlconfig.xml file must always be modified.

   Note: The default server, server1, needs the configuration file, xlconfig.xml as well as all other servers (nondefault) in the cell to share the same security information.

2. Edit the discovery port settings in the following two files:

   - xellerate\config\xlconfig.xml
   - xlclient\config\xlconfig.xml

   For example, the first server other than the default server, uses 2810 as the naming service port.

Configuring WebSphere on a Nondefault Server

The WebSphere administrative console runs on the default server (server1), which is installed with all WebSphere installations. If you install WebSphere, and then use a server name other than server1 (the default), you must manually configure server1 to recognize Oracle Identity Manager.

> **Note:** In the following procedure, the name of the nondefault server is xlServer.

To configure WebSphere on a nondefault server (named something other than server1):

1. Open the server.xml file in the following directory:

   ```
   <WEBSPHERE_HOME>\config\cells\<cellname>\nodes\<nodename>\servers\server1\
   ```

2. Modify the server.xml file for server1 to include a XL.HomeDir system property that specifies the Oracle Identity Manager home directory.

   For example:

   ```
   <systemProperties xmi:id="Property_1119378049482" name="XL.HomeDir"
   value="C:/xlserver/xellerate" description="Xellerate Home Directory"
   required="true"/>
   ```

   Add the system property to the jvm entry, for example:

   ```
   <jvmEntries xmi:id="JavaVirtualMachine_1" verboseModeClass="false"
   verboseModeGarbageCollection="false" verboseModeJNI="false" runHProf="false"
   hprofArguments="" debugMode="false" debugArgs="-Djava.compiler=NONE -Xdebug
   -Xnoagent -Xrunjdwp:transport=dt_socket,server=y,suspend=n,address=7777"
   genericJvmArguments="">
         <systemProperties xmi:id="Property_1119378049482" name="XL.HomeDir"
   value="C:/xlserver/xellerate" description="Xellerate Home Directory"
   required="true"/>
       </jvmEntries>
   ```

   > **Note:** Refer to the WebSphere installation documentation for detailed information on setting a HomeDir system property.

3. Start the servers using the following command with arguments:

   ```
   startServer <servername> –user xelsysadm -password xelsysadm
   ```

Enabling xelsysadm Access to the Dead Letter Queue

When an Oracle Identity Manager request is created, the Oracle Identity Manager server sends a message to the JMS server. However, there are some cases where the process time is very long.

When this happens, the Oracle Identity Manager server sends a response to the end user (so that wait time is minimized) and also a message to the JMS server, asynchronously. The JMS server then sends a message to Message Driven Bean (MDB) and the MDB digests the message.

If the MDB fails to process the message, it throws an exception. The transaction is rolled back and WebSphere resends the message to MDB until it reaches the maximum retry count.

If the MDB still fails, it again rolls back the transaction. If the retry count is reached, WebSphere does not resend the message MDB. Instead, it sends the message to SYSTEM.DEAD.LETTER.QUEUE. This measure prevents an infinite loop.

SYSTEM.DEAD.LETTER.QUEUE is a system resource that is protected by the Embedded Java Message Server, so, an authorized client is required to access it. For Oracle Identity Manager, the WebSphere administrative user, xelsysadm, is the user id that must be authorized. You must add xelsysadm in the integral-jms-authorizations.xml file so that xelsysadm has permission to access SYSTEM.DEAD.LETTER.QUEUE.

Note: If you used a user ID or password other than xelsysadm for WebSphere, enter it instead of xelsysadm in the procedure that follows.

To add xelsysadm as an authorized user:

1. Navigate to the following location:

   `<WebSphere_Home>config\cells\<cell_name>`

2. Open the file integral-jms-authorizations.xml in a text editor.
3. Search for the tag <queue-admin-userids>.

   Note: There are two <queue-admin-userids> tags in the file. One is commented out and the other is not. Modify the tag that is not commented out.

4. Add the line <userid>xelsysadm</userid>, so that it looks like the following:

```
<queue-admin-userids>
   <userid>xelsysadm</userid>
  </queue-admin-userids>
```

5. Save your changes.
6. Restart the server.

Set the Maximum Retries for JMS Listener

If the maximum retries for JMS Listener is less than or equal to 5, it shuts down the JMS Listener before the Embedded Java Message Server sends the message to SYSTEM.DEAD.LETTER.QUEUE. To prevent the JMS Listener from shutting down, change the default value to a number greater than 5.

To change the retries for the JMS Listener:

1. Launch the WebSphere administrative console.
2. Click **Servers** on the left pane and navigate to **Application Servers**, select **<Server_Name>**.
3. On the **Configuration** tab, scroll to the **Additional Properties** section, then select **Message Listener Service**, and click **Listener Ports**.

4. Click **MessageHandlerMDB_JMSPort**.
5. Modify **maximum retries** from 5 to a greater value.
6. Click **OK** and then click **Save**.

Configuring the ORB Service

When a business transaction, for example, searching for multiple requests or users, returns a large dataset object (greater than 500KB), it may cause the system to throw an exception. When this happens using WebSphere, CORBA_NO_MEMORY is recorded in the WebSphere log file and System Error is displayed as an error message window in the Oracle Identity Manager Administrative and User Console.

WebSphere documentation explains that this exception happens because an Application Server can record totally out of heap space or insufficient heap space to satisfy allocation request when the Java virtual machine is unable to allocate a block contiguous space on the heap to allocate a large object.

To avoid this exception, you must enable WebSphere to pass parameters by reference through ORB. If enabled, ORB passes parameters by reference, instead of by value, which avoids making an object copy. If you do not enable Pass by reference, the parameters are copied to the stack before every remote method call is made.

Use the following steps to enable the Pass by Reference parameter for the ORB Service:

1. Open the WebSphere Administrative Console.
2. Select **Servers**, then **Application Servers**, then **<Server_Name>**, and then **ORB Service**. The ORB Service window appears.
3. Locate the **Pass by reference** parameter and enable the check-box by selecting it.
4. Click **Apply**.
5. Save the service settings.

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 following file:

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

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

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

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

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

     to the following:

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

6. Restart your application server.

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

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

Setting Log Levels

Oracle Identity Manager uses log4j for logging. 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. You can change the log level universally for all components or for an individual component.

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

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 described in the following procedure.

To configure log levels:

1. Open the <*XL_HOME*>\xellerate\config\log.properties file in a text editor.

   This file contains a general setting for Oracle Identity Manager and specific settings for the components and modules that comprise Oracle Identity Manager.

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

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

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

2. Set the general value to the desired log level.
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*MetaLink* Note 394670.1 for additional information about configuring Single Sign-On for Oracle Identity Manager with Oracle Access Manager. You can access the Oracle*MetaLink* Web site at:

https://metalink.oracle.com/

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

To enable Single Sign-On for Oracle Identity Manager:

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

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

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

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

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

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

Replace <*SSO_HEADER_NAME*> with the appropriate header configured in your Single Sign-On system

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

8

Starting the Oracle Identity Manager Server

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

> **Note:** You must complete all relevant post-installation steps before starting Oracle Identity Manager. See the "Post-Install Configuration for Oracle Identity Manager and WebSphere" on page 7-1 for more information.

Removing Backup xlconfig.xml Files After Starting or Restarting

After starting any Oracle Identity Manager component either the first time, or after changing any passwords in xlconfig.xml, passwords are encrypted and saved. However, Oracle Identity Manager also keeps a backup copy of xlconfig.xml (named xlconfig.xml.<x>, where x is the latest available number, for example xlconfig.xml.0, xlconfig.xml.1, and so on) before saving. This backup xlconfig.xml.<x> file contains the passwords in plain text.

> **Note:** 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.

Starting the Oracle Identity Manager Server

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

To start the Oracle Identity Manager server:

1. Verify that your database is up and running.
2. Start the Oracle Identity Manager server by starting the WebSphere application server. Run one of the following scripts appropriate for your operating system to start the WebSphere application server and Oracle Identity Manager:

On Windows

```
<WEBSPHERE_HOME>\bin\startServer.bat <server name>
```

On UNIX or Linux

```
<WEBSPHERE_HOME>/bin/startServer.sh <server name>
```

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 WebSphere application server by running one of the following scripts appropriate for your operating system.

On Windows

```
<WEBSPHERE_HOME>\bin\stopServer.bat <server name>
```

On UNIX or Linux

```
<WEBSPHERE_HOME>/bin/stopServer.sh <server name>
```

Accessing the Administrative and User Console

After starting the Websphere application server and Oracle Identity Manager you can access the Administrative and User Console using the following procedure.

To access the Administrative and User Console:

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

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

   Where <*hostname*> represents the name of the machine hosting the application server and <*port*> refers to the port on which the server is listening. The default port number for WebSphere is 9080.

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

   For example:

   ```
   http://localhost:9080/xlWebApp
   ```

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

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

Using Diagnostic Dashboard to Verify Installation

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

- A trusted store

- Single sign-on configuration
- Messaging capability
- A task scheduler
- A Remote Manager

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

Note: See "Using the Diagnostic Dashboard" on page 2-8 for information on installing and using the Diagnostic Dashboard.

9

Deploying in a Clustered WebSphere Configuration

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

This chapter discusses the following topics:

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

About Clustered WebSphere Configurations

For a clustered environment, several host computers are required. Your configuration may vary, but these instructions describe using 4+n machines. The following table describes the entities needed for a cluster, the computers that they run on, and the software required for the entities. Host computers and entities are labeled descriptively.

Table 9–1 WebSphere-based Oracle Identity Manager Cluster Host Computers

Host Computer	Entities	Software	Description
NDM_HOST	XL_MODEL_ NODE XL_MODEL_ SERVER XL_ CLUSTER	WebSphere Oracle Identity Manager	Use the model node and server as a template. Configure the model server and copy it to the nodes for each application server in the cluster. Note: The model node is not part of the cluster.
JMS_HOST	XL_JMS_ NODE	WebSphere	This is the Oracle Identity Manager message queue host computer. Create the XL_JMS_ NODE on this computer.
IIS_HOST	IIS server	IIS WebSphere Plug-in	This is the IIS web server. The IIS server acts as the front end to the WebSphere cluster, and handles the load balancing. Install IIS and the WebSphere plug-in on this computer.
XL_NODEn_HOST	XL_NODEn	WebSphere Oracle Identity Manager	Each application server in your cluster runs Oracle Identity Manager. The application servers run on one or more node host computers (replace n with the node number, such as XL_ NODE1). You can have more than one application server for each node host computer.

Overview of Setting Up a WebSphere Oracle Identity Manager Cluster

The following are the high-level tasks involved in setting up a WebSphere Oracle Identity Manager cluster.

Note: Before setting up a clustered environment for WebSphere, make sure that all cluster members (machines) have their clock synchronized so that the Scheduler can operate properly.

Task overview: Setting up a WebSphere Oracle Identity Manager cluster:

1. Install and upgrade the Network Deployment Manager on NDM_HOST.

   See "Installing WebSphere Network Deployment Manager" on page 9-5 for more information.

2. Install and upgrade WebSphere application server on NDM_HOST.

   For steps 2-4, see "Installing WebSphere Application Server for a Cluster" on page 9-6 for more information.

3. Install and upgrade WebSphere application server on JMS_HOST.

4. Install and upgrade WebSphere application server on each node host (XL_NODE1_HOST, XL_NODE2_HOST, and so on.).

5. Add the XL_MODEL_NODE and XL_JMS_NODE to the Network Deployment Manager.

   See "Adding the Model and JMS Nodes to the Node Manager" on page 9-8 for more information.

6. Create the XL_MODEL_SERVER on the XL_MODEL_NODE.

   See "Creating the Model Server" on page 9-9 for more information.

7. Create the XL_CLUSTER.

   See "Creating the Cluster" on page 9-10 for more information.

8. Prepare your database.

   See "Using an Oracle Database for Oracle Identity Manager" on page 4-1 or "Using a SQL Server Database for Oracle Identity Manager" on page 4-4 for more information.

9. Install Oracle Identity Manager on NDM_HOST.

   See "Installing Oracle Identity Manager on the Node Manager" on page 9-11 for more information.

10. Copy the <XL_HOME> directory from NDM_HOST to JMS_HOST.

    See "Copying the Oracle Identity Manager Directory to JMS_NODE" on page 9-12 for more information.

11. Set up the WebSphere custom registry on NDM_HOST, XL_MODEL_NODE and XL_JMS_NODE.

    See "Setting up a Custom Registry" on page 9-13 for more information.

12. To add a node, copy the <XL_HOME> directory from NDM_HOST to XL_NODE1_HOST.

    For steps 12-15, see "Adding Nodes and Servers to the Cluster" on page 9-14 for more information.

13. Add Node XL_NODEn (for example, XL_NODE1) to the Node Manager.

14. Create a server (for example, XL_SERVER_ON_NODE1) on XL_NODE1 as a cluster member.

15. Set up virtual host information for the server.
16. Repeat steps 14-15 for each server you want to add to the node.
17. Repeat steps 12-15 for each node you want to add to the cluster.
18. Get the JNDI URL and update the JNDI references in the xlconfig.xml file associated with each server.

    See "Updating the JNDI References" on page 9-17 for more information.
19. Install the WebSphere Plug-in on IIS_HOST.

    See "Installing the WebSphere Plug-in for IIS" on page 9-7 for more information.
20. Set up the IIS server.

    See "Configuring the IIS Plug-in" on page 9-19 for more information.
21. Set up the Design Console.

    See "Post-install Requirements for the Design Console" on page 10-3 for more information.
22. Perform the post-installation tasks after deploying Oracle Identity Manager in your cluster.

    See "Post-Install Configuration for Oracle Identity Manager and WebSphere" on page 7-1 for more information.

WebSphere Software Host Requirements

WebSphere host (and component) computers require the IBM JVM. Conflicts may arise if any of the following is true:

- Other JVM instances exist in PATH.
- JAVA_HOME or CLASSPATH point to anything other than an IBM JVM 1.4.x installation.

If you have any other JVMs on the cluster machines, remove (uninstall) them before proceeding.

Unset the JAVA_HOME, ANT_HOME and CLASSPATH variables.

The version of the WebSphere required is 5.1.1.5. You must install version 5.1, and upgrade it to 5.1.1.5. Obtain the necessary installers from IBM. For a full installation, you need the application server, application client and Network Deployment Manager installers.

Backing Up the Configurations

Oracle recommends that at various points during the cluster setup, you make backups of the various components. This enables you to roll back changes rather than restart the entire process. WebSphere provides a script (backupconfig.bat) that makes a compressed (zip) file of the configuration settings. This script takes the backup file name (with complete path) as an argument.

The configuration backup script stops the Node Manager as well as all the nodes on which it is run. (It is possible to get backups without stopping the nodes or Node Manager. However, Oracle recommends that you stop them before making the configuration backups.) After completing the configuration backups, make sure to restart the Node Manager (startmanager.bat) as well as the Nodes (startnode.bat).

Note: After Oracle Identity Manager is installed and the custom registries are created, you must specify the user name and password to start the Node Manager or the nodes.

When setting up the cluster, run the script at various times to save the current settings.

To back up your server configurations:

1. On the server host computer, create backup directories for the configurations you are backing up.

   For example, to make a back up the Node Manager configuration, use the following command to create a directory for the backup:

   mkdir C:\WAS_Backups\PreXL\NodeManagerConfig

2. Change directories to the application server bin directory. For example:

   cd <*WEBSPHERE_HOME*>\bin

3. Run the batch file backupconfig.bat, and specify a file name that is in the backup directory you created. For example, use the command:

   backupconfig.bat

   c:\WAS_Backups\PreXL\NodeManagerConfig\ConfigBkp.zip

4. Zip the installedApps directory under application server home directory, and store that in the same backup directory:

   C:\WAS_Backups\PreXL\NodeManagerConfig\installedApps.zip

Installing WebSphere Network Deployment Manager

To install and upgrade Network Deployment Manager (NDM) on NDM_HOST you need the WebSphere NDM 5.1 installer. Ensure that your host meets the WebSphere requirements. See "WebSphere Software Host Requirements" on page 9-4 for more information.

To install the NDM for Oracle Identity Manager:

1. Launch the NDM installer (double click Install.exe).

   Note: Node and host names are case-sensitive.

   - For Host Name, enter a host name or enter the IP address of the host.
   - For Node Name, enter XL_MANAGER_NODE.
   - For Cell Name enter XL_CELL.

2. When you get to the node information screen:
3. Continue with the installation. When the NDM installer launches the WebSphere "First Steps" application, exit it and finish the installation.
4. To upgrade the NDM from 5.1 to 5.1.1 to 5.1.1.5 run the upgrade script from IBM.
   - Install the relevant fix packs.
   - Accept default values.
5. To verify Node Manager installation:

- Use a browser to connect to the Node Manager administrative console using the following URL:

  http://<NDM_HOST>:9090/admin

  Note: If the Node Manager is not running, use the Start menu on the host computer to start it.

- Log in and check the Cell name (which is displayed as the User ID) and the version number.

Creating a Backup of the Node Manager Configuration Settings

Back up the Node Manager. See "Backing Up the Configurations" on page 9-4 for more information on creating backups.

1. Create back up directories, for example, use the commands:

   mkdir C:\WAS_Backups

   mkdir C:\WAS_Backups\Basic\NodeManagerConfig

2. Change directories to the Deployment manager bin directory, for example, use the command:

   cd C:\Program Files\WebSphere\DeploymentManager\bin

3. Run the back up batch file backupconfig.bat, for example, use the command:

   backupconfig.bat c:\WAS_Backups\Basic

   \NodeManagerConfig\ConfigBkp.zip

   Note: The previous example commands assume that the Node Manager is installed in the following directory:

   C:\Program Files\WebSphere\DeploymentManager

4. Zip the installedApps directory under DeploymentManager and store that in the same backup directory (C:\WAS_Backups\Basic\NodeManagerConfig).

Installing WebSphere Application Server for a Cluster

To install and upgrade WebSphere application server, you need the WebSphere 5.1 installer and upgrade scripts. Ensure that your host meets the WebSphere requirements. See "WebSphere Software Host Requirements" on page 9-4 for more information.

Install WebSphere on:

- NDM_HOST (for the model node)
- JMS_HOST
- Any node host computers (XL_NODE1, XL_NODE2, and so on.)

For each WebSphere host computer:

1. Install the server.

   See Installing WebSphere Application Server on page 9-7 for more information.

2. Upgrade the server.

   See "Upgrading WebSphere Server" on page 9-7 for more information.

3. Enable SOAP communications.

   See "Enabling SOAP Communication to WebSphere" on page 9-7 for more information.

4. Verify the installation.

   See "Verifying Installation" on page 9-8 for more information.

5. Create Backups.

   See "Creating Backups" on page 9-8 for more information.

Installing WebSphere Application Server

Install version 5.1 of WebSphere with the full (default) installation option. During installation, specify the following values for the **Node Name**:

- XL_MODEL_NODE for the Oracle Identity Manager model node (on NDM_HOST).
- XL_JMS_NODE for the JMS host (on JMS_HOST).
- XL_NODEn for any node host computers (on XL_NODE1, XL_NODE2, and so on.).

Note: node names are case-sensitive.

If you select a custom installation of WebSphere:

- The path you specify for the application server location must end with AppServer (for example C:\IBM\WebSphere\AppServer).
- Make sure that the following WebSphere components are installed during the WebSphere installation:
  - Admin scripting
  - Ant utilities
  - Assembly and Deployment tools
  - Embedded Messaging Server and Client

Upgrading WebSphere Server

Once you install the WebSphere server, update it to the latest fix packs from IBM. Upgrade the WebSphere server to version 5.1.1.5.

Enabling SOAP Communication to WebSphere

The Oracle Identity Manager installer communicates with WebSphere as a SOAP client (using JACL commands to create data sources, set up message queues, and other operations).

To enable SOAP:

1. Edit the following properties in the <*WEBSPHERE_HOME*>\properties\soap.client.props file on all application servers in the cluster:

```
com.ibm.SOAP.securityEnabled=true
com.ibm.SOAP.loginUserid=xelsysadm
com.ibm.SOAP.loginPassword=xelsysadm
```

2. Edit the following properties in the <*NDM_HOME*>\properties\soap.client.props file, where <*NDM_HOME*> is the location of the WebSphere Network Deployment Manager and includes the /WebSphere/DeploymentManager/ directories.

```
com.ibm.SOAP.securityEnabled=true
com.ibm.SOAP.loginUserid=xelsysadm
com.ibm.SOAP.loginPassword=xelsysadm
```

Note: If you used a user ID or password other than xelsysadm for WebSphere, enter those here.

Verifying Installation

Once you have installed and upgraded the WebSphere application server, use the First Steps interface to verify the installation and stop the server.

1. Open the First Steps interface.

   From the **Start** menu, select **IBM WebSphere**, then select **Application Server v5.1**, and then select **First Steps**.

2. Click **Verify Installation**.

3. Once you have verified the installation, click **Stop the Server**.

Creating Backups

Back up the Nodes. See "Backing Up the Configurations" on page 9-4 for more information on creating backups.

Back up the configurations of the following components:

- MODEL_NODE
- JMS_NODE
- Each XL_NODEn

To create the backups, for each node:

1. Create a backup directory for each node you have installed.

   For example, create the following:

   C:\WAS_Backups\Basic\<*Node*>Config

2. Run the backup script from the application server's bin directory.

3. Zip the installedApps directory, and save it in the same location.

Adding the Model and JMS Nodes to the Node Manager

Once you have installed WebSphere on the NDM_HOST and JMS_HOST, add those nodes to the Node Manager. Follow these instructions for each host computer.

Note: Make sure the Node Manager is running.

To add a node:

1. On the node host computer, open a command prompt.
2. Change directories to the bin directory on the application server.
3. Run the addNode.bat script, specifying the Node Manager host name.

   For example, use the following command:

   addNode.bat <*NDM_HOST*>

   Note that <*NDM_HOST*> is the host name of the node manager's computer.

   Note: Host name is case-sensitive.

To verify that the nodes have been added:

1. Use a browser to connect to the Node Manager administrative console at the following URL:

   http://<NDM_HOST>:9090/admin

2. Log in to the system.
3. Click **System Administration**.
4. Click **Nodes**.

   If the nodes were added, they should be displayed with status as synchronized. You can see the status by rolling your mouse over the icon displayed for the Node name in the Administrative and User Console.

5. Log out, then log back in again to refresh the list of nodes.

Creating the Model Server

The model server serves as a template to create other servers for the cluster. The model server is not part of the cluster, and it does not serve any requests.

To create the model server:

1. Use a browser to connect to the Node Manager administrative console at the following URL:

   http://<NDM_HOST>:9090/admin

2. Log in to the system.
3. Click **Servers** on the left panel.
4. Click **Application Servers**.
5. Click **New**.
   - Select the model node (XL_CELL/XL_MODEL_NODE).
   - Enter **XL_MODEL_SERVER** as the server name.
   - Make sure that the **Generate Unique Http Ports** option is enabled.
   - Select the first option for the template (default application server template).
   - Click **Next**.
6. Click **Finish**.

XL_MODEL_SERVER is displayed in the list of application servers.

Note: Your changes are not saved until you click **Save**.

7. Select **Synchronize changes with Nodes**.
8. Click **Save** to commit your changes.

Creating the Cluster

A cluster is a group of application servers that appear as one to the client. All application servers that are used to service incoming calls must be part of this cluster. After you create the empty cluster, back up the system.

To create the cluster:

1. Use a browser to connect to the Node Manager administrative console at the following URL:

   http://<NDM_HOST>:9090/admin

2. Log in to the system.
3. Click **Servers** on the left panel.
4. Click **Clusters**.
5. Click **New**.
   - Enter **XL_CLUSTER** as the cluster name.
   - Make sure you select the check boxes labelled **Prefer local enabled** and **Create Replication Domain for this cluster**.
   - Make sure the **Do not include an existing server in this cluster** option is selected.
6. Click **Next**.
7. Click **Next** (without entering any data).
8. Click **Finish**.
9. Click **Save**.

   Your changes are saved.

10. Make sure the **Synchronize changes with Nodes** check-box is selected.
11. Click **Save**.

    The XL_CLUSTER is created. At this point, it is an empty cluster.

Backing Up the Nodes

Back up the Nodes. See "Backing Up the Configurations" on page 9-4 for more information on creating backups.

Back up the configurations of the following components:

- NDM_HOST
- XL_MODEL_NODE
- XL_JMS_NODE

To create the backups, for each node:

1. Create the backup directories:

   C:\WAS_Backups\PreXL\<*Node*>Config

   <*Node*> represents the name of the component.

2. Run the backup script from the bin directory on the application server.

3. Zip the installedApps directory, then save it in the same location.

The configuration backup command stops the Node Manager as well as all the nodes that it is run on. (While it is possible to get backups without stopping the nodes or Node Manager, Oracle recommends that you stop them before getting the configuration backups.) After completing the configuration backups, make sure to restart the Node Manager (use startmanager.bat) as well as the Nodes (use startnode.bat).

Installing Oracle Identity Manager on the Node Manager

In a WebSphere cluster, install Oracle Identity Manager server on the Node Manager. From that installation, deploy Oracle Identity Manager to the application servers in the cluster. Because the Oracle Identity Manager installer needs to communicate with the Node Manager server during the installation, make sure the deployment manager is running.

> **Note:** Stop all other applications running on the NDM_HOST, except for the Node Manager and the Model Node.

To install the Oracle Identity Manager on the Node Manager:

1. Double click the setup_server.exe file.

   After it launches, click **Next**.

2. Choose a language.

3. Select **Oracle Identity Manager** or **Oracle Identity Manager with Audit and Compliance Module** and click **Next**.

4. Select the destination directory to install Oracle Identity Manager and click **OK**.

5. Click **Next**.

6. Click **Next**.

7. Select your database type and click **Next**.

8. Enter the database information and click **Next**.

9. Select the authentication and click **Next**.

10. Select **WebSphere Application Server** and click **Next**.

11. Select **Yes** for clustering.

12. Enter the cluster name and click **Next**.

13. Enter the Network Deployment Manager Information.

    - Provide the location where the Deployment Manager is installed. The default value is C:\Program Files\WebSphere\DeploymentManager.

- Provide the location of the Deployment Manager's JDK. The default value is C:\Program Files\WebSphere\DeploymentManager\java.
- Click **Next**.

14. For the WebSphere information.
    - Provide the hostname of the machine running the Deployment Manager (NDM-HOST)

      Note: Do not use localhost. Specify the hostname or IP address.

    - Enter the cell name (XL_CELL).
    - Enter the model node name (XL_MODEL_NODE).
    - Enter the model server name (XL_MODEL_SERVER).
    - Click **Next**.
15. Enter the name of the JMS node name (XL_JMS_NODE) and click **Next**.
16. Click **Next** and then click **Install** to install Oracle Identity Manager.

    This may take some time. Watch the SystemOut.log file in the C:\Program Files\WebSphere\DeploymentManager\logs\dmgr directory to monitor the progress.
17. Click **Finish** when installation has completed.

Verifying the Installation

After successful installation, the Oracle Identity Manager application is visible on the Deployment Manager administrative console.

To verify the installation:

1. Use a browser to connect to the Node Manager administrative console at the following URL:

   http://<NDM_HOST>:9090/admin

   Note: If you were using an administrative console browser window that you had logged into before the Oracle Identity Manager installation, log out, then log back in to refresh the display.

2. Log in to the system.
3. Click **Applications** on the left panel.
4. Click **Enterprise Applications**.

   Xellerate and Nexaweb are displayed in the list of applications.

Copying the Oracle Identity Manager Directory to JMS_NODE

Copy the <*XL_HOME*> directory (the default is C:\oracle) to JMS_NODE.

Note: All Oracle Identity Manager cluster participant machines must have their <*XL_HOME*> directory in the same location.

Setting up a Custom Registry

Oracle Identity Manager uses J2EE JAAS authentication mechanism to authenticate users. This requires a custom registry. It also requires the JAAS authentication model to be installed on each of the nodes. You must perform the following steps on NDM_HOST, XL_MODEL_NODE and XL_JMS_NODE.

To set up the custom registry on NDM_HOST:

1. Open a command window on NDM_HOST.
2. Change to the Oracle Identity Manager setup directory. For example, use the command.

   ```
   cd C:\oracle\xellerate\setup
   ```

3. Run the setupWebsphereCustomRegistry.cmd <*NDM_HOME*> command, where <*NDM_HOME*> is the location of the WebSphere Network Deployment Manager and includes the /WebSphere/DeploymentManager/ directories.

To set up the custom registry on XL_MODEL_NODE:

1. Open a command window on XL_MODEL_NODE.
2. Make sure the <*XL_HOME*> directory was copied from NDM_HOST to XL_MODEL_NODE.
3. Change to the Oracle Identity Manager setup directory. For example, use the command:

   ```
   cd C:\oracle\xellerate\setup
   ```

4. Run the setupWebsphereCustomRegistry.cmd <*WEBSPHERE_HOME*> command.

To set up the custom registry on JMS_HOST:

1. Open a command window on JMS_HOST.
2. Make sure the <*XL_HOME*> directory was copied from NDM_HOST to JMS_HOST.
3. Change to the Oracle Identity Manager setup directory. For example, use the command:

   ```
   cd C:\oracle\xellerate\setup
   ```

4. Run the setupWebsphereCustomRegistry.cmd <WEBSPHERE_HOME> command.

Backing up Configuration Settings

XL_CLUSTER is now created, but at this point it is an empty cluster that does not contain any Oracle Identity Manager nodes.

Back up the configurations for the following components:

- NODE_MANAGER
- MODEL_NODE
- JMS_NODE

To create the backups for each node:

1. Create the backup directories.

   C:\WAS_Backups\PostXL\<Node>Config

2. Run the backup script from the bin directory of the application server (or Node Manager).
3. Zip the installedApps directory, then save it in the same location.
4. Restart the Node Manager and the Nodes.

The backup command stops the node manager and the node agents (on their respective machines). All these nodes and the node manager must be restarted to continue with the installation.

To restart the node manager on NDM_HOST:

1. Change to the bin directory. For example, use the command:

   cd "C:\Program Files\WebSphere\DeploymentManager\bin"

2. Run the start command and specify the user and password.

   For example, use the following command:

   startmanager.bat -username xelsysadm -password xelsysadm

> **Note:** From this point on, you must specify the proper user name and password to start or stop the Node Manager or the nodes in this cell. This is the result of Oracle Identity Manager setting up the WebSphere custom registry for JAAS authentication.

To restart a node on the node host:

1. Change to the bin directory. For example:

   cd <*WEBSPHERE_HOME*>\bin

2. Run the start command and specify the user and password.

   For example, use the command:

   startnode.bat -username xelsysadm -password xelsysadm

Adding Nodes and Servers to the Cluster

The Oracle Identity Manager WebSphere cluster (XL_CLUSTER) is now created, but it is empty. You need to add servers to the cluster. When you installed WebSphere on your Node hosts (XL_NODE1_HOST, XL_NODE2_HOST… XL_NODEnHOST) you named each node. Before you can add a node, you need the SOAP port number that Node Manager uses to listen for and service administrative commands.

To get the SOAP port:

1. Make sure that Node Manager is running.
2. Use a browser to connect to the Node Manager administrative console at the following URL:

   http://NDM_HOST:9090/admin

3. Log in using **xelsysadm** as the user name and password.
4. Click **System Administration** in the left-hand side panel.

5. Click **DeploymentManager**.
6. Click **End Points**.
7. Click **SOAP CONNECTOR ADDRESS**.
8. The port number displayed on this page is the one that is needed to add a node to the cell. Make note of the port number (SOAP_PORT).

> **Note:** You also need this port number to update the JNDI references See "Updating the JNDI References" on page 9-17 for more information.

To finish setting up the cluster, for each node:

1. Copy the <*XL_HOME*> directory from NDM_HOST to the node host.

   Make sure you copy it to the same location (such as, C:\oracle).

2. On the node host, change directories and move to the Oracle Identity Manager setup directory. For example, use the following command:

   ```
   cd C:\oracle\xellerate\setup
   ```

3. Open the xlAddNode.<*bat/sh*> script and verify that the correct path is set to the WebSphere installation directory on the node host.
4. Run the xlAddNode.<*bat/sh*> script. This script adds the node to the Node Manager, sets up the custom registry, sets the system properties, synchronizes the node with the node manager, and starts the node. Run the script with the following parameters:

   xlAddNode.bat <*NODE_NAME*> <*NDM_HOST*> <*SOAP_PORT*> <*user*> <*password*>

   For example, to add XL_NODE1, use the command:

   ```
   xlAddNode.bat XL_NODE1 NDM_HOST 8879 xelsysadm
   xelsysadm
   ```

   > **Note:** Node names are case-sensitive.

5. Create one or more servers on each node.

   See "Creating a Server" on page 9-15 for more information.

6. Set up virtual host information for each server.

   See "Setting up the Server Virtual Host Information" on page 9-16 for more information.

Creating a Server

On each node, create one or more servers that are members of the XL_CLUSTER. Use the Node Manager administrative console to do this.

To create a server:

1. Make sure that Node Manager is running.
2. Use a browser to connect to the Node Manager administrative console at the following URL:

3. Log in using **xelsysadm** as the user name and password.
4. Click **Servers**.
5. Click **Clusters**.
6. Click **XL_CLUSTER**.
7. Click **Cluster members**.
8. Click **New**.
   - Name the server. Use a descriptive naming convention for the cluster member name (such as XL_SERVER1_ON_NODE1).
   - Select the node to manage this server (NODE1).
   - Make sure the **Generate Unique Http Ports** check-box is selected.
   - In the template section, select the **Existing application server** option.
   - From the list, select **XL_MODEL_NODE/XL_MODEL_SERVER** as the template server.
   - Click **Apply**.
9. Click **Next**.
10. Click **Finish**.
11. At the top of the page, click **Save**.
12. Make sure the **Synchronize changes with Nodes** check-box is selected.
13. Click **Save**.

    The server is created as a member of the XL_CLUSTER.

Setting up the Server Virtual Host Information

The application server uses the virtual host information setup on the Node Manager to properly configure the web server plug-ins to distribute the load and deal with failover. When you add a server to the cluster, update the virtual host information.

To update the virtual host information:

1. Make sure that Node Manager is running.
2. Use a browser to connect to the Node Manager administrative console at the following URL:

   http://NDM_HOST:9090/admin
3. Log in using **xelsysadm** as the user name and password.
4. In the left panel, click **Servers**.
5. Click **Application Servers**.
6. Click **XL_SERVER1_ON_NODE1**.
7. Click **Web Container**.
8. Click **HTTP transports**.
9. Note the port numbers shown on this page, for example, port 9082 for HTTP and 9445 for HTTPS.
10. In the left panel, click **Environment**.

11. Click **Virtual Hosts**.
12. Click **default_host**.
13. Click **Host Aliases**.
14. Click **New**.
    - Enter * for the Host Name.
    - Enter the previously noted HTTP port number in the **Port** field.
15. Click **Apply**.
16. At the top of this page, click **Host Aliases**.
17. Click **New**.
    - Enter * for the **Host Name**.
    - Enter the previously noted HTTPS port number in the **Port** field.
18. Click **Apply**.
19. At the top of this page, click **Save**.
20. Make sure the **Synchronize changes with Nodes** check-box is selected.
21. Click **Save**.

Virtual host setup for the server is complete.

Updating the JNDI References

When cluster members are added or removed, the JNDI references in Oracle Identity Manager must be updated. The JNDI references include the hostname and WebSphere bootstrap port numbers for each server in the cluster. The JNDI references are specified in Oracle Identity Manager's xlconfig.xml file.

Oracle provides a tool that communicates with the Node Manager, gets the list of servers that are part of the cluster (with the corresponding bootstrap ports), constructs the JNDI URL, and prints it out. Update the xlconfig.xml file on each of the nodes with this URL.

To update the JNDI reference:

1. On NDM_HOST, change to the Oracle Identity Manager setup directory.

   For example, use the command:

   ```
   cd C:\oracle\xelleate\setup
   ```

2. Edit the websphereConfigUtility.cmd file to make sure that the values of the WS_HOME and XL.HomeDir variables are set correctly.

   If they aren't, change these values to appropriate values.

3. Execute the command file.

   For example, use the following command with arguments.

   ```
   websphereConfigUtility.cmd <NDM_HOST> <SOAP_PORT>

   xelsysadm xelsysadm getjndiurl
   ```

Note: For instructions on how to get the SOAP_PORT number, see "Adding Nodes and Servers to the Cluster" on page 9-14 for more information.

The output from the tool includes a JNDI URL. For example:

corbaloc:iiop:XL_NODE1_HOST:9812,XL_NODE2_HOST:9813

Note: This sample URL includes references to two cluster members (servers).

4. Edit the xlconfig.xml file in the C:\oracle\xellerate\config directory.

   Replace all four instances of the java.naming.provider.url with the URL from the tool.

   Note: Use the URL for the Design Console also. See "Installing Oracle Identity Manager Cluster using a Shared Directory" on page 9-20 for more information.

5. Save and close the xlconfig.xml file.
6. Copy the modified xlconfig.xml file to all the nodes in XL_CELL (in other words, to the corresponding C:\oracle\xellerate\config directory).
7. After you copy this file to all the nodes, restart the servers in the XL_CLUSTER.

   Use the Node Manager administrative console to do this. Make sure that Node Manager is running.
8. Use a browser to connect to the Node Manager administrative console (http://NDM_HOST:9090/admin).
9. Log in using **xelsysadm** as the user name and password.
10. In the left panel, click **Servers**.
11. Click **Application Servers**.
12. Make sure the check-boxes for all the Oracle Identity Manager servers (<XL_SERVERn_ON_NODEn>) are selected.

    These are the servers that run the Oracle Identity Manager application.
13. Click **Start**.

    After the servers star, the green arrow in the status column indicates that the servers are running.

Verifying the Node Deployment

To verify that the application was deployed properly on the nodes, point a browser at one of these servers. Use the HTTP port number added in the Virtual Host setup section. See "Setting up the Server Virtual Host Information" on page 9-16 for more information.

For example, use the following URL:

http://XL_NODE1_HOST:<HTTP_PORT>/xlWebApp

Setting Up IIS and the WebSphere Plug-in

The front end for your WebSphere cluster is an IIS server (running on IIS_HOST). Clients connect to this server, which sends requests to the servers in your cluster. Install the WebSphere plug-in on IIS_HOST.

To verify that IIS is installed:

1. On IIS_HOST, open the **Control Panel** and select **Add/Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. If IIS is not installed, select the **Internet Information Service (IIS)** check-box.
4. Click **Next**.

   IIS installs.
5. Click **Finish**.

Installing the WebSphere Plug-in for IIS

The WebSphere plug-in is installed by performing a custom WebSphere installation.

To install the plug-in:

1. Launch the WebSphere 5.1 base installer.
2. Choose the **Custom** setup option.
3. Make sure only the **Web Server Plug-ins** and the **Microsoft Internet Information Services** options are selected. De-select all other features.
4. Pick the install location and complete the installation.
5. To enable the plug-in within IIS, then verify that it is working, launch the Internet Services Manager in Administrative Tools.
6. Right-click the icon for the IIS server, then select **Restart IIS** from the shortcut menu.
7. Click **OK** to restart the IIS Service and enable the WebSphere plug-in for IIS.
8. After the restart process finishes, right-click the server, then select **Properties** from the shortcut menu.
9. Click **Edit** beside **WWW Services** under Master Properties.
10. In the ISAPI Filters tab, make sure **sePlugins** is displayed with high priority and a green upward arrow.

Configuring the IIS Plug-in

The following procedure describes how to configure the IIS plug-in, export the configuration from the Node Manager and install it.

To configure the IIS plug-in and install the configuration:

1. Make sure that Node Manager is running.
2. Use a browser to connect to the Node Manager administrative console (http://NDM_HOST:9090/admin).
3. Log in using **xelsysadm** as the user name and password.
4. In the left panel, click **Environment**.
5. Click **Update Web Server Plug-in**.

6. Click **OK**.

   The web server plug-in configuration updates and a message appears at the top of the page.

   The generated file is:

   <*NDM_HOME*>\config\cells\plugin-cfg.xml

   <*NDM_HOME*> is the location of the WebSphere Network Deployment Manager and includes the /WebSphere/DeploymentManager/ directories.

7. Make a backup copy of the existing IIS server WebSphere plug-in configuration file.

   The default location is <*WEBSPHERE_IISPlugin_HOME*>\config\cells\plugin-cfg.xml, where <*WEBSPHERE_IISPlugin_HOME*> refers to the installation directory of the IIS Plugin.

8. Copy the new plugin-cfg.xml file from the Node Manager to the install directory of the IIS server WebSphere plug-in.

9. Open the file on the IIS server.

   Several of the paths in the new configuration file must be updated to reflect the files of the IIS server. Generally the Node Manager is installed in a folder named DeploymentManager, while the plug-in is always installed in AppServer. Change the directories in the configuration file to specify the correct paths for the logs and key files.

10. Save and close the file.

11. Restart the IIS server.

Installing Oracle Identity Manager Cluster using a Shared Directory

Use the following task overview to install Oracle Identity Manager on a WebSphere clustered environment using a shared directory. You must perform the steps in the task overview in the order shown.

Task overview: Installed a cluster using a shared directory:

1. Create a shared directory on the file server designated for Oracle Identity Manager.

   This shared directory can be on a Solaris machine with NFS or on a Windows share.

2. On all the machines that will be hosting Oracle Identity Manager, map this drive using the same drive letter on each machine.

   If the installation is on Solaris, mount the NFS partition on the same mount point.

3. Install Oracle Identity Manager using the standard installation instructions.

   Provide the installation location on the shared drive.

4. When adding a new host to the cluster, map the drive as in step 2, thereby making Oracle Identity Manager home directory available for use.

5. Modify the xlAddNode command to provide the proper Oracle Identity Manager location as well as the WebSphere location.

6. Run the xlAddNode command.

Note: If the log.properties file is modified to include a File Appender to log the Oracle Identity Manager messages into a separate file, make sure to provide a location on the local drive. Also, ensure that the same location exists on all the nodes.

Partitioned Installation on WebSphere

This section describes how to perform a partitioned installation of Oracle Identity Manager onto a WebSphere clustered environment.

WebSphere clustered environments for a partitioned installation are the following:

- An **independent clustered environment** – where Scheduled Task and Front Office are processed.

  Two independent installations of Oracle Identity Manager share the same database.

- A **multiple clustered environment** – where the same Network Deployment Manager (NDM) is used for hosting different components.

Important Points to Consider

Here are some important points to consider before you choose the type of clustered environment you wish to install the partitioned Oracle Identity Manager:

- Adapters and scheduled jobs can invoke APIs and submit messages.

  These API calls are processed where APIs are hosted (at the Core Server). Also, the submitted messages are processed where Message Driven Beans (MDBs) are hosted. Hence, scheduled job execution is truly distributed among three components: the APIs, MDBs and Schedule Job itself.

- All off-lined tasks will be executed partly by the API layer and partly by the MDB layer.

  Currently, request initiation and reconciliation are off-lined, but more tasks are planned to be off-lined in the future.

- In theory, it is possible to install a Scheduler a single machine.

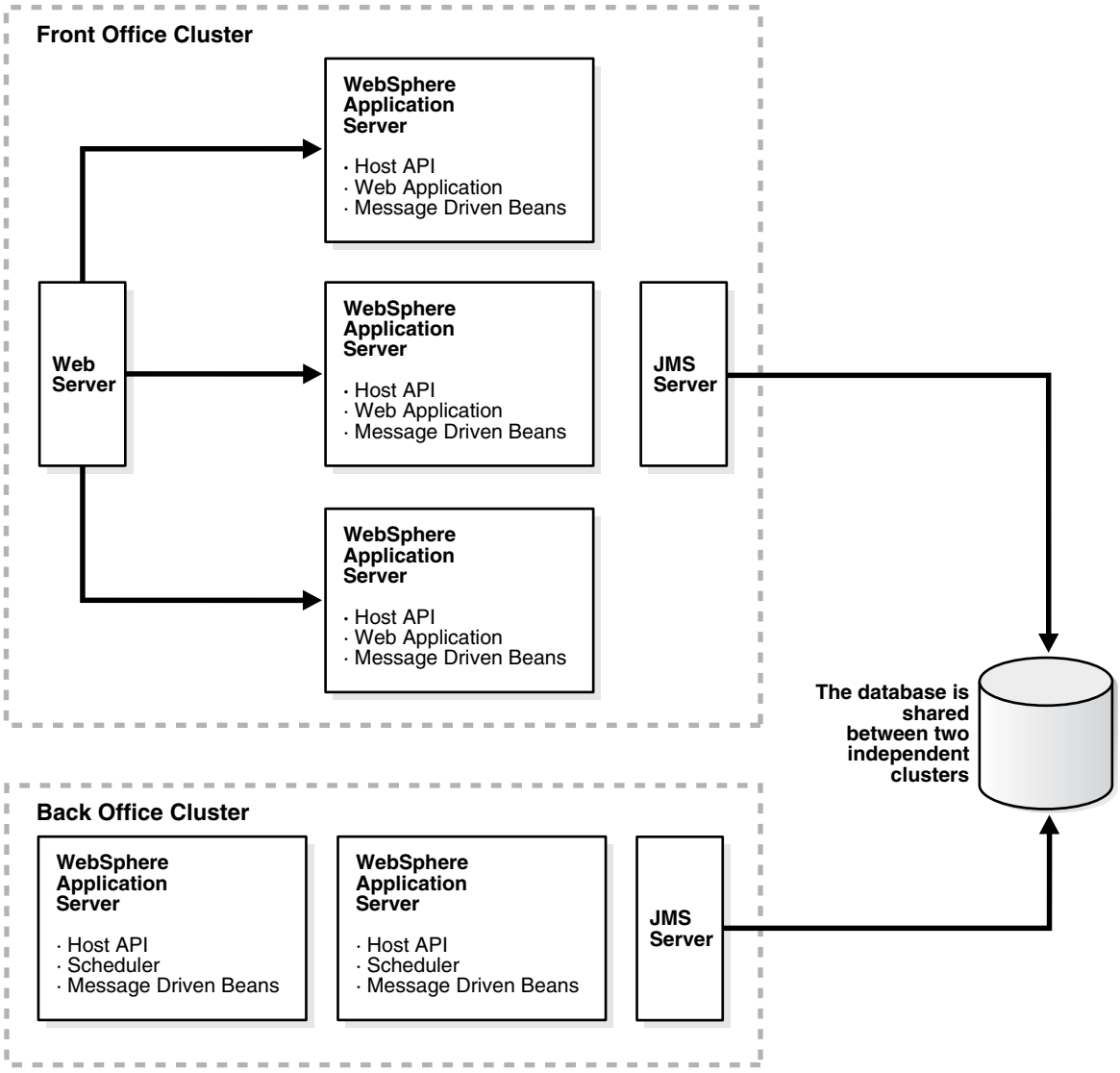
  However when a schedule task executes, it calls the APIs. For the reconciliation tasks, they call APIs as well as submit messages. Hence, true processing of scheduled tasks occurs in the APIs and MDBs.

Independent Clustered Environment

For an independent clustered environment, two separate Oracle Identity Manager installations that will share the same database. The first installation of Oracle Identity Manager is designed to handle Front Office (that is, user requests for administration, provisioning and so on.) The second installation is designed to handle Back Office (for only the Schedule Task execution).

The Figure 9–1 shows two independent clustered environments: Front Office and Back Office:

Figure 9–1 Two Independent Oracle Identity Manager Cluster Environments



Environment Profile

The following items discuss some important points needed for the independent clustered environment:

- The Front Office installation must include MDBs, as the Front Office is unaware of the existence of the Back Office.

  However, it is possible to overcome this limitation by using WebSphere MQ.

- The Back Office installation must include APIs, as they are called by the Scheduled Tasks.

- Both installations can be either clustered or non-clustered.

  For example, Front Office can be a cluster, while Back Office runs on a single (but powerful) machine.

- Caching must be configured as a single cluster by using the same multi-cast IP address between both the clusters.

- If the same IP cannot be used, the cache must be flushed in both the clusters after an import or a change to process definition, resource object definition, and so on.

Environment Advantages

The following advantages inhere to the independent clustered environment:

- The clustered environments use different platform types.

  For example, the Front Office can be Windows-based, while the Back Office is Solaris-based.

- The entire Schedule Task execution is processed in the Back Office cluster with reasonable predictability.
- There is one Java Virtual Machine (JVM) for each machine (or one application server instance running for each machine).

Environment Disadvantages

The following disadvantages inhere to the independent clustered environment:

- The clusters are rigid in their processing duties.

  For example, the Front Office processing cannot be delegated to the Back Office cluster, and vice-versa even if the other cluster is under-utilized at that time. Therefore, under no circumstances can the Front Office cluster share the load on the Back Office cluster.

- The Design Console must be configured to work with the Back Office cluster and be able to schedule jobs, and so on.
- Since the Back Office cluster does not qualify as a true “back-office cluster”, it causes the limitation of off-lined tasks.

  It also restricts processing to the Front Office cluster. For example, off-lining task approvals occur in the Front Office cluster.

Installation Considerations

The following are guidelines for installation:

- Install Oracle Identity Manager in the Front Office cluster by following the clustered installation steps in this guide.
  - During the installation, select Database Install to install the database.
  - During the installation deselect Scheduler, as you do not want the Scheduler to execute in the Front Office cluster.
- Install Oracle Identity Manager in the Back Office cluster by following the instructions in this guide.

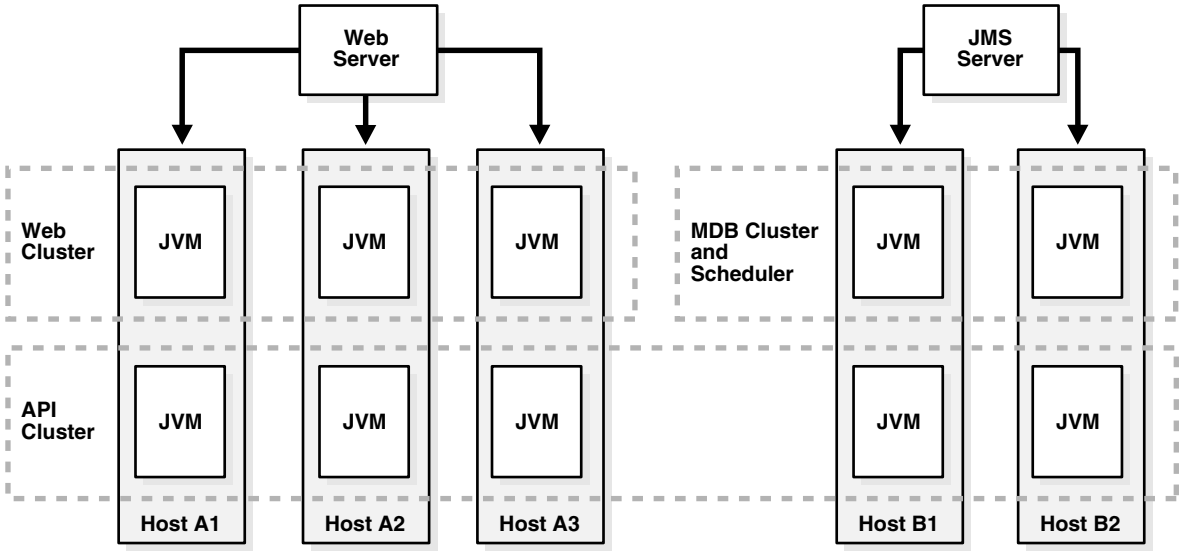
  For the Back Office you must use the appropriate steps (clustered or non-clustered) based on how you configure your environment.
  - During the installation, do not select "Install Database" for the Back Office.
  - During the installation, do not select the web application.
- Make sure the Cache\MultiCastAddress is same for both the Front Office and Back Office installations to ensure cache flushing on both clusters.

Multiple Clustered Environment

After installing Oracle Identity Manager in a multiple-clustered environment, where clusters share the same Node Domain Manager (NDM), you can add more servers and create more clusters. You can also map modules to different clusters using the WebSphere administrative console.

Figure 9–2 shows that the multiple-clustered environment is hosting different modules. If you need to configure a machine (host) for multiple functions, then you can map multiple modules to this host.

Figure 9–2 Multiple Oracle Identity Manager Cluster Environments Hosting Different Modules



Note: When creating the Oracle Identity Manager Cluster using the WebSphere administrative console, make sure that you select the Prefer Local checkbox so that the local EJBs are "preferred" over the remote EJBs.

Environment Advantages

The following are advantages of the multiple-clustered environment:

- Has the ability to load balance processing where the Back Office cluster can take on work, and vice versa.

  For example, there are times when the API cluster on the Front Office can process scheduled tasks.

- The Back Office cluster represents a true "Back Office" where designated off-lined tasks are processed within the Back Office machines.
- The Design Console points to the same cluster for all operations.
- There is a central administration of the WebSphere cluster.

Environment Disadvantages

The following are disadvantages of the multiple-clustered environment:

- Multiple JVMs will be running on all the machines within the cluster.

  The impact on performance is unknown.

- After applying patches, you must perform manual steps to map modules into the proper cluster, as the current patch mechanism cannot accommodate the two separate deployments.

Installation Considerations

- Install WebSphere by following the clustered installation steps in this guide, but name the cluster XL_API_CLUSTER (instead of XL_CLUSTER).
- Create additional clusters: XL_API_CLUSTER, WebCluster and BackOfficeCluster.

  Add servers into the clusters using the same model server for all of them.
- In the web cluster, add servers into the nodes participating in the Front Office.

  Note: To indicate that the server is hosting web components, append the word "Web" to the end of the server name. For example, Node1Server1Web.

  a. In the Back Office cluster add servers into the nodes participating in the "Back Office." Use the suffix, BackOffice or BO.

  b. Create servers in XL_API_CLUSTER and add the suffix API to the servers.
- Map modules into different clusters:

  a. Click **Enterprise Applications**, then click **Oracle Identity Manager**.

  b. Click **Map modules to Application Servers**.

  c. Select the **xlWebApp.war** and then select the **WebCluster** from the list on the top.

  d. Click **Apply**.

  e. xlWebApp.war runs on Web Cluster.

  f. Select **xlBackOfficeBeans**, **xlScheduler.war**, and **SchedulerBean**, then map them to the BackOffice cluster.

  g. Save the changes.
- Modify xlconfig.xml and change the Discovery section. Include the boot strap ports of the correct servers to find the various components.

  a. Edit the websphere.profile and make sure the cluster name is XL_API_CLUSTER.

  b. Run websphereConfigUtility.cmd to get the list URL to be used for CoreServer component.

  c. Perform the same steps for "BackOfficeCluster" to get the JNDI URL to be used for BackOffice, Scheduler and JMSServer components.
- Start all the clusters.
- Restart the application.

Scaling

Follow these guidelines when scaling up your environment:

- To add more machines to handle Front Office requests, add a new node then add servers in both the WebCluster and the API Cluster.
- To add more processing power in the Back Office cluster, add a new node, then add servers to the API Cluster and the Back Office Cluster on that node.

Variation

It is possible to keep Web and API on the same cluster so that only one JVM is running on the Front Office machines. On the other hand, the generated plug-in configuration must be modified to remove the Back Office machines.

Setting Up Supported Integrations on a WebSphere Cluster

To deploy an Oracle Identity Manager-supported integration on your WebSphere clustered environment, you must make sure that the integration is accessible for all cluster members. Refer to the Oracle Identity Manager Connector Pack Release Notes located at the Oracle Technology Network site to learn about supported connectors for Oracle Identity Manager.

Shared Directory

During the Oracle Identity Manager installation, the Oracle Identity Manager folder, Oracle (by default) is generated. This folder contains configuration information, for example, third-party libraries, keystores, scheduled tasks, adapter classes, and so on. In a WebSphere clustered environment, make sure that this folder is installed as a shared folder and is centrally located so that all cluster members can access the latest configuration information referenced by the application server.

Note: See "Installing Oracle Identity Manager Cluster using a Shared Directory" on page 9-20 for detailed instructions.

Using SSL

For any Oracle Identity Manager-supported integrations that are deployed using a Secure Socket Layer (SSL) connection between the target system (for example, Active Directory) and the clustered WebSphere application server, you must import the target system SSL certificate file into the trusted store for each cluster member machine.

For a standard WebSphere deployment, the target system SSL certificate must be imported to *<WEBSPHERE_HOME>*/etc/DummyServerTrustFile.jks. The default password for this file is WebAS. In a customized WebSphere deployment where a different trusted store is used, you must import the target system SSL certificate to that store.

Time Synchronization of Clustered Machines

Make sure that all cluster members (computers) have their system clocks synchronized. Oracle recommends that you do not run clustering on separate machines unless their system clocks are synchronized using some form of time-sync service (daemon) that runs frequently. The clocks must be within a second of each

other. See http://www.boulder.nist.gov/timefreq/service/its.htm for more information using the time-sync service.

Caution: Never start a non-clustered instance against the same set of tables that another instance is running against. You will experience serious data corruption and erratic behavior.

Post-Installation Configuration for Clustered Environments

After completing the steps in this chapter, be sure to perform the post-installation configuration tasks for your clustered environment by referring to "Post-Install Configuration for Oracle Identity Manager and WebSphere" on page 7-1 to complete the cluster deployment.

10

Installing and Configuring the Oracle Identity Manager Design Console

This chapter 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 includes the following topics:

Requirements

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

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

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

- The Design Console must be installed on the same machine as the WebSphere Client Application.
- Make sure the WebSphere Application Client is configured with the appropriate server certificate.

  See "Setting Environment Variables" on page 3-4 for more information.

Installing the Design Console

The following procedure describes how to install the Design Console.

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

To install the Design Console on a Windows host:

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

   The Welcome page appears.
5. On the Welcome page, click **Next**.
6. On the Target directory screen, complete one of the following sub-steps:
   a. The default directory for the Design Console is C:\oracle. To install the Design Console into this directory, click **Next**.
   b. To install the Design Console into another directory, enter the path in the Directory field, then click **Next**.

      or

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

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

   The Application Client Location page appears.
8. Specify the JRE to use with the Design Console, choosing between the JRE bundled with Oracle Identity Manager, or point to an existing and compatible JRE on the system.

   Click Next.
9. On the Application Server configuration page, enter the information appropriate for the application server hosting your Oracle Identity Manager server:
   a. Enter the host name or IP address in the upper text box.

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

Note: The host name is case-sensitive.

c. Click **Next**.

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

    Follow these instructions and then click **OK**.
14. Click **Finish** to complete the installation process.

Removing the Design Console Installation

To remove the Design Console installation, 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-install Requirements for the Design Console

To run the Design Console, three jar files must be copied from the WebSphere application server installation to your Design Console installation. Two jar files can be copied directly. One of the jar files must be extracted from the Oracle Identity Manager ear file.

To set up the jar files:

1. Copy the files sas.jar and naming.jar from the following directory:

   <*WEBSPHERE_HOME*>\lib

   to the following directory:

<*XL_DC_HOME*>\xlclient\ext

2. Extract the xlDataObjectBeans.jar file from the Oracle Identity Manager ear file.
3. Copy xlDataObjectBeans.jar into the following directory:

   <*XL_DC_HOME*>\xlclient\lib

   Click **OK** to replace the old xlDataObjectBeans.jar file.

Extracting xlDataObjectBeans.jar

To obtain the EAR file, export it from the WebSphere server using the WebSphere administrative console. You must also extract the xlDataObjectBeans.jar file from the EAR file so you can copy the JAR file to the Oracle Identity Manager Design Console's lib directory.

To extract the xlDataObjectBeans.jar file:

1. Launch a browser, then connect to the WebSphere administrative console using the following URL:

   http://localhost:9090/admin

2. Enter **xelsysadm** as the user name and password.
3. Click **Applications**, then select **Enterprise Applications**.
4. Select the **Xellerate** application check box.
5. Click **Export**.
6. Save the EAR file.
7. Extract the xlDataObjectBeans.jar file. (Make sure to extract xlDataObjectBeans.jar and *NOT* xlDataObjects.jar.)

Configuring the WebSphere AppClient in a Non-Clustered Environment

The certificate for the application server must be installed in the trusted store for the WebSphere AppClient. This required step establishes a trust relationship between the WebSphere server and client. Use the keytool included with WebSphere to perform this task.

> **Note:** If you use the default WebSphere certificate, this task is not necessary, as the certificate is already present in the keystore of the client.

To enable trust between the server and client:

1. Move to the <*WEBSPHERE_HOME*>\etc directory using the following command:

   ```
   cd <WEBSPHERE_HOME>\etc
   ```

2. Export the server certificate using the following commands:

   ```
   <WEBSPHERE_HOME>\java\jre\bin\keytool.exe -export
   -alias server -keystore DummyServerKeyFile.jks
   -storepass WebAS -file servercert
   ```

3. Copy the exported server certificate to the client host machine.

4. Import the server certificate into the trusted store for the client using the following commands, or similar commands to fit the specifics of your system. <*WEBSPHERE_CLIENT_HOME*> is the home directory for the WebSphere client, typically this is \WebSphere\AppClient\.

   a. Move to the <*WEBSPHERE_CLIENT_HOME*>\etc directory using the following command:

   ```
   cd <WEBSPHERE_CLIENT_HOME>\etc
   ```

   b. Import the server certificate using the following:

   ```
   <WEBSPHERE_CLIENT_HOME>\java\jre\bin\keytool.exe -import
   -alias servertrust -trustcacerts -keystore
   DummyClientTrustFile.jks -storepass WebAS -file
   servercert
   ```

Configuring the Design Console in a WebSphere Cluster

If you are running Oracle Identity Manager in a WebSphere cluster, you must configure the Design Console. During deployment you update the JNDI references for each of the Nodes. You must also update the JNDI references for the Design Console.

To specify the JNDI URL for the Design Console:

1. On the computer that hosts the Design Console, open the <*XL_DC_HOME*>/xlclient/Config/xlconfig.xml file.
2. In the <Discovery> section, locate the java.naming.provider.url property.
3. Set this property to the JNDI URL.

   See "Updating the JNDI References" on page 9-17 for instructions on how to obtain this value. For example, you could set the property to the following:

   ```
   <java.naming.provider.url>corbaloc:iiop:XL_NODE1_HOST:
   9812,:XL_NODE2_HOST:9813</java.naming.provider.url>
   ```

4. Save your changes.
5. Start or restart the Design Console.

Configuring WebSphere Client Communication with the Node Manager in Clusters

The certificate of the Node Manager must be installed in the trusted store of the WebSphere Client. This step is necessary to establish a trust relationship between the Node Manager server and WebSphere Application Client. Use the keytool included with WebSphere to perform this task.

To enable trust between the Node Manager and client:

1. Export the Node Manager certificate using the following commands. <*NODE_MANAGER_HOME*> is the home directory for WebSphere Network Deployment Manager.

   a. Move to the <*NODE_MANAGER_HOME*>\etc directory using the following:

   ```
   cd <NODE_MANAGER_HOME>\etc
   ```

   b. Export the server certificate using the following commands and command-line arguments:

   ```
   <NODE_MANAGER_HOME>\java\jre\bin\keytool.exe -export
   ```

```
-alias server -keystore DummyServerKeyFile.jks
-storepass WebAS -file servercert
```

2. Copy the exported server certificate to the client host machine.
3. Import the Node Manager certificate into the client's trusted store using the following commands. <*WEBSPHERE_CLIENT_HOME*> is the home directory for the WebSphere Client, typically this is \WebSphere\AppClient\.
   a. Move to the <WEBSPHERE_CLIENT_HOME>\etc directory using the following command:

      ```
      cd <WEBSPHERE_CLIENT_HOME>\etc
      ```

   b. Import the Node Manager certificate into the client's trusted store

      ```
      <WEBSPHERE_CLIENT_HOME>\java\jre\bin\keytool.exe -import
      -alias servertrust -trustcacerts -keystore DummyClientTrustFile.jks
      -storepass WebAS -file
      servercert
      ```

Starting the Design Console

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

11

Installing and Configuring Oracle Identity Manager Remote Manager

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

Installing the Remote Manager for Windows

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

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

To install the Remote Manager on a Windows host:

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

or

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

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

---

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

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

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

   a. Enter the Service Name.

   b. Enter the Remote Manager binding port.

   c. Enter the Remote Manager SSL port.

   d. Click **Next**.

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

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

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

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

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

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

Note: You must configure the Remote Manager before you can start it. See Configuring the Remote Manager on page 11-4 for more information.

Installing the Remote Manager for UNIX or Linux

To install the Remote Manager on UNIX or Linux:

1. Before installing the Remote Manager you must set the JAVA_Home variable to the appropriate JDK.

   On Solaris or Linux, set JAVA_HOME to Sun JDK 1.4.2_08 or higher, for example 1.4.2_xx—but not versions 1.5 or higher.

   On AIX, set JAVA_HOME to the WebSphere JDK. For example, use the following commands on AIX:

   - `export JAVA_HOME=$<WEBSPHERE_HOME>/java`

- Add $JAVA_HOME/bin to the $PATH environment variable using the following command: export PATH=$JAVA_HOME/bin:$PATH

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

   Note: If the autostart routine is enabled for your machine, proceed to Step 5.

3. From the File Manager, access the root CD directory (or the installServer directory, if you are installing from a tar file).
4. Run the install_rm.sh file.

   The command-line installer starts.
5. Choose a language from the list by entering a number and then entering **0** to apply the language.

   The Welcome panel appears.
6. On the Welcome panel, enter **1** to move to the next panel.

   The Target directory panel appears.
7. 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.

8. Specify the JRE to use with Remote Manager:

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

   The Remote Manager Configuration panel appears.
9. On the Remote Manager Configuration panel, enter the Remote Manager configuration information.

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

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

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

   d. Enter 1 to move to the next panel.

   The Remote Manager installation summary panel appears.

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

    Oracle Identity Manager installs and the Post Install Summary panel appears.
11. Enter **3** to finish the Remote Manager installation.

> **Note:** You must configure the Remote Manager before you can start it. See "Configuring the Remote Manager" on page 11-4 for more information.

Configuring the Remote Manager

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

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

Trusting the Remote Manager Certificate

To configure the Remote Manager:

1. Copy the Remote Manager certificate to the server computer.

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

   > **Note:** The server certificate located 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 value instead of 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 property <RMIOverSSL> and set it to true.

   For example:

   <RMIOverSSL>true</RMIOverSSL>

7. Locate the <KeyManagerFactory> property.

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

   <KeyManagerFactory>IBMX509</KeyManagerFactory>

   or

   <KeyManagerFactory>SUNX509</KeyManagerFactory>

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

Using Your Own Certificate

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

On the Remote Manager System:

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

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

2. Copy this new keystore to the <*XL_RM_HOME*>\xlremote\config\ directory.
3. Open <*XL_RM_HOME*>\xlremote\config\xlconfig.xml using a text editor.
4. Locate the <RMSecurity> tag and change the value in the <Location> and <Password> tags as follows:

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

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

   - For all other JREs, change the values to:

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

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

On the Oracle Identity Manager Server System:

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

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

2. Copy this new keystore to the <*XL_HOME*>\xellerate\config directory.

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

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

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

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

   - For all other JREs, change the values to:

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

5. Restart the 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 the <*XL_RM_HOME*>\xlremote\config\xlconfig.xml file.

2. Locate the <ClientAuth> property and set it to true, for example:

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

3. Locate the <RMIOverSSL> property and verify it is set to true, for example:

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

4. Locate the <KeyManagerFactory> property.

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

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

   or

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

5. Save the <XL_RM_HOME>\xlremote\config\xlconfig.xml file.
6. Copy the server certificate to the Remote Manager computer.

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

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

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

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

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

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

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

Starting Remote Manager

To start Remote Manager on Windows, execute the following script:

```
<XL_RM_HOME>\xlremote\remotemanager.bat
```

To start Remote Manager on UNIX or Linux, execute the following script:

```
<XL_RM_HOME>/xlremote/remotemanager.sh
```

Removing the Remote Manager Installation

To remove the Remote Manager installation:

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

12

Troubleshooting Your Oracle Identity Manager Installation

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

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

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

Task Scheduler fails in a Clustered Environment

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

Default Login Not Working

If the default login is not working for the Design Console or Administrative and User Console and you are using an SQL Server, make sure that the Distributed Transaction Coordinator is running (it should have been set as a default).

Index

A

C

D

E

G

H

W

X