Oracle® Identity Manager

Installation and Upgrade Guide for WebSphere

Release 9.0

B28762-01

May 2006

ORACLE®

Oracle Identity Manager Installation and Upgrade Guide for WebSphere Release 9.0

B28762-01

Primary Author: Don Biasotti

Contents

9 Starting Oracle Identity Manager

10 Deploying in a Clustered WebSphere Configuration

Preface

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

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

This document explains how to:

- install Oracle Identity Manager 9.0 on a WebSphere application server
- upgrade to Oracle Identity Manager 9.0.1 from Oracle Xellerate Identity Provisioning versions 8.5.2 or 8.5.3

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

Audience

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

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading

technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

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

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Best Practices Guide*

Documentation Updates

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

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

Conventions

The following text conventions are used in this document:

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

Convention	Meaning
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.
<*_HOME>	The directory where an application is installed. The directory where you install Oracle Identity Manager server is referred to as <XL_HOME>. Each Oracle Identity Manager component includes an abbreviation: <XL_DC_HOME> for the Design Console and <XL_RM_HOME> for the Remote Manager. Where needed to distinguish between Oracle Identity Manager versions, you may see 85x included in the directory convention. For example <XL_85x_HOME>, which refers to directory where Oracle Identity Manager version 8.5.2 or 8.5.3 is installed. Additional examples of this convention include the following: <WEBSPHERE_HOME>, <XL_HOME>, <XL_DC_HOME>, <XL_RM_HOME>, <XL_85x_HOME>, <XL_85x_DC_HOME>, and <XL_85x_RM_HOME>.

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

1

Introduction

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

Product Overview

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

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

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

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

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

Architecture

Oracle Identity Manager uses a three-tier architecture: the Presentation Tier, the Server Tier, and the Data and Enterprise Integration Tier.

The Presentation tier contains the following components:

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

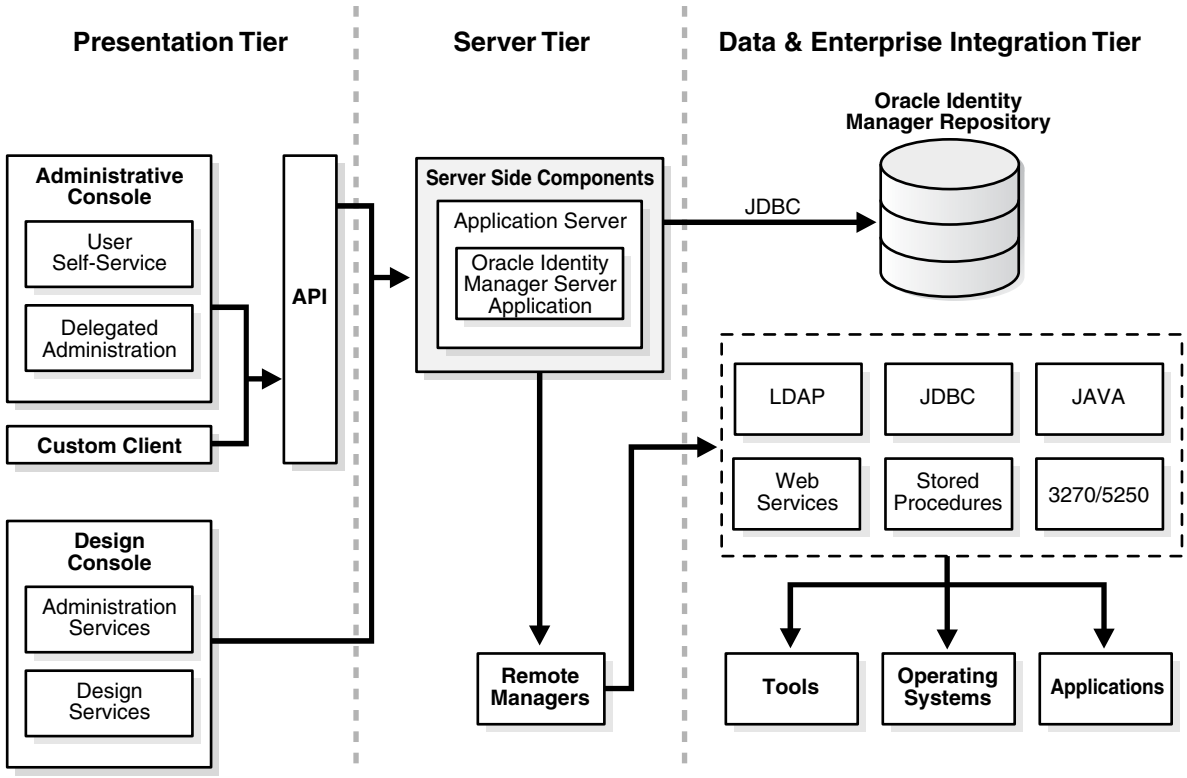
The Server tier contains the Oracle Identity Manager Server component, which serves as a bridge between the Presentation and Data and Enterprise Integration tiers. All requests between the clients and the database are processed through the Server tier.

The Data and Enterprise Integration tier contains the database server, which holds the Oracle Identity Manager data structure.

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



Software

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

2

Planning the Installation or Upgrade to 9.0.1

Oracle strongly recommends that you familiarize yourself with the components required for your deployment before starting to install Oracle Identity Manager. Oracle also recommends that you install and use the included Diagnostic Dashboard to ensure that your system is ready for installation. See "Using the Diagnostic Dashboard" on page 2-8 for more information.

Installation Components

Oracle Identity Manager consists of the following:

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

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

- A database server
- An application server
- An Oracle Identity Manager server (running in the application server)
- A JMS server (WebSphere-based clustered installations only)
- A Design Console
- An Administrative and User Console (running in a web-browser)

Hardware and Software Requirements

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

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

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

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

Supported 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
- RedHat Linux AS 4.1 or 4.2
- Solaris 9
- 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

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

Host Requirements for Oracle Identity Manager Components

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

Oracle Identity Manager Server Host Requirements

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

Table 2–1 Oracle Identity Manager Server Host Requirements

Server Platform	Item	Requirement
Windows	Processor Type	Intel Xeon or Pentium IV
	Processor Speed	2.4 GHz or higher, 400 MHz FSB or higher
	Number of Processors	1 (or more, if needed)
	Memory: Use whichever is greater	■ 2 GB (or more, if needed) or ■ 2 GB for each Oracle Identity Manager Server instance
	Hard Disk Space	20 GB (initial size)
	Operating System	Microsoft Windows 2003 Server with SP1
Linux	Processor Type	Intel Xeon or Pentium IV
	Processor Speed	2.4 GHz or higher, 400 MHz FSB or higher
	Number of Processors	1 (or more, if needed)
	Memory: Use whichever is greater	■ 2 GB (or more, if needed) or ■ 2 GB for each Oracle Identity Manager Server instance
	Hard Disk Space	20 GB (initial size)
	Operating System	RedHat Linux AS 4.1 or 4.2
Solaris	Sun Fire 210 Server	
	Number of Processors	1 (or more, if needed)
	Memory: Use whichever is greater	■ 2 GB (or more, if needed) or ■ 2 GB for each Oracle Identity Manager Server instance
	Hard Disk Space	20 GB (initial size)
	Operating System	Solaris 9
AIX	Processor Type	PowerPC
	Number of Processors	1 (or more, if needed)
	Memory: Use whichever is greater:	■ 2 GB (or more, if needed) or ■ 2 GB for each Oracle Identity Manager Server instance
	Hard Disk Space	20 GB (initial size)
	Operating System	AIX 5L 5.3

Database Server Host Requirements

Table 2-2 provides sample database host requirements for selective supported operating systems and should be considered only as guidelines. Consult your SQL Server or Oracle database documentation for the specific database host requirements.

Table 2–2 Sample Database Server Host Requirements

Database Server Platform	Item	Requirement
Windows	Processor Type	Intel Xeon
	Processor Speed	2.4 GHz or higher, 400 MHz FSB or higher
	Number of Processors	2 (or more, if needed)
	Memory	2 GB for each CPU (or more, if needed)
	Hard Disk Space	40 GB (initial size)
	Operating System	Microsoft Windows 2000 and 2003 Server
Linux	Processor Type	Intel Xeon
	Processor Speed	2.4 GHz or higher, 400 MHz FSB or higher
	Number of Processors	2 (or more, if needed)
	Memory	2 GB for each CPU (or more, if needed)
	Hard Disk Space	20 GB (initial size)
	Number of Hard Disks	1 Disk (or more, as data grows and if needed)
	Operating System	RedHat Linux AS 4.1 or 4.2
Solaris	Sun Fire 250 Server	
	Number of Processors	2 (or more, if needed)
	Memory	2 GB for each CPU (or more, if needed)
	Hard Disk Space	40 GB (initial size)
	Number of Hard Disks	1 Disk (or more, as data grows and if needed)
	Operating System	Solaris 9
AIX	Processor Type	PowerPC
	Number of Processors	2 (or more, if needed)
	Memory	2 GB for each CPU (or more, if needed)
	Hard Disk Space	40 GB (initial size)
	Operating System	AIX 5L 5.3

Design Console Host Requirements

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

Table 2–3 Design Console Host Requirements

Design Console Platform	Item	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 host requirements for the JMS Server:

Table 2–4 JMS Server Host Requirements

JMS Sever Platform	Item	Requirement
Windows	Processor Type	Intel Pentium IV
	Processor Speed	2.4 GHz or higher
	Number of Processors	1 (or more, if needed)
	Memory	512 MB (or more, if needed)
	Hard Disk Space	10 - 20 GB (or more, if needed)
	Software	IBM WebSphere Application Server
	Operating System	Microsoft Windows 2003 Server with SP1
Linux	Processor Type	Intel Pentium IV
	Processor Speed	2.4 GHz or higher
	Number of Processors	1 (or more, if needed)
	Memory	512 MB (or more, if needed)
	Hard Disk Space	10 - 20 GB (or more, if needed)
	Software	IBM WebSphere Application Server
	Operating System	RedHat Linux AS 4.1 or 4.2
Solaris	Sun Fire V100 Server	
	Number of Processors	1 (or more, if needed)
	Memory	512 MB (or more, if needed)
	Hard Disk Space	10 - 20 GB (or more, if needed)
	Software	IBM WebSphere Application Server
	Operating System	Solaris 9

Table 2–4 (Cont.) JMS Server Host Requirements

JMS Sever Platform	Item	Requirement
AIX	Processor Type	PowerPC
	Number of Processors	1 (or more, if needed)
	Memory	512 MB (or more, if needed)
	Hard Disk Space	10 - 20 GB (or more, if needed)
	Software	IBM WebSphere Application Server
	Operating System	AIX 5L 5.3

Remote Manager Host Requirements

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

Table 2–5 Remote Manager Host Requirements

Remote Manager Platform	Item	Requirement
Windows	Processor Type	Intel Pentium IV
	Processor Speed	1.4 GHz or higher
	Number of Processors	1
	Memory	512 MB
	Hard Disk Space	1 GB
	Operating System	Microsoft Windows 2000 or 2003 Server
Linux	Processor Type	Intel Pentium IV
	Processor Speed	1.4 GHz or higher
	Number of Processors	1
	Memory	512 GB
	Hard Disk Space	1 GB
	Operating System	RedHat Linux AS 4.1 or 4.2
Solaris	Sun Fire 210 Server	
	Number of Processors	1 (or more, if needed)
	Memory: Use whichever is greater	■ 2 GB (or more, if needed) ■ 2 GB for each Oracle Identity Manager Server instance
	Hard Disk Space	20 GB (initial size)
	Operating System	Solaris 9 or 10
AIX	Processor Type	PowerPC
	Number of Processors	1
	Memory	512 MB
	Hard Disk Space	1 GB

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

Remote Manager Platform	Item	Requirement
	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, including clustering
Oracle 10g Release 2	10.2.0.1.0
Oracle9i	9.2.0.7
SQL Server	2000, with SP3a
Microsoft Windows Server	2003 Enterprise Edition SP1
RedHat Linux	AS 4.1 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

Before You Start

Before installing Oracle Identity Manager, you should read "Hardware and Software Requirements" on page 2-1 and "Installation Worksheet" on page 2-8 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

Check Box	Item	Default	User Selection
	The base directory for installing Oracle Identity Manager.	Windows: C:\Oracle UNIX: /opt/oracle	
	The name or IP address of the machine where the Oracle Identity Manager database is installed.	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*	
	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**: /opt/WebSphere/AppServer/java	
	The WebSphere install directory	**Windows**: C:\Program Files\WebSphere\AppServer **UNIX**: /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 Java Virtual Machine (JVM)
- A supported Database
- Database Encryption Key Generation
- For WebSphere clusters only, an embedded JMS server

3

Installation Overview

Note: f you are using a clustered WebSphere environment, follow the instructions in the chapter

To install and configure WebSphere-based Oracle Identity Manager:

1. Install the WebSphere Application Server—see"Installing the WebSphere Application Server" on page 4-1 for more information.
2. Install WebSphere Application Client—see "Installing the WebSphere Application Client" on page 4-2 for more information.
3. Enable SOAP Communication to WebSphere—see "Enabling SOAP Communication with WebSphere" on page 4-2 for more information.
4. Upgrade WebSphere server and client software—see "Upgrading the WebSphere Server and Client" on page 4-3 for more information.
5. Prepare the environment—see "Setting Environment Variables" on page 4-3 for more information.
6. Increase the memory setting for the Java Virtual Machine—see "Setting the Memory Size" on page 4-3 for more information.
7. (Optional) Set up and use the Diagnostic Dashboard—see "Using the Diagnostic Dashboard" on page 2-8 for more information.
8. Install and setup your database:

   Oracle

   a. Install Oracle—see "Installing Oracle" on page 5-1for more information.
   b. Create Database—see "Creating an Oracle Database" on page 5-1 for more information.
   c. Prepare Oracle—see "Preparing the Oracle Database" on page 5-2 for more information.

   SQL Server

   a. Install SQL Server—see "Installing and Configuring SQL Server" on page 5-4 for more information.
   b. Register SQL Server—see "Registering SQL Server" on page 5-5 for more information.
   c. Create an SQL Server database—see "Creating an SQL Server Database" on page 5-5 for more information.

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

9. Install Oracle Identity Manager software:

Windows

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

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

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

Solaris or Linux

a. Install the server—see "Installing Oracle Identity Manager Server on UNIX" on page 7-1 for more information.

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

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

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

12. Change the initial state of the server—see "Creating the Initial State of the JMS Server" on page 8-4 for more information.

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

14. Configure the Design Console—see "Post-install Requirements for the Design Console" on page 11-3 for more information.

15. If you installed WebSphere using a nondefault port, configure settings for that port—see "Configuring WebSphere on Nondefault Ports" on page 8-4 for more information.

16. If you installed WebSphere using a nondefault server name, configure host information—"Configuring WebSphere on a Nondefault Server" on page 8-5

17. Enable access to the dead letter queue—see "Enabling xelsysadm Access to the Dead Letter Queue" on page 8-6 for more information.

18. Start Oracle Identity Manager:

Windows

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

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

c. Access the Administrative and User Console—see "Accessing the Administrative and User Console" on page 9-1 for more information.

Solaris or Linux

a. Start the server—see "Using Diagnostic Dashboard to Verify Installation" on page 9-2 for more information.

b. Access the Administrative and User Console—see "Accessing the Administrative and User Console" on page 9-1 for more information.

4

Installing and Configuring WebSphere for Oracle Identity Manager

This chapter explains how to set up WebSphere before and after installing Oracle Identity Manager. You must perform the following pre- and post-installation tasks:

> **Note:** Refer to "Deploying in a Clustered WebSphere Configuration" on page 10-1 if you are using WebSphere in an application server cluster.

1. Install the WebSphere Application Server—see "Installing the WebSphere Application Server" on page 4-1 for more information.
2. Install WebSphere Application Client—see "Installing the WebSphere Application Client" on page 4-2 for more information.
3. Enable SOAP Communication to WebSphere—see "Enabling SOAP Communication with WebSphere" on page 4-2 for more information.
4. Upgrade WebSphere server and client software—see "Upgrading the WebSphere Server and Client" on page 4-3 for more information.
5. Prepare the environment—see "Setting Environment Variables" on page 4-3 for more information.
6. Increase the memory setting for the Java Virtual Machine—see "Setting the Memory Size" on page 4-3 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 4-4 for more information.
8. Install Oracle Identity Manager—see "Installing Oracle Identity Manager with WebSphere" on page 4-4 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, heed the following points:

- Make sure that the path you specify for the application server location ends with **AppServer** (For example on Windows, a valid path might be: **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
- The default WebSphere installation uses the application server name **server1**. However, you can use any server name for your Oracle Identity Manager installation. See "Configuring WebSphere on a Nondefault Server" on page 8-5 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, setup message queues, and perform other operations).

1. To enable SOAP, edit the following properties in the file **soap.client.props**, which resides in the directory **<WEBSPHERE_HOME>\AppServer\properties**. The lines you edit should look like this:

```
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 get 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 get 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 10-19 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:

- Be sure the JAVA_HOME system variable is set to the appropriate 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:

```
set 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.

1. Connect to the WebSphere administrative console using the following URL: http://<WebSphere Host>:<WebSphere Admin Port>/admin
2. Select **Servers>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 steps 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:

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

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

2. Click **Servers** on the left pane.
3. Click **Application Servers** under **Servers**.
4. Click the **server instance** (server1, default) on the right pane.
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 startServer.bat script located in the <WEBSPHERE_HOME>\AppServer\bin\ directory. For example, run:

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

To start WebSphere on UNIX, use the startServer.sh script located in the <WEBSPHERE_HOME>/AppServer/bin/ directory. For example, run:

<WEBSPHERE_HOME>/AppServer/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 6-1 or "Installing Oracle Identity Manager Server on UNIX" on page 7-1 for more information.

5

Database Setup

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

- Setting Up the Oracle Database—see "Setting Up the Oracle Database" on page 5-1 for more information.
- Setting Up the SQL Server—see "Setting Up the SQL Server" for more information.

Setting Up the Oracle Database

To use Oracle for your database, you must:

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

Installing Oracle

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

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

Creating an Oracle Database

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

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

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

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

Preparing the Oracle Database

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

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

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

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

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

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

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

You must observe the following prerequisites when using these scripts:

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

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

UNIX/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:
   1. The location of your Oracle home **(ORACLE_HOME)**
   2. The name of your database **(ORACLE_SID)**
   3. The name of the Oracle Identity Manager **database user** to be created
   4. The **password** for the Oracle Identity Manager database user

5. The name of the **tablespace** to be created for storing Oracle Identity Manager data
6. The **directory in which to store the data file** for the Oracle Identity Manager tablespace
7. The name of the **data file** (you do not need to append the .dbf extension)
8. The name of the **temporary tablespace**.

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

Windows

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

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

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

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

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

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

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

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

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

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

Setting Up the SQL Server

To use SQL Server for your database, you must:

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

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

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

Installing and Configuring SQL Server

To install and configure SQL Server for Oracle Identity Manager, complete the following steps:

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

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

   Note: Perform steps 2–4 on the machine hosting the application server.

2. Download the SQL Server 2000 Driver for JDBC Service Pack 3 from `http://www.microsoft.com`
3. Install SQL Server 2000 Driver for JDBC Service Pack 3.

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

4. Locate the JDBC driver files (**mssqlserver.jar**, **msbase.jar**, and **msutil.jar**). Add their location to the system **CLASSPATH** environment variable. If the **CLASSPATH** environment variable does not exist, you must create it. The string you add should look something like the following:

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

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

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

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

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

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

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

Registering SQL Server

To register the SQL server, complete the following perform:

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

Creating an SQL Server Database

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

1. Start the Microsoft SQL Server Enterprise Manager application. From the Windows **Start Menu**, select **Programs**, select **Microsoft SQL Server**, then select **Enterprise Manager**.
2. In the left pane of the SQL Server Enterprise Manager application window, select **Console Root**, select **Microsoft SQL Servers**, select the **server group** to which your server belongs, then double-click the icon representing **your server**.
3. Right-click **Databases**, then select **New Database**.

4. In the Database Properties dialog, select the **General** tab, then type **XELL** in the text box labelled **Name**.

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

5. Select the **Data Files** tab, then, for the **Initial Size** and **Filegroup** columns in the Database files matrix, enter the information from the corresponding columns in Table 3-1.

   Note: Table 3-1 lists initial sizes for a production environment. For non-production installations, you can use the default initial sizes provided for the filegroups.

Table 5–1 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 3-1. You can vary the File Name and Location strings to match the database name and the location of your SQL Server installation.

   1. Select **Automatically Grow File**.
   2. Select **By Percent**, then type **10** in the associated text box.
   3. Select **Unrestricted file growth**.

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

6. Select the **Transaction Log** tab, then change the initial size to 500MB. Leave all the other options on the tab at their default values.

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

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

Creating an SQL Server Database Account

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

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

1. Launch the Microsoft SQL Server Enterprise Manager application. From the Windows **Start Menu**, select **Programs**, select **Microsoft SQL Server**, then select **Enterprise Manager**.
2. In the left pane of the SQL Server Enterprise Manager application window, select **Console Root**, select **Microsoft SQL Servers**, select the **server group** to which your server belongs, then double-click the icon representing **your server**.
3. Select **Security**, right-click **Logins**, then select **New Login**.
4. In the SQL Server Login Properties dialog, select the **General** tab. In the **Name** field type **xladm** (or whatever account name you prefer).
5. Select **SQL Server Authentication**, then type the **password** associated with the account you specified in the Password text box.
6. In the Database combo box within the Defaults section, select **XELL** from the drop-down list. Leave the Language text box set to <default>.
7. Select the **Database Access** tab. In the upper panel, select the check box associated with **XELL**.
8. In the lower panel, select the check-boxes associated with all of the following:
   - public
   - db_owner
   - db_accessadmin
   - db_securityadmin
   - db_ddladmin
   - db_datareader
   - db_datawriter
9. Click **OK** to commit your changes. When prompted, confirm the password and click **OK**.
10. To check your database settings, right-click the icon representing your server, then select **Properties** from the shortcut menu.
11. On the SQL Server Properties page, select the **Security** tab, then verify that Authentication is set to **SQL Server and Windows**.
12. Click the **General** tab, then verify that the check boxes associated with **Autostart SQL Server** and **Autostart MSDTC** are selected. If **Autostart SQL Server Agent** is selected, do not change the existing setting, because that setting may be required by other applications. Click **OK** to close the **SQL Server Properties** page.

6

Installing Oracle Identity Manager Server on Windows

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

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

Oracle Identity Manager Components

Oracle Identity Manager for Windows includes the following components:

- Oracle Identity Manager Server—see "Installing the Oracle Identity Manager Server on Windows" on page 6-2 for more information.
- Oracle Identity Manager Design Console—see "Installing and Configuring Oracle Identity Manager Design Console" on page 11-1 for more information.
- Oracle Identity Manager Remote Manager—see "Installing the Remote Manager for Windows" on page 12-1 for more information.

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

Installing the Database Schema

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

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

Installing Documentation

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

Installing the Oracle Identity Manager Server on Windows

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

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

   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 backup your original Oracle Identity Manager home by renaming that directory.

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

6. After the Target directory screen appears, complete one of the following bulleted actions:
   - The default directory for the Oracle Identity Manager server is C:\Oracle. To install the Oracle Identity Manager server into this directory, click Next.

- To install the Oracle Identity Manager server into another directory, enter the path in the Directory field, then click Next.

or

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

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

---

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

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

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

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

Note: When setting the preceding items, refer to the configuration settings specified in "Setting Up the Oracle Database" on page 5-1 or "Setting Up the SQL Server" on page 5-3 to be sure you set consistent information.

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

- Select the appropriate database options:
  - If a database exists, and the connectivity is good, proceed to Step 9.
  - If no connectivity is detected, you are prompted to enter new information or to fix the connection. After you do that, click **Next**.

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

> **Note:** If you are deploying in a clustered environment, select **Yes**, enter the cluster name, and see "Deploying in a Clustered WebSphere Configuration" on page 10-1 for more information.

12. On the WebSphere Directory Information page, type the information appropriate for your application server and Java installation:
    a. Type the full path to **your WebSphere installation**. Make sure to include **AppServer** in this path. (For example: C:\Program Files\WebSphere \AppServer).

       or

       Navigate to the **location of your WebSphere installation**.

    b. Type 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>\AppServer\java.

       or

       Navigate to the **location of your JDK installation**.

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

    WebSphere Server Information for a non-Clustered Installation

    a. Type the **host name** or I**P address** for the machine on which your application server is running. You can enter **localhost** for a local installation.

    b. Type the **cell name**, which is the name of the folder under **<WEBSPHERE_ HOME>\AppServer\config\cells**.)

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

    d. For the WebSphere **server name**, type your Oracle Identity Manager server name. If you are using a server other than server1, see "Configuring WebSphere on a Nondefault Server" on page 8-5 for more information.

    e. Click **Next**.

14. Backup your application server when the Application Server Configuration Backup screen appears, then click **Next** to initiate server installation.
15. On the Summary screen, click **Install** to initiate the server software installation.
16. 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**.
17. 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 8-1 to continue with the installation process.

7

Installing Oracle Identity Manager Server on UNIX

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

Oracle Identity Manager Components

Oracle Identity Manager for UNIX includes the following components.

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

Installing the Database Schema

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

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

Installing Documentation

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

Installing Oracle Identity Manager on UNIX

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

- Choose from among list of options

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

- Enter information at a prompt

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

The installer contains logical sections (panels).

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

To install Oracle Identity Manager server for UNIX:

1. Before installing the Oracle Identity Manager server you must set the JAVA_Home variable to the appropriate JDK. On Solaris and Linux, set JAVA_Home to Sun JDK 1.4.2 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>/AppServer/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
   ```

5. The installer starts in console mode, and the product Welcome Message panel appears.
   a. Type **1** to display the next panel. The Oracle Identity Manager Application panel appears.
   b. Type **1** to display the next panel. The Application Selection panel appears.

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

6. Select the application to install:
   a. Type **1** for **Oracle Identity Manager**.
   b. Type **2** for the **Oracle Identity Manager with Audit and Compliance Module**.

   Type **0** when you are finished and then type **1** to move to the next section. The Target directory panel appears.
7. On the Target directory panel, complete one of the sub-steps that follow:

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

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

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

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

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

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

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

- Type **1** to move to the next panel.

The Database Information panel appears.

9. Enter your database information:
   a. Enter the database **host name** or **IP address**.
   b. Enter (or accept the default) **port number**.
   c. Enter the **SID** for the database name.
   d. Enter the database **user name** for the account that Oracle Identity Manager uses to connect to the database.
   e. Enter the **password** for the database account that Oracle Identity Manager uses to connect to the database.
   f. Type **1** to move to the next panel.

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

      The Application Server Selection panel appears.
11. Specify your application server type.
    - Type **2** for **IBM WebSphere**.
    - Type **0** when you are finished.
    - Type **1** to move to the next panel.

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

    The Application Server Information panel appears.

    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 10-1 for information on installing in a clustered WebSphere environment.
13. Enter the application server information at the prompts:

a. Specify the path to the application server or press **Enter** to accept the default.

b. Specify the path to the application server's JDK directory or press **Enter** to accept the default.

c. Type **1** to move to the next section.

14. 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. Type **1** to move to the next section.

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

16. On the Installation summary information page, verify the information displayed, then do one of the following:

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

17. After Oracle Identity Manager installs, the Completed panel appears. Type 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 8-1 to continue the installation process.

8

Post-Install Configuration for Oracle Identity Manager and WebSphere

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

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

General Post-Installation Tasks

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

Changing Keystore Passwords (optional)

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

To change the keystore password:

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

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

where <JAVA_HOME> is the location of the Java directory associated with your application server, <new_password> is the new password for the keystore, the keystore option is the keystore whose password you are changing the (.xlkeystore for the Oracle Identity Manager server, or .xldatabasekey for the database), and the storetype option is JKS for .xlkeystore and JCEKS for .xldatabasekey.

4. Launch a plain-text editor, then open the file **xlconfig.xml**, which is located in the directory **<XL_HOME>\xellerate\config**.

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

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

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

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

     to the following:

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

6. Restart your application server.

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

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

Setting Log Levels (optional)

Oracle Identity Manager uses log4j for logging. For WebSphere-based Oracle Identity Manager installations, logging is configured in the logging properties file, <XL_HOME>/xellerate/config/log.properties.

By default, Oracle Identity Manager is configured to output at the Warning level. You can change the log level universally for all components or for an individual component. For normal operation of Oracle Identity Manager, this post-installation configuration step is not required.

Oracle Identity Manager Component Logging

The components are listed in the <XL_HOME>\xellerate\config\log.properties file in the **XELLERATE** section. They are:

```
log4j.logger.XELLERATE.ACCOUNTMANAGEMENT
log4j.logger.XELLERATE.SERVER
log4j.logger.XELLERATE.RESOURCEMANAGEMENT
log4j.logger.XELLERATE.REQUESTS
log4j.logger.XELLERATE.WORKFLOW
```

```
log4j.logger.XELLERATE.WEBAPP
log4j.logger.XELLERATE.SCHEDULER
log4j.logger.XELLERATE.SCHEDULER.Task
log4j.logger.XELLERATE.ADAPTERS
log4j.logger.XELLERATE.JAVACLIENT
log4j.logger.XELLERATE.POLICIES
log4j.logger.XELLERATE.RULES
log4j.logger.XELLERATE.DATABASE
log4j.logger.XELLERATE.APIS
log4j.logger.XELLERATE.OBJECTMANAGEMENT
log4j.logger.XELLERATE.JMS
log4j.logger.XELLERATE.REMOTEMANAGER
log4j.logger.XELLERATE.CACHEMANAGEMENT
log4j.logger.XELLERATE.ATTESTATION
log4j.logger.XELLERATE.AUDITOR
```

Setting Log Levels for WebSphere

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

Complete the following steps to set log levels:

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

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

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

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

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

2. Set the general value to the desired log level. The following is a list of the supported log levels, appearing in descending order of information logged (DEBUG logs the most information and FATAL logs the least information):

   - DEBUG
   - INFO
   - WARN
   - ERROR
   - FATAL

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

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

4. Save your changes.

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

Post-Installation Steps for WebSphere

If you are using WebSphere for your application server, after you install the Oracle Identity Manager software, perform the tasks in this section after stopping and restarting WebSphere.

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 a text editor (the file is located in <WEBSPHERE_HOME>/Appserver/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.

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 non-standard ports for a WebSphere configuration. Therefore, you must set the Virtual Host for non-standard 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.

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

Note: For this procedure, the name of the nondefault server is **xlServer**.

1. Open the server.xml file, which resides in the directory **<WEBSPHERE_HOME>\config\cells\<cellname>\nodes\<nodename>\servers\server1**.

   where <cellname> is the cell name.

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 **<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:

```
<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. Therefore, 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>Application Servers><Server_Name>>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.

Enabling SIngle Sign-On (SSO)

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

1. Stop the application server gracefully.

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

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

4. Edit the SSO configuration to be the following:

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

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

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

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

9

Starting Oracle Identity Manager

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

> **Note:** You must complete all relevant post-installation steps before starting Oracle Identity Manager. See the "Post-Install Configuration for Oracle Identity Manager and WebSphere" on page 8-1 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>) 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. The backup file is named xlconfig.xml.<x>, where x is the latest available number, for example xlconfig.xml.0, xlconfig.xml.1, and so on.

Starting Oracle Identity Manager

To start Oracle Identity Manager, perform the following steps:

1. Verify that your database is up and running
2. Start your application server

Accessing the Administrative and User Console

After starting your application server and Oracle Identity Manager, you can access the Administrative and User Console using the following steps:

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, login with your user name and password.

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

Using Diagnostic Dashboard to Verify Installation

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

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

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

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

10

Deploying in a Clustered WebSphere Configuration

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

> **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.

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 10–1 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.

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

Host Computer	Entities	Software	Description
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.

Setting Up a WebSphere Oracle Identity Manager Cluster Overview

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.

To set 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 10-4 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 10-5 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 10-7 for more information.
6. Create the XL_MODEL_SERVER on the XL_MODEL_NODE—see "Creating the Model Server" on page 10-8 for more information.
7. Create the XL_CLUSTER—see "Creating the Cluster" on page 10-9 for more information.
8. Prepare your database—see "Setting Up the Oracle Database" on page 5-1 or "Setting Up the SQL Server" on page 5-3 for more information.
9. Install Oracle Identity Manager on NDM_HOST—see "Installing Oracle Identity Manager on the Node Manager" on page 10-10 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 10-11 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 10-11 for more information.

12. To add a node, copy the <XL_HOME> directory from NDM_HOST to XL_NODE1_HOST—for steps 12-16, see "Adding Nodes and Servers to the Cluster" on page 10-13 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. Setup virtual host information for the server.
16. Repeat steps 14-15 for each server you want to add to the node.
17. Repeat steps 12-16 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 10-16 for more information.
19. Install the WebSphere Plug-in on IIS_HOST—see "Installing the WebSphere Plug-in for IIS" on page 10-6 for more information.
20. Setup the IIS server—see "Configuring the IIS Plug-in" on page 10-18 for more information.
21. Setup the Design Console—see "Post-install Requirements for the Design Console" on page 11-3 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 8-1 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 backup 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, use the command:

   cd C:\Program Files\WebSphere\AppServer\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 10-3 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 Node Name, enter XL_MANAGER_NODE.
   - 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.

   - Login 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 10-3 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 at 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 10-3 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—Installing WebSphere Application Server on page 10-6 for more information.
2. Upgrade the server—see "Upgrading WebSphere Server" on page 10-6 for more information.
3. Enable SOAP communications—see "Enabling SOAP Communication to WebSphere" on page 10-6 for more information.
4. Verify the installation—see "Verifying Installation" on page 10-7 for more information.
5. Create Backups—see "Creating Backups" on page 10-7 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, setup message queues, and other operations). To enable SOAP, edit the following properties in the file **soap.client.props**, which resides in the directory **<WEBSPHERE_HOME> \AppServer\properties**:.

```
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 (**Start**, select **IBM WebSphere**, select **Application Server v5.1**, 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 10-3 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:

   C:\WAS_Backups\Basic\<Node>Config

   where <Node> is the name of a node you have installed.
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>

   where <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. Login 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. Login 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** radio button 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 10-3 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

   where <Node> is 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. Select **Oracle Identity Manager** or **Oracle Identity Manager with Audit and Compliance Module** and click **Next**.
3. Select the destination directory to install Oracle Identity Manager and click **OK**.
4. Click **Next**.
5. Click **Next**.
6. Select your database type and click **Next**.
7. Enter the database information and click **Next**.
8. Select the authentication and click **Next**.
9. Select **WebSphere Application Server** and click **Next**.
10. Select **Yes** for clustering.
11. Enter the cluster name and click **Next**.
12. 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**.
13. 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**.

14. Enter the name of the JMS node name (XL_JMS_NODE) and click **Next**.
15. 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.
16. 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. Login 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 setup 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.

To setup 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, where < WEBSPHERE_HOME> is the home directory of WebSphere Application Server.

To setup 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, where <WEBSPHERE_HOME> is the home directory of WebSphere.

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, use the command:

   cd “C:\Program Files\WebSphere\AppServer\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. Login 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 10-16 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 to the Oracle Identity Manager setup directory. For example, use the command:

   cd C:\Oracle\xellerate\setup

3. Run the **xlAddNode.bat** 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.

4. Create one or more servers on each node. See "Creating a Server" on page 10-14 for more information.

5. Set up virtual host information for each server. See "Setting up the Server Virtual Host Information" on page 10-15 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. Login 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** radio button.
   - From the drop-down 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. Login 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 10-13 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 10-19 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, the servers in the XL_CLUSTER must be restarted. 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. Login 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 10-15 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 **Control Panel > 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

To configure the IIS plug-in, export the configuration from the Node Manager and install it by completing the following steps:

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. Login 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:

   <WEBSPHERE_HOME>\WebSphere\DeploymentManager\config\cells\

   plugin-cfg.xml
7. Make a copy of the IIS server's WebSphere plug-in configuration file. (The default location is C:\apps\IBM\WebSphere\AppServer\config\cells\plugin-cfg.xml).
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 steps to install Oracle Identity Manager on a WebSphere clustered environment using a shared directory. You must perform the steps in the following order:

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.

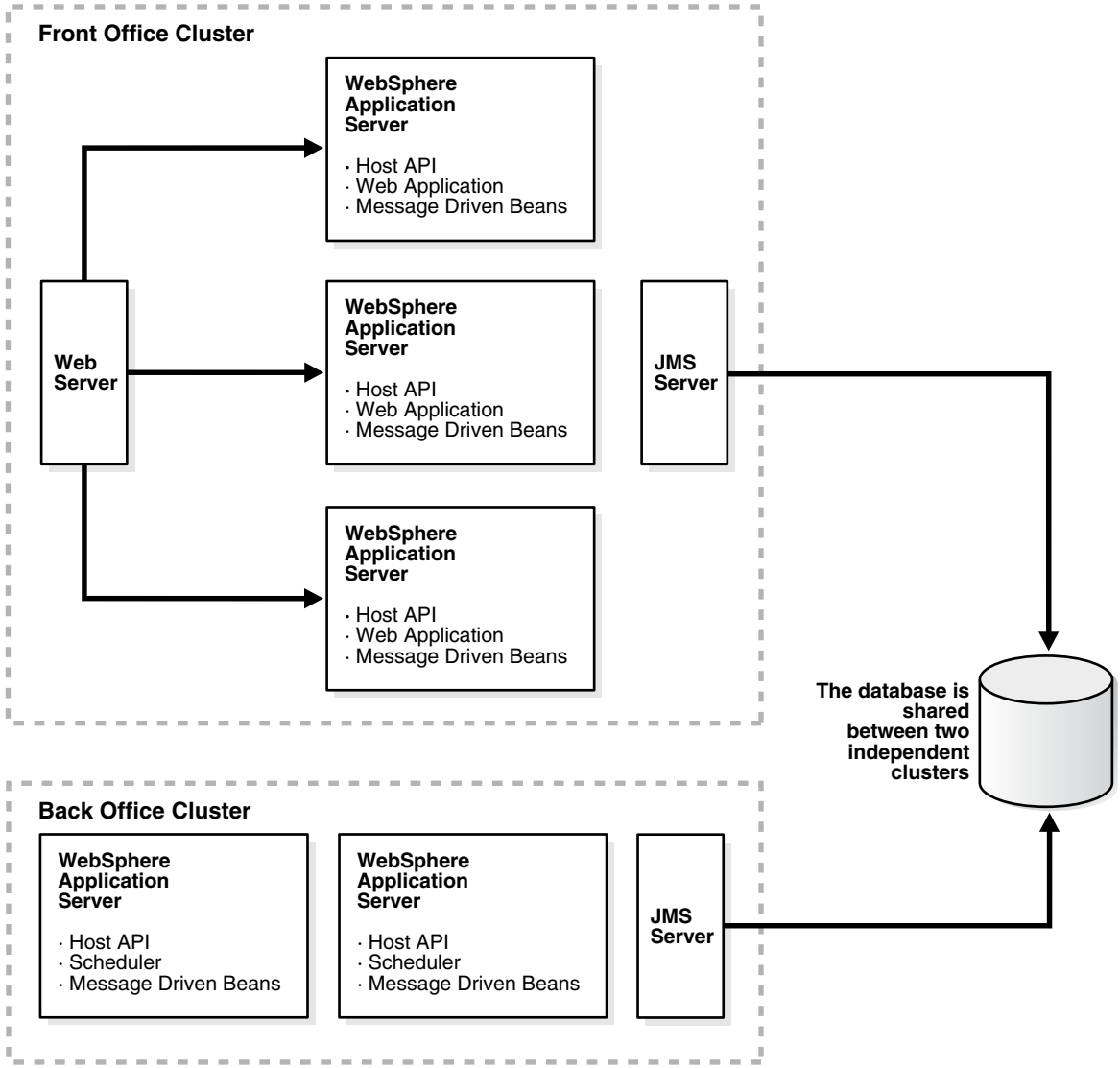
- In theory, it is possible to install a Scheduler a single machine. However when a schedule task executes, it calls the APIs. For the reconciliation tasks, they call APIs as well as submit messages. Hence, true processing of scheduled tasks occurs in the APIs and MDBs.

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 10–1 shows two independent clustered environments: Front Office and Back Office:

Figure 10–1 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

- 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.

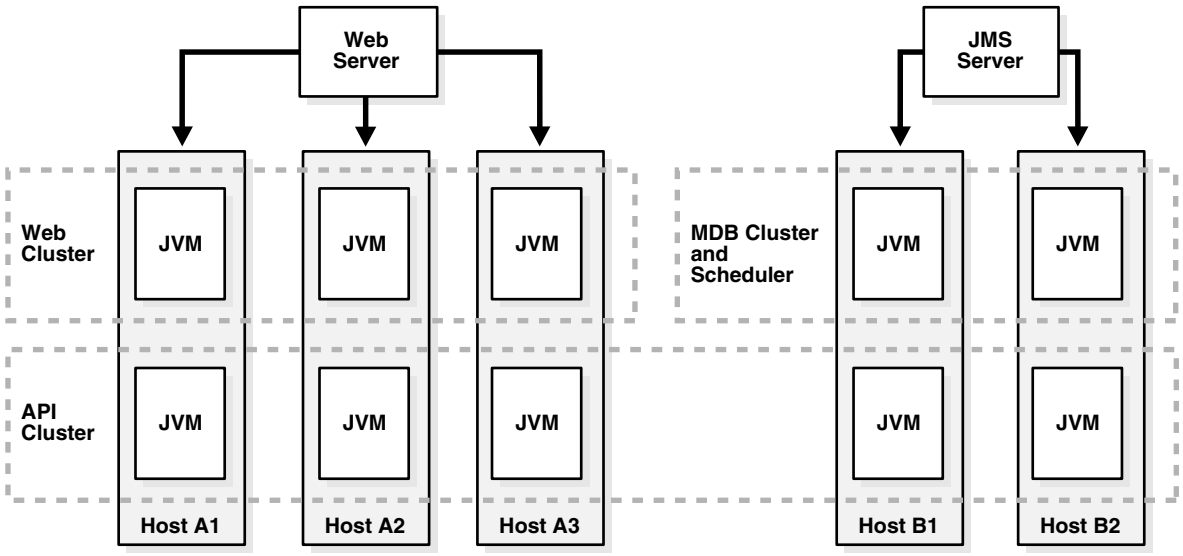
- Install Oracle Identity Manager in the Back Office cluster by following the instructions in this guide. For the Back Office you must use the appropriate steps (clustered or non-clustered) based on how you configure your environment.
  - During the installation, do not select "Install Database" for 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 10–2 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 10–2 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 advantages inhere to 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 suffix the servers with **API**.

- 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

1. To add more machines to handle Front Office requests, add a new node then add servers in both the WebCluster and the API Cluster.
2. 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 (such as, third-party libraries, keystores, scheduled tasks, adapter classes, and so on.). Therefore, 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 10-19 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 (such as, 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 (machines) 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 8-1 to complete the cluster deployment.

11

Installing and Configuring Oracle Identity Manager Design Console

This section explains how to install the Oracle Identity Manager Design Console, which is a Java client. You have the option to install the Design Console on the same computer as your Oracle Identity Manager server or on a separate computer.

Requirements

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

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

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

- 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 4-3 for more information.

Installing the Design Console

To install the Design Console on a Windows host,

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

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

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

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

      or

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

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

6. On the Application Server page, select WebSphere, then click Next. The Application Client Location page appears.
7. Specify the JRE to use with the Design Console, choosing between the JRE bundled with Oracle Identity Manager, or point to an existing and compatible JRE on the system. Click Next.
8. On the Application Server configuration page, enter the information appropriate for the application server hosting your Oracle Identity Manager server:
   a. Type the **host name** or IP address in the upper text box.
   b. Type the **naming port** for the application server on which Oracle Identity Manager is deployed in the lower text box.

      Note: The host name is case-sensitive.

   c. Click **Next**.
9. On the Graphical Workflow Rendering Information page, enter the Application server configuration information:
   a. Enter the Oracle Identity Manager server host **IP address**. 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**.

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

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

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

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

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

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

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

Post-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.

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

   <WEBSPHERE_HOME>\AppServer\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**.)

Setting up the WebSphere AppClient for the WebSphere Server 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, complete the following steps:

1. Export the server certificate.

   For example, to export the server certificate, use the commands:

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

   where <WEBSPHERE_HOME> is the home directory for the WebSphere Application Server.

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

3. Import the server certificate into the trusted store for the client. For example, use the following commands, or similar commands to fit the specifics of your system:

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

   where *WS_CLIENT_HOME* is the home directory for the WebSphere client.

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 in a text editor the **xlconfig.xml** file, located in the **<XL_DC_HOME>/xlclient/config** directory.

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 10-16 for instructions on how to obtain this value. For example, set the property to:

   ```
   <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.

Setting up the WebSphere Client to Communicate with the Node Manager in Clustered Environments

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.

   For example, to export the server certificate, execute the following commands with command-line arguments:

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

   where <NODE_MANAGER_HOME> is the home directory for WebSphere Network Deployment Manager.
2. Copy the exported server certificate to the client host machine.
3. Import the Node Manager certificate into the client's trusted store.

   For example, to import the Node Manager certificate into the trusted store of the client, use the commands:

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

   where <WS_CLIENT_HOME> is the home directory for the WebSphere Client.

Starting the Design Console

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

12

Installing and Configuring Oracle Identity Manager Remote Manager

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

Installing the Remote Manager for Windows

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

1. Insert the Oracle Identity Manager Installation CD into your CD-ROM drive.
2. Launch Windows Explorer, then navigate to the installServer directory on the installation CD.
3. Double-click the setup_rm.exe file.
4. On the Welcome page, click **Next**.
5. On the Target directory page, complete one of the following sub-steps:

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

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

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

      or

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

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

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

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

   e. Click **Next**.
8. On the **Shortcut** page, select (or deselect) the check boxes for the shortcut options according to your preferences:
   a. Choose to create a shortcut for the Remote Manager on the **desktop**.
   b. Choose to create a shortcut for the Remote Manager on the **Start Menu**.
   c. Click **Next** when you are satisfied with the check box settings.
9. On the Summary page, review the configuration details, and then click **Install** to initiate installation.
10. 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 12-4 for more information.

Installing the Remote Manager for UNIX

To install the Remote Manager on UNIX (Linux, AIX, or Solaris):.

1. Before installing the Remote Manager you must set the JAVA_Home variable to the appropriate JDK. On Solaris and Linux, set JAVA_Home to Sun JDK 1.4.2 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 6.

3. From the File Manager, access the root CD directory (or the installServer directory, if you are installing from a tar file).
4. Double-click the **install_rm.sh** file.
5. The command-line installer starts, and the Welcome panel appears. Type **1**, to move to the next panel.

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

6. On the Target directory panel, enter the path to the directory where you want to install the Oracle Identity Manager Remote Manager. The default directory is /opt/oracle.
   - Type **1**, to move to the next panel.
   - If the directory does not exist, you are asked to create it. Type **y**, for yes.
7. On the Remote Manager Configuration panel, enter the Remote Manager configuration information.
   a. Enter the Service Name, or press **Enter** to accept the default.
   b. Enter the Remote Manager binding port, or press **Enter** to accept the default.
   c. Enter the Remote Manager SSL port, or press **Enter** to accept the default.
   d. Type **1** to select yes and enable RMI over SSL communication between the Remote Manager and the server.

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

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

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

Oracle Identity Manager installs and the Post Install Summary panel appears.

9. Type **3** to finish.

> **Note:** You must configure the Remote Manager before you can start it. See Configuring the Remote Manager on page 12-4 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
   ```

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

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

4. Type **Y** at the prompt to trust the certificate.

5. Launch a plain-text editor, then open the file **xlconfig.xml**, which resides in the directory **<XL_HOME>\xellerate\config**.
6. Locate the property <RMIOverSSL> and set it to true. For example:

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

   <KeyManagerFactory>IBMX509</KeyManagerFactory>

   or

   <KeyManagerFactory>SUNX509</KeyManagerFactory>
8. Save the file.
9. Restart your application server.

Using Your Own Certificate

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

On the Remote Manager 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
```

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

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

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

Starting Remote Manager

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

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

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

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

13

Upgrading to Oracle Identity Manager 9.0.1 from Versions 8.5.2 or 8.5.3

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

Upgrade Overview

Both Oracle Identity Manager and the Oracle Identity Manager Audit and Compliance module run on the WebSphere application server version 5.1.1.5. Upgrading from Oracle Xellerate Identity Provisioning version 8.5.2 or 8.5.3 (henceforth referred to collectively as version 8.5.x) to Oracle Identity Manager version 9.0.1, and upgrading from the Oracle Xellerate Audit and Compliance Manager 8.5.x to Oracle Identity Manager Audit and Compliance module 9.0.1 requires upgrading with the Oracle Identity Manager version 9.0.1 application.

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

1. Upgrade the database you used for Oracle Xellerate Identity Provisioning 8.5.x. Refer to "Upgrading Your Database" on page 13-2 for more information.
2. Prepare for the upgrade to Oracle Identity Manager 9.0.1 by performing the pre-upgrade configuration tasks. Refer to "Pre-Upgrade Configuration" on page 13-8 for more information.
3. Migrating any version 8.5.x custom code to your new Oracle Identity Manager 9.0.1 deployment. Refer to "Migrating Custom Code to 9.0.1" on page 13-14 for more information.
4. Upgrade your legacy Oracle Xellerate Identity Provisioning 8.5.x deployment to Oracle Identity Manager 9.0.1. Refer to "Migrating Custom Code to 9.0.1" on page 13-14 for more information.
5. Perform the post-upgrade configuration tasks. Refer to "Post-Upgrade Configuration" on page 13-16 for more information.
6. Update the Design Console xlDataObjectBeans.jar file. Refer to "Updating the Design Console xlDataObjectBeans.jar" on page 13-18 for more information.
7. Upgrade to the version 9.0.1 Diagnostic Dashboard. Refer to "Upgrading the Diagnostic Dashboard" on page 13-18 for more information.

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

The Oracle Identity Manager 9.0.1 upgrade package is contained in upg_852_853_to_901.zip. Extract the contents of this package to a temporary directory on the machine where your existing 8.5.x installation is located. Henceforth, this document refers to this temporary directory as <Patch>.

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

Note: his document only covers upgrading to Oracle Identity Manager 9.0.1 from an Oracle Xellerate Identity Provisioning 8.5.x installation deployed on WebSphere application server.

Upgrading Your Database

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

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

Upgrading an Existing Database Instance

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

1. Extract the contents of the Oracle Identity Manager 9.0.1 upgrade package (upg_852_853_to_901.zip) to a temporary directory on the machine that you plan to install Oracle Identity Manager 9.0.1. Henceforth, this document refers to this temporary directory as <Patch>.
2. Backup your existing database. As appropriate to your particular database, use the export/backup utilities provided with the Oracle database or SQL Server to perform a complete backup of your production database. Production database backup includes, but is not limited to, complete export or backup of the Oracle Xellerate Identity Provisioning 8.5.x database instance to ensure that no data is lost during the upgrade process. If the upgrade fails, this backup can be used to restore the database to its original state.
3. Verify your database configuration. Make sure that your existing database is properly configured. As appropriate for your database, consult the following documentation:

   Oracle

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

   SQL Server

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

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

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

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

   Oracle

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

   For Oracle on Unix/Linux:

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

   ```
   chmod 755 xl_db_upg_852_853_to_901.sh
   ```

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

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

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

   For Oracle on Windows:

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

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

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

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

   SQL Server

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

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

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

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

SQL Server

a. Launch a plain-text editor, then open:

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

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

c. Run the script:

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

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

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

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

Oracle

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

b. Run the

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

script.

SQL Server

a. Run the following script:

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

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

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

   Windows

   a. Run the

      <Patch>\Database\Utilities\LoadXML.bat

      bat file.

   UNIX

   a. Run the

      <Patch>\Database\Utilities\LoadXML.sh

      script.

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

Creating a New, Upgraded Database Instance

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

1. Backup your existing database. As appropriate to your particular database, use the **export/backup** utilities provided with the Oracle database or SQL Server to perform a complete backup of your production database. Production database backup includes, but is not limited to, complete export or backup of the Oracle Xellerate Identity Provisioning 8.5.x database instance to ensure that no data is lost during the upgrade process. If the upgrade fails, this backup can be used to restore the database to its original state.
2. Export the existing database data using the export/backup utilities for your Oracle or SQL Server database.
3. Create a new database. See "Setting Up the Oracle Database" on page 5-1 or "Setting Up the SQL Server" on page 5-3 for more information.

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

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

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

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

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

   Oracle

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

   For Oracle on Unix/Linux:

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

      chmod 755 xl_db_upg_852_853_to_901.sh

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

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

   c. Enter the appropriate information for the Oracle database when prompted by the

      xl_db_upg_852_853_to_901.sh

      script.

   For Oracle on Windows:

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

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

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

      xl_db_upg_852_853_to_901.bat <ORACLE_SID>

      <ORACLE_HOME> <ORACLE_XELL_USER>

      <ORACLE_XELL_USER_PWD> <PATCH>

   SQL Server

   a. Run the

      <Patch>\Database\SQLServer\Scripts\upg_852_853_to_901.bat

bat file.

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

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

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

SQL Server

a. Launch a plain-text editor, then open

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

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

c. Run the script

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

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

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

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

Oracle

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

b. Run the

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

script.

SQL Server

a. Run the script

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

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

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

   Windows

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

   UNIX

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

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

Pre-Upgrade Configuration

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

- Oracle Identity Manager Server
- Remote Manager
- Design Console

Pre-Upgrade Configuration for the Oracle Identity Manager Server

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

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

1. Backup the following directories.
   - <XL_85x_HOME>\xellerate\bin
   - <XL_85x_HOME>\xellerate\config
   - <XL_85x_HOME>\xellerate\DDTemplates
   - <XL_85x_HOME>\xellerate\ext
   - <XL_85x_HOME>\xellerate\lib
   - <XL_85x_HOME>\xellerate\setup
   - <XL_85x_HOME>\xellerate\webapp
   - <XL_85x_HOME>\documentation

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

Table 13–1 Oracle Identity Manager Server Pre-Upgrade Files to Copy

Copy From...	To
Patch\xellerate\config	<XL_HOME>\xellerate\config
Patch\xellerate\DD Templates	<XL_HOME>\xellerate\DD Templates
Patch\xellerate\ext	<XL_HOME>\xellerate\ext
Patch\xellerate\lib	<XL_HOME>\xellerate\lib
Patch\xellerate\bin	<XL_HOME>\xellerate\bin
Patch\xellerate\webapp	<XL_HOME>\xellerate\webapp
Patch\documentation	<XL_HOME>\documentation
Patch\xellerate\readme.htm	<XL_HOME>

3. Copy the following files from Patch\xellerate\setup to <XL_HOME>\xellerate\setup:
   - setup.xml
   - websphere-setup.xml
   - patch_websphere.cmd
   - patch_websphere.sh
4. Edit the <XL_HOME>\xellerate\setup\patch_websphere script as follows:

   Windows

   a. Open patch_weblogic.cmd and make the following changes:

      replace @java_home with the path to the Java installation directory

      replace @wasHome with the path to the WebSphere installation directory

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

   UNIX

   a. Open patch_weblogic.sh and make the following changes:

      replace @java_home with the path to directory containing the JDK

      replace @loc with the path to the Oracle Identity Manager server installation directory
5. Use a text editor to edit the PurgeCache script in the <XL_HOME>\xellerate\bin\ directory. For Windows, edit the PurgeCache.bat file. For UNIX, edit the PurgeCache.sh file.
   - Replace oscache-2.0.2-22Jan04.jar with oscache.jar in the definition of the CLASSPATH environment variable.
6. Modify the <XL_HOME>/xellerate/config/xlconfig.xml file. See "Upgrading the Server Configuration File" on page A-3 for more information.
7. Modify the <XL_HOME>/xellerate/config/FormMetaData.xml. See "Upgrading the Metadata File" on page A-5 for more information.

8. As of version 9.0.1, and for all future releases, the log.properties file replaces the log.conf file as the Oracle Identity Manager server configuration log file. Complete the following steps to migrate all the version 8.5.x logging settings:

   a. Copy any version 8.5.x custom logging-related settings that exist in the log.conf file, which resides in the backup directory **<XL_85x_HOME>/config/**, to the **log.properties** file, which resides in the directory **<XL_HOME>/xellerate/config/**.

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

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

   ```
   Logger.module.ADAPTERS=WARN
   ```

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

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

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

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

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

9. Edit the <XL_HOME>/xellerate/config/log.properties file. Locate log4j.logger.XELLERATE.CACHEMANAGEMENT and add the following lines after it:

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

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

   Uncomment these two lines as needed and set appropriate log levels to enable logging for attestation and auditing respectively.

10. Remove the following libraries from the <XL_HOME>\xellerate\ext directory:

    - classes12.zip
    - csv-1.0.jar
    - oscache-2.0.2-22Jan04.jar
    - sax.jar
    - dom.jar
    - jaxp-api.jar

11. Edit the <XL_HOME\xellerate\Profiles\websphere.profile file as follows according to your database:

    Oracle

    a. Locate the database.type property and add the following lines immediately after it:

    ```
    # Reporting data source
    ```

datasource.report=jdbc/xlXADS

b. Locate the datasource.database.driver.classpath. Change the value to the following:

<XL_HOME>/ext/ojdbc14.jar

SQL Server

a. Locate the database.type property and add the following lines immediately after it:

Reporting data source

datasource.report=jdbc/xlXADS

Pre-Upgrade Configuration for the Design Console

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

1. Backup the following files and directories:
   - <XL_85x_DC_HOME>\xlclient\XLDesktopClient.ear
   - <XL_85x_DC_HOME>\xlclient\CustomClient.zip
   - <XL_85x_DC_HOME>\xlclient\ext
   - <XL_85x_DC_HOME>\xlclient\lib
   - <XL_85x_DC_HOME>\documentation
2. Copy the following files form Patch\xlclient\ to the <XL_DC_HOME>\xlclient directory, overwriting existing files if necessary:
   - Patch\xlclient\ws.properties
   - Patch\xlclient\fvc.properties
   - Patch\xlclient\FVCutil_websphere.cmd
   - Patch\xlclient\XLDesktopClient.ear
   - Patch\xlclient\CustomClient.zip
   - Patch\xlclient\xlFvcUtil.ear
3. Copy the contents of the Patch\documentation directory to <XL_DC_HOME>\documentation, overwriting files if necessary.
4. Copy Patch\xellerate\readme.htm to <XL_DC_HOME>\xlclient\, overwriting the existing file if necessary.
5. Copy the contents of the Patch\xlclient\ext directory to <XL_DC_HOME>\xlclient\ext, overwriting files if necessary.
6. Copy the contents of the Patch\xlclient\lib directory to <XL_DC_HOME>\xlclient\lib, overwriting files if necessary.
7. Remove the following from the <XL_DC_HOME>\xlclient\ext\ directory:
   - classes12.zip
   - csv-1.0.jar
   - oscache-2.0.2-22Jan04.jar

8. Open the <XL_DC_HOME>\xlclient\FVCutil_websphere.cmd file. Set the following environment variable values:
   - WS_HOME to the path of the WebSphere application server client installation directory
   - XLCLIENT_HOME to the path of the Design Console installation directory
9. Open the <XL_DC_HOME>\xlclient\wsxlclient.cmd file. Add an argument called propfile in place of classpath. For example, replace the following lines:

```
"%WS_HOME%\bin\launchclient" XLDesktopClient.ear ^
-CCclasspath=%CLASSPATH% ^ -CCsecurityMgrPolicy=./config/xl.policy ^
-CCDXL.HomeDir=. ^ -CCDjava.security.auth.login.config=./config/authws.conf ^
-CCDwas.home="%WS_HOME%"
```

   with

```
"%WS_HOME%\bin\launchclient" XLDesktopClient.ear
-CCpropfile=<XL_DC_HOME>/ws.properties
-CCsecurityMgrPolicy=@loc/config/xl.policy
-CCDXL.HomeDir=@loc
-CCDjava.security.auth.login.config=@loc/config/authws.conf
-CCDwas.home="%WS_HOME%"
```

10. Open the <XL_DC_HOME>\xlclient\xlCustomClient.bat file. Replace java.naming.provider.url with log4j.configuration.

    Note: Skip this step if <XL_DC_HOME>\xlclient\xlCustomClient.bat is not present

    For example, replace the following:

```
java -Djava.security.manager -DXL.HomeDir=.
-DXL.ClientClassName=%CLIENT_CLASS%
-Djava.security.policy=config\xl.policy
-Djava.security.auth.login.config=config\auth.conf
-Djava.naming.provider.url=jnp://10.1.1.58:1099/
com.thortech.xl.client.CustomAPIClient
```

    with

```
java -Djava.security.manager -DXL.HomeDir=.
-DXL.ClientClassName=%CLIENT_CLASS%
-Djava.security.policy=config\xl.policy
-Djava.security.auth.login.config=config\auth.conf
-Dlog4j.configuration=config\log.properties
com.thortech.xl.client.CustomAPIClient
```

Pre-Upgrade Configuration for the Remote Manager

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

1. Backup the <XL_85x_RM_HOME>\xlremote\lib directory.
2. Copy the contents of the Patch\xlremote\lib directory to the <XL_RM_HOME>\xlremote\lib directory, overwriting files if necessary.

3. Open the <XL_RM_HOME>\xlremote\remotemanager.bat file. Locate the following entries:

   -cp %CLASSPATH%

   and

   -DXL.HomeDir

   > **Note:** The -cp %CLASSPATH% and -DXL.HomeDir entries are not on separate lines in the remotemanager.bat file, but are listed separately here for clarity.

   Add the following between these two lines:

   -Dlog4j.configuration=config\log.properties

   For example, replace

   ```
   <XL_RM_HOME>\xlremote\java\bin\java -cp %CLASSPATH%
   -DXL.HomeDir=<XL_RM_HOME>\xlremote
   com.thortech.xl.remotemanager.RemoteManager
   ```

   with

   ```
   <XL_RM_HOME>\xlremote\java\bin\java -cp %CLASSPATH%
   -Dlog4j.configuration=config\log.properties
   -DXL.HomeDir=<XL_RM_HOME>\xlremote
   ```

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

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

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

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

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

      Logger.module.RemoteManager=WARN

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

      # log4j.logger.XELLERATE.RemoteManager=DEBUG

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

      log4j.logger.XELLERATE.RemoteManager=WARN

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

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

Migrating Custom Code to 9.0.1

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

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

Recompiling Custom Code

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

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

Migrating Adapters

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

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

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

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

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

Migrating Scheduled Tasks

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

The recompiled custom scheduled tasks in **<XL_85x_HOME>/xellerate/ScheduleTask** need to be copied to the directory **<XL_HOME>/xellerate/ScheduleTask**.

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

Migrating Event Handlers

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

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

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

Migrating xlWebApp Customizations

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

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

Migrating Custom Clients

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

Performing the Upgrade to 9.0.1

Upgrading from an existing Oracle Xellerate Identity Provisioning 8.5.x deployment to Oracle Identity Manager 9.0.1 involves assembling a new enterprise application archive (EAR) file from the latest libraries, then redeploying the EAR. For clustered WebSphere deployments, this is done on the deployment manager. For a non-clustered WebSphere deployment, this is done on the application server.

Perform the following steps to upgrade an existing Oracle Xellerate Identity Provisioning 8.5.x deployment to Oracle Identity Manager 9.0.1 in a Websphere environment:

1. Enable SOAP communication to NDM/WAS for the patch utility. Edit the <NDM|WAS_INSTALL_DIR>\properties\soap.client.props to enable security with the following properties:

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

2. Make sure the WebSphere application server is running. For clustered environments, make sure WebSphere application server and Deployment Manager is running on all nodes in the cluster. Run the patch_websphere script:

   Windows

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

   UNIX

   - Run <XL_HOME>\xellerate\setup\patch_webpshere.sh

3. Perform the following steps after running the patch_websphere script:

   a. Stop the application server. If upgrading in a clustered environment, stop the application server on all nodes.

   b. Remove classes12.zip from the <WEBSPHERE_HOME>\AppServer\lib\ext directory. If upgrading in a clustered environment, remove classes12.zip from the <WEBSPHERE_HOME>\AppsServer\lib\ext directory on all nodes.

   c. For clustered environments, you must also copy the following files from Patch\xellerate\lib to <WEBSPHERE_HOME>\AppServer\lib\ext on all nodes:

      xlAuthentication.jar

      xlUtils.jar

      xlLogger.jar

      xlCrypto.jar

   d. For clustered environments, you must also copy the ojdbc14.jar file from Patch\xellerate\ext to <WEBSPHERE_HOME>\AppServer\lib\ext on all nodes.

   e. For clustered environments, you must also copy Patch\xellerate\ext\nexaweb-common.jar to <WEBSPHERE_HOME>\AppServer\lib on all nodes in the cluster.

   f. Start the application server.

Post-Upgrade Configuration

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

Post-Upgrade Configuration for the Audit and Compliance Module

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

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

Setting the User Profile Audit Level

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

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

Generating User Snapshots

If you installed the Oracle Identity Manager Audit and Compliance module (previously named Oracle Xellerate Auditing and Compliance Manager in 8.5.x), you must generate new snapshots for all existing users in the system when either of the following two situations occur:

- You upgrade from version 8.5.x to version 9.0.1 with the Oracle Xellerate Auditing and Compliance Manager module
- You elevate the audit level for Audit and Compliance module

To generate new snapshots, complete the following steps:

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

      ```
      set APP_SERVER=websphere
      ```

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

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

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

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

to the following:

set SQL_SERVER_DRIVER_DIR=<Set appropriate value here>

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

Windows

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

UNIX

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

Updating the Design Console xlDataObjectBeans.jar

You must copy the xlDataObjectBeans.jar file in the newly patched EAR (xellerate.ear) to the design console libraries folder. Use the following steps:

1. Extract xlDataObjectBeans.jar from xellerate.ear using the following steps:
   a. Log into WebSphere Admin Console
   b. Navigate to Applications à Enterprise Applications
   c. Choose Xellerate and click Export
   d. Save the generated xellerate.ear
   e. Extract xlDataObjectBeans.jar from xellerate.ear
2. Copy this xlDataObjectBeans.jar to <XL_DC_HOME>\xlclient\lib

Upgrading the Diagnostic Dashboard

To upgrade your existing 8.5.x Diagnostic Dashboard to version 9.0.1, you must install a new instance of the Diagnostic Dashboard. Use the following steps to upgrade to the 9.0.1 Diagnostic Dashboard:

1. Remove the existing XIMDD application
2. Install a new instance of the XIMDD application using the new, version 9.0.1 XIMDD.war file in the Patch\DiagnosticDashboard directory
3. Refer to "Installing the Diagnostic Dashboard" on page 2-8 for more information.

14

Troubleshooting Your Oracle Identity Manager Installation

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

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).

A

Supplementary Upgrade Information

Use the additional information in this Appendix as a supplement to Chapter 13, "Upgrading to Oracle Identity Manager 9.0.1 from Versions 8.5.2 or 8.5.3" on page 13-1 when performing the upgrade.

Creating a User Profile Audit File Group in SQL Server

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

1. From the Windows **Start Menu**, select **Programs**, select **Microsoft SQL Server**, then select **Enterprise Manager**.
2. In the left pane of the SQL Server Enterprise Manager application window, select **Console Root**, select **Microsoft SQL Servers**, select the **server group** to which your server belongs, then double-click the icon representing the **server on which your database is running**.
3. Double-click **Databases**, right-click the database that needs to be upgraded, then click **Properties**.
4. Click the **Data Files** tab, specify the filename and location of the .NDF file as well as the amount of space allocated for this file.
5. Add a new **filegroup** named **XELL_UPA**.
6. Click **OK**.

Executing the SQL Server Upgrade Script

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

Table A–1 Parameters for Command Line Scripts

Arguments	Descriptions
<server-name[\instance-name]>	The name of the server under the "SQL Server Group" in Enterprise Manager. **\instance-name** represents the instance running under the server.

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

Arguments	Descriptions
<db-user>	The database user ID.
<password>	The password of db-user.
<db_name>	The name of the database.
<script_location>	The absolute path to the command line script.

For example:

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

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

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

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

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

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

Loading Metadata into the Database

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

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

   SQL Server and Windows

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

      ```
      REM SET SQL_SERVER_DRIVER_DIR=
      ```

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

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

   Oracle and Windows

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

   ```
   REM SET ORACLE_DRIVER_DIR=
   ```

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

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

Oracle and UNIX/Linux

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

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

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

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

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

   Oracle

   1. JDBC URL (example: jdbc:oracle:thin:@<db_host_ip>:<port>:<SID>)
   2. Database user name
   3. Password

   SQL Server

   1. JDBC URL (example: jdbc:microsoft:sqlserver://<ipaddress>:<port>)
   2. Database name
   3. Database user name
   4. Password

Upgrading the Server Configuration File

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

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

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

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

- Insert the following block of lines:

```
<AuditorOfflineMessage>com.thortech.xl.audit.engine.jms.XLAuditMessageHandl
er</AuditorOfflineMessage>
<AttestationRequestMessage>com.thortech.xl.schedule.jms.attestation.process
OfflinedAttestationRequests</AttestationRequestMessage>
<AttestationTaskMessage>com.thortech.xl.schedule.jms.attestation.processOff
linedAttestationTasks</AttestationTaskMessage>
<AttestationWorkflowTaskMessage>com.thortech.xl.schedule.jms.attestation.pr
ocessOfflinedAttestationWorkflowTasks</AttestationWorkflowTaskMessage>
<ProcessOfflineMessage>com.thortech.xl.schedule.jms.processOfflineProcesses
.processOfflinedProvisioningProcesses</ProcessOfflineMessage>
<ProcessTaskOfflineMessage>com.thortech.xl.schedule.jms.processTaskOffline.
processOfflinedProcessTask</ProcessTaskOfflineMessage>
```

- after the string:
<xl-configuration>.<Offlining>.<MessageHandlerMDB>.<message-handler-task>.<ReconOfflineMessage>. For example, locate the line containing the given XML tag and insert the text in the next line.
- but before the string:
<xl-configuration>.<Offlining>.<MessageHandlerMDB>.<message-handler-task>.<TestMessage>. For example, locate the line containing the given XML tag and insert the text in the previous line.

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

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

- and before the following string:

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

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

---

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

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

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

4. Add the following XML tag <BlockMode> ECB </BlockMode> under the following two locations:
   - <xl-configration>.<Security>.<XLSymmetricProvider>.<Keys>.<DBSecretKey>
   - <xl-configration>.<Security>.<XLSymmetricProvider>.<Keys>.<JMSKey>
5. Locate the following XML tag:

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

   Change it to the following value:

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

6. Save and close the file.

Upgrading the Metadata File

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

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

2. Locate the XML element **<FormManagementMetaData>.<Attribute name="-30">**.

3. Change the value of **dataLength** from **256** to **30**. For example, change something like the following string:

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

   to something like the following:

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

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

```
</FormManagementMetaData>
```

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

   This is the block to insert:

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

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

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

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

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

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

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

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

Upgrading the Remote Manager Configuration File

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

Adding New Configuration Parameters

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

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

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

3. Insert the following block:

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

   <AttestationWorkflowTaskMessage>com.thortech.xl.schedule.jms.attestation.proces
   sOfflinedAttestationWorkflowTasks</AttestationWorkflowTaskMessage>

   <ProcessOfflineMessage>com.thortech.xl.schedule.jms.processOfflineProcesses.pro
   cessOfflinedProvisioningProcesses</ProcessOfflineMessage>

   <ProcessTaskOfflineMessage>com.thortech.xl.schedule.jms.processTaskOffline.proc
   essOfflinedProcessTask</ProcessTaskOfflineMessage>
   ```

   - after the following line:

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

   - and preceding the following line:

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

4. Locate the following parameter:

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

5. Insert the following block:

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

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

- after the following line:

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

- and preceding the following line:

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

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

6. Save and close the file.

Upgrading Existing Configuration Parameters

To update Remote Manager-related configuration parameters.

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

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

   and change it to the following value:

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