Oracle® Identity Manager

Upgrade Guide

Release 9.1.0 (9.0.1.5 Upgrade)

E12912-01

August 2008

ORACLE®

Oracle Identity Manager Upgrade Guide Release 9.1.0 (9.0.1.5 Upgrade)

E12912-01

Primary Author: Debapriya Datta

Contributing Authors: Shiladitya Guha, Lyju Vadassery

Contents

Preface

This guide explains how to upgrade from Oracle Identity Manager release 9.0.1.5 to Oracle Identity Manager release 9.1.0.

This guide also describes how to upgrade to the Oracle Identity Manager Audit and Compliance Module from release 9.0.1.5 to release 9.1.0. If you did not install the Oracle Identity Manager Audit and Compliance Module in your release 9.0.1.5 deployment, then you can use the instructions provided in this guide to install the module when you upgrade to release 9.1.0.

Audience

This guide is intended for system administrators of Oracle Identity Manager.

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, 7 days a week. For TTY support, call 800.446.2398. Outside the United States, call +1.407.458.2479.

Related Documents

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

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation and Configuration Guide for JBoss Application Server*
- *Oracle Identity Manager Installation and Configuration Guide for BEA WebLogic Server*
- *Oracle Identity Manager Installation and Configuration Guide for IBM WebSphere Application Server*
- *Oracle Identity Manager Installation and Configuration Guide for Oracle Application Server*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Globalization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Tools Reference*
- *Oracle Identity Manager Audit Report Developer's Guide*
- *Oracle Identity Manager Integration Guide for Crystal Reports*
- *Oracle Identity Manager API Usage Guide*
- *Oracle Identity Manager Concepts*
- *Oracle Identity Manager Reference*

Documentation Updates

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

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

Conventions

The following text conventions are used in this document:

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

Convention	Meaning
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen (or text that you enter), and names of files, directories, attributes, and parameters.
**_HOME*	The directory in which an application is installed. The directory in which you install Oracle Identity Manager is referred to as *OIM_HOME*. Each Oracle Identity Manager component includes its own abbreviation, for example: *OIM_DC_HOME* for the Design Console and *OIM_RM_HOME* for the Remote Manager. *JBOSS_HOME* represents the location where JBoss Application Server is installed. *WEBSPHERE_HOME* represents the location where IBM WebSphere Application Server is installed. *BEA_HOME* represents the location where BEA WebLogic Server is installed.
Release 9.1.0	Refers specifically to Oracle Identity Manager release 9.1.0.
Release 9.0.1.5	Refers specifically to Oracle Identity Manager release 9.0.1.5.

1

Overview of the Upgrade Process

This chapter provides an overview of the Oracle Identity Manager upgrade process. It also explains how the upgrade information is organized in the subsequent chapters of this guide.

This chapter contains the following topics:

1.1 Upgrading to Release 9.1.0 (9.0.1.5 Upgrade)

This guide deals with upgrading to Oracle Identity Manager release 9.1.0 from Oracle Identity Manager release 9.0.1.5.

This guide refers to the Oracle Identity Manager releases as follows:

- Oracle Identity Manager release 9.1.0 is referred to as **release 9.1.0**.
- Oracle Identity Manager release 9.0.1.5 is referred to as **release 9.0.1.5**.

> **Note:** You can upgrade to release 9.1.0 from release 9.0.1.5. Do not attempt to upgrade to release 9.1.0 from any other previous Oracle Identity Manager release.
>
> If you currently run a release of Oracle Identity Manager earlier than release 9.0.1.5, then contact Oracle Technical Support for the appropriate upgrade instructions.

To get started, you must extract the contents of the release 9.1.0 upgrade package to a temporary directory on your existing release 9.0.1.5 host computer. In this guide, the temporary directory is referred to as *PATCH*.

Table 1–1 provides details of the supported upgrade scenarios.

Table 1–1 Supported Upgrade Scenarios

Application Server	Supported Upgrade Scenarios for Release 9.0.1.5
Oracle Application Server	Not applicable

Table 1–1 (Cont.) Supported Upgrade Scenarios

Application Server	Supported Upgrade Scenarios for Release 9.0.1.5
JBoss Application Server	Existing database and Oracle Identity Manager installation
BEA WebLogic Server	Existing database and Oracle Identity Manager installation
IBM WebSphere Application Server	New Oracle Identity Manager installation after upgrading the existing database

1.2 Supported Release of Application Servers

Oracle Identity Manager release 9.1.0 is certified for the following application servers:

- BEA WebLogic Server 8.1 with SP6
- IBM WebSphere Application Server 6.1.0.9
- JBoss Application Server 4.0.3 with SP1

1.3 Supported Release of Databases

Oracle Identity Manager release 9.1.0 is certified for the following databases:

- Oracle9i Database Enterprise Edition release 9.2.0.7 and later patch sets
- Oracle 10*g* Enterprise Edition Releases:
  - 10.1.0.5
  - 10.2.0.1
  - 10.2.0.2
  - 10.2.0.3
  - 10.2.0.3 with RAC
- Oracle 10*g* Standard Edition Release:
  - 10.2.0.3

Note: Microsoft SQL Server support will be available in the 9.1 Porting releases at a later time. Oracle Identity Manager release 9.1.0 does not support Microsoft SQL Server.

1.4 Overview of the Upgrade Procedure

To upgrade to release 9.1.0 from release 9.0.1.5, you must complete the following tasks:

Note: Depending on the application server you use and the release from which you upgrade, there may be variations in the tasks.

- Extracting the contents of the release 9.1.0 upgrade package to a temporary directory on your existing release 9.0.1.5 system.
- Upgrading the database for Oracle Identity Manager
- Preparing Oracle Identity Manager for upgrade
- Preparing the Administrative and User Console for upgrade

- Preparing the Design Console for upgrade
- Preparing the Remote Manager for upgrade
- Performing the upgrade
- Migrating custom code
- Upgrading the Diagnostic Dashboard
- Postupgrade configuration

1.5 Organization of This Guide

The upgrade process is explained in detail in the chapters listed in this section. You can refer to the relevant chapters based on the application server on which you have installed Oracle Identity Manager.

1.5.1 Oracle Identity Manager on JBoss Application Server

Chapter 2, "Upgrading to Release 9.1.0 (9.0.1.5 Upgrade) on JBoss Application Server"

This chapter explains how to upgrade to release 9.1.0 from release 9.0.1.5 on JBoss Application Server.

1.5.2 Oracle Identity Manager on BEA WebLogic Server

Chapter 3, "Upgrading to Release 9.1.0 on BEA WebLogic Server"

This chapter explains how to upgrade to release 9.1.0 from release 9.0.1.5 on BEA WebLogic Server.

1.5.3 Oracle Identity Manager on IBM WebSphere Server

Chapter 4, "Upgrading to Release 9.1.0 (9.0.1.5 Upgrade) on IBM WebSphere Application Server"

This chapter explains how to upgrade to release 9.1.0 from release 9.0.1.5 on IBM WebSphere Application Server.

2

Upgrading to Release 9.1.0 (9.0.1.5 Upgrade) on JBoss Application Server

This chapter explains how to upgrade to Oracle Identity Manager release 9.1.0 from release 9.0.1.5 on JBoss Application Server. Do not attempt to upgrade to release 9.1.0 from any other previous release of Oracle Identity Manager.

Extract the contents of the release 9.1.0 upgrade package to a temporary directory on your existing release 9.0.1.5 system.

The following steps (detailed in this chapter) explain how to upgrade from release 9.0.1.5 to release 9.1.0 on JBoss Application Server:

1. Creating a Backup of the Existing Deployment
2. Upgrading the Oracle Identity Manager Database
3. Preparing for the Upgrade from Release 9.0.1.5 to Release 9.1.0
   - Preparing Oracle Identity Manager for Upgrade
   - Preparing and Upgrading the Design Console
   - Preparing and Upgrading the Remote Manager
4. Performing the Upgrade from Release 9.0.1.5 to Release 9.1.0
5. Migrating Custom Java Code
6. Postupgrade Configuration
7. Upgrading the Diagnostic Dashboard

2.1 Creating a Backup of the Existing Deployment

The first step for upgrading to release 9.1.0 is to create a backup of your existing Oracle Identity Manager installation. If the upgrade fails, then you can use this backup to restore the existing Oracle Identity Manager installation to its original state.

Create a backup of the following:

- Oracle Identity Manager

  Create a backup of the *OIM_HOME* directory in which you have installed Oracle Identity Manager.

- Oracle Identity Manager Design Console

  Create a backup of the *OIM_DC_HOME* directory in which you have installed the Oracle Identity Manager Design Console.

- JBoss Application Server

  Create a backup of the directory in which JBoss Application Server is installed.

- Oracle Identity Manager Remote Manager

  Create a backup of the *OIM_RM_HOME* directory in which you have installed the Oracle Identity Manager Remote Manager.

- Database used for release 9.0.1.5

  Follow the standard backup procedure for the database.

2.2 Upgrading the Oracle Identity Manager Database

For details about upgrading the Oracle Identity Manager database, refer to Chapter 5, "Upgrading the Oracle Identity Manager Database".

2.3 Preparing for the Upgrade from Release 9.0.1.5 to Release 9.1.0

Before you upgrade to Oracle Identity Manager release 9.1.0, you must prepare for the upgrade by performing preupgrade configuration tasks on the following:

- Oracle Identity Manager
- Design Console
- Remote Manager

2.3.1 Preparing Oracle Identity Manager for Upgrade

To prepare Oracle Identity Manager for the upgrade to release 9.1.0, you must update the release 9.0.1.5 libraries, scripts, and configuration files by performing the following steps:

1. Extract the contents of the Oracle Identity Manager release 9.1.0 upgrade package to a temporary directory in the computer on which the Oracle Identity Manager release 9.0.1.5 is installed. This document refers to this temporary directory as *PATCH*.
2. Copy the directories and files listed in the location of the **From** column to the location listed in the **To** column in Table 2–1. Overwrite the existing files in the **To** location if necessary.

Table 2–1 Oracle Identity Manager Preupgrade Files to Copy

Copy From	To
PATCH/documentation/	*OIM_HOME*/documentation/
PATCH/readme.html	*OIM_HOME*/
PATCH/xellerate/bin/	*OIM_HOME*/xellerate/bin/
PATCH/xellerate/config/	*OIM_HOME*/xellerate/config/
PATCH/xellerate/ConnectorDefaultDirectory/	*OIM_HOME*/xellerate/ConnectorDefaultDirectory/
PATCH/xellerate/DDTemplates/	*OIM_HOME*/xellerate/DDTemplates/
PATCH/xellerate/ext/	*OIM_HOME*/xellerate/ext/
PATCH/xellerate/GTC/	*OIM_HOME*/xellerate/GTC/

Table 2–1 (Cont.) Oracle Identity Manager Preupgrade Files to Copy

Copy From	To
PATCH/xellerate/JavaTasks/	*OIM_HOME*/xellerate/JavaTasks/
PATCH/xellerate/lib/	*OIM_HOME*/xellerate/lib/
PATCH/xellerate/SPMLWS/	*OIM_HOME*/xellerate/SPMLWS/
PATCH/xellerate/webapp/	*OIM_HOME*/xellerate/webapp/
PATCH/xellerate/connectorResources/	*OIM_HOME*/xellerate/connectorResources/
PATCH/xellerate/customResources/	*OIM_HOME*/xellerate/customResources/

Note: While copying the *PATCH*/xellerate/lib/ directory, do not copy xlUpgradeAttestation.jar. Copy it only when you run the UpgradeAttestation script.

3. Copy the following files from the *PATCH*/xellerate/setup/ directory to the *OIM_HOME*/xellerate/setup/ directory:
   - setup.xml
   - patch_jboss.cmd
   - patch_jboss.sh
   - jboss-setup.xml
   - spml_jboss.cmd
   - spml_jboss.sh
   - upgradeAttestation.sh
   - upgradeAttestation.cmd
4. Copy *PATCH*/xellerate/config/xl-jms-service.xml to the *JBOSS_HOME*/server/default/deploy/jms/ and *OIM_HOME*/xellerate/config/ directories. For information about multiple JMS queues, see "Multiple JMS Queues" on page 2-7.
5. Edit the scripts specific to your operating system in the *OIM_HOME*/xellerate/setup/ directory as listed in Table 2–2.

Table 2–2 JBoss Upgrade Patch Scripts and Parameters to Edit

Operating System	Script to Edit	Parameter to Edit
Microsoft Windows	patch_jboss.cmd	Replace @loc with the path to Oracle Identity Manager installation directory.
	spml_jboss.cmd	▪ Replace @java_loc with the path to the Java installation directory. ▪ Replace @loc with the path to the Oracle Identity Manager installation directory.
	UpgradeAttestation.bat	Replace @java_home with the path to the Java installation directory.

Table 2–2 (Cont.) JBoss Upgrade Patch Scripts and Parameters to Edit

Operating System	Script to Edit	Parameter to Edit
Linux	patch_jboss.sh	▪ Replace @loc with the path to the Oracle Identity Manager installation directory. ▪ Replace @java_loc with the path to the Java installation directory.
	spml_jboss.sh	▪ Replace @java_loc with the path to the Java installation directory. ▪ Replace @loc with the path to the Oracle Identity Manager installation directory.
	UpgradeAttestation.sh	▪ Replace @java_home with the path to the Java installation directory. ▪ Replace @loc with the path to Oracle Identity Manager installation directory.

6. Migrate any customizations you made to the release 9.0.1.5 Web application, for example JSP customizations. To do so, apply the 9.0.1.5 customizations to the new release 9.1.0 xlWebApp.war Web application file located in the *OIM_HOME*/xellerate/webapp/ directory.

   See Also: "Migrating Custom Java Code" on page 2-10 for more information about migrating customizations

7. Update your existing Oracle Identity Manager 9.0.1.5 server xlconfig.xml configuration file in the *OIM_HOME*/xellerate/config/ directory with the new cache-related setting for release 9.1.0. To do so:

   a. Open the *OIM_HOME*/xellerate/config/xlconfig.xml file and locate the <xl-configuration><Cache> parameter.

   b. After `</ProcessDefinition>`, add the following:

```
<EmailDefinition>
<Enable>false</Enable>
<ExpireTime>14400</ExpireTime>
</EmailDefinition>
```

   c. Change:

```
<ServerProperties>
<Enable>false</Enable>
<ExpireTime>14400</ExpireTime>
</ServerProperties>
```

   To:

```
<ServerProperties>
<Enable>true</Enable>
<ExpireTime>14400</ExpireTime>
</ServerProperties>
```

   d. After `</ColumnMetaData>`, add the following:

```
<!-- API Data -->
<API>
     <Enable>false</Enable>
     <ExpireTime>14400</ExpireTime>
```

```
</API>
<CustomResourceBundle>
     <Enable>true</Enable>
     <ExpireTime>-1</ExpireTime>
</CustomResourceBundle>
<CustomDefaultBundle>
     <Enable>true</Enable>
     <ExpireTime>-1</ExpireTime>
</CustomDefaultBundle>
<ConnectorResourceBundle>
     <Enable>true</Enable>
     <ExpireTime>-1</ExpireTime>
</ConnectorResourceBundle>
<LinguisticSort>
     <Enable>true</Enable>
     <ExpireTime>-1</ExpireTime>
</LinguisticSort>
<GenericConnector>
     <Enable>true</Enable>
     <ExpireTime>-1</ExpireTime>
</GenericConnector>
<GenericConnectorProviders>
     <Enable>true</Enable>
     <ExpireTime>-1</ExpireTime>
</GenericConnectorProviders>
```

e. After `</AttestationTaskMessage>`, add the following:

```
<AttestationTaskDetailMessage>com.thortech.xl.schedule.jms
.attestation.processOfflinedAttestationTaskDetails</Attest
ationTaskDetailMessage>
```

Note: The aforementioned code must be added as a single line without any line breaks.

f. Inside:

```
<recon_offline_queue>
```

Replace:

```
<queueName>queue/xlQueue</queueName>
```

With:

```
<queueName>queue/xlReconQueue</queueName>
```

g. Inside:

```
<auditor_offline_queue>
```

Replace:

```
<queueName>queue/xlQueue</queueName>
```

With:

```
<queueName>queue/xlAuditQueue</queueName>
```

h. Inside:

```
<attestation_request_queue>
```

Replace:

```
<queueName>queue/xlQueue</queueName>
```

With:

```
<queueName>queue/xlAttestationQueue</queueName>
```

i. Inside:

```
<attestation_task_queue>
```

Replace:

```
<queueName>queue/xlQueue</queueName>
```

With:

```
<queueName>queue/xlAttestationQueue</queueName>
```

j. Inside:

```
<attestation_workflow_task_queue>
```

Replace:

```
<queueName>queue/xlQueue</queueName>
```

With:

```
<queueName>queue/xlAttestationQueue</queueName>
```

k. Inside:

```
<process_offline_queue>
```

Replace:

```
<queueName>queue/xlQueue</queueName>
```

With:

```
<queueName>queue/xlProcessQueue</queueName>
```

l. Inside:

```
<process_task_offline_queue>
```

Replace:

```
<queueName>queue/xlQueue</queueName>
```

With:

```
<queueName>queue/xlProcessQueue</queueName>
```

m. After </attestation_task_queue>, add the following:

```
<attestation_task_detail_queue>
        <queueName>queue/xlAttestationQueue</queueName>
        <autoAcknowledge>true</autoAcknowledge>
        <replyTo></replyTo>
```

```
        <persistentFlag>true</persistentFlag>
        <disableMessageId>true</disableMessageId>
        <disableTimeStampe>false</disableTimeStampe>
        <messageEncrypt>false</messageEncrypt>
</attestation_task_detail_queue>
```

Redeploying SPML Web Service

If you are using SPML Web service in the existing Oracle Identity Manager setup, then you must redeploy the SPML Web service for that setup whenever the setup is upgraded.

> **See Also:** Chapter12: "SPML Web Service" in *Oracle Identity Manager Tools Reference*

Multiple JMS Queues

Previously, Oracle Identity Manager used a single JMS queue (named xlQueue) for all asynchronous operations including requests, reconciliation, attestation, and offline tasks. In release 9.1.0, by default, Oracle Identity Manager uses separate JMS queues for specific operations to optimize JMS queue processing. The following is a list of the default JMS queue configuration and their related operations:

- xlQueue for request operations
- xlReconQueue for reconciliation operations
- xlAuditQueue for auditing operations
- xlAttestationQueue for attestation operations
- xlProcessQueue for usage in future Oracle Identity Manager releases

Additional JMS queues are created in step 7 in the "Preparing Oracle Identity Manager for Upgrade" on page 2-2.

2.3.2 Preparing and Upgrading the Design Console

To prepare the Oracle Identity Manager Design Console for the upgrade to release 9.1.0, you must update your release 9.0.1.5 Design Console libraries, scripts, and configuration files by performing the following steps:

1. Create a backup of the *OIM_DC_HOME* directory.
2. Copy the directories and files listed in the location of the **From** column to the location listed in the **To** column in Table 2–3. Overwrite the existing files in the **To** location if necessary.

> **Note:** Delete the release 9.0.1.5 files in the *OIM_DC_HOME*/documentation/ directory before copying the release 9.1.0 files from *PATCH*/documentation/ directory.

Table 2–3 Oracle Identity Manager Design Console Preupgrade Files to Copy

Copy From	To
PATCH/xlclient/XLDesktopClient.ear	*OIM_DC_HOME*/xlclient/
PATCH/readme.html	*OIM_DC_HOME*/xlclient
PATCH/xlclient/CustomClient.zip	*OIM_DC_HOME*/xlclient/

Table 2–3 (Cont.) Oracle Identity Manager Design Console Preupgrade Files to Copy

Copy From	To
PATCH/xlclient/xlFvcUtil.ear	*OIM_DC_HOME*/xlclient/
PATCH/xlclient/lib/	*OIM_DC_HOME*/xlclient/lib/
PATCH/documentation/	*OIM_DC_HOME*/documentation/
PATCH/xlclient/ext/	*OIM_DC_HOME*/ext/

3. Edit the *OIM_DC_HOME*/xlclient/classpath.bat file and add the following string to the end of CLASSPATH:

```
".\ext\oscache.jar;.\ext\commons-logging.jar;.\ext\javagroups-all.jar"
```

4. Specify the multicast address in the xlconfig.xml file of the Design Console as follows:
   a. Open the *OIM_DC_HOME*/xlclient/Config/xlconfig.xml file in a text editor.
   b. Add the following lines before the </xl-configuration> tag:

```
<!--  Value of MultiCastAddress must be the same as that of Oracle Identity
Manager -->
<Cache>
  <XLCacheProvider>
    <MultiCastAddress>MULTICASTADDRESS_VALUE</MultiCastAddress>
  </XLCacheProvider>
</Cache>
```

   c. Replace *MULTICASTADDRESS_VALUE* with the value of the multicast address for Oracle Identity Manager.

Note: After Oracle Identity Manager and the Design Console are upgraded, go to Adapter Manager on the Design Console and recompile all the adapters.

2.3.3 Preparing and Upgrading the Remote Manager

Prepare the Oracle Identity Manager Remote Manager for the upgrade to release 9.1.0 by updating your release 9.0.1.5 Remote Manager libraries, scripts, and configuration files by performing the following steps:

1. Create a backup of the *OIM_RM_HOME*/xlremote/lib/ directory.
2. Copy the contents of the *PATCH*/xlremote/lib/ directory to the *OIM_RM_HOME*/xlremote/lib/ directory by overwriting files if necessary.

2.4 Performing the Upgrade from Release 9.0.1.5 to Release 9.1.0

Perform the following steps to upgrade to release 9.1.0 (9.0.1.5 upgrade) on a single installation of JBoss Application Server:

1. Ensure that the JBoss Application Server is **not** running.

Note: If JBoss Application Server is running, then you can stop it by running one of the following commands, as appropriate for the operating system on the Oracle Identity Manager host computer:

For Microsoft Windows:

```
JBOSS_HOME\bin\shutdown.bat -S
```

For UNIX:

```
JBOSS_HOME/bin/shutdown.sh -S
```

2. For upgrading attestation, see Appendix H, "Attestation Upgrade Utility". This is a mandatory step.
3. Delete the *OIM_HOME*/xellerate/webapp/precompiled/ directory.
4. Start JBoss Application Server and run the patch_jboss script:

   For **Microsoft Windows**:

   Run *OIM_HOME*\xellerate\setup\patch_jboss.cmd *OIM_DB_USER_ PASSWORD*

   For **UNIX**:

   Run *OIM_HOME*/xellerate/setup/patch_jboss.sh *OIM_DB_USER_ PASSWORD*

   Replace *OIM_DB_USER_PASSWORD* with the database password for Oracle Identity Manager installation.
5. Copy *PATCH*/xellerate/ext/ojdbc14.jar to the *JBOSS_HOME*/server/default/lib/ directory. If this JAR file already exists in the destination directory, then overwrite the existing file.
6. Edit the login-config.xml file in the *JBOSS_HOME*/server/default/conf/ directory.

   In the login-config.xml file, search for:

   ```
   <login-module code="com.thortech.xl.security.jboss.XLClientLoginModule"
   flag="required">
   ```

   Change this code to:

   ```
   <login-module code="org.jboss.security.ClientLoginModule" flag="required">
   ```

   Save the changes in the file.
7. Restart JBoss Application Server.
8. Run the Re-Issue Audit Message Task scheduled task to ensure that all the pending audit messages in the aud_jms table are processed.

Note: While running the Re-Issue Audit Message Task scheduled task, ensure that the database and Oracle Identity Manager have been upgraded. If you are running the scheduled task through the Design Console, then ensure that the Design Console has also been upgraded.

2.5 Migrating Custom Java Code

You can migrate the custom Java code from the release 9.0.1.5 environment into the new release 9.1.0 environment. Before you migrate the custom Java code from the release 9.0.1.5 environment, you must first recompile it by using the release 9.1.0 libraries located in the *OIM_HOME*/xellerate/lib/ directory.

Using the integrated development environment that originally compiled the release 9.0.1.5 custom Java code, which are Eclipse, JDeveloper, WASD or command-line javac, recompile all custom Java code by using the release 9.1.0 libraries.

The following is a list of the custom items that you can migrate from release 9.0.1.5 and reuse in release 9.1.0 after recompiling.

> **Note:** For clustered environments, after recompiling the following items by using the release 9.1.0 libraries, copy them to each participant node of the cluster.

- Custom Java libraries bound to functional Oracle Identity Manager release 9.0.1.5 adapters recompiled by using release 9.1.0 libraries.

  You must copy the recompiled custom Java libraries in the *OIM_HOME*/xellerate/JavaTasks/ directory to the same directory in release 9.1.0. In addition, you must copy the recompiled custom Java libraries in the release 9.0.1.5 *OIM_RM_HOME*/xellerate/JavaTasks/ directory to the same directory in release 9.1.0.

- Custom scheduled tasks recompiled by using release 9.1.0 libraries.

  You must copy the recompiled custom event handlers to the *OIM_HOME*/xellerate/ScheduleTask/ directory release 9.1.0.

  > **Note:** If you want to see the built-in scheduled task on the Administrative and User Console, then copy the xlScheduler.jar file from the *OIM_HOME*/lib directory to the *OIM_HOME*/xellerate/ScheduledTask directory. If the ScheduledTask directory does not exist, then create it.

- Custom event handlers recompiled by using release 9.1.0 libraries.

  You must copy the recompiled custom scheduled tasks to the *OIM_HOME*/xellerate/EventHandlers/ directory in release 9.1.0.

- Connector resource bundles by copying the *OIM_HOME*/xellerate/connectorResources/ directory release 9.0.1.5 to the *OIM_HOME*/xellerate/connectorResources/ directory in release 9.1.0.

- Custom resources by copying the *OIM_HOME*/xellerate/customResources/ directory release 9.0.1.5 to the *OIM_HOME*/xellerate/customResources/ directory in release 9.1.0.

- Custom Administrative and User Console deployments.

  Several Administrative and User Console files are modified in release 9.1.0. If you customized your release 9.0.1.5 Administrative and User Console, that is, you made changes to the default Administrative and User Console files that shipped with release 9.0.1.5, then you must add your customizations into the new release 9.1.0 Administrative and User Console files.

2.6 Postupgrade Configuration

You must perform the following postupgrade configuration procedures:

- Setting the User Profile Audit Level
- Generating User Snapshots
- Generating GPA Snapshots
- Loading Data for Exception-Based Reporting

2.6.1 Setting the User Profile Audit Level

If you want to change the audit level, perform the following steps:

1. Define a secondary data source for reporting, if required.

   See Also: *Oracle Identity Manager Audit Report Developer's Guide* for information about defining a secondary data source

2. Start the application server on which the Oracle Identity Manager installation is running.
3. Set the audit level. The permissible values are in descending order:
   - Process Task
   - Resource Form
   - Resource
   - Membership
   - Core
   - None
4. To specify an audit level, perform the following steps:
   a. Log in to the Design Console as an administrator.
   b. Navigate to the System Configuration form.
   c. Locate XL.UserProfileAuditDataCollection and set its value to `Resource Form` or the appropriate audit level as listed in step 3 of this procedure.
5. To collect user profile audit data in the secondary reporting data store, perform the following steps:
   a. Log in to the Design Console as an administrator.
   b. Navigate to the System Configuration form.
   c. Locate XL.UserProfileAuditInSecondaryDS and set its value to `TRUE`.

2.6.2 Generating User Snapshots

For detailed information about generating user snapshots, see Appendix E, "Generating User Snapshots".

2.6.3 Generating GPA Snapshots

For detailed information about generating GPA snapshots, see Appendix G, "Generating GPA Snapshots".

2.6.4 Loading Data for Exception-Based Reporting

To load data for exception-based reporting, run the UPA Form Data Upgrade utility. For information about the UPA Form Data Upgrade utility, see Appendix F, "UPA Form Data Upgrade Utility".

2.7 Upgrading the Diagnostic Dashboard

To upgrade to the release 9.1.0 Diagnostic Dashboard XIMDD application on JBoss Application Server, install a new instance of the XIMDD application by copying the release 9.1.0 XIMDD.war file from the *PATCH*/DiagnosticDashboard/ directory to the *JBOSS_HOME*/server/default/deploy/ directory.

Note:

- You need not remove the existing version of release 9.0.1.5 Diagnostic Dashboard XIMDD application to upgrade to the 9.1.0 Diagnostic Dashboard on JBoss Application Server.
- For clustered installations, copy the application (XIMDD.war) to *JBOSS_HOME*/server/all/deploy/ directory.

See Also: The "Working with the Diagnostic Dashboard" chapter in the *Oracle Identity Manager Administrative and User Console Guide* for information about the Diagnostic Dashboard

3

Upgrading to Release 9.1.0 on BEA WebLogic Server

This chapter explains how to upgrade to Oracle Identity Manager release 9.1.0 from release 9.0.1.5 on BEA WebLogic Server. Do not attempt to upgrade to release 9.1.0 from any other previous Oracle Identity Manager release.

Run the contents of the release 9.1.0 upgrade package to a temporary directory on your existing release 9.0.1.5 system.

The following steps (detailed in this chapter) explain how to upgrade from release 9.0.1.5 to release 9.1.0 on BEA WebLogic Server:

1. Creating a Backup of the Existing Deployment
2. Upgrading the Oracle Identity Manager Database
3. Preparing for the Upgrade from Release 9.0.1.5 to Release 9.1.0
   a. Preparing Oracle Identity Manager for Upgrade
   b. Preparing and Upgrading the Design Console
   c. Preparing and Upgrading the Remote Manager
4. Performing the Upgrade from Release 9.0.1.5 to Release 9.1.0
5. Migrating Custom Java Code
6. Postupgrade Configuration
7. Upgrading the Diagnostic Dashboard

3.1 Creating a Backup of the Existing Deployment

The first step for upgrading to release 9.1.0 is to create a backup of your existing release 9.0.1.5 deployment to ensure that no data is lost during the upgrade process. If the upgrade fails, then you can use this backup to restore the release 9.0.1.5 deployment to its original state.

You must create a backup of the following:

- Oracle Identity Manager

  Back up the *OIM_HOME* directory in which you have installed Oracle Identity Manager.

- Oracle Identity Manager Design Console

  Back up the *OIM_DC_HOME* directory in which you have installed the Oracle Identity Manager Design Console.

- Back up BEA WebLogic Server

  Back up BEA WebLogic Server domain directory, for example, the C:\bea\user_projects\domains\mydomain directory. Also back up the *BEA_HOME*/weblogic81/server/lib/ directory.

  Note: For a clustered installation, repeat this step on each node of the cluster.

- Oracle Identity Manager Remote Manager

  Back up the *OIM_RM_HOME* directory in which you have installed the Oracle Identity Manager Remote Manager.

- Database used for release 9.0.1.5

  Follow the standard backup procedure for the database.

3.2 Upgrading the Oracle Identity Manager Database

For details about upgrading the Oracle Identity Manager database, refer to Chapter 5, "Upgrading the Oracle Identity Manager Database".

3.3 Preparing for the Upgrade from Release 9.0.1.5 to Release 9.1.0

Before you upgrade to Oracle Identity Manager release 9.1.0, you must prepare for the upgrade by performing preupgrade configuration tasks on the following:

- Oracle Identity Manager
- Design Console
- Remote Manager

3.3.1 Preparing Oracle Identity Manager for Upgrade

Prepare Oracle Identity Manager for upgrade to release 9.1.0 by updating the release 9.0.1.5 libraries, scripts, and configuration files. To do so:

Note: If you are upgrading to release 9.1.0 in a WebLogic cluster, then perform the steps in this section on the WebLogic Admin Server computer.

1. For upgrading from release 9.0.1.5, extract the contents of the Oracle Identity Manager release 9.1.0 upgrade package to a temporary directory on the computer in which the Oracle Identity Manager release 9.0.1.5 is installed.

   Note: This guide refers to this temporary directory as *PATCH*.

2. Back up the *OIM_HOME* directory.
3. Copy the directories and files listed in the location of the **From** column to the location listed in the **To** column in Table 3–1.

   Overwrite the existing files in the **To** location if necessary.

Note: Delete the release 9.0.1.5 files in the *OIM_HOME*/documentation/ directory before copying the release 9.1.0 files from *PATCH*/documentation/.

Table 3–1 Oracle Identity Manager Preupgrade Files to Copy

From	To
PATCH/documentation/	*OIM_HOME*/documentation/
PATCH/readme.html	*OIM_HOME*
PATCH/xellerate/bin/	*OIM_HOME*/xellerate/bin/
PATCH/xellerate/config/	*OIM_HOME*/xellerate/config/
PATCH/xellerate/ConnectorDefaultDirectory/	*OIM_HOME*/xellerate/ConnectorDefaultDirectory/
PATCH/xellerate/connectorResources/	*OIM_HOME*/xellerate/connectorResources/
PATCH/xellerate/customResources/	*OIM_HOME*/xellerate/customResources/
PATCH/xellerate/DDTemplates/	*OIM_HOME*/xellerate/DDTemplates/
PATCH/xellerate/ext/	*OIM_HOME*/xellerate/ext/
PATCH/xellerate/GTC/	*OIM_HOME*/xellerate/GTC/
PATCH/xellerate/JavaTasks/	*OIM_HOME*/xellerate/JavaTasks/
PATCH/xellerate/lib/	*OIM_HOME*/xellerate/lib/
PATCH/xellerate/SPMLWS/	*OIM_HOME*/xellerate/SPMLWS/
PATCH/xellerate/webapp/	*OIM_HOME*/xellerate/webapp/

Note: While copying the *PATCH*/xellerate/lib/ directory, do not copy xlAttestationUpgrade.jar. Copy it only before running the UpgradeAttestation script.

4. Copy the following files from the *PATCH*/xellerate/setup/ directory to the *OIM_HOME*/xellerate/setup/ directory according to the Oracle Identity Manager installation:
   - setup.xml
   - patch_weblogic.cmd
   - patch_weblogic.sh
   - weblogic-setup.xml
   - setup_wl_server.xml
   - spml_weblogic.sh
   - spml_weblogic.cmd
   - UpgradeAttestation.sh
   - UpgradeAttestation.cmd

5. Update your existing release 9.0.1.5 Oracle Identity Manager xlconfig.xml configuration file in the *OIM_HOME*/xellerate/config/ directory with the new cache-related setting for release 9.1.0. To do so:

   a. Open the *OIM_HOME*/xellerate/config/xlconfig.xml file and locate the <xl-configuration>< Cache> parameter.

   b. After </ProcessDefinition>, add the following:

```
<EmailDefinition>
            <Enable>false</Enable>
            <ExpireTime>14400</ExpireTime>
</EmailDefinition>
```

   c. Change:

```
<ServerProperties>
            <Enable>false</Enable>
            <ExpireTime>14400</ExpireTime>
</ServerProperties>
```

   To:

```
<ServerProperties>
            <Enable>true</Enable>
            <ExpireTime>14400</ExpireTime>
</ServerProperties>
```

   d. After </ColumnMetaData>, add the following:

```
<!-- API Data -->
<API>
            <Enable>false</Enable>
            <ExpireTime>14400</ExpireTime>
</API>
<CustomResourceBundle>
            <Enable>true</Enable>
            <ExpireTime>-1</ExpireTime>
</CustomResourceBundle>
<CustomDefaultBundle>
            <Enable>true</Enable>
            <ExpireTime>-1</ExpireTime>
</CustomDefaultBundle>
<ConnectorResourceBundle>
            <Enable>true</Enable>
            <ExpireTime>-1</ExpireTime>
</ConnectorResourceBundle>
<LinguisticSort>
            <Enable>true</Enable>
            <ExpireTime>-1</ExpireTime>
</LinguisticSort>
<GenericConnector>
            <Enable>true</Enable>
            <ExpireTime>-1</ExpireTime>
</GenericConnector>

<GenericConnectorProviders>
            <Enable>true</Enable>
            <ExpireTime>-1</ExpireTime>
</GenericConnectorProviders>
```

   e. After </AttestationTaskMessage>, add the following:

```
<AttestationTaskDetailMessage>com.thortech.xl.schedule.jms.attestation.proc
essOfflinedAttestationTaskDetails</AttestationTaskDetailMessage>
```

Note: The aforementioned line of code must be entered as a single line without any line breaks.

---

f. Inside:

```
<recon_offline_queue>
```

Replace:

```
<queueName>queue/xlQueue</queueName>
```

With:

```
<queueName>queue/xlReconQueue</queueName>
```

g. Inside:

```
<auditor_offline_queue>
```

Replace:

```
<queueName>queue/xlQueue</queueName>
```

With:

```
<queueName>queue/xlAuditQueue</queueName>
```

h. Inside:

```
<attestation_request_queue>
```

Replace:

```
<queueName>queue/xlQueue</queueName>
```

With:

```
<queueName>queue/xlAttestationQueue</queueName>
```

i. Inside:

```
<attestation_task_queue>
```

Replace:

```
<queueName>queue/xlQueue</queueName>
```

With:

```
<queueName>queue/xlAttestationQueue</queueName>
```

j. Inside:

```
<attestation_workflow_task_queue>
```

Replace:

```
<queueName>queue/xlQueue</queueName>
```

With:

```
<queueName>queue/xlAttestationQueue</queueName>
```

k. Inside:

```
<process_offline_queue>
```

Replace:

```
<queueName>queue/xlQueue</queueName>
```

With:

```
<queueName>queue/xlProcessQueue</queueName>
```

l. Inside:

```
<process_task_offline_queue>
```

Replace:

```
<queueName>queue/xlQueue</queueName>
```

With:

```
<queueName>queue/xlProcessQueue</queueName>
```

m. After </attestation_task_queue> add the following:

```
<attestation_task_detail_queue>
            <queueName>queue/xlAttestationQueue</queueName>
            <autoAcknowledge>true</autoAcknowledge>
            <replyTo></replyTo>
            <persistentFlag>true</persistentFlag>
            <disableMessageId>true</disableMessageId>
            <disableTimeStampe>false</disableTimeStampe>
            <messageEncrypt>false</messageEncrypt>
</attestation_task_detail_queue>
```

3.3.2 Preparing and Upgrading the Design Console

Prepare the Oracle Identity Manager Design Console for upgrade to release 9.1.0 by updating your release 9.0.1.5 Design Console libraries, scripts, and configuration files. To do so:

1. Back up the *OIM_DC_HOME* directory.
2. Copy the directories and files listed in the location of the **From** column to the location listed in the **To** column in Table 3–2.

   Overwrite the existing files in the **To** location if necessary.

> **Note:** Delete the release 9.0.1.5 files in the *OIM_DC_HOME*/documentation/ directory before copying the release 9.1.0 files from the *PATCH*/documentation/ directory.

Table 3–2 Oracle Identity Manager Design Console Preupgrade Files to Copy

From	To
PATCH/xlclient/XLDesktopClient.ear	*OIM_DC_HOME*/xlclient/

Table 3–2 (Cont.) Oracle Identity Manager Design Console Preupgrade Files to Copy

From	To
PATCH/readme.html	*OIM_DC_HOME*/xlclient/
PATCH/xlclient/CustomClient.zip	*OIM_DC_HOME*/xlclient/
PATCH/xlclient/xlFvcUtil.ear	*OIM_DC_HOME*/xlclient/
PATCH/xlclient/lib/	*OIM_DC_HOME*/xlclient/lib/
PATCH/documentation/	*OIM_DC_HOME*/documentation/
PATCH/xellertate/ext/	*OIM_DC_HOME*/ext/

3. Edit the *OIM_DC_HOME*/xlclient/classpath.bat file and add the following string to the end of CLASSPATH:

```
".\ext\oscache.jar;.\ext\commons-logging.jar;.\ext\javagroups-all.jar"
```

4. Specify the multicast address in the xlconfig.xml file of the Design Console as follows:

   a. Open the *OIM_DC_HOME*/xlclient/Config/xlconfig.xml file in a text editor.

   b. Add the following lines before the </xl-configuration> tag:

```
<!--  Value of MultiCastAddress must be the same as that of Oracle Identity
Manager -->
<Cache>
  <XLCacheProvider>
    <MultiCastAddress>MULTICASTADDRESS_VALUE</MultiCastAddress>
  </XLCacheProvider>
</Cache>
```

   c. Change *MULTICASTADDRESS_VALUE* to the value of the multicast address for Oracle Identity Manager.

Note: After the server and Design Console are upgraded, go to Adapter Manager on the Design Console and recompile all the adapters.

3.3.3 Preparing and Upgrading the Remote Manager

To prepare the Oracle Identity Manager Remote Manager for the upgrade to release 9.1.0 by updating your release 9.0.1.5 Remote Manager libraries, scripts, and configuration files. To do so:

1. Create a backup of the *OIM_RM_HOME*/xlremote/lib/ directory.
2. Copy the contents of the *PATCH*/xlremote/lib/ directory to the *OIM_RM_HOME*/xlremote/lib/ directory by overwriting the files if necessary.

3.3.4 Undeploy Applications

You must manually undeploy the applications running on BEA WebLogic Server before upgrading Oracle Identity Manager. To do so:

1. Login to the WebLogic Administrative Console.
2. In the left pane, go to **Deployments**, **Applications**, and then to **Nexaweb**.

3. In the right pane, click the **Deploy** tab, and then click **Stop Application**.
4. In the left pane, go to **Deployments**, **Applications**, and then to **Xellerate**.
5. In the right pane, click the **Deploy** tab, and then click **Stop Application**.
6. In the left pane, go to **Deployment**, and then to **Applications**.
7. Click **Delete** to delete the Nexaweb application. Click **Yes** to confirm the deletion.
8. In the left pane, go to **Deployments**, and then to **Applications**.
9. Click **Delete** to delete the Xellerate application. Click **Yes** to confirm the deletion.
10. Restart BEA WebLogic Server.

Note: For a clustered installation, restart all the application servers including the Admin server after deleting the applications from the WebLogic Administrative Console.

3.3.5 Multiple JMS Queues

Previously, Oracle Identity Manager used a single JMS queue (named xlQueue) for all asynchronous operations including requests, reconciliation, attestation, and offline tasks. In release 9.1.0, by default, Oracle Identity Manager uses separate JMS queues for specific operations to optimize JMS queue processing. The following is a list of the default JMS queue configuration and their related operations:

- xlQueue for request operations
- xlReconQueue for reconciliation operations
- xlAuditQueue for auditing operations
- xlAttestationQueue for attestation operations
- xlProcessQueue for usage in future Oracle Identity Manager releases

This section provides details that help to create the additional JMS queues.

For a nonclustered installation, implement only the changes mentioned in "Creating JMS Queues for JMS Server (For Noncluster Installation Only)" on page 3-8.

For a clustered installation, implement only the changes mentioned in the following sections:

- Creating JMS Queues for JMS Servers (For Clustered Installation Only)
- Creating JMS Distributed Queues (For Clustered Installation Only)

3.3.5.1 Creating JMS Queues for JMS Server (For Noncluster Installation Only)

To create JMS queues for JMS server:

1. Log in to the WebLogic Administrative Console.
2. Navigate to **Services**, **JMS**, and then to **Servers**.
3. Expand the tree for the **xlJMSServer**.
4. Click **Destinations**.
5. Click the **Clone** icon for xlQueue.
6. Enter the values for Name and JNDI name as follows:
   - Name: `xlReconQueue`

- JNDI Name: `queue/xlReconQueue`

7. Click **Clone**, and then click the **Redelivery** tab.
8. Select the Error Destination that starts with queue/xlErrorQueue.
9. Repeat steps 4 through 8 with the following Name and JNDI Name values:
   - Name: `xlAuditQueue`
   - JNDI Name: `queue/xlAuditQueue`
   - Name: `xlAttestationQueue`
   - JNDI Name: `queue/xlAttestationQueue`
   - Name: `xlProcessQueue`
   - JNDI Name: `queue/xlProcessQueue`

3.3.5.2 Creating JMS Queues for JMS Servers (For Clustered Installation Only)

To create JMS queues for JMS servers:

1. Log in to the WebLogic Administrative Console.
2. Go to **Services**, **JMS**, and then **Servers**.
3. Expand the tree for the xlJMSServer JMS server that starts with xlJMSServer *SERVER_NAME*.
4. Click **Destinations**.
5. Click the **Clone** icon for xlQueue *SERVER_NAME*.
6. Enter the values for Name and JNDI Name as follows:
   - **Name:** `xlReconQueue` *SERVER_NAME*
   - **JNDI Name:** `queue/xlReconQueue` *SERVER_NAME*
7. Click the **Clone** icon, and then click the **Redelivery** tab.
8. Select the Error Destination that starts with queue/xlErrorQueue *SERVER_NAME*.
9. Repeat steps 4 through 8 with the following Name and JNDI Name values:
   - Name: `xlAuditQueue` *SERVER_NAME*
   - JNDI Name: queue/xlAuditQueue *SERVER_NAME*
   - Name: xlAttestationQueue *SERVER_NAME*
   - JNDI Name: queue/xlAttestationQueue *SERVER_NAME*
   - Name: xlProcessQueue *SERVER_NAME*
   - JNDI Name: queue/xlProcessQueue *SERVER_NAME*
10. Repeat steps 3 through 9 for all available JMS servers starting with XlJMSServer *SERVER_NAME*.

3.3.5.3 Creating JMS Distributed Queues (For Clustered Installation Only)

To create JMS distributed queues only for clustered installation:

1. Login in to the WebLogic Administrative Console.
2. Go to **Services**, **JMS**, and then to **Distributed Destination**.
3. Click **Configure a new Distributed Queue...**.

4. Enter the values for Name and JNDI Name as follows:
   - Name: `xlReconQueue`
   - JNDI Name: `queue/xlReconQueue`
5. Click **Create** at the bottom of the page.
6. Click the **Members** tab, and then click the **Configure a new Distributed Queue Member** link.
7. Provide the following details:
   - Name: Specify the name as *SERVER_NAME*`_queue_member`
   - JMS Queue: Select `xlReconQueue` *SERVER_NAME*
8. Repeat steps 6 and 7 for the available servers. For example, for two managed servers (XL_SERVER1, XL_SERVER2) in the cluster, create the distributed queue members as listed in the following table:

Name	JMS Queue Name
XL_SERVER1_queue_member	xlReconQueueXL_SERVER1
XL_SERVER2_queue_member	xlReconQueueXL_SERVER2

9. Click **Configure a new Distributed Queue...**.
10. Enter the values for Name and JNDI Name as follows:
    - Name: `xlAuditQueue`
    - JNDI Name: `queue/xlAuditQueue`
11. Clcik **Create** at the bottom of the page.
12. Click the **Members** tab, and then click the **Configure a new Distributed Queue Member** link.
13. Provide the following details:
    - Name: Specify the name as *SERVER_NAME*`_queue_member`
    - JMS Queue: Select `xlAuditQueue` *SERVER_NAME*
14. Repeat steps 12 and 13 for the available servers. For example, for two managed servers (XL_SERVER1, XL_SERVER2) in the cluster, create the distributed queue members as listed in the following table:

Name	JMS Queue Name
XL_SERVER1_queue_member	xlAuditQueueXL_SERVER1
XL_SERVER2_queue_member	xlAuditQueueXL_SERVER2

15. Click **Configure a new Distributed Queue...**.
16. Enter the values for Name and JNDI Name as follows:
    - Name: `xlAttestationQueue`
    - JNDI Name: `queue/xlAttestationQueue`
17. Clcik **Create** at the bottom of the page.

18. Click the **Members** tab, and then click the **Configure a new Distributed Queue Member** link.
19. Provide the following details:
    - Name: Specify the name as *SERVER_NAME*_queue_member
    - JMS Queue: Select xlAttestationQueue *SERVER_NAME*
20. Repeat steps 18 and 19 for the available servers. For example, for two managed servers (XL_SERVER1, XL_SERVER2) in the cluster, create the distributed queue members as listed in the following table:

Name	JMS Queue Name
XL_SERVER1_queue_member	xlAttestationQueueXL_SERVER1
XL_SERVER2_queue_member	xlAttestationQueueXL_SERVER2

21. Click **Configure a new Distributed Queue...**
22. Enter the values for Name and JNDI Name as follows:
    - Name: xlProcessQueue
    - JNDI Name: queue/xlProcessQueue
23. Click **Create** at the bottom of the page.
24. Click the **Members** tab, and then click the **Configure a new Distributed Queue Member** link.
25. Provide the following details:
    - Name: Specify the name as *SERVER_NAME*_queue_member
    - JMS Queue: Select xlProcessQueue *SERVER_NAME*
26. Repeat steps 24 and 25 for the available servers. For example, for two managed servers (XL_SERVER1, XL_SERVER2) in the cluster, create the distributed queue members as listed in the following table:

Name	JMS Queue Name
XL_SERVER1_queue_member	xlProcessQueueXL_SERVER1
XL_SERVER2_queue_member	xlProcessQueueXL_SERVER2

3.4 Performing the Upgrade from Release 9.0.1.5 to Release 9.1.0

Upgrading from an existing Oracle Identity Manager release 9.0.1.5 deployment to Oracle Identity Manager release 9.1.0 involves assembling a new enterprise application archive (EAR) file from the latest libraries, and then redeploying the EAR file.

Perform the following steps to upgrade to release 9.1.0 on a single BEA WebLogic Server installation and WebLogic cluster:

To upgrade from release 9.0.1.5:

1. Install the JDK version that is supported with Oracle Identity Manager release 9.1.0 for BEA WebLogic Server.

See Also: *Oracle Identity Manager Installation and Configuration Guide for BEA Weblogic Server* for more information about installing JDK for BEA WebLogic Server

2. Stop BEA WebLogic Server.
3. Navigate to *BEA_HOME*\user_projects\domains*NAME_OF_DOMAIN_DIRECTORY*. For example, `C:\bea\user_projects\domains\mydomain`.
4. In a text editor, open the WebLogic start script file. The start script is:
   - For Microsoft Windows:

     ```
     startWebLogic.cmd
     ```

   - For UNIX:

     ```
     startWebLogic.sh
     ```

5. JVM memory settings must be changed for production environments and when processing a large volume of data in nonproduction environments. Edit the script to specify memory options as follows:

   For Microsoft Windows, locate the line that starts with the following:

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

   Add either of the following lines just before it:

   - If Sun JVM is used:

     ```
     set MEM_ARGS=-Xms1280m -Xmx1280m -XX:PermSize=128m -XX:MaxPermSize=256m
     ```

   - If BEA JRockit JVM is used:

     ```
     set MEM_ARGS=-Xms1280m -Xmx1280m
     ```

   For UNIX, locate the line that starts with the following:

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

   Add either of the following lines just before it:

   - If Sun JVM is used:

     ```
     MEM_ARGS="-Xms1280m -Xmx1280m -XX:PermSize=128m -XX:MaxPermSize=256m"
     export MEM_ARGS
     ```

   - If BEA JRockit JVM is used:

     ```
     MEM_ARGS="-Xms1280m -Xmx1280m"
     export MEM_ARGS
     ```

6. If BEA JRockit JVM is being used, add the -XnoOpt option to the existing JAVA_OPTIONS. This option turns off adaptive optimization and is required for stable Oracle Identity Manager operation.

   For Microsoft Windows, locate the line that starts with the following:

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

   Add the following line just before it:

   ```
   set JAVA_OPTIONS=%JAVA_OPTIONS% -XnoOpt
   ```

For UNIX, locate the line that starts with the following:

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

Add the following line just before it:

```
JAVA_OPTIONS="$JAVA_OPTIONS -XnoOpt"
export JAVA_OPTIONS
```

7. Save and close the file.
8. In a text editor, open the following files and change the JAVA_HOME and JAVA_VENDOR variables to point to the newly installed JDK directory:
   - *BEA_HOME*/weblogic81/common/bin/commEnv.cmd or commEnv.sh
   - *BEA_HOME*/weblogic81/server/bin/ant.bat or ant.sh
   - *BEA_HOME*/user_projects/domains/*NAME_OF_DOMAIN_DIRECTORY*/setEnv.cmd or setEnv.sh
   - *BEA_HOME*/user_projects/domains/*NAME_OF_DOMAIN_DIRECTORY*/startWebLogic.cmd or startWebLogic.sh

   Rename the jdk1.4.2_11 directory used for release 9.0.1.5 to OLD_jdk1.4.2_11 or LEGACY_jdk1.4.2_11 to avoid confusion when running and troubleshooting the upgrade scripts.
9. Edit the scripts specific to your operating system in the *OIM_HOME*/xellerate/setup/ directory as listed in Table 3–3.

Table 3–3 WebLogic Upgrade Patch Scripts and Parameters to Edit

Operating System	Script to Edit	Parameter to Edit
Microsoft Windows	patch_weblogic.cmd	■ Replace @loc with the path to the Oracle Identity Manager installation directory. ■ Replace @bea_home with the path to the WebLogic installation directory. ■ Replace @java_loc with the path to the Java installation directory.
	UpgradeAttestation.bat	Replace @java_home with the path to the Java installation directory.
Linux	patch_weblogic.sh	■ Replace @loc with the path to the Oracle Identity Manager installation directory. ■ Replace @bea_home with the path to the WebLogic installation directory ■ Replace @java_loc with the path to the Java installation directory.
	UpgradeAttestation.sh	■ Replace @java_home with the path to the Java installation directory. ■ Replace @loc with the path to the Oracle Identity Manager installation.

10. Edit the spml_weblogic script specific to your operating system in the *OIM_HOME*/xellerate/setup/ directory. Edit spml_weblogic.cmd for Microsoft Windows and spml_weblogic.sh for UNIX.

    For upgrade from release 9.0.1.5:

- Replace @loc with the path to the Oracle Identity Manager installation directory.
- Replace @bea_home with the path to the Weblogic Server installation directory.
- Replace @java_loc with the path to the Java installation directory.

11. Delete the *OIM_HOME*/xellerate/webapp/precompiled/ directory.
12. Start BEA WebLogic Server.

    Note: For a cluster installation, before proceeding, ensure that the following fields and values are set on the Remote Start tab for all Managed Servers:

    - Java Home
    - BEA Home

    Ensure that the Listen Address field on the Configuration tab for all Managed Servers contains the Host Address.

13. Copy the *PATCH*/xellerate/ext/ojdbc14.jar file to the *BEA_HOME*/weblogic81/server/lib/ directory. If the file already exists, then overwrite it.

    Note: For a clustered installation, copy the ojdbc14.jar file to the *BEA_HOME*/weblogic81/server/lib/ directory on all cluster participants including the Admin Server, and overwrite the existing files if necessary.

14. For upgrading attestation, see Appendix H, "Attestation Upgrade Utility". This is a mandatory step.
15. Run one of the following patch_weblogic scripts on the application server:

    Note: Before running the patch scripts, ensure that the application server is in running state.

    Microsoft Windows:

    Run *OIM_HOME*\xellerate\setup\patch_weblogic.cmd by using the WebLogic administrator password and the Oracle Identity Manager database user password as command arguments, for example:

    ```
    OIM_HOME\xellerate\setup\patch_weblogic.cmd WEBLOGIC_ADMIN_PASSWORD OIM
    DATABASE_USER_PASSWORD
    ```

    UNIX:

    Run *OIM_HOME*/xellerate/setup/patch_weblogic.sh by using the WebLogic administrator password and the Oracle Identity Manager database user password as command arguments, for example:

    ```
    $ OIM_HOME/xellerate/setup/patch_weblogic.sh -WEBLOGIC_ADMIN_PASSWORD -OIM
    DATABASE_USER_PASSWORD
    ```

16. Select **Security**, **Realms**, **myrealm**, **Providers**, and **Authentication** in the order specified.
17. Delete the XellerateAuthenticator.
18. Shut down BEA WebLogic Server gracefully.

> **Note:** For a clustered installation, stop the cluster by right-clicking the name of the cluster, and then selecting the **Start/Stop this cluster** option. Shut down all Managed Servers by selecting the **Graceful Shutdown of all Managed Servers** option in the right pane.

19. Copy *OIM_HOME*/xellerate/lib/wlXLSecurityProviders.jar to the *BEA_HOME*/weblogic81/server/lib/mbeantypes/ directory.
20. Start BEA WebLogic Server.
21. Select **Security**, **Realms**, **myrealm**, **Providers**, and then **Authentication**. Then select **Configure a new OIMAuthenticator** and create a OIMAuthenticator with the SUFFICIENT Control Flag.
22. Shut down BEA WebLogic Server gracefully.
23. Start BEA WebLogic Server.

> **Note:** For a clustered installation:
>
> 1. Copy the *OIM_HOME* directory from the WebLogic Admin Server to all Managed Servers by maintaining the same directory structure.
> 2. Copy *OIM_HOME*/xellerate/lib/wlXLSecurityProviders.jar to the *BEA_HOME*/weblogic81/server/lib/mbeantypes/ directory on all Managed Servers in the cluster. If the file already exists, then overwrite it.
> 3. Copy *OIM_HOME*/xellerate/lib/nexaweb-common.jar to the *BEA_HOME*/weblogic81/server/lib/ directory on all Managed Servers in the cluster by overwriting the existing files if necessary.
> 4. Start the WebLogic Admin server, and then start the Managed Servers.

24. Run the Re-Issue Audit Message Task scheduled task to ensure that all the pending audit messages in the aud_jms table are processed.

> **Note:** While running the Re-Issue Audit Message Task scheduled task, ensure that the database and the server are upgraded. If you are running the scheduled task by using the Design Console, then make sure that the Design Console has also been upgraded.

3.4.1 Redeploying SPML Web Service

If you are using SPML Web service in the existing Oracle Identity Manager setup, then you must redeploy the SPML Web service whenever the setup is upgraded.

> **See Also:** The "SPML Web Service" section in *Oracle Identity Manager Tools Reference*

3.5 Migrating Custom Java Code

You can migrate the custom Java code from release 9.0.1.5 environment into the new release 9.1.0 environment. Before you migrate the custom Java code from the release 9.0.1.5 environment, you must first recompile the custom code by using the release 9.1.0 libraries located in the *OIM_HOME*/xellerate/lib/ directory.

Using the integrated development environment that was originally used to compile the release 9.0.1.5 custom Java code, which are Eclipse, JDeveloper, WASD or command-line javac, recompile all custom Java code by using the release 9.1.0 libraries.

The following is a list of the custom items you can migrate from release 9.0.1.5 and reuse in release 9.1.0 after recompiling.

> **Note:** For clustered environments, after recompiling the following items by using the release 9.1.0 libraries, copy them to each participant node of the cluster.

- Custom Java libraries bound to functional Oracle Identity Manager release 9.0.1.5 adapters recompiled by using release 9.1.0 libraries.

  You must copy the recompiled custom Java libraries in the *OIM_HOME*/xellerate/JavaTasks/ directory of release 9.0.1.5 to the *OIM_HOME*/xellerate/JavaTasks/ directory of release 9.0.1. In addition, you must copy the recompiled custom Java libraries in the *OIM_RM_HOME*/xellerate/JavaTasks/ directory of release 9.0.1.5 to the *OIM_RM_HOME*/xellerate/JavaTasks/ directory of release 9.1.0.

- Custom scheduled tasks recompiled by using release 9.1.0 libraries.

  You must copy the recompiled custom event handlers to the *OIM_HOME*/xellerate/ScheduleTask/ directory of release 9.1.0.

  > **Note:** If you want to see the built-in scheduled task on the Administrative and User Console, then copy the xlScheduler.jar file from the *OIM_HOME*/lib directory to the *OIM_HOME*/xellerate/ScheduledTask directory. If the ScheduledTask directory does not exist, then create it.

- Custom event handlers recompiled by using release 9.1.0 libraries.

  You must copy the recompiled custom scheduled tasks to the *OIM_HOME*/xellerate/EventHandlers/ directory of release 9.1.0.

- Connector Resource bundles by copying the *OIM_HOME*/xellerate/connectorResources/ directory of release 9.0.1.5 to the *OIM_HOME*/xellerate/connectorResources/ directory release 9.1.0.

- Custom Resources by copying the *OIM_HOME*/xellerate/customResources/ directory release 9.0.1.5 to the *OIM_HOME*/xellerate/customResources/ directory of release 9.1.0.

- Custom Administrative and User Console deployments. Several Administrative and User Console files are modified in release 9.1.0. If you customized your release 9.0.1.5 Administrative and User Console, that is, you made changes to the default Administrative and User Console that shipped with release 9.0.1.5, then you must

add your customizations to the new release 9.1.0 Administrative and User Console files.

3.6 Postupgrade Configuration

The following postupgrade configuration procedures are required if you are upgrading from an Oracle Identity Manager release 9.0.1.5 installation without the Oracle Identity Manager Audit and Compliance module to an Oracle Identity Manager release 9.1.0 installation with the Auditing and Compliance module:

- Setting the User Profile Audit Level
- Generating User Snapshots
- Generating GPA Snapshots
- Loading Data for Exception-Based Reporting

3.6.1 Setting the User Profile Audit Level

To set the user profile audit level:

1. Define a secondary data source for reporting, if required.

   Refer to *Oracle Identity Manager Audit Report Developer's Guide* for more information about defining a secondary data source.

2. Start the application server on which the Oracle Identity Manager installation is running.
3. Set the audit level. The permissible values are (in descending order):
   - Process Task
   - Resource Form
   - Resource
   - Membership
   - Core
   - None
4. To specify an audit level by performing the following steps:
   a. Log on to the Design Console as an administrator.
   b. Navigate to the System Configuration form.
   c. Locate XL.UserProfileAuditDataCollection and set its value to `Resource Form` or the appropriate audit level as listed in step 3 of this procedure.
5. To collect user profile audit data in the secondary reporting data store, complete the following steps:
   a. Log on to the Design Console as an administrator.
   b. Navigate to the System Configuration form.
   c. Locate XL.UserProfileAuditInSecondaryDS and set its value to `TRUE`.

3.6.2 Generating User Snapshots

For detailed information about generating user snapshots, see Appendix E, "Generating User Snapshots".

3.6.3 Generating GPA Snapshots

For detailed information about generating GPA snapshots, see Appendix G, "Generating GPA Snapshots".

3.6.4 Loading Data for Exception-Based Reporting

To load data for exception-based reporting, run the UPA Form Data Upgrade utility. For information about the UPA Form Data Upgrade utility, see Appendix F, "UPA Form Data Upgrade Utility".

3.7 Upgrading the Diagnostic Dashboard

To upgrade the existing release 9.0.1.5 Diagnostic Dashboard XIMDD application to the release 9.1.0 Diagnostic Dashboard on BEA WebLogic Server:

1. Remove the existing XIMDD application by using the WebLogic Administrative Console.
2. Install a new instance of the XIMDD application by using the Release 9.1.0 (9.0.1.5 Upgrade) XIMDD.war file in the *PATCH*/DiagnosticDashboard/ directory.

> **See Also:** The "Installing the Diagnostic Dashboard" section in the "Working with the Diagnostic Dashboard" chapter in the *Oracle Identity Manager Administrative and User Console Guide* for complete steps on how to install the Diagnostic Dashboard on the application server

4

Upgrading to Release 9.1.0 (9.0.1.5 Upgrade) on IBM WebSphere Application Server

This chapter explains how to upgrade to release 9.1.0 from release 9.0.1.5 on IBM WebSphere Application Server. Do not attempt to upgrade to release 9.1.0 from any other previous Oracle Identity Manager release.

> **Note:** You can upgrade the existing database and then perform a new installation of Oracle Identity Manager release 9.1.0.
>
> For information about installing Oracle Identity Manager, refer to *Oracle Identity Manager Installation and Configuration Guide for IBM WebSphere Application Server*.

Extract the contents of the release 9.1.0 upgrade package to a temporary directory on your existing release 9.0.1.5 system.

The following steps explain how to upgrade from Oracle Identity Manager release 9.0.1.5 to release 9.1.0 on IBM WebSphere Application Server:

1. Creating a backup of the Existing Deployment
2. Upgrading the Oracle Identity Manager Database
3. Installing and Upgrading to WebSphere 6.1.0.9
4. Installing Release 9.1.0 By Using the Oracle Identity Manager Installer
5. Running the Re-Issue Audit Message Task Scheduled Task
6. Postupgrade Configuration
7. Migrating Custom Java Code
8. Upgrading the Diagnostic Dashboard

4.1 Creating a backup of the Existing Deployment

The first step for upgrading to release 9.1.0 is to create a backup of your existing release 9.0.1.5 deployment to ensure that no data is lost during the upgrade process. If the upgrade fails, then you can use this backup to restore the release 9.0.1.5 deployment to its original state.

Create a backup of the following:

- Oracle Identity Manager

Create a backup of the *OIM_HOME* directory in which you have installed Oracle Identity Manager.

- Oracle Identity Manager Design Console

  Create a backup of the *OIM_DC_HOME* directory in which you have installed the Oracle Identity Manager Design Console.

- Oracle Identity Manager Remote Manager

  Create a backup of the *OIM_RM_HOME* directory in which you have installed the Oracle Identity Manager Remote Manager.

- Database used for release 9.0.1.5

  Follow the procedures in this section to install release 9.1.0 if you are upgrading to IBM WebSphere Application Server v6.1.0.9.

4.2 Upgrading the Oracle Identity Manager Database

For details about upgrading the Oracle Identity Manager database, refer to Chapter 5, "Upgrading the Oracle Identity Manager Database".

4.3 Installing and Upgrading to WebSphere 6.1.0.9

Release 9.1.0 is certified on IBM WebSphere Application Server v6.1.0.9. Install or upgrade to IBM WebSphere Application Server v6.1.0.9 before upgrading to Oracle Identity Manager release 9.1.0.

Ensure that you upgrade the WebSphere client to 6.1.0.9 for the release 9.1.0 Design Console.

Note: For a clustered installation of IBM WebSphere Application Server, you must upgrade the Network Deployment Manager and all Node Managers to IBM WebSphere Application Server v6.1.0.9.

Refer to the IBM WebSphere Application Server documentation for details on upgrading to IBM WebSphere Application Server v6.1.0.9. For setting up WebSphere, see the *Oracle Identity Manager Installation and Configuration Guide for IBM WebSphere Application Server*.

Do not install Oracle Identity Manager before upgrading the database as mentioned in the following pages.

Note: When upgrading to IBM WebSphere Application Server v6.1.0.9, review the information about IBM WebSphere Application Server Daylight Savings Time Changes for the United States. Also ensure that you install the JDK upgrade as appropriate for the 6.1.0.9 release. Note that this is different from the WebSphere 6.1.0.0 to WebSphere 6.1.0.9 upgrade.

Go to the IBM support and downloads Web site at the following URL:

`http://www.ibm.com/support/us/`

To install release 9.1.0:

1. Install IBM WebSphere Application Server and upgrade it to release 6.1.0.9.

2. Install release 9.1.0.
3. Copy UpgradeAttestation.bat from *PATCH*/xellerate/setup/ to *OIM_HOME*/xellerate/setup/.
4. For upgrading attestation, see Appendix H, "Attestation Upgrade Utility".

4.4 Installing Release 9.1.0 By Using the Oracle Identity Manager Installer

This section discusses the steps involved in installing or upgrading Oracle Identity Manager components. It consists of the following topics:

- Installing Oracle Identity Manager
- Installing the Design Console
- Installing the Remote Manager

4.4.1 Installing Oracle Identity Manager

For details on installing Oracle Identity Manager, refer to the *Oracle Identity Manager Installation and Configuration Guide for IBM WebSphere Application Server*.

Note: When installing release 9.1.0, ensure that you point to the existing database you upgraded to release 9.1.0 on the Database Server Selection screen in the installer program. Enter the information for the database that you upgraded to release 9.1.0 in the following fields on the Database Server Selection screen:

- Host
- Port
- Database SID
- User Name
- Password

When Oracle Identity Manager is installed on an existing database, the .xldatabasekey file from the existing Oracle Identity Manager installation must be copied to the new *OIM_HOME*/xellerate/config/ directory. Create the /config directory in the new *OIM_HOME*/xellerate/ path if it does not already exist.

4.4.1.1 Multiple JMS Queues

Previously, Oracle Identity Manager used a single JMS queue (named xlQueue) for all asynchronous operations including requests, reconciliation, attestation, and offline tasks. In release 9.1.0, by default, Oracle Identity Manager uses separate JMS queues for specific operations to optimize JMS queue processing. The following is a list of the default JMS queue configurations and their related operations:

- xlQueue for request operations
- xlReconQueue for reconciliation operations
- xlAuditQueue for auditing operations
- xlAttestationQueue for Attestation operations
- xlProcessQueue for usage in future Oracle Identity Manager releases

By default, multiple JMS queues are configured in Oracle Identity Manager release 9.1.0.

4.4.2 Installing the Design Console

Refer to the "Installing and Configuring the Oracle Identity Manager Design Console" section in the *Oracle Identity Manager Installation and Configuration Guide for IBM WebSphere Application Server* for the steps to install the Design Console on the application server.

4.4.3 Installing the Remote Manager

Refer to the section "Installing and Configuring the Oracle Identity Manager Remote Manager" of the *Oracle Identity Manager Administrative and User Console Guide* for the steps to install the Remote Manager on the application server.

4.5 Running the Re-Issue Audit Message Task Scheduled Task

Start the server and run the Re-Issue Audit Message Task scheduled task to ensure that all the pending audit messages in the aud_jms table are processed.

Note: While running the Re-Issue Audit Message Task scheduled task, ensure that the database and server is upgraded. If you are running the scheduled task by using the Design Console, then make sure that the Design Console has also been upgraded.

4.6 Postupgrade Configuration

The following postupgrade configuration procedures are required if you are upgrading an Oracle Identity Manager release 9.0.1.5 installation without the Oracle Identity Manager Audit and Compliance module to an Oracle Identity Manager release 9.1.0 installation with the Auditing and Compliance module:

- Setting the User Profile Audit Level
- Generating User Snapshots
- Generating GPA Snapshots
- Loading Data for Exception-Based Reporting

4.6.1 Setting the User Profile Audit Level

To set the user profile audit level:

1. Define a secondary data source for reporting, if required.

   See Also: *Oracle Identity Manager Audit Report Developer's Guide* for information about defining a secondary data source

2. Start the application server on which the Oracle Identity Manager installation is running.
3. Set the audit level. The permissible values are (in descending order):
   - Process Task
   - Resource Form

- Resource
- Membership
- Core
- None

4. To specify an audit level, perform the following steps:
   a. Log in to the Design Console as an administrator.
   b. Navigate to the System Configuration form.
   c. Locate XL.UserProfileAuditDataCollection and set its value to `Resource Form` or the appropriate audit level as listed in step 3 of this procedure.
5. To collect user profile audit data in the secondary reporting data store, perform the following steps:
   a. Log in to the Design Console as an administrator.
   b. Navigate to the System Configuration form.
   c. Locate XL.UserProfileAuditInSecondaryDS and set its value to `TRUE`.

4.6.2 Generating User Snapshots

For detailed information about generating user snapshots, see Appendix E, "Generating User Snapshots".

4.6.3 Generating GPA Snapshots

For detailed information about generating GPA snapshots, see Appendix G, "Generating GPA Snapshots".

4.6.4 Loading Data for Exception-Based Reporting

To load data for exception-based reporting, run the UPA Form Data Upgrade utility. For information about the UPA Form Data Upgrade utility, see Appendix F, "UPA Form Data Upgrade Utility".

4.7 Migrating Custom Java Code

You can migrate the custom Java code from the release 9.0.1.5 environment into the new release 9.1.0 environment. Before you migrate the custom Java code from the release 9.0.1.5 environment, you must first recompile it by using the release 9.1.0 libraries located in the *OIM_HOME*/xellerate/lib/ directory.

Using the integrated development environment that was originally used compile the release 9.0.1.5 custom Java code, which are Eclipse, JDeveloper, WASD or command-line javac, recompile all custom Java code by using the release 9.1.0 libraries.

The following is a list of the custom items you can migrate from release 9.0.1.5 and reuse in release 9.1.0 after recompiling by using the release 9.1.0 libraries.

Note: For clustered environments, after recompiling the following items by using the release 9.1.0 libraries, copy them to each participant node of the cluster.

- Custom Java libraries bound to functional Oracle Identity Manager release 9.0.1.5 adapters recompiled by using release 9.1.0 libraries.

  You must copy the recompiled custom Java libraries in the *OIM_HOME*/xellerate/JavaTasks/ directory of release 9.0.1.5 to the *OIM_HOME*/xellerate/JavaTasks/ directory of release 9.1.0. You must copy the recompiled custom Java libraries in the *OIM_RM_HOME*/xellerate/JavaTasks/ directory of release 9.0.1.5 to the *OIM_RM_HOME*/xellerate/JavaTasks/ directory of release 9.1.0.

- Custom scheduled tasks recompiled by using release 9.1.0 libraries.

  You must copy the recompiled custom event handlers to the *OIM_HOME*/xellerate/ScheduleTask/ directory release 9.1.0.

  Note: If you want to see the built-in scheduled task on the Administrative and User Console, then copy the xlScheduler.jar file from the *OIM_HOME*/lib directory to the *OIM_HOME*/xellerate/ScheduledTask directory. If the ScheduledTask directory does not exist, then create it.

- Custom event handlers recompiled by using release 9.1.0 libraries.

  You must copy the recompiled custom scheduled tasks to the *OIM_HOME*/xellerate/EventHandlers/ directory of release 9.1.0.

- Connector resource bundles by copying the *OIM_HOME*/xellerate/connectorResources/ directory of release 9.0.1.5 to the *OIM_HOME*/xellerate/connectorResources/ directory of release 9.1.0.

- Custom resources by copying the *OIM_HOME*/xellerate/customResources/ directory of release 9.0.1.5 to the *OIM_HOME*/xellerate/customResources/ directory of release 9.1.0.

- Custom Administrative and User Console deployments. Several Administrative and User Console files are modified in release 9.1.0. If you customized your release 9.0.1.5 Administrative and User Console, that is, you made changes to the default Administrative and User Console that shipped with release 9.0.1.5, then you must add your customizations into the new release 9.1.0 Administrative and User Console files.

4.8 Upgrading the Diagnostic Dashboard

See the "Installing the Diagnostic Dashboard" section in the *Oracle Identity Manager Installation and Configuration Guide for IBM WebSphere Application Server* for the steps to install the Diagnostic Dashboard on the application server.

5

Upgrading the Oracle Identity Manager Database

Before you upgrade your database, perform the following steps:

1. Extract the contents of the Oracle Identity Manager release 9.1.0 upgrade package to a temporary directory on the computer on which the database is installed.

   This guide refers to this temporary directory as *PATCH*.

2. Enable execute permissions on the scripts in the *PATCH* directory.

3. Choose one of the following approaches to upgrade the database used by the Oracle Identity Manager release 9.0.1.5 deployment:

   - Perform an upgrade of the existing database configured for release 9.0.1.5.

     For details, see "Upgrading an Existing Database Instance In-Place" on page 5-1.

   - Create a new instance of the database for release 9.1.0, and then import the data used by your release 9.0.1.5 deployment into the new database and perform the upgrade.

     For details, see "Creating a New Database Instance for the Upgrade" on page 5-4.

5.1 Upgrading an Existing Database Instance In-Place

Perform the following steps to upgrade your existing release 9.0.1.5 database instance to release 9.1.0:

1. Create a backup of your existing database.

   Use the export/backup utilities provided with the database 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 Identity Manager release 9.0.1.5 database instance to ensure that the database can be restored to its original state, if required.

2. Upgrade your database schema from release 9.0.1.5 to release 9.1.0 by using one of the following scripts appropriate for your database and operating system. Run the script on the computer on which the database is installed.

   For **Oracle Database on UNIX**:

a. To upgrade the database schema, run the *PATCH*/db/oracle/Scripts/oim_db_upg_9015_to_9100.sh script on the computer on which the database for release 9.0.1.5 is installed.

b. Enter the required information for the Oracle database when prompted by the script.

For **Oracle Database on Microsoft Windows:**

To upgrade the database schema, run the *PATCH*\db\oracle\Scripts\oim_db_upg_9015_to_9100.bat batch script on the system on which the release 9.0.1.5 database is installed.

The command-line usage for the Oracle oim_db_upg_9015_to_9100 script is:

```
oim_db_upg_9015_to_9100.bat ORACLE_SID ORACLE_HOME
ORACLE_IDENTITY_MANAGER_DB_USER_NAME ORACLE_IDENTITY_MANAGER_DB_USER_PASSWORD
DIRECTORY_IN_WHICH_DB_UPGRADE_ZIP_FILE_IS_EXTRACTED
```

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

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

   For Oracle Database:

   a. Log in to SQL *Plus with the credentials of the Oracle Identity Manager release 9.0.1.5 database schema owner.

   b. Run the *PATCH*/db/oracle/Scripts/Oracle_Enable_XACM.sql script.

4. 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 Oracle Identity Manager host computer, load Oracle Identity Manager metadata into your database by running one of the following commands:

   If Oracle Identity Manager is installed without the Audit and Compliance module, then:

   - For Microsoft Windows, run the following file:

     ```
     PATCH\db\Utilities\LoadXML.bat
     ```

   - For UNIX, run the following script:

     ```
     PATCH/db/Utilities/LoadXML.sh
     ```

   If Oracle Identity Manager is installed with the Audit and Compliance module, then:

   - For Microsoft Windows, run the following file:

     ```
     PATCH\db\Utilities\LoadXML_XACM.bat
     ```

   - For UNIX, run the following script:

     ```
     PATCH/db/Utilities/LoadXML_XACM.sh
     ```

See Also: Appendix A, "Loading Report Metadata Into the Database" for more information about running the LoadXML or LoadXML_XACM script

5. The e-mail definition templates must be loaded into the database. As appropriate for the operating system on the Oracle Identity Manager host computer, load Oracle Identity Manager e-mail templates into your database by running one of the following commands:

   For Microsoft Windows:

   Run *PATCH*\db\Utilities\LoadXLIF.bat

   For UNIX:

   Run *PATCH*/db/Utilities/LoadXLIF.sh

   Note: Running LoadXLIF.bat or LoadXLIF.sh only inserts the newly added e-mail templates, and does not update the existing e-mail templates. Therefore, if you want to update the existing templates, then delete all the entries from the EMD table and run LoadXLIF.bat or LoadXLIF.sh.

   See Also: "Loading E-Mail Templates into the Database" on page 5-5 for more information about running the LoadXLIF script

5.1.1 Using Oracle Identity Manager Database Validator

While performing an upgrade, you can use the Oracle Identity Manager Database Validator utility to compare database objects. The Database Validator is a command-line interface (CLI) utility that compares objects of two databases. The utility generates a report of the missing and mismatched objects in the destination database. You can also use this utility to verify an upgrade that you might install.

See Also: Appendix B, "Oracle Identity Manager Database Validator" for more information about the Database Validator

5.1.2 Using Reconciliation Archival

The purpose of the Reconciliation Archival utility is to archive data from active reconciliation tables to archival reconciliation tables and to delete data from active and archival reconciliation tables. See Appendix C, "Reconciliation Archival" for more details.

See Also: *Oracle Identity Manager Best Practices Guide* for information about running the Reconciliation Archival utility

5.1.3 Using Task Archival

The purpose of the Task Archival utility is to archive data from active task tables to archival task tables and to delete data from active task tables. See Appendix D, "Task Archival" for more details.

See Also: *Oracle Identity Manager Best Practices Guide* for information about running the Task Archival utility

5.2 Creating a New Database Instance for the Upgrade

You can create a new database instance, and then upgrade it to the database schema for Oracle Identity Manager release 9.1.0. This method ensures that your current working database remains available if a rollback is required. Perform the following steps for creating a new, upgraded database instance:

1. Use the export/backup utilities provided with the database 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 Identity Manager release 9.0.1.5 database instance. If the upgrade fails, then this backup can be used to restore the database to its original state.

2. Create a new database by referring to the database vendor's documentation and Oracle Identity Manager Installation and Configuration Guide specific to your application server.

   Note: If you create a new database, then you must specify the same login credentials for the new database as used for the original database instance.

3. Using the import utility provided by the database, import the data you exported from the original database into the newly created database. This creates an exact copy of the original database instance.

4. Upgrade the database schema from Oracle Identity Manager release 9.0.1.5 to release 9.1.0 by using one of the following scripts appropriate for your database and operating system. Ensure that you run the script on the computer in which the database is stored.

   For Oracle Database running on UNIX:

   Run the following script on the new release 9.1.0 database system and enter the appropriate information when prompted to upgrade the database schema:

   To upgrade from release 9.0.1.5:

   PATCH/db/oracle/Scripts/oim_db_upg_9015_to_9100.sh

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

   For Oracle Database running on Microsoft Windows:

   Run the following batch script on the new release 9.1.0 database system to upgrade the database schema:

   To upgrade from release 9.0.1.5:

   PATCH/db/oracle/Scripts/oim_db_upg_9015_to_9100.bat

   The following is the command-line usage for the Oracle oim_db_upg_9015_to_9100.bat file:

   oim_db_upg_9015_to_9100.bat *ORACLE_SID ORACLE_HOME ORACLE_OIM_USER ORACLE_OIM_USER_PWD UPGRADE_FOLDER*

5. Perform the following steps appropriate for the database to upgrade the Oracle Identity Manager Audit and Compliance module:

   a. Log in to SQL *Plus with the credentials of the Oracle Identity Manager release 9.0.1.5 database schema owner.

   b. Run the *PATCH*/db/oracle/Scripts/Oracle_Enable_XACM.sql script.

6. The user profile auditing feature and the reports feature require that certain metadata be loaded to the database. As appropriate for the operating system on the Oracle Identity Manager host computer, load Oracle Identity Manager metadata to the database by running one of the following commands:

   If Oracle Identity Manager is installed without the Audit and Compliance module, then:

   - For Microsoft Windows, run the following file:

     ```
     PATCH\db\Utilities\LoadXML.bat
     ```

   - For UNIX, run the following script:

     ```
     PATCH/db/Utilities/LoadXML.sh
     ```

   If Oracle Identity Manager is installed with the Audit and Compliance module, then:

   - For Microsoft Windows, run the following file:

     ```
     PATCH\db\Utilities\LoadXML_XACM.bat
     ```

   - For UNIX, run the following script:

     ```
     PATCH/db/Utilities/LoadXML_XACM.sh
     ```

   See Also: Appendix A, "Loading Report Metadata Into the Database" for more information about running the LoadXML or LoadXML_XACM script

7. The e-mail definition templates must be loaded into the database. As appropriate for the operating system on the Oracle Identity Manager host computer, load Oracle Identity Manager e-mail templates into the database by running one of the following commands:

   For Microsoft Windows:

   Run *PATCH*\db\Utilities\LoadXLIF.bat

   For UNIX:

   Run *PATCH*/db/Utilities/LoadXLIF.sh

   See Also: "Loading E-Mail Templates into the Database" on page 5-5 for more information about running the LoadXLIF script

5.3 Loading E-Mail Templates into the Database

You must load e-mail templates into your database. To do so:

1. As appropriate for the operating system on the Oracle Identity Manager host computer, open either LoadXLIF.bat or LoadXLIF.sh located in the *PATCH*/db/Utilities/ directory, and update the JAVA_HOME variable.

Note:

- For upgrade from release 9.0.1.5 to release 9.1.0, the location is *PATCH*/db/Utilities/.
- The xlUtils.jar file is in the *PATCH*/db/Utilities/ directory. Do not copy this JAR to the *OIM_HOME*/lib/ directory.

2. Run LoadXLIF to populate the e-mail template for Default English Email Templates.

Note: If your database supports languages other than English according to globalization support guidelines of Oracle Identity Manager release 9.1.0, then edit the XLIFsequence.properties file located at *PATCH*/db/Utilities/xliff/ to include e-mail templates for that language. You must refer to the XML file corresponding to your locale. The XML file name is xlif_*locale*.xml. For example, for French, you include xlif_fr.xml.

3. As appropriate for the database and operating system on the Oracle Identity Manager host computer, perform the following steps:

   a. **For Oracle Database on Microsoft Windows:**

   In a text editor, open LoadXLIF.bat, and uncomment the following line:

   ```
   REM SET ORACLE_DRIVER_DIR=
   ```

   Assign the path to the Oracle driver directory containing the Oracle JDBC drivers, as shown:

   ```
   SET ORACLE_DRIVER_DIR=PATH_TO_ORACLE_DRIVER
   ```

   For Oracle Database on UNIX:

   In a text editor, open LoadXLIF.sh and uncomment the following lines:

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

   Assign the path to the JDBC driver for Oracle, as shown:

   ```
   ORACLE_DRIVER_DIR=PATH_TO_ORACLE_DRIVER
   export ORACLE_DRIVER_DIR
   ```

   b. In the command prompt, run the *PATCH*/db/Utilities/LoadXLIF.bat or LoadXLIF.sh script.

   The command-line usage of the LoadXLIF script for Oracle Database is as shown:

   ```
   LoadXLIF JDBC_URL DB_USERNAME DB_PASSWORD AUDIT_ON_OFF
   ```

   When you run the LoadXLIF command:

   – Replace *JDBC_URL* with the JDBC URL, for example, jdbc:oracle:thin:@*DB_HOST_IP*:*PORT*:*SID*.

   – Replace *DB_USERNAME* with the database user name.

- Replace *DB_PASSWORD* with the database password.
- Replace *AUDIT_ON_OFF* with `True` if Oracle Identity Manager is installed with the Audit and Compliance Module. Otherwise, specify `False`.

A

Loading Report Metadata Into the Database

You must load the metadata into the database by running the LoadXML or LoadXML_XACM utilities. The utility must be run after running oim_db_upg_9015_to_9100.bat or oim_db_upg_9015_to_9100.sh.

To load metadata into the database:

1. As appropriate for the operating system on the Oracle Identity Manager host computer, open either LoadXML.bat or LoadXML.sh (LoadXML_XACM.bat or LoadXML_XACM.sh) located in the *PATCH*/db/Utilities/ directory, and set the JAVA_HOME variable to the directory on which Java is installed..

   Note: Run the LoadXML script if Oracle Identity Manager is installed without the Audit and Compliance module, and run the LoadXML_XACM script if Oracle Identity Manager is installed with the Audit and Compliance module.

2. As appropriate for the database and operating system of the computer hosting Oracle Identity Manager, perform one of the following steps:

   For Oracle Database on Microsoft Windows:

   a. In a text editor, open LoadXML.bat (or LoadXML_XACM.bat), and uncomment the following line:

      ```
      REM SET ORACLE_DRIVER_DIR=
      ```

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

      ```
      SET ORACLE_DRIVER_DIR=PATH_TO_ORACLE_DRIVER
      ```

   For Oracle Database on UNIX:

   a. In a text editor, open LoadXML.sh (or LoadXML_XACM.sh), and uncomment the following lines:

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

   b. Assign the path to the JDBC driver for Oracle, as shown:

      ```
      ORACLE_DRIVER_DIR=PATH_TO_ORACLE_DRIVER
      export ORACLE_DRIVER_DIR
      ```

3. From a command prompt, run the *PATCH*/db/Utilities/LoadXML.bat or LoadXML.sh script (LoadXML_XACM.bat or LoadXML_XACM.sh script if you are using Oracle Identity Manager with the Audit and Compliance Module).

   The command-line usage of the LoadXML script for Oracle Database is as shown:

   ```
   LoadXML JDBC_URL DB_USERNAME DB_PASSWORD
   ```

   When you run the LoadXML command:

   - Replace *JDBC_URL* with the JDBC URL, for example, jdbc:oracle:thin:@*DB_HOST_IP*:*PORT*:*SID*.
   - Replace *DB_USERNAME* with the database user name.
   - Replace *DB_PASSWORD* with the database password.

B

Oracle Identity Manager Database Validator

The Oracle Identity Manager Database Validator is a command-line interface (CLI) utility that compares objects of two databases and generates a report of the missing and mismatched objects in the destination database.

You can also use this utility to verify an upgrade that you perform.

B.1 Introduction

The Oracle Identity Manager Database Validator compares objects of a standard Oracle Identity Manager schema or a customized Oracle Identity Manager database (source) with a destination database that you specify.

The utility gathers source database details in a table. This information is the standard for comparison. For Oracle Database, the information is saved in a file that is created by the database export utility.

In upgrade scenarios, you can use this utility to verify an upgrade that you perform. You can compare the upgraded Oracle Identity Manager database with the provided standard dump (as source dump). This is to verify the success of Oracle Identity Manager database upgrade after the upgrade patch is applied.

Scenario: You upgrade your Oracle Identity Manager installation from release x.x.1 to release x.x.2 by using a standard upgrade package. Oracle Identity Manager Database Validator identifies the missing and mismatched objects, if any, after the upgrade has been completed.

B.2 Location and Components

The Oracle Identity Manager Database Validator files are at the following location:

Oracle Database

PATCH\db\oracle\Utilities\OIMDBValidator

All Oracle Identity Manager Database Validator files are located in the OIMDBValidator directory.

Table B–1 provides details of the files that are part of the Oracle Identity Manager Database Validator.

Table B–1 Files of the Oracle Identity Manager Database Validator

File	Description
oim_ddl_create_oim_src_db.sql	Creates the oim_src_db table.

Table B–1 (Cont.) Files of the Oracle Identity Manager Database Validator

File	Description
oim_dml_populate_oim_src_db.sql	Populates the oim_src_db table with metadata details.
oim_dml_src_do_counts.sql	Takes the row count of Oracle Identity Manager standard tables. This file is optional and is based on your inputs.
If Source is a standard database, then: oim_std_src_db.dmp	If Source is a standard/vanilla database, then the standard dump file is named oim_std_src_db.dmp. For a successful standard vanilla installation, a standard dump accompanies the utility. This standard file for Oracle Database is available at the following location: *PATCH*\db\oracle\Utilities\OIMDBValidator\SrcInfo
If Source is a customized database, then: oim_src_db.dmp	You can opt to generate the dump file on your own. This file is created when you want to create a dump file from a source Oracle Identity Manager database of your choice. It is named oim_src_db.dmp, and for Oracle Database, it is available at the following location: *PATCH*\db\oracle\Utilities\OIMDBValidator\SrcInfo
oim_dml_check_oim_version.sql	Selects the version from the oim_src_db table and compares it with the version of the XSD table of the Destination Oracle Identity Manager schema.
oim_ddl_create_oim_dest_db.sql	Creates the oim_dest_db table in the destination Oracle Identity Manager database. This file is used to store the data dictionary information of Oracle Identity Manager.
oim_dml_populate_oim_dest_db.sql	Populates the oim_dest_db table with metadata details.
oim_dml_dest_do_counts.sql	Counts the number of records in the Oracle Identity Manager standard tables. This file is optional and is based on your input.
oim_db_compare.sql	This main comparison script creates a comparison report named COMPARISON_SUMMARY_*YYYY_MM_DD_HH_MM*.log that lists details of the missing or mismatched objects and the row count difference if any.
oim_ddl_drop_oim_src_dest_db.sql	Drops the tables that are created at the destination. This file is optional and is based on your input.
oim_db_validator.bat (Microsoft Windows) oim_db_validator.sh (UNIX and Linux)	Runs the utility.
oim_db_input.bat (Microsoft Windows) oim_db_input.sh (UNIX and Linux)	The oim_db_validator.bat file calls the oim_db_input.bat file to get the user input and validate the provided information. The oim_db_validator.sh file calls the oim_db_input.sh file to get the user input and validate the provided information.

B.3 Oracle Identity Manager Database Validator Functionality

To use the Database Validator utility, run the following script:

- On Microsoft Windows: oim_db_validator.bat
- On UNIX: oim_db_validator.sh

  After you run the script, a log file is generated with the following name:

  For Microsoft Windows:

  – If the utility runs without error: oim_db_validator_*YYYY_MM_DD_HH_MM*.log

  – In case of error: oim_db_validator_err_*YYYY_MM_DD_HH_MM*.log

  For UNIX:

  – If the utility runs without any error: oim_db_validator_*YYYY_MM_DD_HH_MM*.log

  – In case of any error: oim_db_validator_err_*YYYY_MM_DD_HH_MM*.log

Authentication

When you run the script, you are prompted to enter the following information:

- Oracle Home name
- Database Name
- Database User name
- Database Password

The utility permits only three connection attempts.

Functionality

The following options are available:

- **Collect Details about the Source Oracle Identity Manager Database:**

  Enter **1** to select this option.

  Select this option to collect details of a specific source.

  The utility generates a .dmp file that is named based on your input of whether or not the source is a standard Oracle Identity Manager installation.

  – **For standard Oracle Identity Manager installation:** The file is named oim_std_src_db.dmp.

    This file is shipped along with the utility and is available in the following directory:

    PATCH\db\oracle\Utilities\OIMDBValidator\SrcInfo

    You can use this file for comparison or upgrade verification.

  – **For nonstandard Oracle Identity Manager installation:** The file is named oim_src_db.dmp.

- **Compare Source Oracle Identity Manager Database with a Destination Oracle Identity Manager Database:**

  Enter **2** to select this option.

Choose either to compare against a standard dump or a user-created dump for a specific source:

– To compare against a standard dump, copy oim_std_src_db.dmp from SoureMetadataDump910 to SrcInfo. If SrcInfo is not already available, then create a new directory. The oim_std_src_db.dmp file is a dump of OIM 910 Vanilla installation.

Note: If the comparison with the standard dump indicates any difference, then contact Oracle support.

– To compare against a user-created dump, copy your dump file to SrcInfo. The name of the dump file must be oim_src_db.dmp.

Note: For Microsoft SQL Server, the dump file extension is .bcp instead of .dmp.

You have options for choosing the source for comparison, whether to calculate the number of rows in the destination Oracle Identity Manager database tables, or to drop the comparison tables.

- **Exit:** Enter **3** to select this option.

  Choose this option to close the utility.

B.4 Sample Comparison Summary Report

The following is a sample summary report of the Database Validator utility:

```
################################################################################
#################       R E P O R T        ##########################
################################################################################
Start Time (hh:mi:ss:mmm) : 15:09:39:370
================================================================
======================  S U M M A R Y  ==========================
================================================================
 OIM OBJECT TYPE SOURCE      DESTINATION    COMPARE STATUS
 --------------- ----------- ----------- --------------------
-------------------
 TABLE                    6           5 1 TABLE MISSING
 COLUMN                  26          23 3 COLUMNS MISSING
 PK                       6           5 1 PKS MISSING
 PK COL                   7           6 1 PK COLS MISSING
 FK                       1           0 1 FKS MISSING
 FK COL                   1           0 1 FK COLS MISSING
 U INDEX                  2           2 SUCCESSFUL
 UIDX COL                 5           5 SUCCESSFUL
 NU INDEX                 1           1 SUCCESSFUL
 NUIDX COL                1           1 SUCCESSFUL
 VIEW                     1           1 SUCCESSFUL
 PROCEDURE                1           1 SUCCESSFUL
 FUNCTION                 1           1 SUCCESSFUL
 TRIGGER                  1           1 SUCCESSFUL

============================================================  DETAILS OF
DIFFERENCES  ============================================================
 ######################## MISSING OBJECTS  ##########################
```

```
 MISSING OBJECT'S NAME          MISSING OBJECT'S TYPE
 ------------------------------ ------------------------------
 AAP                             TABLE
 PK_AAP                          PK
 FK_AAD_FK_AAD_AC_ACT         FK

######################MIS-MATCHEDOBJECTS  #################
**********************
MISSING TABLE COLUMNS
**********************
 OBJECT NAME        OBJECT TYPE PARENT OBJECT      PARENT OBJECT TYPE DATATYPE
COLUMN LENGTH ISNULL
 -------------------- ----------- -------------------- ------------------
--------------- ------------- -----
 AAP_KEY           COLUMN     AAP              TABLE           numeric
9 NO
 ACT_KEY           COLUMN     AAP              TABLE           numeric
9 NO
 AAP_VALUE         COLUMN     AAP              TABLE           varchar
200 YES

******************************************************
COLUMN DETAILS OF PRIMARY KEYS, FOREIGN KEYS & INDEXES
******************************************************
 OBJECT NAME          OBJECT TYPE PARENT OBJECT        PARENT OBJECT TYPE COLUMN
POSITION CHILD TABLE          CHILD TABLE COLUMN
 -------------------- ----------- -------------------- ------------------
--------------- -------------------- --------------------
 AAP_KEY             PK COL      PK_AAP               PK
1
 ACT_KEY             FK COL      FK_AAD_FK_AAD_AC_ACT FK
1 ACT                  ACT_KEY

================================================================  SEED METADATA
COMPARISION  ==================================================================
 NO DIFFERENCES FOUND.

End Time (hh:mi:ss:mmm) : 15:09:39:387
```

C

Reconciliation Archival

The Reconciliation Archival utility archives data from active reconciliation tables to archival reconciliation tables and to delete data from the active and archival reconciliation tables.

This utility is added to increase performance. Run this utility only if you want to archive the reconciliation data. Data is transferred from the active reconciliation tables to the new archival tables. As a result, extracting active reconciliation data takes less time, and the performance improves.

This appendix discusses the following topics:

C.1 Location and Components

All Oracle Identity Manager database reconciliation archival files are located in the *PATCH*/db/oracle/Utilities/ReconArchival directory when you are using Oracle Database. Table C–1 provides details of the files that are part of the Oracle Identity Manager Reconciliation Archival utility:

Table C–1 Reconciliation Archival Files

File	Description
cr_recon_ddl_table.sql	Creates the OIM_RECON_DDL table. This table is used by the Reconciliation Archival utility, which calls the OIM_SP_ReconArchival stored procedure to store the DDL statements that are generated when the tool archives or deletes the reconciliation data.
Create_recon_arch_tables.sql	Creates arch_rc* tables with the same structure as the active reconciliation tables. In addition, a primary key is added by the script to the tables.
OIM_SP_ReconArchival.sql	Archives reconciliation data into the reconciliation archival tables and deletes the archived data from active reconciliation tables. It also allows you to clean up the data in archival and active reconciliation tables.

C.2 Oracle Identity Manager Reconciliation Archival Functionality

To use the Reconciliation Archival utility, run the following script:

For Microsoft Windows, run OIM_ReconArch.bat.

For UNIX, run OIM_ReconArch.sh.

After you run the script, a log file is generated with the following name:

For Microsoft Windows:

- If the utility runs without error:

  `Arch_Recon_YYYY_MM_DD_hh_mi.log`

- If running the utility generates an error:

  `Err_Arch_Recon_YYYY_MM_DD_hh_mi.log`

For UNIX:

- If the utility runs without error:

  `Arch_Recon_YYYY_MM_DD_hh_mi.log`

- If the running the utility generates an error:

  `Err_Arch_Recon_YYYY_MM_DD_hh_mi.log`

C.2.1 Authentication

When you run the Reconciliation Archival utility, you are prompted to enter the following information:

- Name of the Oracle home directory
- Database name
- Database user name
- Database password

The utility permits only three connection attempts.

C.2.2 Functionality

The following options are present in the Reconciliation Archival utility main menu:

- Archive data from active reconciliation tables: Provides options to archive selective data or all the data
- Delete all data from archival reconciliation tables: Provides options to delete all the data from the reconciliation archival tables
- Delete all data from active reconciliation tables: Provides the options to delete all the data from the active reconciliation tables
- Exit: Exits the Archival Utility

D

Task Archival

You run this utility to archive the task data. When you run this utility, data is transferred from the active task tables to the new archival tables. As a result, extracting active task data takes less time and the performance improves.

This appendix discusses the following topics:

D.1 Location and Components

All Oracle Identity Manager Task Archival files are located in the *PATCH*/db/oracle/Utilities/TaskArchival directory when you are using Oracle Database. Table D–1 provides details of the files that are part of the Oracle Identity Manager Task Archival utility:

Table D–1 Task Archival Files

File	Description
cr_taskarchival_ddl_table.sql	Creates the OIM_TASK_ARCH_DDL table. This table is used by the Task Archival utility, which calls the OIM_SP_TASKS_ARCHIVAL stored procedure to store the DDL statements that are generated when the tool archives or deletes the tasks data.
Create_TasksArch_Tables.sql	Creates the arch_* tables that have the same structure as the active tasks tables. In addition, this script adds a primary key to tables.
OIM_SP_TASKS_ARCHIVAL.sql	Archives task data into the task archival tables and deletes the archived data from the active task tables.

D.2 Oracle Identity Manager Task Archival Functionality

To use the Task Archival utility, run the following script:

For Microsoft Windows: OIM_TasksArch.bat

For UNIX: OIM_TasksArch.sh

After you run the script, a log file is generated with the following name:

For Microsoft Windows:

- If the utility runs without error:

  `Arch_Tasks_YYYY_MM_DD_HH_MM.log`

- If running the utility generates an error:

  `Err_Arch_Tasks_YYYY_MM_DD_HH_MM.log`

For UNIX:

- If the utility runs without error:

  `Arch_Tasks_YYYY_MM_DD_HH_MM.log`

- If running the utility generates an error:

  `Err_Arch_Tasks_YYYY_MM_DD_HH_MM.log`

D.2.1 Authentication

When you run the script, you are prompted to enter the following information:

- Name of the Oracle home directory
- Database name
- User name
- Database password

The utility permits only three connection attempts.

D.2.2 Functionality

The following options are present in the Task Archival utility main menu:

- Archive all the provisioning tasks on resource instances, which have been revoked for disabled/deleted users
- Archive all the provisioning tasks on resource instances, which have been revoked
- Archive all the approval tasks in which the request status is Request Complete/Request Cancelled/Object Approval Complete
- Exit

E

Generating User Snapshots

User snapshots must be generated if you are upgrading an Oracle Identity Manager release 9.0.1.5 installation without the Audit and Compliance module to an Oracle Identity Manager release 9.1.0 installation with the Audit and Compliance module.

If release 9.0.1.5 installation was with the Audit and Compliance module, then you do not need to generate new snapshots.

> **See Also:** *Oracle Identity Manager Audit Report Developer's Guide* for detailed information about generating user snapshots

To generate new snapshots:

1. In a text editor, open the GenerateSnapshot script located in the *OIM_HOME*/xellerate/bin/ directory. For Microsoft Windows, open GenerateSnapshot.bat. For 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 in which you installed Oracle Identity Manager, which is *OIM_HOME*/xellerate.
   b. Modify the set APP_SERVER=@appserver variable as follows:

      For JBoss Application Server:

      ```
      set APP_SERVER=jboss
      ```

      For BEA WebLogic Server:

      ```
      set APP_SERVER=weblogic
      ```

      For IBM WebSphere Application Server:

      ```
      set APP_SERVER=websphere
      ```

   c. Modify the set APP_SERVER_HOME=@app_server_home variable to point to the directory in which you installed the application server.
   d. Modify the set JAVA_HOME=@jdk_loc variable to point to the directory containing the JDK.
3. Run one of the following GenerateSnapshot scripts as appropriate for the operating system on the Oracle Identity Manager host computer:

   For Microsoft Windows, run:

   ```
   OIM_HOME\xellerate\bin\GenerateSnapshot.bat
   ```

   For UNIX, run:

```
OIM_HOME/xellerate/bin/GenerateSnapshot.sh
```

Note: Do not run the GenerateSnapshot script if release 9.0.1.5 deployment is already with the Audit and Compliance module.

F

UPA Form Data Upgrade Utility

This appendix provides information about the UPA Form Data Upgrade utility. This utility is mandatory and facilitates exception-based reporting. You must run this utility after running the GenerateSnapshot utility.

F.1 Introduction

Oracle Identity Manager release 9.1.0 features exception-based reporting for resource access and fine-grained attributes related to the resource instance. The form data and changes to it on which these exception reports work are available in the two newly introduced tables in release 9.1.0: UPA_UD_FORMS and UPA_UD_FORMFIELDS. These two tables are populated only if the value of the XL.EnableExceptionReports system configuration property is set to `TRUE`.

Suppose the exception reports feature is disabled and you plan to enable the feature by changing the value of the XL.EnableExceptionReports property to `TRUE`. While the exception reports feature is disabled, there is no baseline process form data in the newly introduced UPA_UD_FORMS and UPA_UD_FORMFIELDS tables. As a result, the exception reports will fail.

The UPA Form Data Upgrade utility helps you solve this problem. To run this utility, the exception reporting feature is enabled. The utility runs through all the entitlements. For provisioning instances that have a resource with either a process or an object form attached, the utility reads the data on the form and stores them in the two database tables.

Subsequent changes to the form is automatically captured after the upgrade. With the baseline available, the exception reports start reporting on exceptions. The utility creates a log file named UPA_Form_Data_Upgrade_*TIMESTAMP*.log after the process is complete.

> **Note:** In this release, provisioning is initiated from Oracle Identity Manager. As a result, the two database tables contain the baseline for the process form data. Any successive updates through reconciliation are captured and reported as an exception if the values differ.

F.2 Generating Process/Object Form Data by Using the UPA Form Data Upgrade Utility

If you have installed Oracle Identity Manager Audit and Compliance module, then you must generate the process or object form data only if the following conditions apply together:

Note: Use this utility only after enabling the exception reporting feature. If some previous runs resulted in some kind of error, then the utility could be run multiple times at the time of enabling the exception reporting feature. The utility should not be used at any other time when the environment is functional.

- You have enabled the exception reporting feature.
- Audit level for an existing Oracle Identity Manager Audit and Compliance module environment is at the Resource Form or Process Task level.

In case of audit related failures in a functional environment, use the Generate Snapshot utility. Do not use this utility if the Generate Snapshot utility is being used as part of the upgrade process because the Generate Snapshot utility will perform the task of this utility also.

See Also: Appendix G, "Generating GPA Snapshots" for more information about the GenerateGPASnapshot utility

F.2.1 Working with the UPA Form Data Upgrade Utility

To use the UPA Form Data Upgrade utility, perform the following steps:

- Copying the UPA Form Data Upgrade Utility Files
- Configuring the Scripts
- Compiling the Stored Procedure
- Running the Utility

Copying the UPA Form Data Upgrade Utility Files

Copy the UPA Form Data Upgrade utility files to your local computer. Before using the utility, copy the UPAFormDataUpgradeUtility directory from the *PATCH*/db/oracle/Utilities directory on the installation media to your local computer.

Configuring the Scripts

Following are the **settings for the Oracle Database Batch/Shell file**:

- **For Microsoft Windows:** Edit the following file:

  PATCH\db\oracle\Utilities\UPAFormDataUpgradeUtility\UPAFormDataUpgrade.bat

- **For Linux or UNIX:** Edit the following file:

  PATCH/db/oracle/Utilities/UPAFormDataUpgradeUtility/UPAFormDataUpgrade.sh

Table F–1 shows the values of the variables that must be set before you run the utility:

Table F–1 Variables of the UPA Form Data Upgrade Utility

Variables	Description
ORACLE_HOME	Oracle home directory.
OIM_DB_USERNAME	Username for the Oracle Identity Manager database user
OIM_DB_USER_PASSWORD	Password for the Oracle Identity Manager database user

Table F–1 (Cont.) Variables of the UPA Form Data Upgrade Utility

Variables	Description
OIM_DB_REMOTE	Describes if the database is running on a remote computer. Set a value for this parameter if `OIM_DB_REMOTE = Y` or `OIM_DB_REMOTE = N`.
OIM_DB_ORACLE_SID	SID of the database. Set a value for this parameter only if `OIM_DB_REMOTE = N`.
OIM_DB_SERVICE_NAME	TNS service name that points to the remote database. Set a value for this parameter only if `OIM_DB_REMOTE = Y`.

Compiling the Stored Procedure

For Oracle, perform the following steps:

1. Log in to SQL *Plus with the credentials of the Oracle Identity Manager release database schema owner.
2. Run the following script:

   PATCH/db/oracle/Utilities/UPAFormDataUpgradeUtility/ compile_all_XL_SP_UPA.sql

Running the Utility

Oracle Database

On Microsoft Windows:

Run the UPAFormDataUpgrade.bat batch file from the following location:

PATCH\db\oracle\Utilities\UPAFormDataUpgradeUtility

On UNIX:

Run the UPAFormDataUpgrade.sh shell file from the following location:

PATCH/db/oracle/Utilities/UPAFormDataUpgradeUtility

G

Generating GPA Snapshots

Group snapshots must be generated in either of the following scenarios:

- If you are upgrading an Oracle Identity Manager release 9.0.1.5 installation without the Audit and Compliance module to an Oracle Identity Manager release 9.1.0 installation with the Audit and Compliance module.
- If Oracle Identity Manager release 9.0.1.5 installation is already with the Audit and Compliance module.

The group snapshots must be generated only after user snapshots have been generated.

> **See Also:** *Oracle Identity Manager Audit Report Developer's Guide* for detailed information about generating group snapshots

To generate new snapshots:

1. In a text editor, open the GenerateGPASnapshot script located in the *OIM_HOME*/xellerate/bin/ directory. For Microsoft Windows, open GenerateGPASnapshot.bat. For UNIX, open GenerateGPASnapshot.sh.
2. Edit the following variables in the GenerateGPASnapshot script:
   a. Modify the set APP_SERVER=@appserver variable as follows:

      For JBoss Application Server:

      ```
      set APP_SERVER=jboss
      ```

      For BEA WebLogic Server:

      ```
      set APP_SERVER=weblogic
      ```

      For IBM WebSphere Application Server:

      ```
      set APP_SERVER=websphere
      ```

   b. Modify the set APP_SERVER_HOME=@app_server_home variable to point to the directory in which you installed the application server. Modify the set JAVA_HOME=@jdk_loc variable to point to the directory containing the JDK.
3. Run one of the following GenerateGPASnapshot scripts as appropriate for the operating system on the Oracle Identity Manager host computer:

   For Microsoft Windows, run:

   ```
   OIM_HOME\xellerate\bin\GenerateGPASnapshot.bat
   ```

   For UNIX, run:

```
OIM_HOME/xellerate/bin/GenerateGPASnapshot.sh
```

H

Attestation Upgrade Utility

In Oracle Identity Manager release 9.1.0, attestation design has been modified to merge few columns and put the data in a newly added column in XML format as a CLOB data. After upgrading to release 9.1.0, old attestation does not work because of this change. Therefore, the Upgrade Attestation utility must be run to perform data conversion.

To upgrade attestations:

1. Create a backup of the APD table because the Upgrade Attestation utility deletes some columns from this table.
2. Copy the *PATCH*/xellerate/lib/xlAttestationUpgrade.jar file to the *OIM_HOME*/lib/ directory.
3. Run the Upgrade Attestation script. Run the following file located at *OIM_HOME*/setup/ directory as appropriate for the operating system:

   For Microsoft Windows:

   ```
   UpgradeAttestation.bat  JDBC_DRIVER DB_URL OIM_DB_USERNAME OIM_DB_PASSWORD
   ```

   For UNIX:

   ```
   UpgradeAttestation.sh  JDBC_DRIVER DB_URL OIM_DB_USERNAME OIM_DB_PASSWORD
   ```

   The UpgradeAttestation script parameters are:

   - *JDBC_DRIVER*: JDBC driver
   - *DB_URL*: URL for the database
   - *OIM_DB_USERNAME*: User name for the database
   - *OIM_DB_PASSWORD*: Password for the database
4. Delete the xlAttestationUpgrade.jar from the *OIM_HOME*\lib\ directory.

Index

U