Oracle® Identity Manager

Release Notes

Release 9.0.1.1

Part No. B31202-01

June 2006

This document contains release notes for Oracle Identity Manager Release 9.0.1.1. It includes these topics:

Notes:

- Oracle Identity Manager was previously known as Oracle Xellerate Identity Provisioning.
- Oracle Identity Manager Connectors, which were previously referred to as resource adapters, are no longer bundled with Oracle Identity Manager. Oracle Identity Manager Connectors are now distributed several times a year in the Oracle Identity Manager Connector Pack, independent from Oracle Identity Manager.

See Also: *Oracle Identity Manager 9.0.1.0 Release Notes*

ORACLE®

See Also: The following documentation, located on your installation media, for detailed information on Oracle Identity Manager:

- *Oracle Identity Manager Installation and Upgrade Guide for JBoss*
- *Oracle Identity Manager Installation and Upgrade Guide for WebLogic*
- *Oracle Identity Manager Installation and Upgrade Guide for WebSphere*
- *Oracle Identity Manager Best Practices 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 Guide*
- *Oracle Identity Manager API Usage Guide*
- *Oracle Identity Manager Audit Report Developer's Guide*
- *Oracle Identity Manager Glossary of Terms*

1 What's New in Oracle Identity Manager?

Oracle Identity Manager Release 9.0.1.1 includes support for additional platforms, as listed in "Certified Configurations" on page 3. The following enhancements have also been made to the Administrative and User Console:

- Attestation support for suborganizations within parent organizations
- API support for reissuing failed audit messages
- Proxies end dates are now required
- Lookup results can now be sorted by organization name

Updates to Oracle Identity Manager's reporting functionality include:

- Reporting support for subgroups within parent groups
- Reporting support for date ranges

The following new reports have also been added in Release 9.0.1.1:

- **Policy List**: Provides administrators and auditors with the ability to view currently defined policies and key policy information. This report can be used for operational and compliance purposes. The Policy List report displays a current snapshot of defined policies, not a historical report.
- **Entitlements Summary**: Provides administrators and auditors with the ability to view currently defined entitlements (provisioned resources), account statuses, and the number of users in each account status. This report can be used for operational and compliance purposes. The Entitlements Summary report displays a current snapshot of defined entitlements, not a historical report.
- **User Membership History**: Provides administrators and auditors with the ability to view the group membership history of a user. This report can be

used for compliance and forensic auditing purposes. The User Membership History report displays the entire history of a user's group memberships, not a snapshot of the user's current group memberships.

- **Group Membership History**: Provides administrators and auditors with the ability to view a group's membership history. This report can be used for compliance and forensic auditing purposes. The Group Membership History displays the entire history of a group's membership, not a snapshot of the group's current user membership.

> **Note:** The preceding four reports are not compatible with Oracle Identity Manager Release 9.0.1 and earlier versions of Oracle Identity Manager. To use them, you must upgrade to Oracle Identity Manager Release 9.0.1.1.

2 Certified Configurations

Oracle Identity Manager Release 9.0.1.1 is certified for clustered and non-clustered installations with the configurations listed in Table 1.

Table 1 Oracle Identity Manager Release 9.0.1.1 Certified Configurations

Application Server	Platform	Database
WebSphere 5.1.1.5	Windows 2003	Oracle 10.2.0.1
	Windows 2003	Oracle 9.2.0.7
	Windows 2003	SQL Server 2000 SP3a
	RedHat Linux AS 4.2	Oracle 10.2.0.1
	RedHat Linux AS 4.1	Oracle 10.2.0.1
	RedHat Linux AS 4.1	Oracle 9.2.0.7
	Solaris 9	Oracle 10.2.0.1
	Solaris 9	Oracle 9.2.0.7
	AIX 5L 5.3	Oracle 10.2.0.1
WebLogic 8.1 SP4	Windows 2003	Oracle 10.2.0.1
	Windows 2003	Oracle 9.2.0.7
	Windows 2003	SQL Server 2000 SP3a
	Solaris 10	Oracle 10.2.0.1
	Solaris 10	Oracle 9.2.0.7
JBoss 4.0.2	Windows 2003	Oracle 10.2.0.1
	Windows 2003	Oracle 9.2.0.7
	Windows 2003	SQL Server 2000 SP3a
	RedHat Linux AS 4.1	Oracle 10.2.0.1
	RedHat Linux AS 4.1	SQL Server 2000 SP3a
	Solaris 10	Oracle 10.2.0.1

The following additional components have been certified as part of the Release 9.0.1.1:

- Single Sign-On with COREid 7.0/RSA ClearTrust 5.5
- Microsoft Internet Explorer 6.0
- Oracle Identity Manager Design Console OS Support
  - Windows 2003 (all versions)
  - Windows XP (all versions)

3 Upgrading from Oracle Identity Manager Release 9.0.1 to Release 9.0.1.1

This section describes how to upgrade to Oracle Identity Manager version 9.0.1.1 from Oracle Identity Manager version 9.0.1 deployments running on the following application servers:

- JBoss version 4.0.2
- WebSphere version 5.1.1.5
- WebLogic version 8.1 SP4

This section also describes how to upgrade to the Oracle Identity Manager Audit and Compliance Module version 9.0.1.1 from version 9.0.1. If you did not install the Oracle Identity Manager Audit and Compliance Module in your version 9.0.1 deployment, you can use these instructions to install it when you upgrade to version 9.0.1.1.

The Oracle Identity Manager 9.0.1.1 upgrade package is contained in upg_901_to_9011.zip. Extract the contents of upg_901_to_9011.zip to a temporary directory on your existing version 9.0.1 system—this document refers to this temporary directory as <Patch>.

If you are running a version of Oracle Identity Manager earlier than 9.0.1, contact Oracle Technical Support for the appropriate upgrade materials.

3.1 Upgrade Overview

The following is a list of the steps required to upgrade to Oracle Identity Manager and the Oracle Identity Manager Audit and Compliance module version 9.0.1.1:

1. Step 1: Upgrading Your 9.0.1 Database
   a. Upgrading an Existing Database Instance
   b. Creating a New Database Instance for the Upgrade
2. Step 2: Preparing for the Upgrade
   a. Preparing the Oracle Identity Manager Server for Upgrade
   b. Preparing the Design Console for Upgrade
   c. Preparing the Remote Manager for Upgrade
3. Step 3: Performing the Upgrade to 9.0.1.1
4. Step 4: Migrating 9.0.1 Custom Code

5. Step 5: Performing Post-Upgrade Configuration Tasks
   a. Post-Upgrade Configuration for the Audit and Compliance Module
   b. Upgrading the Diagnostic Dashboard

3.2 Step 1: Upgrading Your 9.0.1 Database

Upgrade the database used by your Oracle Identity Manager 9.0.1 installation. You can choose among the following upgrade methods:

- Perform an in-place upgrade of the existing database configured for Oracle Identity Manager 9.0.1.
- Create a new instance of the database, then import the data used by your Oracle Identity Manager 9.0.1 installation into that new database and perform the upgrade.

Before you upgrade your database, extract the contents of the Oracle Identity Manager 9.0.1.1 upgrade package (upg_901_to_9011.zip) to a temporary directory on the database machine—this document refers to this temporary directory as <Patch>. After you extract the upgrade package, enable execute permissions on the scripts in the <Patch> directory.

3.2.1 Upgrading an Existing Database Instance

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

1. Backup your existing database. As appropriate to your particular database, use the export/backup utilities provided with the Oracle database or SQL Server to perform a complete backup of your production database. Production database backup includes, but is not limited to, complete export or backup of the Oracle Identity Manager 9.0.1 database instance to ensure that no data is lost during the upgrade process. If the upgrade fails, this backup can be used to restore the database to its original state.
2. Verify your database is properly configured by referring to the database vendor's documentation and the *Oracle Identity Manager Installation and Upgrade Guide* specific to your application server.
3. Upgrade your database schema from Oracle Identity Manager 9.0.1 to Oracle Identity Manager 9.0.1.1 by using the one of the following scripts appropriate for your database and operating system. Be sure to run the script on the machine where the database resides.

   Note: The xl_db_upg_901_to_9011 script also upgrades the required stored procedures for Oracle.

   Oracle on Unix and Linux:

   a. Run the following script on the system where the version 9.0.1 database is installed to upgrade the database schema:

   ```
   <Patch>/Database/Oracle/Scripts/xl_db_upg_901_to_9011.sh
   ```

   b. Enter the appropriate information for the Oracle database when prompted by the xl_db_upg_901_to_9011.sh script.

Oracle on Windows:

Run the following batch script on the system where the version 9.0.1 database is installed to upgrade the database schema:

```
<Patch>\Database\Oracle\Scripts\xl_db_upg_901_to_9011.bat
```

The following is the command line usage for the Oracle xl_db_upg_901_to_9011.bat script:

```
xl_db_upg_901_to_9011.bat <ORACLE_SID> <ORACLE_HOME> <ORACLE_XELL_USER>
<ORACLE_XELL_USER_PWD> <PATCH>
```

SQL Server:

Run the <Patch>\Database\SQLServer\Scripts\upg_901_to_9011.bat batch file.

> **Note:** Refer to "Executing the SQL Server Upgrade Scripts" on page -19 for more information on executing these scripts on an SQL Server database.

4. Perform the following steps to recompile the stored procedures for your version 9.0.1.1 database:

> **Note:** If you are using an Oracle database, you can skip this step as running the xl_db_upg_901_to_9011 script already created the required stored procedures for Oracle.

SQL Server:

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

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

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

c. Run the script:

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

> **Note:** Refer to "Executing the SQL Server Upgrade Scripts" for more information on executing these scripts on an SQL Server database.

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

Oracle:

a. Log in to SQL *Plus with the credentials of the Oracle Identity Manager 9.0.1 database schema owner.

b. Run the following script:

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

SQL Server:

Run the following script:

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

> **Note:** Refer to "Executing the SQL Server Upgrade Scripts" for more information on executing these scripts on an SQL Server database.

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

   Windows:

   Run the following .bat file:

   ```
   <Patch>\Database\Utilities\LoadXML.bat
   ```

   UNIX and Linux:

   Run the following script:

   ```
   <Patch>/Database/Utilities/LoadXML.sh
   ```

   > **Note:** Refer to "Loading Metadata into the Database" for more information on executing this script.

3.2.2 Creating a New Database Instance for the Upgrade

In this approach, you create a new database instance, then upgrade it to the database schema for Oracle Identity Manager 9.0.1.1. This method ensures that your current working database remains available if a rollback is required. Use the following steps for creating a new, upgraded database instance:

1. Backup your existing database. As appropriate to your particular database, use the **export/backup** utilities provided with the Oracle database or SQL Server to perform a complete backup of your production database. Production database backup includes, but is not limited to, complete export or backup of the Oracle Identity Manager 9.0.1 database instance to ensure that no data is lost during the upgrade process. If the upgrade fails, this backup can be used to restore the database to its original state.

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

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

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

4. Upgrade your database schema from Oracle Identity Manager 9.0.1 to Oracle Identity Manager 9.0.1.1 by using one of the following scripts appropriate for your database and operating system. Be sure to run the script on the machine where the database resides.

   Oracle on Unix and Linux:

   Run the following script on the system where the version 9.0.1 database is installed to upgrade the database schema and enter the appropriate information for the Oracle database when prompted:

   ```
   <Patch>/Database/Oracle/Scripts/xl_db_upg_901_to_9011.sh
   ```

   Note: The xl_db_upg_901_to_9011 script also upgrades the required stored procedures for Oracle.

   Oracle on Windows:

   Run the following batch script on the system where the version 9.0.1 database is installed to upgrade the database schema:

   ```
   <Patch>\Database\Oracle\Scripts\xl_db_upg_901_to_9011.bat
   ```

   The following is the command line usage for the Oracle xl_db_upg_901_to_9011.bat script:

   ```
   xl_db_upg_901_to_9011.bat <ORACLE_SID> <ORACLE_HOME> <ORACLE_XELL_USER>
   <ORACLE_XELL_USER_PWD> <PATCH>
   ```

   SQL Server:

   Run the following script:

   ```
   <Patch>\Database\SQLServer\Scripts\upg_901_to_9011.bat
   ```

   Note: Refer to "Executing the SQL Server Upgrade Scripts" for more information on executing these scripts on an SQL Server database.

5. Perform the following steps to recompile the stored procedures for your version 9.0.1.1 database:

   Note: If you are using an Oracle database, you can skip this step as running the xl_db_upg_901_to_9011 script already created the required stored procedures for Oracle.

SQL Server:

a. Launch a plain-text editor and open the following script:

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

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

c. Run the script:

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

Note: Refer to "Executing the SQL Server Upgrade Scripts" for more information on executing these scripts on an SQL Server database.

---

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

   Oracle:

   a. Log in to SQL *Plus with the credentials of the Oracle Identity Manager 9.0.1 database schema owner.

   b. Run the following script:

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

   SQL Server:

   Run the following script:

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

Note: Refer to "Executing the SQL Server Upgrade Scripts" for more information on executing these scripts on an SQL Server database.

---

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

   Windows:

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

   UNIX and Linux:

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

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

3.3 Step 2: Preparing for the Upgrade

Before you upgrade to Oracle Identity Manager 9.0.1.1, you must prepare for the upgrade by performing pre-upgrade configuration tasks on the following components:

- Oracle Identity Manager server
- Design Console
- Remote Manager

3.3.1 Preparing the Oracle Identity Manager Server for Upgrade

Prepare the Oracle Identity Manager server for upgrade to 9.0.1.1 by updating the version 9.0.1 libraries, scripts, and configuration files using the information in this section. If you are upgrading to version 9.0.1.1 in a WebSphere cluster, perform the steps in this section on the NDM host machine. If you are upgrading to version 9.0.1.1 in a WebLogic cluster, perform the steps in this section on the Admin Server machine.

1. Extract the contents of the Oracle Identity Manager 9.0.1.1 upgrade package (upg_901_to_9011.zip) to a temporary directory on the machine where the Oracle Identity Manager version 9.0.1 server is installed—this document refers to this temporary directory as <Patch>.
2. Backup the following directories.
   - <XL_HOME>\xellerate\ext
   - <XL_HOME>\xellerate\config
   - <XL_HOME>\xellerate\DDTemplates
   - <XL_HOME>\xellerate\lib
   - <XL_HOME>\xellerate\setup
   - <XL_HOME>\xellerate\webapp
   - <XL_HOME>\xellerate\bin
   - <XL_HOME>\documentation
3. Copy the directories and files listed in the location of the **From** column in the following table to the location listed in the **To** column in the following table. Overwrite the existing files in the **To** location if necessary.

   > **Note:** Delete the version 9.0.1 files in <XL_HOME>\documentation\ before copying the new version 9.0.1.1 files from <Patch>\documentation\.

Table 2 Oracle Identity Manager Server Pre-Upgrade Files to Copy

Copy From....	To
<Patch>\xellerate\DDTemplates\	<XL_HOME>\xellerate\DDTemplates\
<Patch>\xellerate\lib\	<XL_HOME>\xellerate\lib\
<Patch>\xellerate\webapp\	<XL_HOME>\xellerate\webapp\
<Patch>\xellerate\bin\	<XL_HOME>\xellerate\bin\

Table 2 (Cont.) Oracle Identity Manager Server Pre-Upgrade Files to Copy

Copy From....	To
<Patch>\xellerate\config\	<XL_HOME>\xellerate\config\
<Patch>\documentation\	<XL_HOME>\documentation\
<Patch>\xellerate\ext\	<XL_HOME>\xellerate\ext\
<Patch>\xellerate\readme.htm	<XL_HOME>

4. Copy the files listed in the following table specific to your application server from the <Patch>\xellerate\setup directory to the <XL_HOME>\xellerate\setup directory:

Table 3 Oracle Identity Manager Server Files to Copy to the setup Directory

JBoss	WebSphere	WebLogic
■ setup.xml ■ patch_jboss.cmd ■ patch_jboss.sh ■ jboss-setup.xml	■ setup.xml ■ patch_websphere.cmd ■ patch_websphere.sh ■ websphere-setup.xml	■ setup.xml ■ patch_weblogic.cmd ■ patch_weblogic.sh ■ weblogic-setup.xml ■ setup_wl_server.xml

5. Edit the patch script specific to your application server in the <XL_HOME>/xellerate/setup/ directory as listed in the following tables:

Table 4 Upgrade Patch Scripts and Parameters to Edit Per Application Server

Application Server	Operating System	Script to Edit	Parameter to Edit
JBoss	Windows	patch_jboss.cmd	Replace @loc with the path to the Oracle Identity Manager server installation directory.
	Linux	patch_jboss.sh	■ Replace @java_loc with the path to the Java installation directory. ■ Replace @loc with the path to the Oracle Identity Manager server installation directory.
WebSphere	Windows	patch_websphere.cmd	■ Replace @java_home with the path to the Java installation directory. ■ Replace @wasHome with the path to the WebSphere installation directory. ■ Replace @loc with the path to the Oracle Identity Manager server installation directory.
	Unix and Linux	patch_websphere.sh	■ Replace @java_home with the path to directory containing the JDK. ■ Replace @loc with the path to the Oracle Identity Manager server installation directory.

Table 4 (Cont.) Upgrade Patch Scripts and Parameters to Edit Per Application

Application Server	Operating System	Script to Edit	Parameter to Edit
WebLogic	Windows	patch_weblogic.cmd	■ Replace @bea_home with the path to the WebLogic installation directory ■ Replace @loc with the path to the Oracle Identity Manager server installation directory
	Unix	patch_weblogic.sh	■ Replace @bea_home with the path to the WebLogic installation directory ■ Replace @loc with the path to the Oracle Identity Manager server installation directory

6. Migrate any customizations you made to the version 9.0.1 xlWebApp web application, for example JSP customizations. Apply the 9.0.1 customizations to the new, out-of-box version 9.0.1.1 xlWebApp.war web application file located in the <XL_HOME>/xellerate/webapp/ directory.

3.3.2 Preparing the Design Console for Upgrade

Prepare the Oracle Identity Manager Design Console for upgrade to 9.0.1.1 by updating version 9.0.1 libraries, scripts, and configuration files using the following steps:

1. Backup the following files and directories:
   - <XL_DC_HOME>\xlclient\XLDesktopClient.ear
   - <XL_DC_HOME>\xlclient\CustomClient.zip
   - <XL_DC_HOME>\xlclient\xlFvcUtil.ear
   - <XL_DC_HOME>\xlclient\lib
   - <XL_DC_HOME>\xlclient\ext
   - <XL_DC_HOME>\documentation
2. Copy the directories and files listed in the location of the **From** column in the following table to the location listed in the **To** column in the following table. Overwrite the existing files in the **To** location if necessary.

   Note: Delete the version 9.0.1 files in the <XL_DC_ HOME>\documentation\ directory before copying the new version 9.0.1.1 files from Patch\documentation\.

Table 5 Oracle Identity Manager Design Console Pre-Upgrade Files to Copy

Copy From....	To
<Patch>\xlclient\XLDesktopClient.ear	<XL_DC_HOME>\xlclient\
<Patch>\xlclient\CustomClient.zip	<XL_DC_HOME>\xlclient\
<Patch>\xlclient\xlFvcUtil.ear	<XL_DC_HOME>\xlclient\

Table 5 (Cont.) Oracle Identity Manager Design Console Pre-Upgrade Files to Copy

Copy From....	To
<Patch>\documentation\	<XL_DC_HOME>\documentation\
<Patch>\xellerate\readme.htm	<XL_DC_HOME>\xlclient\
<Patch>\xlclient\lib\	<XL_DC_HOME>\xlclient\lib\
<Patch>\xlclient\ext\	<XL_DC_HOME>\xlclient\ext\

3.3.3 Preparing the Remote Manager for Upgrade

Prepare the Oracle Identity Manager Remote Manager for upgrade to 9.0.1.1 by updating version 9.0.1 libraries, scripts, and configuration files using the following steps:

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

3.4 Step 3: Performing the Upgrade to 9.0.1.1

Upgrading from an existing Oracle Identity Manager version 9.0.1 deployment to Oracle Identity Manager 9.0.1.1 involves assembling a new enterprise application archive (EAR) file from the latest libraries, then redeploying the EAR.

Perform the following steps in the section specific to your application server after completing all the pre-upgrade tasks to upgrade an existing Oracle Identity Manager version 9.0.1 deployment to Oracle Identity Manager 9.0.1.1:

3.4.1 JBoss

Use the following steps to perform the upgrade to version 9.0.1.1 on a single JBoss application server:

1. Make sure the JBoss application server is not running.
2. Run the patch_jboss script:

   Windows:

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

   Linux:

   - Run <XL_HOME>/xellerate/setup/patch_jboss.sh
3. Restart the JBoss application server.

Use the following steps to perform the upgrade to version 9.0.1.1 in a clustered JBoss environment:

1. Upgrade the first node in the JBoss cluster using the steps in the previous procedure for a single JBoss application server.
2. Backup the JBoss and Oracle Identity Manager installation directories on the second node in the cluster that you want to upgrade to 9.0.1.1.
3. Delete the JBoss and Oracle Identity Manager installation directories on the second node in the cluster.

4. Copy the JBoss and Oracle Identity Manager installation directories from the first node in the cluster that you upgraded to 9.0.1.1 in Step 1 to the second node in the cluster.

> **Note:** If you made any changes to the original, default configuration (for example, a different port number was configured) on the node in the cluster you are copying to, you must reapply those changes to the node after copying the JBoss and Oracle Identity Manager installation directories from the first node in the cluster that you upgraded to 9.0.1.1.

5. Repeat these steps and restart the nodes to upgrade all cluster participants.

3.4.2 WebSphere

Use the following steps to perform the upgrade to version 9.0.1.1 for a single WebSphere application server and WebSphere clusters:

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

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

2. For a single WebSphere application server, make sure the WebSphere application server is running and execute one of the following patch_websphere scripts.

   For a WebSphere cluster, make sure the WebSphere application server is running on all nodes in the cluster and that the Deployment Manager is running on the NDM host. Execute one of the following patch_websphere scripts on the NDM host.

   Windows:

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

   UNIX and Linux:

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

3. For a single WebSphere application server, stop and restart the application server after running the patch_websphere script to complete the upgrade to 9.0.1.1.

   For a WebSphere cluster, stop the cluster components in the following order and proceed to the next step:

   a. Stop the cluster using the Admin Console

   b. Stop the JMS server using the Admin Console

   c. Stop the NDM

4. Complete the upgrade to 9.0.1.1 for a WebSphere cluster using the following steps:

a. Copy the <XL_HOME> directory from the NDM host to all cluster participants—including the JMS host— while maintaining the same directory hierarchy structure.

b. Run the setupWebSphereCustomRegistry.cmd script on the NDM host, JMS host, and all cluster participants. The setupWebSphereCustomRegistry.cmd script is located in the <XL_HOME>/xellerate/setup/ directory. Run the setupWebSphereCustomRegistry.cmd script as follows, where <WEBSPHERE_HOME> is the home directory of WebSphere:

```
setupWebSphereCustomRegistry.cmd <WEBSPHERE_HOME>
```

c. Start the NDM, start the JMS server, and then start the cluster using the Admin Console to complete the cluster upgrade to 9.0.1.1.

3.4.3 WebLogic

Use the following steps to perform the upgrade to version 9.0.1.1 for a single WebLogic application server and WebLogic cluster:

1. Make sure the WebLogic application server is running. For a WebLogic cluster, make sure the Admin Server and Managed Servers are running.

2. Run one of the following patch_weblogic scripts on the application server. For a WebLogic cluster, run the patch_weblogic script on the Admin Server.

   Windows:

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

   UNIX:

   - Run <XL_HOME>/xellerate/setup/patch_weblogic.sh

3. Stop and restart the WebLogic application server after running the patch_weblogic script to complete the upgrade to 9.0.1.1 for a single WebLogic application server.

   For a WebLogic cluster, stop the cluster and then stop the Admin Server after running the patch_weblogic script and proceed to the next step.

4. Complete the upgrade to 9.0.1.1 for a WebLogic cluster using the following steps:

   a. Copy the <XL_HOME> directory from the Admin Server to all Managed Servers while maintaining the same directory hierarchy structure.

   b. Copy the wlXLSecurityProviders.jar file from the <XL_HOME>\Xellerate\lib directory to the <WEBLOGIC_HOME>\weblogic81\server\lib\mbeantypes\ directory on all cluster participants, including the Admin Server.

   c. Copy the <XL_HOME>\ext\nexaweb-common.jar file to the <WEBLOGIC_HOME>\weblogic81\server\lib\ directory on all cluster participants, including the Admin Server.

   d. Start the Admin Server and then start the cluster using the Admin Console to complete the cluster upgrade to 9.0.1.1.

3.5 Step 4: Migrating 9.0.1 Custom Code

In a version 9.0.1.1 environment, you can recycle custom code used in your version 9.0.1 environment.

> **Important:** Before you migrate custom code from the 9.0.1 environment, you must first recompile the custom code using the Oracle Identity Manager 9.0.1.1 libraries.

The following is a list of the customized items you can migrate from your 9.0.1 environment and reuse in version 9.0.1.1 after recompiling using the 9.0.1.1 libraries:

> **Note:** For clustered environments, after recompiling the following customized items using the 9.0.1.1 libraries, copy the recompiled code to the remaining participants in the cluster.

- Custom java code recompiled using the integrated development environment (that is, Eclipse, JDeveloper, WASD or command line javac) and 9.0.1.1 libraries.
- Custom java libraries bound to functional Oracle Identity Manager 9.0.1 adapters recompiled using 9.0.1.1 libraries. You do not need to recompile the adapters.
- Custom scheduled tasks recompiled using 9.0.1.1 libraries.
- Custom event handlers recompiled using 9.0.1.1 libraries.
- Custom clients that were built using Oracle Identity Manager 9.0.1 APIs must be updated to make them compatible with the Oracle Identity Manager 9.0.1.1 APIs. For example, certain APIs might have been deprecated and replaced by new APIs. Refer to "API Changes" on page 22 for information on API changes between Oracle Identity Manager versions 9.0.1 and 9.0.1.1.

3.6 Step 5: Performing Post-Upgrade Configuration Tasks

The following post-upgrade configurations are required to complete the upgrade to version 9.0.1.1.

3.6.1 Post-Upgrade Configuration for the Audit and Compliance Module

The following post-upgrade configuration procedures might be necessary if you are upgrading from an Oracle Identity Manager 9.0.1 installation **without** the Oracle Identity Manager Audit and Compliance module to Oracle Identity Manager 9.0.1.1 **with** the Auditing and Compliance module:

1. Setting the User Profile Audit Level
2. Generating User Snapshots

3.6.1.1 Setting the User Profile Audit Level

1. Define a secondary data source for reporting, if necessary. Refer to the *Oracle Identity Manager Audit Report Developer's Guide* for more information on defining a secondary data source.
2. Start the application server hosting your Oracle Identity Manager server.

3. Set the audit level. The permissible values are (in descending order):
   - Process Task
   - Resource Form
   - Resource
   - Membership
   - Core
   - None

   Specify an audit level by completing the following sub-steps:

   a. Log in to the Design Console as an administrator

   b. Navigate to the System Configuration page

   c. Locate XL.UserProfileAuditDataCollection and set its value to Resource Form or the appropriate audit level

4. To collect user profile audit data in the secondary reporting data store, complete the following sub-steps:

   a. Log into the Design Console as an administrator

   b. Navigate to the System Configuration page

   c. Locate XL.UserProfileAuditInSecondaryDS and set its value to TRUE.

3.6.1.2 Generating User Snapshots If you are upgrading from an Oracle Identity Manager 9.0.1 installation **without** the Oracle Identity Manager Audit and Compliance module to Oracle Identity Manager 9.0.1.1 **with** the Auditing and Compliance module, you must generate new snapshots for all existing users in the system when either of the following two situations occur:

- You upgrade from version 9.0.1 to version 9.0.1.1 with the Oracle Identity Manager Auditing and Compliance Manager module
- You elevate the audit level for Oracle Identity Manager Audit and Compliance module

To generate new snapshots, complete the following steps:

1. Launch a plain-text editor and open the file GenerateSnapshot script located in the <XL_HOME>/xellerate/bin/ directory. If you are running on Windows, open GenerateSnapshot.bat. If you are running on UNIX, open GenerateSnapshot.sh.

2. Edit the following variables in the GenerateSnapshot script:

   a. Modify the set XEL_HOME= variable to point to the directory where you installed Oracle Identity Manager.

   b. Modify the set APP_SERVER=@appserver variable as follows:

Table 6 APP_SERVER Variables for the GenerateSnapshot Script

JBoss	WebSphere	WebLogic
`set APP_SERVER=jboss`	`set APP_SERVER=websphere`	`set APP_SERVER=weblogic`

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

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

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

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

To the following:

```
set SQL_SERVER_DRIVER_DIR=<Set appropriate value here>
```

3. Execute one of the following GenerateSnapshot scripts as appropriate for the operating system on the machine hosting the Oracle Identity Manager server:

Windows:

- Run <XL_HOME>\xellerate\bin\GenerateSnapshot.bat.

UNIX and Linux:

- Run <XL_HOME>/xellerate/bin/GenerateSnapshot.sh.

3.6.2 Upgrading the Diagnostic Dashboard

The procedure for upgrading your existing version 9.0.1 Diagnostic Dashboard to version 9.0.1.1 differs depending on the application server you installed Oracle Identity Manager on. Use the following steps in the section for your application server to upgrade to the 9.0.1.1 Diagnostic Dashboard:

3.6.2.1 JBoss You are not required to remove the existing version 9.0.1 Diagnostic Dashboard XIMDD application to upgrade to the 9.0.1.1 Diagnostic Dashboard on JBoss. Use the following steps:

1. Install a new instance of the XIMDD application by copying the version 9.0.1.1 XIMDD.war file in the <Patch>\DiagnosticDashboard directory to the <JBOSS_HOME>/server/default/deploy directory.
2. Restart the application server.
3. Refer to the "Working with the Diagnostic Dashboard" chapter in the *Oracle Identity Manager Administrative and User Console Guide* for more information.

3.6.2.2 WebSphere and WebLogic You must remove the existing version 9.0.1 Diagnostic Dashboard XIMDD application before upgrading to the 9.0.1.1 Diagnostic Dashboard on WebSphere and WebLogic. Use the following steps:

1. Remove the existing XIMDD application using the Admin Console.
2. Install a new instance of the XIMDD application using the version 9.0.1.1 XIMDD.war file in the <Patch>\DiagnosticDashboard directory.

   Refer to 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 your application server.

3.7 Executing the SQL Server Upgrade Scripts

The upgrade package includes command line scripts that will upgrade the Oracle Identity Manager version 9.0.1 SQL Server database and associated stored procedures to Oracle Identity Manager 9.0.1.1. These command line scripts execute a set of SQL Server scripts through the OSQL interface on the SQL Server database. The command line scripts support the following five arguments:

Table 7 Parameters for Command Line Scripts

Arguments	Description
<server-name[\instance-name]>	The name of the server under the “SQL Server Group” in Enterprise Manager. \instance-name represents the instance running under the server.
<db-user>	The database user ID
<password>	The password of db-user
<db-name>	The name of the database
<script-location>	The absolute path to the command line script

For example:

- To upgrade the database, run <Patch>\Database\SQLServer\Scripts\upg_901_to_9011.bat with the following command-line arguments:

  ```
  <Patch>\Database\SQLServer\Scripts\upg_901_to_9011.bat
  <server-name[\instance-name]> <db-user> <password> db-name>
  <Patch>\Database\SQLServer\Scripts
  ```

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

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

- To upgrade and enable the optional Oracle Identity Manager Audit and Compliance module, run <Patch>\Database\SQLServer\Scripts\SQLServer_Enable_XACM.bat with the following command-line arguments:

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

3.8 Loading Metadata into the Database

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

1. As appropriate for the operating system of the machine hosting your Oracle Identity Manager server, edit either LoadXML.bat or LoadXML.sh located in <Patch>/Database/Utilities/, and update the JAVA_HOME variable.

2. As appropriate for your database and operating system of the machine hosting your Oracle Identity Manager server, complete one of the following sub-steps:

   SQL Server:

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

      ```
      REM SET SQL_SERVER_DRIVER_DIR=
      ```

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

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

   Oracle on Windows:

   a. Launch a plain-text editor, open the file **LoadXML.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>
      ```

   Oracle on UNIX and Linux:

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

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

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

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

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

   Oracle:

   a. JDBC URL (for example: jdbc:oracle:thin:@<db_host_ip>:<port>:<SID>)

   b. Database user name

   c. Password

   SQL Server:

   a. JDBC URL (for example: jdbc:microsoft:sqlserver://<ipaddress>:<port>)

   b. Database name

   c. Database user name

   d. Password

4 Installation and Configuration Issues and Workarounds

This section describes installation and configuration issues and their workarounds for Oracle Identity Manager Release 9.0.1.1. It contains the following topics:

- Installing Oracle Identity Manager on RedHat Linux (Bug 5246780)
- Unused Log File Created (Bug 5249948)
- Post-Installation Steps for WebLogic Missing from Installation and Upgrade Guide
- Diagnostic Dashboard Fails to Return JMS Server Status for WebSphere (Bug 5326498)
- Resolved Installation Issues

See Also: *Oracle Identity Manager 9.0.1.0 Release Notes*

4.1 Installing Oracle Identity Manager on RedHat Linux (Bug 5246780)

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

4.2 Unused Log File Created (Bug 5249948)

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

4.3 Post-Installation Steps for WebLogic Missing from Installation and Upgrade Guide

Step 4 of the "Configuring WebLogic for Oracle Identity Manager" section in Chapter 8 of the *Oracle Identity Manager Installation and Upgrade Guide for WebLogic* does not contain the correct instructions for editing the WebLogic start script file. The correct instructions are as follows:

For Windows:

Locate the line that starts with:

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

and add the following line just above it:

```
SET MEM_ARGS=-Xmx1024m
```

For UNIX/Linux:

Locate the line that starts with:

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

and add the following lines just above it:

```
MEM_ARGS="-Xmx1024m"
export MEM_ARGS
```

4.4 Diagnostic Dashboard Fails to Return JMS Server Status for WebSphere (Bug 5326498)

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

4.5 Resolved Installation Issues

Table 8 lists installation and configuration issues that are resolved in Release 9.0.1.1:

Table 8 Resolved Installation and Configuration issues in Release 9.0.1.1

Issue #	Description
5180574	Remote Manager installer provides an option to install without SSL.
5180579	<XL_HOME>/WORK directory created in WebLogic cluster environment.

5 General Issues and Workarounds

This section describes general issues and their workarounds for Oracle Identity Manager Release 9.0.1.1. It contains the following topics:

- API Changes
- Group Membership History Report Does Not Distinguish Between Active and Deleted Groups (Bug 5249535)
- Group Membership History Report Does Not Display Some Sectional Header Values (Bug 5243112)
- Updates to Operational Tables Used in Historical Reports
- Incorrect Usage of "Resetting Passwords" in Administrative and User Console and Documentation Set (Bug 5241541)
- Cannot Reuse an Existing User ID (5218621)
- Restart Required After Importing Form with Encrypted Attributes (Bug 5181102)
- Resolved General Issues

> **See Also:** *Oracle Identity Manager 9.0.1.0 Release Notes*

5.1 API Changes

This section describes the API changes that were introduced as part of Oracle Identity Manager Release 9.0.1.1.

Table 9 lists the modifications to existing APIs.

Table 9 Modified APIs

Operation	API	Changes
Group	`public tcResultSet getAllMembers(long plGroupKey) throws tcGroupNotFoundException, tcAPIException`	Modified to prevent users from being returned by indirect inclusion from subgroups.
Group	`public tcResultSet getMemberUsers(long plGroupKey)throws tcAPIException, tcGroupNotFoundException`	Modified to prevent users from being returned by indirect inclusion from subgroups.
Request	`public int getNumberOfApprovalTasksAssignedToUser(long userKey, String[] statuses) throws tcUserNotFoundException, tcAPIException`	Optimized for better performance with Oracle databases.
Request	`public tcResultSet getApprovalTasksAssignedToUser(long userKey, Map attributeList)throws tcUserNotFoundException, tcAPIException, tcAttributeNotFoundException`	Optimized for better performance with Oracle databases.
Request	`public tcResultSet getApprovalTasksAssignedToManagedUsers(long userKey,Map attributeList)throws tcAPIException, tcUserNotFoundException, tcAttributeNotFoundException`	Optimized for better performance with Oracle databases.
Report	`public tcResultSet getOperationalReports(long userKey) throws tcUserNotFoundException, tcAPIException`	Modified to prevent the return of duplicate rows for users who belong to multiple groups with the same allowed reports.
Report	`public tcResultSet getHistoricalReports(long userKey) throws tcUserNotFoundException, tcAPIException`	Modified to prevent the return of duplicate rows for users who belong to multiple groups with the same allowed reports.
Report	`public tcResultSet getPagedReportData(ReportInput reportInput)throws tcAPIException`	Modified to retrieve the date format from system properties.
Audit	`public void reIssueAuditMessage(int audJmsKey) throws tcAPIException`	Modified to allow the reissuing of failed audit messages.
Audit	`public void reIssueAuditMessageByIdentifier(String auditor, String identifier) throws tcAPIException`	Modified to allow the reissuing of failed audit messages.
Attestation Definition	`public long createAttestationDefinition(AttestationProcessDefinition definition)throws DuplicateAttestationProcessException, tcAPIException`	Enhanced to allow users to specify whether to include users in the sub organizations to be attested when the attestation scope is Organization Users

Table 9 (Cont.) Modified APIs

Operation	API	Changes
Attestation Definition	`public void updateAttestationDefinition(long processDefKey, AttestationProcessDefinition definition) throws DuplicateAttestationProcessException, tcInvalidPermissionsException, tcAPIException, AttestationProcessNotFoundException`	Enhanced to allow users to specify whether to include users in the sub organizations to be attested when the attestation scope is Organization Users
Attestation Definition	`public AttestationProcessDefinition getAttestationProcessDefinition(long processDefKey) throws tcAPIException, AttestationProcessNotFoundException`	Enhanced to allow users to specify whether to include users in the sub organizations to be attested when the attestation scope is Organization Users

Table 10 lists the new APIs that were added in Oracle Identity Manager Release 9.0.1.1.

Table 10 New APIs

Operation	API
Group	`public tcResultSet getAllMemberUsersAndGroups(long groupKey) throws tcGroupNotFoundException, tcAPIException`
Audit	`public String[] getUsersWithNoSnapshots() throws tcAPIException`

See Also:

- The API JavaDocs included with Release 9.0.1.1 for a full description of all implemented interface functionality
- *Oracle Identity Manager API Usage Guide*

5.2 Group Membership History Report Does Not Distinguish Between Active and Deleted Groups (Bug 5249535)

When you run a Group Membership History report, the report results do not distinguish between active and deleted groups.

5.3 Group Membership History Report Does Not Display Some Sectional Header Values (Bug 5243112)

When you run a Group Membership History report, the report results may not display some sectional header values for deleted groups.

5.4 Updates to Operational Tables Used in Historical Reports

The tables and constraints listed in the "Writing User Profile Audit to Secondary Datasource" section of the *Oracle Identity Manager Audit Report Developer's Guide* have been updated in Release 9.0.1.1. The tables and constraints as of Release 9.0.1.1 are listed in Table 11:

Table 11 Updates to Operational Tables Used in Historical Reports

Table Name	Foreign Key Constraint Name	Referenced Table Name	Referenced Column Name
AAD	FK_AAD_FK_ AAD_AC_ACT	ACT	ACT_KEY
	FK_AAD_FK_ AAD_UG_UGP	UGP	UGP_KEY
ACT	FK_ACT_ACT	ACT	PARENT_KEY
	FK_ACT_SRP	SRP	SRP_KEY
GPG	FK_GPG_UGP	UGP	UGP_KEY
	FK_GPG_UGP_ KEY_UGP	UGP	GPG_UGP_KEY
OUG	FK_OUG_OBJ	OBJ	OBJ_KEY
	FK_OUG_UGP	UGP	UGP_KEY
POL			
PTY			
REQ	FK_REQ_ORC	ORC	ORC_KEY
	FK_REQ_OST	OST	OST_KEY
	FK_REQ_USR	USR	USR_KEY
UGP			
USG	FK_USG_RUL	RUL	RUL_KEY
	FK_USG_UGP	UGP	UGP_KEY
	FK_USG_USR	USR	USR_KEY
USR	FK_USR_ACT	ACT	ACT_KEY

5.5 Incorrect Usage of "Resetting Passwords" in Administrative and User Console and Documentation Set (Bug 5241541)

The Oracle Identity Manager Administrative and User Console and documentation set incorrectly refer to the process of "changing passwords" as "resetting passwords". Therefore, any references to *resetting* passwords should be assumed to mean *changing* passwords.

5.6 Cannot Reuse an Existing User ID (5218621)

An exception is thrown when you attempt to reuse an existing user ID after setting the User ID Reuse property to true in the Design Console. To resolve this issue, you must drop the unique index for the `USR_LOGIN` column in the `USR` table, and then create a non-unique index.

5.7 Restart Required After Importing Form with Encrypted Attributes (Bug 5181102)

If you are importing forms with encrypted attributes for a clustered configuration, you need to restart all nodes of the cluster.

5.8 Resolved General Issues

The following general issues have been resolved in Release 9.0.1.1:

Table 12 Resolved General issues in Release 9.0.1.1

Issue #	Description
5229011	System error displays when attempting to remove a user from a group.
5180578	SQL exception is thrown when saving an attestation action with an empty delegated reviewer.
5180576	The purge cache utility requires log4j classes in the class path.
5250305	Exception occurs when a default value is set in an IT resource lookup field.
5204295	The GenerateSnapshot utility does not generate a snapshot of missing users.

6 Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Oracle Identity Manager Release Notes, Release 9.0.1.1 for Windows or UNIX
B31202-01