

## **Oracle® Identity Manager**

Connector Guide for Oracle Internet Directory

Release 9.0.3

**B32363-02**

March 2007

Copyright © 1991, 2007, Oracle. All rights reserved.

Primary Authors: Debapriya Datta, Shiladitya Guha

Contributing Authors: Don Gosselin, Vijaykarthik Sathiyamurthy, Lyju Vadassery

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

---

---

# Contents

<b>Preface</b> .....	v
Audience .....	v
Documentation Accessibility .....	v
Related Documents .....	vi
Documentation Updates .....	vi
Conventions .....	vi
 <b>What's New in the Oracle Identity Manager Connector for Oracle Internet Directory?</b> .....	vii
Software Updates .....	vii
Documentation-Specific Updates.....	vii
 <b>1 About the Connector</b>	
<b>Supported Functionality</b> .....	1-1
<b>Multilanguage Support</b> .....	1-2
<b>Reconciliation Module</b> .....	1-3
Lookup Fields Reconciliation .....	1-3
User Reconciliation .....	1-3
Reconciled Resource Object Fields .....	1-3
Reconciled Xellerate User Fields.....	1-4
<b>Provisioning Module</b> .....	1-4
<b>Files and Directories That Comprise the Connector</b> .....	1-4
<b>Determining the Release Number of the Connector</b> .....	1-5
 <b>2 Deploying the Connector</b>	
<b>Step 1: Verifying Deployment Requirements</b> .....	2-1
<b>Step 2: Configuring the Target System</b> .....	2-2
<b>Step 3: Copying the Connector Files and External Code</b> .....	2-2
<b>Step 4: Configuring the Oracle Identity Manager Server</b> .....	2-3
Customizing the xlconfig.xml File .....	2-3
Changing to the Required Input Locale.....	2-3
Clearing Content Related to Connector Resource Bundles from the Server Cache .....	2-4
Enabling Logging .....	2-4
<b>Step 5: Importing the Connector XML Files</b> .....	2-6
Defining IT Resources .....	2-7

<b>Step 6: Configuring Reconciliation.....</b>	<b>2-8</b>
Configuring Trusted Source Reconciliation.....	2-8
Creating the Reconciliation Scheduled Tasks .....	2-9
Specifying Values for the Scheduled Task Attributes .....	2-9
Lookup Fields Reconciliation Scheduled Task.....	2-9
User Reconciliation Scheduled Task.....	2-11
<b>Step 7: Compiling Adapters .....</b>	<b>2-12</b>
<b>Step 8: Configuring SSL.....</b>	<b>2-13</b>
<b>Configuring the Connector for Multiple Installations of the Target System .....</b>	<b>2-13</b>
<b>Customizing the Mapping of the User ID Field .....</b>	<b>2-14</b>

### **3 Testing and Troubleshooting**

<b>Running Test Cases .....</b>	<b>3-1</b>
<b>Troubleshooting.....</b>	<b>3-2</b>
Connection Errors .....	3-2
Create User Errors.....	3-3
Delete User Errors .....	3-4
Modify User Errors .....	3-4
Child Data Errors .....	3-5

### **4 Known Issues**

#### **A Attribute Mappings Between Oracle Identity Manager and Oracle Internet Directory**

#### **Index**

---

---

# Preface

*Oracle Identity Manager Connector Guide for Oracle Internet Directory* provides information about integrating Oracle Identity Manager with Oracle Internet Directory.

---

---

**Note:** Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

---

---

## Audience

This guide is intended for users who want to deploy the Oracle Identity Manager connector for Oracle Internet Directory.

## Documentation Accessibility

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

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

### Accessibility of Code Examples in Documentation

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

### Accessibility of Links to External Web Sites in Documentation

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

## TTY Access to Oracle Support Services

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

## Related Documents

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

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation Guide for JBoss*
- *Oracle Identity Manager Installation Guide for Oracle Containers for J2EE*
- *Oracle Identity Manager Installation Guide for WebLogic*
- *Oracle Identity Manager Installation Guide for WebSphere*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Audit Report Developer Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Globalization Guide*
- *Oracle Identity Manager Glossary of Terms*

The following document is available in the Oracle Identity Manager Connector Pack documentation library:

- *Oracle Identity Manager Connector Framework Guide*

## Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.3 connector documentation set, visit Oracle Technology Network at

<http://www.oracle.com/technology/documentation/index.html>

## Conventions

The following text conventions are used in this document:

Convention	Meaning
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

---

---

# What's New in the Oracle Identity Manager Connector for Oracle Internet Directory?

This chapter provides an overview of the updates made to the connector and documentation for Oracle Internet Directory in release 9.0.3.1 of the Oracle Identity Manager connector pack.

**See Also:** The 9.0.3 release of this guide for information about updates that were new for the 9.0.3 release

The updates discussed in this chapter are divided into the following categories:

- [Software Updates](#)

These include updates made to the connector software.

- [Documentation-Specific Updates](#)

These include major changes made to the connector documentation. These changes are not related to software updates.

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

## Software Updates

This section discusses updates made to this release of the connector software.

### Customizing the Mapping of the User ID Field

In this release of the connector, you can customize the mapping between the user ID fields of Oracle Internet Directory and Oracle Identity Manager. The procedure to achieve this is described in the "[Customizing the Mapping of the User ID Field](#)" section on page 2-14.

## Documentation-Specific Updates

There are no documentation-specific updates in this release of the guide.





---

## About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with third-party applications. The connector for Oracle Internet Directory is used to integrate Oracle Identity Manager with Oracle Internet Directory.

---

**Note:** Oracle Identity Manager connectors were referred to as *resource adapters* prior to the acquisition of Thor Technologies by Oracle.

---

This chapter contains the following sections:

- [Supported Functionality](#)
- [Multilanguage Support](#)
- [Reconciliation Module](#)
- [Provisioning Module](#)
- [Files and Directories That Comprise the Connector](#)
- [Determining the Release Number of the Connector](#)

### Supported Functionality

The following table lists the functions that are available with this connector.

Function	Type	Description
Create User	Provisioning	Creates a user
Delete User	Provisioning	Deletes a user
Enable User	Provisioning	Enables a user
Disable User	Provisioning	Disables a user
Move User	Provisioning	Moves a user from one container to another
Password Updated	Provisioning	Updates the password of a user
First Name Updated	Provisioning	Updates the first name of a user
Last Name Updated	Provisioning	Updates the last name of a user
Department Updated	Provisioning	Updates the department of a user

Function	Type	Description
Email ID Updated	Provisioning	Updates the e-mail address of a user
Location Updated	Provisioning	Updates the location of a user
Middle Name Updated	Provisioning	Updates the middle name of a user
Preferred Language Updated	Provisioning	Updates the language preference of a user
Telephone Updated	Provisioning	Updates the telephone number of a user
Time Zone Updated	Provisioning	Updates the time zone of a user
Title Updated	Provisioning	Updates the title of a user
Organization DN Updated	Provisioning	Updates the organization DN of a user
Add user to group	Provisioning	Adds a user to a group
Remove user from group	Provisioning	Removes a user from a group
Add user to role	Provisioning	Adds a user to a role
Remove user from role	Provisioning	Removes a user from a role
Reconciliation Delete Received	Reconciliation	Deletes a user from Oracle Identity Manager if the user has been deleted from the target system
Reconciliation Insert Received	Reconciliation	Inserts a user in Oracle Identity Manager
Reconciliation Update Received	Reconciliation	Updates a user in Oracle Identity Manager. This operation involves modifying any of the user properties, such as the first name or last name.

---

**Note:** Oracle Internet Directory is a general-purpose directory service that enables fast retrievals and centralized management of information about dispersed users and network resources.

Lightweight Directory Access Protocol (LDAP) is an Internet-ready, lightweight implementation of ISO X.500 standard for directory services.

Oracle Internet Directory implements and combines LDAP with the high performance, scalability, robustness, and availability features of Oracle Database. At some places in this guide, the terms Oracle Internet Directory and LDAP have been used interchangeably.

---

**See Also:** [Appendix A](#) for information about attribute mappings between Oracle Identity Manager and Oracle Internet Directory.

## Multilanguage Support

This release of the connector supports the following languages:

- English
- Brazilian Portuguese

- French
- German
- Italian
- Japanese
- Korean
- Simplified Chinese
- Spanish
- Traditional Chinese

**See Also:** *Oracle Identity Manager Globalization Guide* for information about supported special characters

## Reconciliation Module

This section discusses the elements that the reconciliation module extracts from the target system to construct reconciliation event records.

Reconciliation can be divided into the following types:

- [Lookup Fields Reconciliation](#)
- [User Reconciliation](#)

### Lookup Fields Reconciliation

Lookup fields reconciliation involves reconciling the lookup values for groups and roles.

### User Reconciliation

This section provides information about user reconciliation.

#### Reconciled Resource Object Fields

The following fields are reconciled:

- User ID
- First Name
- Last Name
- Middle Name
- Department
- Location
- Telephone
- Email
- Preferred Language
- Timezone
- Logon Script
- Title

- Server Name (IT resource)
- UserGroup
- UserRole

### Reconciled Xellerate User Fields

The following fields are reconciled only if reconciliation is implemented in trusted mode:

- User ID
- First Name
- Last Name
- Organization
- Xellerate Type
- Role

## Provisioning Module

The following fields are provisioned:

- ldapObjectClass
- ldapUserObjectClassPrimary
- ldapUserObjectClassSecondary
- ldapFirstName
- ldapLastName
- ldapUserID
- ldapPassword
- ldapUserDNPrefix
- ldapUserDisableAttr
- ldapOrgDNPrefix
- ldapGroupDNPrefix
- ldapGroupMemberAttr

---

---

**Note:** The names of the fields are case-sensitive.

---

---

## Files and Directories That Comprise the Connector

The files and directories that comprise this connector are compressed in the following directory on the installation media.

Directory Servers\Oracle Internet Directory

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
Files in the Batch\custom directory	When you run the custom.bat file, a required object class and an attribute are added to the existing Oracle Internet Directory schema.  Refer to the " <a href="#">Step 2: Configuring the Target System</a> " section on page 2-2 for more information.
lib\xliOID.jar	This JAR file contains the class files required for provisioning and reconciliation.
Files in the resources directory	Each of these resource bundle files contains language-specific information that is used by the connector.  <b>Note:</b> A <b>resource bundle</b> is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.
Files in the Troubleshoot directory	These files are used to perform basic tests on the connector, even before Oracle Identity Manager is installed.
xml\oimOIDUser.xml	This XML file contains definitions for the following components of the connector: <ul style="list-style-type: none"> <li>■ IT resource type</li> <li>■ Custom process form</li> <li>■ Process task and adapters (along with their mappings)</li> <li>■ Resource object</li> <li>■ Xellerate User</li> <li>■ Provisioning process</li> <li>■ Pre-populate rules</li> <li>■ Reconciliation process</li> <li>■ Lookup definitions</li> </ul>
xml\oimUser.xml	This XML file contains the configuration for the Xellerate User. You must import this file only if you plan to use the connector in trusted source reconciliation mode.

---

**Note:** The files in the Troubleshoot directory are used only to run tests on the connector.

---

The "[Step 3: Copying the Connector Files and External Code](#)" section on page 2-2 provides instructions to copy these files into the required directories.

## Determining the Release Number of the Connector

To determine the release number of the connector that you have deployed:

1. Extract the contents of the xliOID.jar file. For a connector that has been deployed, this file is in the following directory:

`OIM_home\xellerate\JavaTasks`

2. Open the `manifest.mf` file in a text editor. The `manifest.mf` file is one of the files bundled inside the `xliOID.jar` file.

In the `manifest.mf` file, the release number of the connector is displayed as the value of the `Version` property.

**See Also:** *Oracle Identity Manager Design Console Guide*

---

## Deploying the Connector

Deploying the connector involves the following steps:

- [Step 1: Verifying Deployment Requirements](#)
- [Step 2: Configuring the Target System](#)
- [Step 3: Copying the Connector Files and External Code](#)
- [Step 4: Configuring the Oracle Identity Manager Server](#)
- [Step 5: Importing the Connector XML Files](#)
- [Step 6: Configuring Reconciliation](#)
- [Step 7: Compiling Adapters](#)
- [Step 8: Configuring SSL](#)

The following sections discuss procedures to customize the connector:

- [Configuring the Connector for Multiple Installations of the Target System](#)
- [Customizing the Mapping of the User ID Field](#)

### Step 1: Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3 or later
Target systems	Oracle Internet Directory 9.x (9.2.0.1) or 10.x
Target system host platforms	The target system host platform can be any one of the following: <ul style="list-style-type: none"><li>■ Microsoft Windows 2000</li><li>■ Solaris 8 or 9</li></ul>
Target system user account	User account to which the BROWSE, ADD, DELETE, READ, WRITE, and SEARCH rights have been assigned  You provide the credentials of this user account while performing the procedure in the " <a href="#">Defining IT Resources</a> " section on page 2-7.

## Step 2: Configuring the Target System

You must add a custom object class and custom attribute to the Oracle Internet Directory schema for the provisioning and reconciliation of user roles.

To add a custom object class and custom attribute:

1. Ensure that Oracle Internet Directory is running.
2. Copy the contents of the `Batch\custom` directory from the installation media ZIP file to a directory on the target Oracle Internet Directory server.
3. Using any text editor, open the `custom.bat` file.
4. In the commands listed in the `custom.bat` file, provide the host name, port, and Oracle Internet Directory superuser DN and password.

The following is the syntax for providing these values:

```
ldapmodify -h hostname -p port_number -D SuperUser_DN -w SuperUser_Password -c -f customRoleOccupant.ldif
ldapadd -h hostname -p port_number -D SuperUser_DN -w SuperUser_Password -c -f customIndex.ldif
ldapmodify -h hostname -p port_number -D SuperUser_DN -w SuperUser_Password -c -f customOrganizationalRole.ldif
```

For example:

```
ldapmodify -h bk2b3f-2809 -p 4389 -D "cn=orcladmin" -w "welcome" -c -f customRoleOccupant.ldif
ldapadd -h bk2b3f-2809 -p 4389 -D "cn=orcladmin" -w "welcome" -c -f customIndex.ldif
ldapmodify -h bk2b3f-2809 -p 4389 -D "cn=orcladmin" -w "welcome" -c -f customOrganizationalRole.ldif
```

5. Run the `custom.bat` file.
6. Open Oracle Directory Manager and click **Schema Management** in the left pane. The details of all schema elements are displayed in the right pane. Check if the `customOrganizationalRole` object class and `customRoleOccupant` attributes have been added to the schema.

## Step 3: Copying the Connector Files and External Code

The connector files to be copied and the directories to which you must copy them are given in the following table.

---

**Note:** The directory paths given in the first column of this table correspond to the location of the connector files in the following directory on the installation media:

Directory Servers\Oracle Internet Directory

Refer to the ["Files and Directories That Comprise the Connector"](#) section on page 1-4 for more information about these files.

---



File in the Installation Media Directory	Destination Directory
Files in the Batch\custom directory	Refer to the " <a href="#">Step 2: Configuring the Target System</a> " section on page 2-2 for instructions on copying these files.
lib\xliOID.jar	<i>OIM_home</i> \xellerate\JavaTasks
Files in the resources directory	<i>OIM_home</i> \xellerate\connectorResources
Files in the Troubleshoot directory	<i>OIM_home</i> \xellerate\Troubleshoot
Files in the xml directory	<i>OIM_home</i> \xellerate\OID\xml

---

**Note:** While installing Oracle Identity Manager in a clustered environment, you copy the contents of the installation directory to each node of the cluster. Similarly, you must copy the connectorResources directory and the JAR files to the corresponding directories on each node of the cluster.

---

## Step 4: Configuring the Oracle Identity Manager Server

Configuring the Oracle Identity Manager server involves performing the following procedures:

---

**Note:** In a clustered environment, you must perform this step on each node of the cluster.

---

- [Customizing the xlconfig.xml File](#)
- [Changing to the Required Input Locale](#)
- [Clearing Content Related to Connector Resource Bundles from the Server Cache](#)
- [Enabling Logging](#)

### Customizing the xlconfig.xml File

In the xlconfig.xml file, you must provide a higher value, 50,000 or more, for the checkouttimeout attribute. This XML file is in the *OIM\_home*\xellerate\config directory. You must modify the checkouttimeout attribute value to ensure that the connector XML files are correctly imported.

### Changing to the Required Input Locale

Changing to the required input locale (language and country setting) involves installing the required fonts and setting the required input locale.

To set the required input locale:

---

**Note:** Depending on the operating system used, you may need to perform this procedure differently.

---

1. Open Control Panel.

2. Double-click **Regional Options**.
3. On the Input Locales tab of the Regional Options dialog box, add the input locale that you want to use and then switch to the input locale.

## Clearing Content Related to Connector Resource Bundles from the Server Cache

Whenever you add a new resource bundle in the `OIM_home\xellerate\connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

To clear content related to connector resource bundles from the server cache:

1. In a command window, change to the `OIM_home\xellerate\bin` directory.
2. Enter one of the following commands:

---

---

**Note:** You must perform Step 1 before you perform this step. If you run the command as follows, then an exception is thrown:

```
OIM_home\xellerate\bin\batch_file_name
```

---

---

- On Microsoft Windows:

```
PurgeCache.bat ConnectorResourceBundle
```

- On UNIX:

```
PurgeCache.sh ConnectorResourceBundle
```

In this command, `ConnectorResourceBundle` is one of the content categories that you can remove from the server cache. Refer to the following file for information about the other content categories:

```
OIM_home\xellerate\config\xlConfig.xml
```

---

---

**Note:** You can ignore the exception that is thrown when you perform Step 2.

---

---

## Enabling Logging

When you enable logging, Oracle Identity Manager automatically stores in a log file information about events that occur during the course of provisioning and reconciliation operations. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- ALL

This level enables logging for all events.

- DEBUG

This level enables logging of information about fine-grained events that are useful for debugging.

- INFO

This level enables logging of informational messages that highlight the progress of the application at coarse-grained level.

- **WARN**

This level enables logging of information about potentially harmful situations.

- **ERROR**

This level enables logging of information about error events that may still allow the application to continue running.

- **FATAL**

This level enables logging of information about very severe error events that could cause the application to stop functioning.

- **OFF**

This level disables logging for all events.

The file in which you set the log level and the log file path depend on the application server that you use:

- **For JBoss Application Server**

To enable logging:

1. In the *JBoss\_home*\server\default\conf\log4j.xml file, locate the following lines:

```
<category name="XELLERATE">
  <priority value="log_level"/>
</category>
```

2. In the second XML code line, replace *log\_level* with the log level that you want to set. For example:

```
<category name="XELLERATE">
  <priority value="INFO"/>
</category>
```

After you enable logging, log information is written to the following file:

*JBoss\_home*\server\default\log\server.log

- **For IBM WebSphere:**

To enable logging:

1. Add the following line in the *OIM\_home*\xellerate\config\log.properties file:

```
log4j.logger.XELLERATE=log_level
```

2. In this line, replace *log\_level* with the log level that you want to set.

For example:

```
log4j.logger.XELLERATE=INFO
```

After you enable logging, log information is written to the following file:

*WebSphere\_home*\AppServer\logs\server\_name\startServer.log

- **For BEA WebLogic**

To enable logging:

1. Add the following line in the *OIM\_home*\xellerate\config\log.properties file:

```
log4j.logger.XELLERATE=log_level
```

2. In this line, replace *log\_level* with the log level that you want to set.

For example:

```
log4j.logger.XELLERATE=INFO
```

After you enable logging, log information is written to the following file:

```
WebLogic_home\user_projects\domains\domain_name\server_name\server_name.log
```

#### ■ For OC4J

To enable logging:

1. Add the following line in the

*OIM\_home\xellerate\config\log.properties* file:

```
log4j.logger.XELLERATE=log_level
```

2. In this line, replace *log\_level* with the log level that you want to set.

For example:

```
log4j.logger.XELLERATE=INFO
```

After you enable logging, log information is written to the following file:

```
OC4J_home\opmn\logs\default_group-home-default_group~1.log
```

## Step 5: Importing the Connector XML Files

To import the connector XML files:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the *oimOIDUser.xml* file, which is in the *OIM\_home\xellerate\OID\xml* directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File**. The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Next**. The Provide IT Resource Instance Data page for the *OID Server IT* resource is displayed.
8. Specify values for the parameters of the *OID Server IT* resource. Refer to the table in the ["Defining IT Resources"](#) section on page 2-7 for information about the values to be specified.
9. Click **Next**. The Provide IT Resource Instance Data page for a new instance of the *LDAP Server IT* resource type is displayed.
10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.
11. Click **View Selections**.

The contents of the XML file are displayed on the Import page. You may see a cross-shaped icon along with some nodes. Remove these nodes by right-clicking each node and then selecting **Remove**.

**12. Click Import.** The connector XML file is imported into Oracle Identity Manager.

After you import the connector XML files, proceed to the ["Step 6: Configuring Reconciliation"](#) section on page 2-8.

## Defining IT Resources

You must specify values for the `OID_Server` IT resource parameters listed in the following table.

Parameter	Description
Admin Id	DN value of the user who has administrator rights on the Oracle Internet Directory server Sample value: <code>cn=Admin,ou=People,o=xyz</code>
Admin Password	Password of the user who has administrator rights on the target Oracle Internet Directory server
Server Address	IP address of the Oracle Internet Directory server
Port	Port number to connect to the Oracle Internet Directory server Sample value: 389
Root DN	Base DN on which all the user operations are to be carried out Sample value: <code>dc=host_name, dc=com</code>  Here, <i>host_name</i> is the host name under which Oracle ConText is created.
SSL	If this parameter is set to <code>true</code> , then SSL is used to secure communication between Oracle Identity Manager and the Oracle Internet Directory server. In this case, the authentication certificate of the Oracle Internet Directory server must be imported into the Oracle Identity Manager server.  If this parameter is set to <code>false</code> , then SSL is not used to secure communication between Oracle Identity Manager and the Oracle Internet Directory server.  <b>Note:</b> It is recommended that you enable SSL to secure communication with the target system.
Prov Attribute Lookup Code	Name of the lookup definition that has the target attribute mappings required for provisioning The value must be <code>AttrName.Prov.Map.OID</code> .
Recon Attribute Lookup Code	Name of the lookup definition that has the target attribute mappings required for reconciliation The value must be <code>AttrName.Recon.Map.OID</code> .
Use XL Org Structure	If set to <code>true</code> , then the Oracle Identity Manager Organization structure is used during provisioning and reconciliation.  If set to <code>false</code> , then the value of the Organization field in the process form is used for provisioning and the organization or container in the target Oracle Internet Directory is used for reconciliation.

Parameter	Description
Last Recon TimeStamp	For the first reconciliation run, the timestamp value is not set. For subsequent rounds of reconciliation, the time at which the previous round of reconciliation was completed is stored in this parameter.  You do not need to provide a value for this parameter.  Sample value: 20060524110907Z

After you specify values for these IT resource parameters, proceed to Step 9 of the procedure to import connector XML files.

## Step 6: Configuring Reconciliation

Configuring reconciliation involves the following steps:

- [Configuring Trusted Source Reconciliation](#)
- [Creating the Reconciliation Scheduled Tasks](#)

### Configuring Trusted Source Reconciliation

---

**Note:** Perform this step of the procedure only if you want to configure trusted source reconciliation. Only one connector can be configured for trusted source reconciliation. If you import the `oimUser.xml` file while you have another trusted source configured, then both connector reconciliations would stop working.

Refer to *Oracle Identity Manager Connector Framework Guide* for conceptual information about reconciliation configurations.

---

To configure trusted source reconciliation, you must first import the XML file for trusted source reconciliation as follows:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the `oimUser.xml` file, which is in the `OIM_home\xellerate\OID\xml` directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File**. The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Import**.
8. In the message that is displayed, click **Import** to confirm that you want to import the XML file and then click **OK**.

Then, set the value of the `IsTrusted` reconciliation scheduled task attribute to `True` while performing the procedure described in the following section.

## Creating the Reconciliation Scheduled Tasks

To create the scheduled tasks for lookup fields and user reconciliations:

1. Open the Oracle Identity Manager Design Console.
  2. Expand the **Xellerate Administration** folder.
  3. Select **Task Scheduler**.
  4. Click **Find**. The details of the predefined scheduled tasks are displayed on two different tabs.
  5. For the first scheduled task, enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the `ERROR` status to the task.
  6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.
  7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, select the date and time at which you want the task to run.
  8. In the Interval region, set the following schedule parameters:
    - To set the task to run on a recurring basis, select the **Daily**, **Weekly**, **Recurring Intervals**, **Monthly**, or **Yearly** option.  
If you select the **Recurring Intervals** option, then you must also specify the time interval at which you want the task to run on a recurring basis.
    - To set the task to run only once, select the **Once** option.
  9. Provide values for the attributes of the scheduled task. Refer to the ["Specifying Values for the Scheduled Task Attributes"](#) section on page 2-9 for information about the values to be specified.
- See Also:** *Oracle Identity Manager Design Console Guide* for information about adding and removing task attributes
10. Click **Save**. The scheduled task is created. The `INACTIVE` status is displayed in the **Status** field, because the task is not currently running. The task is run at the date and time that you set in Step 7.

11. Repeat Steps 5 through 10 to create the second scheduled task.

After you create both scheduled tasks, proceed to the ["Step 7: Compiling Adapters"](#) section on page 2-12.

### Specifying Values for the Scheduled Task Attributes

This section provides information about the values to be specified for the following scheduled tasks:

- [Lookup Fields Reconciliation Scheduled Task](#)
- [User Reconciliation Scheduled Task](#)

**Lookup Fields Reconciliation Scheduled Task** You must specify values for the following attributes of the lookup fields reconciliation scheduled task.

---

**Note:** Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.

---

Attribute	Description	Default/Sample Value
LookupCodeName	Name of the lookup definition to which the master values are to be reconciled	<ul style="list-style-type: none"> <li>For groups: Lookup.OID.Usergroups</li> <li>For roles: Lookup.OID.UserRole</li> </ul>
ITResourceName	Name of the IT resource for setting up the connection to Oracle Internet Directory	OID Server
SearchContext	Search context to be used for searching the master values	DC=mycompany, DC=com cn=Groups, dc=bmphktf120, dc=com cn=Roles, dc=bmphktf120, dc=com
ObjectClass	Object class name of the master value for which lookup fields reconciliation is being performed	<ul style="list-style-type: none"> <li>For groups: groupOfUniqueNames</li> <li>For roles: customOrganizationalRole</li> </ul>
CodeKeyLTrimStr	String value for left-trimming the value obtained from the search  If there is nothing to be trimmed, then specify the value [NONE] .	cn=
CodeKeyRTrimStr	String value for right-trimming the value obtained from the search  If there is nothing to be trimmed, then specify the value [NONE] .	, DC=mycompany, DC=com
ReconMode	Specify REFRESH to completely refresh the existing lookup.  Specify UPDATE to update the lookup with new values.	REFRESH or UPDATE

---

**Note:** The CodeKeyLTrimStr and CodeKeyRTrimStr attributes control the value that becomes the code key of the lookup definition. The description of the value is the cn of the master value.

---

For lookup reconciliation for groups in Oracle Identity Manager:

1. Perform steps 1 through 4 of the procedure to create scheduled tasks.
2. Select **OID Group Lookup Reconciliation Task**.
3. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.
4. Provide values for the attributes of the scheduled task. For example:
  - ObjectClass as groupOfUniqueNames
  - LookupCodeName as Lookup.OID.UserGroup
  - SearchContext as cn=Groups, dc=bmphktf120, dc=com

For lookup reconciliation for roles in Oracle Identity Manager:

1. Perform steps 1 through 4 of the procedure to create scheduled tasks.



2. Select **OID Group Lookup Reconciliation Task**.
3. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.
4. Provide values for the attributes of the scheduled task. For example:
  - ObjectClass as customOrganizationalRole
  - LookupCodeName as Lookup.OID.UserRole
  - SearchContext as cn=Roles,dc=bmphktf120,dc=com

After you specify values for these task attributes, proceed to Step 10 of the procedure to create scheduled tasks.

**User Reconciliation Scheduled Task** You must specify values for the following attributes of the user reconciliation scheduled task.

---

**Note:** Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.

---

Attribute	Description	Default/Sample Value
ITResourceName	Name of the IT resource for setting up a connection to Oracle Internet Directory	OID Server
ResourceObjectName	Name of the resource object into which users are to be reconciled	OID User
XLDeleteUsersAllowed	If this attribute is set to true, then the Delete reconciliation event is started. Users who are deleted from the target system are removed from Oracle Identity Manager. This requires all the users on the target system to be compared with all the users in Oracle Identity Manager.  <b>Note:</b> This process affects performance.	true or false
UserContainer	DN value from where the users are reconciled from the target system to Oracle Identity Manager	cn=users,dc=hostname,dc=com  Here, <i>users</i> is the name of the user container and <i>hostname</i> is the host name under which the oracle context is created.
Keystore	Directory path to the Oracle Internet Directory keystore  This is required to set up an SSL connection. Specify [NONE] for a non-SSL connection.	C:\j2sdk1.4.2_09\jre\lib\security\cacerts  or [NONE]
IsTrusted	Specifies whether or not reconciliation is to be performed in trusted mode	True or False
Organization	Default organization of the Xellerate User	Xellerate Users
Xellerate Type	Type of Xellerate User  This is a configurable value.	End-User Administrator
Role	Default role of the Xellerate User	Consultant
Password	Default password of the Xellerate User	Admin123

After you specify values for these task attributes, proceed to Step 10 of the procedure to create scheduled tasks.

## Step 7: Compiling Adapters

The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

- OID Create User
- OID Delete User
- OID Modify User
- OID Move User
- OID Add User to Group
- OID Remove User from Group
- OID Add User to Role
- OID Remove User from Role
- OID Prepop String

You must compile these adapters before you can use them to provision accounts on the target system.

To compile adapters by using the Adapter Manager form:

1. Open the Adapter Manager form.
2. To compile all the adapters that you import into the current database, select **Compile All**.

To compile multiple (but not all) adapters, select the adapters you want to compile. Then, select **Compile Selected**.

---

---

**Note:** Click **Compile Previously Failed** to recompile only those adapters that were not compiled successfully. Such adapters do not have an OK compilation status.

---

---

3. Click **Start**. Oracle Identity Manager compiles the selected adapters.
4. If Oracle Identity Manager is installed in a clustered environment, then copy the compiled adapters from the *OIM\_home\xellerate\Adapter* directory to the same directory on each of the other nodes of the cluster. If required, overwrite the adapter files on the other nodes.

To view detailed information about an adapter:

1. Highlight the adapter in the Adapter Manager form.
2. Double-click the row header of the adapter, or right-click the adapter.
3. Select **Launch Adapter** from the shortcut menu that is displayed. Details of the adapter are displayed.

---

**Note:** To compile one adapter at a time, use the Adapter Factory form. Refer to *Oracle Identity Manager Tools Reference Guide* for information about using the Adapter Factory and Adapter Manager forms.

---

## Step 8: Configuring SSL

---

**Note:** This is an optional step of the deployment procedure.

---

To set up SSL connectivity between Oracle Identity Manager and the Oracle Internet Directory server:

1. Export the Oracle Internet Directory server certificate using Wallet Manager.
2. Check if the Oracle Internet Directory server is listening at the SSL port. If it is not, then set it to the SSL port (typically, the default SSL port is 636). Then, restart the server.
3. Import the certificate from the target system into the JSDK (the JSDK that is used during installation of Oracle Identity Manager) `cacerts` keystore as follows:

```
keytool -import -alias alias_name -file
certificate_file_name_with_complete_path -keystore
java_home\jre\lib\security\cacerts
```

4. Restart the Oracle Identity Manager server.
5. In the `OID Server IT` resource definition:
  - Set the `SSL` parameter value to `true`.
  - Set the `Port` parameter value to the SSL port number. Typically, this number is 636.

## Configuring the Connector for Multiple Installations of the Target System

---

**Note:** Perform this procedure only if you want to configure the connector for multiple installations of Oracle Internet Directory. Refer to *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure.

---

To configure the connector for multiple installations of the target system:

1. Create and configure one resource object for each target system installation.

The Resource Objects form is in the Resource Management folder. The `OID User` resource object is created when you import the connector XML file. You can use this resource object as the template for creating the remaining resource objects.

2. Create and configure one IT resource for each resource object.

The IT Resources form is in the Resource Management folder. The `OID Server IT` resource is created when you import the connector XML file. You can use this IT resource as the template for creating the remaining IT resources, of the same resource type.

3. Design one process form for each resource object.

The Form Designer form is in the Development Tools folder. The following process forms are created when you import the connector XML file:

- UD\_OID\_USR (main form)
- UD\_OID\_ROLE (child form for multivalue attributes)
- UD\_OID\_GRP (child form for multivalue attributes)

You can use these process forms as templates for creating the remaining process forms.

4. Create and configure one process definition for each resource object.

The Process Definition form is in the Process Management folder. The `OID User` process definition is created when you import the connector XML file. You can use this process definition as the template for creating the remaining process definitions.

While creating process definitions for each target system installation, the following steps that you must perform are specific to the creation of each process definition:

- From the **Object Name** lookup field, select the resource object that you create in Step 1.
  - From the **Table Name** lookup field, select the process form that you create in Step 3.
  - While mapping the adapter variables for the IT Resource data type, ensure that you select the IT resource that you create in Step 2 from the **Qualifier** list.
5. Configure reconciliation for each target system installation. Refer to the "[Step 6: Configuring Reconciliation](#)" section on page 2-8 for instructions. Note that only the values of the following attributes are to be changed for each reconciliation scheduled task:

- `ITResourceName`
- `ResourceObjectName`
- `IsTrusted`

Set the `IsTrusted` attribute to `True` for the Oracle Internet Directory installation that you want to designate as a trusted source. You can designate either a single or multiple installations of Oracle Internet Directory as the trusted source. For the remaining Oracle Internet Directory installations, set this attribute to `False`.

6. If required, modify the fields to be reconciled for the Xellerate User resource object.

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the Oracle Internet Directory installation to which you want to provision the user.

## Customizing the Mapping of the User ID Field

---

**Note:** The procedure described in this section is not part of the deployment procedure. You must perform this procedure only if you want to customize the mapping between the user ID fields of Oracle Internet Directory and Oracle Identity Manager.

---

While creating a user account on Oracle Internet Directory through Oracle Identity Manager, the user ID that you specify is assigned to the `cn` field of Oracle Internet Directory. If required, you can customize the mapping so that the user ID is assigned to the `uid` field of Oracle Internet Directory.

**See Also:** *Oracle Identity Manager Design Console Guide* for information about modifying lookup definitions

1. In the Design Console, open the `AttrName.Prov.Map.OID` lookup definition.
2. Change the decode value of the `ldapUserDNPrefix` code key to `uid`.
3. Save the changes.

Now, when you create a user account on Oracle Internet Directory through Oracle Identity Manager, the user ID assigned in Oracle Identity Manager will be assigned to the `uid` field of Oracle Internet Directory.



---

## Testing and Troubleshooting

After you deploy the connector, you must test it to ensure that it functions as expected. This chapter discusses the following topics related to connector testing:

- [Running Test Cases](#)
- [Troubleshooting](#)

### Running Test Cases

You can use the troubleshooting utility to identify the cause of problems associated with connecting to the target system and performing basic operations on the target system.

To use the troubleshooting utility:

1. Specify the required values in the `config.properties` file.

This file is in the `OIM_home\xellerate\Troubleshoot` directory. The following table describes the sections of this file in which you must provide information for running the tests.

Section	Information
Oracle Internet Directory Connection Parameters	Connection parameters required to connect to the target system  Refer to the " <a href="#">Defining IT Resources</a> " section on page 2-7 for information about the values that you must provide.
Create User Information	Values required to create a user
Modify User Information	Values required to modify a user
Delete User Information	DN of the user to be deleted

2. Add the following to the CLASSPATH environment variable:

```
OIM_home\xellerate\JavaTasks\xliOID.jar  
OIM_home\xellerate\lib\xlLogger.jar  
OIM_home\xellerate\ext\log4j-1.2.8.jar  
OIM_home\xellerate\lib\xlUtils.jar
```

3. Perform the following tests:

---

---

**Note:** When you run a BAT file to perform the corresponding test, the `global.properties` file is automatically created in the same directory. You can view log details in the `Troubleshoot.log` file, which is created in the same directory when you run the tests.

---

---

- Create a user by running the `testcreate.bat` file.  
After you run the BAT file, check if the user is created in Oracle Internet Directory with the details given in the `config.properties` file. If you run the BAT file from a command window, then the `User_Creation_Successful` message is displayed.
- Modify the user by running the `testmodify.bat` file.  
After you run the BAT file, check if the user is modified in Oracle Internet Directory with the details given in the `config.properties` file. If you run the BAT file from a command window, the `User_Modification_Successful` message is displayed.
- Delete the user by running the `testdelete.bat` file.  
After you run the BAT file, check if the specified user is deleted from Oracle Internet Directory. If you run the BAT file from a command window, the `User_Deletion_Successful` message is displayed.

## Troubleshooting

This section provides instructions for identifying and resolving some commonly encountered errors of the following types:

- [Connection Errors](#)
- [Create User Errors](#)
- [Delete User Errors](#)
- [Modify User Errors](#)
- [Child Data Errors](#)

### Connection Errors

The following table provides solutions to some commonly encountered connection errors.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection with Oracle Internet Directory. <b>Returned Error Message:</b> LDAP Connection exception <b>Returned Error Code:</b> <code>INVALID_CONNECTION_ERROR</code>	<ul style="list-style-type: none"> <li>■ Ensure that Oracle Internet Directory is running.</li> <li>■ Ensure that Oracle Identity Manager is running.</li> <li>■ Ensure that all the adapters have been compiled.</li> <li>■ Use the IT Resources form to examine the Oracle Identity Manager record. Ensure that the IP address, admin ID, and admin password are correct.</li> </ul>



Problem Description	Solution
Target not available <b>Returned Error Message:</b> Target server not available <b>Returned Error Code:</b> TARGET_UNAVAILABLE_ERROR	<ul style="list-style-type: none"> <li>■ Ensure that Oracle Internet Directory is running.</li> <li>■ Ensure that the specified Oracle Internet Directory connection values are correct.</li> </ul>
Authentication error <b>Returned Error Message:</b> Authentication error <b>Returned Error Code:</b> AUTHENTICATION_ERROR	Ensure that the specified Oracle Internet Directory connection password is correct.

## Create User Errors

The following table provides solutions to some commonly encountered Create User errors.

Problem Description	Solution
The Create User operation failed because an invalid value was being added. <b>Returned Error Message:</b> Invalid value specified for an attribute <b>Returned Error Code:</b> INVALID_ATTR_VALUE_ERROR	Check the values specified during user creation.
Oracle Identity Manager cannot create a user. <b>Returned Error Message:</b> Required information missing <b>Returned Error Code:</b> INSUFFICIENT_INFORMATION_PROVIDED	<p>Ensure that the following information is provided:</p> <ul style="list-style-type: none"> <li>■ User ID</li> <li>■ User password</li> <li>■ User container</li> <li>■ User first name</li> <li>■ User last name</li> </ul>
Oracle Identity Manager cannot create a user. <b>Returned Error Message:</b> User already exists <b>Returned Error Code:</b> USER_ALREADY_EXISTS	A user with the specified ID already exists in Oracle Internet Directory. Assign a new ID to the user, and try again.
Oracle Identity Manager cannot create a user. <b>Returned Error Message:</b> Naming exception <b>Returned Error Code:</b> INVALID_NAMING_ERROR	Check if the specified user container value already exists in Oracle Internet Directory.

Problem Description	Solution
Oracle Identity Manager cannot create a user. <b>Returned Error Message:</b> User creation failed <b>Returned Error Code:</b> USER_CREATION_FAILED	The user cannot be created because one or more attribute values violate the schema definition.  Check if the Oracle Internet Directory schema is correctly defined and contains all the object classes defined in the lookup definition.

## Delete User Errors

The following table provides solutions to some commonly encountered Delete User errors.

Problem Description	Solution
Oracle Identity Manager cannot delete a user. <b>Returned Error Message:</b> Required information missing <b>Returned Error Code:</b> INSUFFICIENT_INFORMATION_PROVIDED	Ensure that the following information is provided: <ul style="list-style-type: none"> <li>■ User Container</li> <li>■ User ID</li> </ul>
Oracle Identity Manager cannot delete a user. <b>Returned Error Message:</b> User does not exist on the target system. <b>Returned Error Code:</b> USER_DOESNOT_EXIST	The specified user ID does not exist in Oracle Internet Directory.

## Modify User Errors

The following table provides solutions to some commonly encountered Modify User errors.

Problem Description	Solution
The Modify User operation failed because a value was being added to a nonexistent attribute. <b>Returned Error Message:</b> Attribute does not exist <b>Returned Error Code:</b> ATTRIBUTE_DOESNOT_EXIST	<ol style="list-style-type: none"> <li>1. From the corresponding process task, get the value passed for AttrName of the connector.</li> <li>2. Using the name obtained in the previous step, check in the AttrName.Recon.Map.OID lookup definition if the decode value is a valid attribute name in the target.</li> </ol>
Oracle Identity Manager cannot modify an attribute of a user. <b>Returned Error Message:</b> Invalid attribute value or state <b>Returned Error Code:</b> INVALID_ATTR_MODIFY_ERROR	The attribute ID and value specified may be wrong. Check the specified values.

Problem Description	Solution
<p>The Modify User operation failed because a value was being added to an attribute that does not exist in the <code>AttrName.Prov.Map.OID</code> lookup definition.</p> <p><b>Returned Error Message:</b> One or more attribute mappings are missing</p> <p><b>Returned Error Code:</b> <code>ATTR_MAPPING_NOT_FOUND</code></p>	<ol style="list-style-type: none"> <li>1. From the corresponding process task, get the value passed for <code>AttrName</code> of the connector.</li> <li>2. Using the name obtained in the previous step, check if an entry has been made in the <code>AttrName.Prov.Map.OID</code> lookup definition.</li> </ol>
<p>Oracle Identity Manager cannot update information about a user.</p> <p><b>Returned Error Message:</b> Error while updating user info</p> <p><b>Returned Error Code:</b> <code>USER_UPDATE_FAILED</code></p>	<p>Generic error. Review the log for more details.</p>
<p>Oracle Identity Manager cannot move a user from one container to another.</p> <p><b>Returned Error Message:</b> Moving user to different container failed</p> <p><b>Returned Error Code:</b> <code>USER_MOVE_FAILED</code></p>	<p>Generic error. Review the log for more details.</p>

## Child Data Errors

The following table provides solutions to some commonly encountered Child Data errors.

Problem Description	Solution
<p>Oracle Identity Manager cannot add a user to a group.</p> <p><b>Returned Error Message:</b> Group does not exist</p> <p><b>Returned Error Code:</b> <code>GROUP_DOESNOT_EXIST</code></p>	<p>The specified user security group does not exist in Oracle Internet Directory. Check the group name.</p>
<p>Oracle Identity Manager cannot add a role to a user.</p> <p><b>Returned Error Message:</b> Role does not exist</p> <p><b>Returned Error Code:</b> <code>ROLE_DOESNOT_EXIST</code></p>	<p>The specified role for the user does not exist in Oracle Internet Directory. Check the role name.</p>
<p>The operation failed because a duplicate value was being added to an attribute.</p> <p><b>Returned Error Message:</b> Duplicate value</p> <p><b>Returned Error Code:</b> <code>DUPLICATE_VALUE_ERROR</code></p>	<p>The user has already been added to the specified group or role.</p>

Problem Description	Solution
<p>Oracle Identity Manager cannot add a user to a group.</p> <p><b>Returned Error Message:</b> Add user to group failed</p> <p><b>Returned Error Code:</b> ADD_USER_TO_GROUP_FAILED</p>	<p>Generic error. Review the log for more details.</p>
<p>Oracle Identity Manager cannot remove a user from a group.</p> <p><b>Returned Error Message:</b> Remove user from group failed</p> <p><b>Returned Error Code:</b> REMOVE_USER_FROM_GROUP_FAILED</p>	<p>Generic error. Review the log for more details.</p>
<p>Oracle Identity Manager cannot add a user to a role.</p> <p><b>Returned Error Message:</b> Add user to role failed</p> <p><b>Returned Error Code:</b> ADD_USER_TO_ROLE_FAILED</p>	<p>Generic error. Review the log for more details.</p>
<p>Oracle Identity Manager cannot remove a user from a role.</p> <p><b>Returned Error Message:</b> Removing assigned role failed</p> <p><b>Returned Error Code:</b> USER_REMOVE_FROM_ROLE_FAILED</p>	<p>Generic error. Review the log for more details.</p>

---

## Known Issues

The following are known issues associated with this release of the connector:

- The default `modifyTimeStamp` field provided by Oracle Internet Directory does not support the search operation. Therefore, all the users are queried for, regardless of the modified timestamp, and the events to be dropped are determined by using the `ignoreEvent` method of the Oracle Identity Manager API.
- During provisioning, the lookup tables for Time Zone and Preferred Language do not display any values. This will be addressed in the next release. For this release, you can work around this problem by manually updating each lookup table.
- Some Asian languages use multibyte character sets. If the character limit for the fields in the target system is specified in bytes, then the number of Asian-language characters that you can enter in a particular field may be less than the number of English-language characters that you can enter in the same field. The following example illustrates this limitation:

Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you were using the Japanese language and if the character limit for the target system fields were specified in bytes, then you would not be able to enter more than 25 characters in the same field.



## Attribute Mappings Between Oracle Identity Manager and Oracle Internet Directory

The following table discusses attribute mappings between Oracle Identity Manager and Oracle Internet Directory.

Oracle Identity Manager Attribute	Oracle Internet Directory attribute	Description
User ID	cn	Login ID
First Name	givenname	First name
Last Name	sn	Last name or surname
Organization Unit	o	Organization to which the user belongs
Email	mail	E-mail address
ldapUserDisableAttr	orclisEnabled	This attribute specifies whether or not the user account is locked. If the value is <code>DISABLED</code> , then it means that the account is locked. If the value is <code>ENABLED</code> , then it means that the account is not locked.
ldapOrgDNPrefix	cn	Common name of an entry (for example, organization, user, role, and group)
ldapUserDNPrefix	cn	Common name of an entry (for example, organization, user, role, and group)
ldapUserUniqueAttr	cn	Common name of an entry (for example, organization, user, role, and group)
Middle Name	middleName	Middle name
ldapUserObjectClass	inetOrgPerson	Object class for the user (primary)
GroupName	uniquemember	Multivalued attribute for the group object, which shows the number of users in the group
RoleName	customRoleOccupant	Customized object class for role
UserGroup	groupOfUniqueNames	Object class for the group
UserRole	customOrganizational Role	Object class for the role
ldapUserDNPrefix	cn	Common name of an entry (for example, organization, user, role, and group)
ldapObjectClass	objectclass	Object class
ldapGroupDNPrefix	cn	Common name of an entry (for example, organization, user, role, and group)

Oracle Identity Manager Attribute	Oracle Internet Directory attribute	Description
Title	title	Designation
Location	l	City of office address
Telephone	telephoneNumber	Office telephone number
Department	departmentNumber	Department name
Preferred Language	PreferredLanguage	Preferred language for communication
ldapPassword	userPassword	Password
Time Zone	orclTimeZone	Time zone
ldapRoleDNPrefix	cn	Common name of an entry (for example, organization, user, role, and group)
ldapRoleMemberAttr	customRoleOccupant	Custom object class for the role  The " <a href="#">Step 2: Configuring the Target System</a> " section on page 2-2 provides information about how to add a custom object class.
ldapUserObjectClassSecondary	orclUserV2	Object class for the user (secondary)
ldapOrgDNPrefix	cn	Common name of an entry (for example, organization, user, role, and Group)



---

---

# Index

## A

---

Adapter Factory form, 2-13  
Adapter Manager form, 2-12  
adapters, compiling, 2-12  
Administrative and User Console, 2-6, 2-8  
attributes  
    lookup fields reconciliation scheduled task, 2-9  
    user reconciliation scheduled task, 2-11  
attributes mappings, A-1

## C

---

changing input locale, 2-3  
Child Data errors, 3-5  
clearing server cache, 2-4  
compiling adapters, 2-12  
configuring  
    connector for multiple installations of the target  
        system, 2-13  
    Oracle Identity Manager server, 2-3  
    reconciliation, 2-8  
    SSL, 2-13  
configuring target system, 2-2  
connection errors, 3-2  
connector files and directories  
    copying, 2-2  
    description, 1-4  
    destination directories, 2-2  
    installation directory, 1-4, 2-2  
connector release number, determining, 1-5  
connector testing, 3-1  
connector XML files  
    *See* XML files  
Create User errors, 3-3  
creating scheduled tasks, 2-8, 2-9

## D

---

defining  
    IT resources, 2-7  
    scheduled tasks, 2-8, 2-9  
Delete User errors, 3-4  
deployment requirements, 2-1  
Design Console, 2-9  
determining release number of connector, 1-5

## E

---

enabling logging, 2-4  
errors  
    Child Data, 3-5  
    connection, 3-2  
    Create User, 3-3  
    Delete User, 3-4  
    Modify User, 3-4

## F

---

files and directories of the connector  
    *See* connector files and directories  
functionality supported, 1-1  
functions available, 1-1

## G

---

globalization features, 1-2

## I

---

importing connector XML files, 2-6  
input locale, changing, 2-3  
issues, 4-1  
IT resources  
    defining, 2-7  
    OID Server, 2-6, 2-7, 2-10, 2-11, 2-13  
    parameters, 2-7  
    types, LDAP Server, 2-6

## L

---

LDAP, 1-2  
Lightweight Directory Access Protocol  
    *See* LDAP  
limitations, 4-1  
logging enabling, 2-4  
lookup fields reconciliation, 1-3  
lookup fields reconciliation scheduled task, 2-9

## M

---

mapping between attributes of target system and  
    Oracle Identity Manager, A-1  
Modify User errors, 3-4

multilanguage support, 1-2

## O

---

Oracle Identity Manager Administrative and User Console, 2-6, 2-8  
Oracle Identity Manager Design Console, 2-9  
Oracle Identity Manager server, configuring, 2-3

## P

---

parameters for IT resources, 2-7  
problems, 3-2  
process tasks, 1-1  
provisioning  
    fields, 1-4  
    functions, 1-1  
    module, 1-4

## R

---

reconciliation  
    configuring, 2-8  
    functions, 1-1  
    lookup fields, 1-3  
    module, 1-3  
    trusted source, 2-8  
    trusted source mode, 1-5  
    user, 1-3  
release number of connector, determining, 1-5  
requirements for deploying, 2-1

## S

---

scheduled tasks  
    attributes, 2-9  
    defining, 2-8, 2-9  
    lookup fields reconciliation, 2-9  
    user reconciliation, 2-11  
server cache, clearing, 2-4  
SSL, configuring, 2-13  
supported  
    functionality, 1-1  
    languages, 1-2  
    releases of Oracle Identity Manager, 2-1  
    target system host platforms, 2-1  
    target systems, 2-1

## T

---

target system, multiple installations, 2-13  
target systems  
    configuration, 2-2  
    host platforms supported, 2-1  
target systems supported, 2-1  
test cases, 3-1  
testing the connector, 3-1  
troubleshooting, 3-2  
troubleshooting utility, 3-1  
trusted source reconciliation, 1-5, 2-8

## U

---

user attribute mappings, A-1  
user reconciliation, 1-3  
user reconciliation scheduled task, 2-11

## X

---

XML files, 1-5  
    copying, 2-3  
    description, 1-5  
    for trusted source reconciliation, 1-5  
    importing, 2-6