Oracle® Identity Manager

Connector Guide for Oracle Internet Directory

Release 9.0.4

E10165-01

May 2007

ORACLE®

Oracle Identity Manager Connector Guide for Oracle Internet Directory, Release 9.0.4

E10165-01

Primary Authors: Debapriya Datta, Shiladitya Guha

Contributing Authors: Don Gosselin, Vijaykarthik Sathiyamurthy, Lyju Vadassery

Contents

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 Connector Pack Release 9.0.4 documentation library, 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
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

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

This chapter provides an overview of the updates made to the software and documentation for the Oracle Internet Directory connector in release 9.0.4 of the Oracle Identity Manager connector pack.

> **See Also:** The 9.0.3.1 release of this guide for information about updates that were new for the 9.0.3.1 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.

Enabling Provisioning of Users in Organizations and Organizational Units

Functionality for enabling provisioning of users in organizations and organizational units is discussed in the following sections:

- Enabling Provisioning of Users in Organizations and Organizational Units on page 3-9

Provisioning and Reconciliation of Organizational Units, Groups, and Roles

Functionality for provisioning of organizational units, groups, and roles has been added. Changes corresponding to this functionality have been discussed in the following sections:

- Provisioning Organizational Units, Groups, and Roles on page 3-10
- Lookup Fields Reconciliation Scheduled Task on page 3-4

Multiple Trusted Reconciliation

In this release, functionality for Oracle Identity Manager to work with multiple connectors in trusted reconciliation mode has been added. This functionality is discussed in the "Partial Reconciliation" section on page 3-1.

Partial Reconciliation

The `CustomizedReconQuery` parameter has been added to the IT resource definition. You can use this parameter to customize the query that the reconciliation module uses to determine the records to be retrieved from the target system. The `CustomizedReconQuery` parameter is explained in the following sections:

- Defining IT Resources on page 2-7
- Partial Reconciliation on page 3-1
- Testing Partial Reconciliation on page 4-2

Support for New Functions

In the "Supported Functionality" section on page 1-3, the following functions have been added:

Create OU (provisioning)

Change OU Name (provisioning)

Delete OU (provisioning)

Move OU (provisioning)

Create OID Group (provisioning)

Delete OID Group (provisioning)

New Group Name Updated (provisioning)

Create OID Role (provisioning)

Delete OID Role (provisioning)

New Role Name Updated (provisioning)

Create User (reconciliation)

Delete User (reconciliation)

Enable User (reconciliation)

Disable User (reconciliation)

Move User (reconciliation)

Add User to Group (reconciliation)

Remove User from Group (reconciliation)

Assign Role to User (reconciliation)

Remove Assigned Role from User (reconciliation)

Changes in the Supported Target Systems List

In the "Step 1: Verifying Deployment Requirements" section on page 2-1, the information on supported target system host platform has been modified. This release of the connector is not dependent on any target system host platform.

Enabling Logging

By following the instructions in the "Enabling Logging" section on page 2-4, you can configure the generation of log information that is specific to the target system.

Documentation-Specific Updates

The following documentation-specific updates have been made in this release of the guide:

- Instructions in the "Determining the Release Number of the Connector" section on page 1-6 have been revised.

1

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:

> **Note:** At some places in this guide, Oracle Internet Directory has been referred to as the *target system.*

Reconciliation Module

Reconciliation involves duplicating in Oracle Identity Manager additions of and modifications to user accounts on the target system. It is an automated process initiated by a scheduled task that you configure.

> **See Also:** The "Deployment Configurations of Oracle Identity Manager" section in *Oracle Identity Manager Connector Framework Guide* for conceptual information about reconciliation configurations

Based on the type of data reconciled from the target system, reconciliation can be divided into the following types:

Lookup Fields Reconciliation

Lookup fields reconciliation involves reconciling the lookup values for organizations, organizational units, 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
- Title
- Organizational Unit
- 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
- User Type
- Employee Type

Provisioning Module

Provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager. You use the Administrative and User Console to perform provisioning operations.

> **See Also:** The "Deployment Configurations of Oracle Identity Manager" section in *Oracle Identity Manager Connector Framework Guide* for conceptual information about provisioning

For this target system, the following fields are provisioned:

- User ID
- First Name
- Last Name
- Middle Name
- Department
- Location
- Telephone
- Email
- Communication Language
- Title
- Organizational Unit
- Group
- Role

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

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
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

Function	Type	Description
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
Create OU	Provisioning	Creates an organizational unit
Change OU Name	Provisioning	Changes an OU name
Delete OU	Provisioning	Deletes an OU
Move OU	Provisioning	Moves organization sub unit to another parent organizational unit
Create OID Group	Provisioning	Creates Oracle Internet Directory group
Delete OID Group	Provisioning	Deletes Oracle Internet Directory group
New Group Name Updated	Provisioning	Changes the group name
Create OID Role	Provisioning	Creates Oracle Internet Directory role
Delete OID Role	Provisioning	Deletes Oracle Internet Directory role
New Role Name Updated	Provisioning	Changes the role name
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.
Create User	Reconciliation	Create a user is Oracle Identity Manager
Delete User	Reconciliation	Deletes a user from Oracle Identity Manager
Enable User	Reconciliation	Enables a user in Oracle Identity Manager
Disable User	Reconciliation	Disables a user in Oracle Identity Manager
Move User	Reconciliation	Moves a user from one container to another container in Oracle Identity Manager
Add User to Group	Reconciliation	Adds a user to a group in Oracle Identity Manager
Remove User from Group	Reconciliation	Removes a user from a group in Oracle Identity Manager
Assign Role to User	Reconciliation	Assigns a role to a user in Oracle Identity Manager
Remove Assigned Role from User	Reconciliation	Removes a role from a user in Oracle Identity Manager

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 the 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.

Multilanguage Support

This release of the connector supports the following languages:

- Chinese Simplified
- Chinese Traditional
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

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

Files and Directories That Comprise the Connector

The files and directories that comprise this connector are 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 "Step 2: Configuring the Target System" section on page 2-1 for more information.
`lib/xliOID.jar`	This JAR file contains the class files required for provisioning and reconciliation.

File in the Installation Media Directory	Description
Files in the `resources` directory	Each of these resource bundle files contains language-specific information that is used by the connector. **Note:** A **resource bundle** 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: ■ IT resource type ■ Custom process form ■ Process task and adapters (along with their mappings) ■ Resource object ■ Xellerate User ■ Provisioning process ■ Pre-populate rules ■ Reconciliation process ■ Lookup definitions
`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 Files" section on page 2-2 provides instructions to copy these files into the required directories.

Determining the Release Number of the Connector

You can use any one of the following methods to determine the release number of the connector.

Before Deployment

To determine the release number of a connector:

1. Extract the contents of the `xliOID.jar` file. This file is in the following directory on the installation media:

   ```
   Directory Servers/Oracle Internet Directory/lib
   ```

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.

Note: If you maintain a copy of the `xliOID.jar` file after deployment, you can use this method to determine the release number of the connector at any stage. After you deploy the connector, it is recommended that you use the "After Deployment" method, which is described in the following section.

After Deployment

To determine the release number of a connector that has already been deployed:

See Also: *Oracle Identity Manager Design Console Guide*

1. Open the Oracle Identity Manager Design Console.
2. In the Form Designer, open the process form. The release number of the connector is the value of the **Version** field.

2

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 Files
- Step 4: Configuring the Oracle Identity Manager Server
- Step 5: Importing the Connector XML File
- Step 6: Configuring SSL

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 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 "Defining IT Resources" section on page 2-7. If you try to perform an operation for which the required permission has not been assigned to the user account, then the "Insufficient Access Rights" message is displayed.

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 Files

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 1-5 for more information about these files.

File in the Installation Media Directory	Destination Directory
Files in the `Batch/custom` directory	Refer to the "Step 2: Configuring the Target System" section on page 2-1 for instructions on copying these files.
`lib/xliOID.jar`	*OIM_home*`/xellerate/JavaTasks`
Files in the `resources` directory	*OIM_home*`/xellerate/connectorResources`
Files in the `Troubleshoot` directory	*OIM_home*`/xellerate/Troubleshoot`
Files in the `xml` directory	*OIM_home*`/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

Note: In this guide, the term *Oracle Identity Manager server* refers to the computer on which Oracle Identity Manager is installed.

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.

You may require the assistance of the system administrator to change to the required input locale.

Clearing Content Related to Connector Resource Bundles from the Server Cache

While performing the instructions described in the "Step 3: Copying the Connector Files and External Code Files" section on page 2-2, you copy files from the `resources` directory on the installation media into the *`OIM_home`*`/xellerate/connectorResources` directory. Whenever you add a new resource bundle in the `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.

Note: You must perform Step 1 before you perform Step 2. If you run the command described in Step 2 as follows, then an exception is thrown:

OIM_home/xellerate/bin/*batch_file_name*

2. Enter one of the following commands:

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

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

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

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:

- **BEA WebLogic**

  To enable logging:

  1. Add the following lines in the *OIM_home*/xellerate/config/log.properties file:

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.OID=log_level
     ```

  2. In these lines, replace *log_level* with the log level that you want to set.

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     log4j.logger.XL_INTG.OID=INFO
     ```

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

  WebLogic_home/user_projects/domains/*domain_name*/*server_name*/*server_name*.log

- **IBM WebSphere**

  To enable logging:

  1. Add the following lines in the *OIM_home*/xellerate/config/log.properties file:

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.OID=log_level
     ```

  2. In these lines, replace *log_level* with the log level that you want to set.

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     log4j.logger.XL_INTG.OID=INFO
     ```

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

  WebSphere_home/AppServer/logs/*server_name*/startServer.log

- **JBoss Application Server**

  To enable logging:

  1. In the *JBoss_home*/server/default/conf/log4j.xml file, locate or add the following lines:

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

     <category name="XL_INTG.OID">
        <priority value="log_level"/>
     </category>
     ```

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

     ```
     <category name="XELLERATE">
     ```

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

<category name="XL_INTG.OID">
   <priority value="INFO"/>
</category>
```

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

JBoss_home/server/default/log/server.log

- **OC4J**

  To enable logging:

  1. Add the following lines in the *OIM_home*/xellerate/config/log.properties file:

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.OID=log_level
     ```

  2. In these lines, replace *log_level* with the log level that you want to set.

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     log4j.logger.XL_INTG.OID=INFO
     ```

  After you enable logging, the 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 File

As mentioned in the "Files and Directories That Comprise the Connector" section on page 1-5, the connector XML file contains definitions of the components of the connector. By importing the connector XML file, you create these components in Oracle Identity Manager.

To import the connector XML file:

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. These nodes represent Oracle Identity Manager entities that are redundant. Before you import the connector XML file, you must remove these entities 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 file, proceed to the "Step 6: Configuring SSL" 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: `cn=Admin,ou=People, o=xyz`
`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: `dc=host_name, dc=com` Here, *`host_name`* is the host name under which Oracle ConText is created.
`SSL`	If this parameter is set to `true`, 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 `false`, then SSL is not used to secure communication between Oracle Identity Manager and the Oracle Internet Directory server. **Note:** 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 `AttrName.Prov.Map.OID`.
`Recon Attribute Lookup Code`	Name of the lookup definition that has the target attribute mappings required for reconciliation The value must be `AttrName.Recon.Map.OID`.

Parameter	Description
`Use XL Org Structure`	If set to `true`, then the Oracle Identity Manager Organization structure is used during provisioning and reconciliation. If set to `false`, 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.
`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`
`CustomizedReconQuery`	Query condition on which reconciliation must be based If you specify a query condition for this parameter, then the target system records are searched based on the query condition. If you want to reconcile all the target system records, then do not specify a value for this parameter. The query can be composed with the AND (&) and OR (|) logical operators. Sample value: `cn=JOHN` For more information about this parameter, refer to the "Partial Reconciliation" section on page 3-1.

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

Step 6: 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.

3

Configuring the Connector

After you deploy the connector, you must configure it to meet your requirements. This chapter discusses the following connector configuration procedures:

> **Note:** These sections provide both conceptual and procedural information about configuring the connector. It is recommended that you read the conceptual information before you perform the procedures.

- Configuring Reconciliation
- Configuring Provisioning
- Configuring the Connector for Multiple Installations of the Target System
- Configuring the Mapping of the User ID Field

Configuring Reconciliation

As mentioned earlier in this guide, reconciliation involves duplicating in Oracle Identity Manager additions of and modifications to user accounts on the target system. This section discusses the following topics related to configuring reconciliation:

- Partial Reconciliation
- Configuring Trusted Source Reconciliation
- Configuring the Reconciliation Scheduled Tasks

Partial Reconciliation

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. You can customize this process by specifying the subset of added or modified target system records that must be reconciled. You do this by creating filters for the reconciliation module.

For this connector, you create a filter by specifying values for the `CustomizedReconQuery` IT resource parameter while performing the procedure described in the "Defining IT Resources" section on page 2-7.

The following table lists the Oracle Internet Directory attributes, and the corresponding Oracle Identity Manager attributes, that you can use to build the query condition. You specify this query condition as the value of the `CustomizedReconQuery` parameter.

Oracle Internet Directory Attribute	Oracle Identity Manager Attribute
cn	User Id
givenname	First Name
sn	Last Name
mail	Email
middleName	Middle Name
departmentNumber	Department
l	Location
title	Title

The following are sample query conditions:

- `givenname=John&sn=Doe`

  With this query condition, records of users whose first name is John and last name is Doe are reconciled.

- `givenname=John|departmentNumber=23`

  With this query condition, records of users who meet either of the following conditions are reconciled:

  - The user's first name is `John`.
  - The user belongs to the departmentNumber `23`.

If you do not specify values for the `CustomizedReconQuery` parameter, then all the records in the target system are compared with existing Oracle Identity Manager records during reconciliation.

The following are guidelines to be followed while specifying a value for the `CustomizedReconQuery` parameter:

- For the Oracle Internet Directory attributes, you must use the same case (uppercase or lowercase) as given in the table shown earlier in this section. This is because the attribute names are case-sensitive.
- You must not include unnecessary blank spaces between operators and values in the query condition.

  A query condition with spaces separating values and operators would yield different results as compared to a query condition that does not contain spaces between values and operators. For example, the output of the following query conditions would be different:

  ```
  givenname=John&sn=Doe
  ```

  ```
  givenname= John&sn= Doe
  ```

  In the second query condition, the reconciliation engine would look for first name and last name values that contain a space at the start.

- You must not include special characters other than the equal sign (=), ampersand (&), and vertical bar (|) in the query condition.

  Note: An exception is thrown if you include special characters other than the equal sign (=), ampersand (&), and vertical bar (|).

You specify a value for the `CustomizedReconQuery` parameter while performing the procedure described in the "Defining IT Resources" section on page 2-7.

Configuring Trusted Source Reconciliation

While configuring the connector, the target system can be designated as a trusted source or target resource. If you designate the target system as a **trusted source**, then both newly created and modified user accounts are reconciled in Oracle Identity Manager. If you designate the target system as a **target resource**, then only modified user accounts are reconciled in Oracle Identity Manager.

Note: You can skip this section if you do not want to designate the target system as a trusted source for reconciliation.

Configuring trusted source reconciliation involves the following steps:

1. Import the XML file for trusted source reconciliation, `oimUser.xml`, by using the Deployment Manager. This section describes the procedure to import the XML file.

   Note: Only one target system can be designated as a trusted source. If you import the `oimUser.xml` file while you have another trusted source configured, then both connector reconciliations would stop working.

2. Set the `IsTrusted` scheduled task attribute to `True`. You specify a value for this attribute while configuring the user reconciliation scheduled task, which is described later in this guide.

To import the XML file for trusted source reconciliation:

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**.

After you import the XML file for trusted source reconciliation, you must set the value of the `IsTrusted` reconciliation scheduled task attribute to `True`. This procedure is described in the "Configuring the Reconciliation Scheduled Tasks" section on page 3-4.

Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in the "Step 5: Importing the Connector XML File" section on page 2-6, the scheduled tasks for lookup fields and user reconciliations are automatically created in Oracle Identity Manager. To configure these scheduled tasks:

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 3-4 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 configure both scheduled tasks, proceed to the "Configuring Provisioning" section on page 3-7.

Specifying Values for the Scheduled Task Attributes

This section provides information about the attribute 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 `OID Group Lookup Reconciliation Task` 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.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value were left empty, then reconciliation would not be performed.

Attribute	Description	Default/Sample Value

`LookupCodeName`	Name of the lookup definition to which the master values are to be reconciled	The value can be any one of the following:
		■ For groups lookup reconciliation:
		`Lookup.OID.UserGroup`
		■ For roles lookup reconciliation:
		`Lookup.OID.UserRole`
		■ For organization and organizational unit lookup reconciliation:
		`Lookup.OID.Organization`

`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	The following are sample 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	The value can be any one of the following:
		■ For groups lookup reconciliation:
		`groupOfUniqueNames`
		■ For roles lookup reconciliation:
		`customOrganizationalRole`
		■ For organization lookup reconciliation:
		`Organization`
		■ For organizational unit lookup reconciliation:
		`OrganizationalUnit`

`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`

Attribute	Description	Default/Sample Value
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 configure scheduled tasks. These steps are described earlier in this section.
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: groupOfUniqueNames
   - LookupCodeName: Lookup.OID.UserGroup
   - SearchContext: 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 configure scheduled tasks. These steps are described earlier in this section.
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: customOrganizationalRole
   - LookupCodeName: Lookup.OID.UserRole
   - SearchContext: cn=Roles,dc=bmphktf120,dc=com

After you perform the steps required to configure the lookup fields reconciliation scheduled task, 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 OID User Recon 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.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value were left empty, then reconciliation would not be performed.

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 when the scheduled task is run. 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. **Note:** 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, *users* is the name of the user container and *hostname* 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	Default xellerate type for the Xellerate User This is a configurable value.	End-User Administrator
Role	Default role for the Xellerate User	Consultant

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

Configuring Provisioning

As mentioned earlier in this guide, provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager. Refer to the "Supported Functionality" section on page 1-3 for a listing of the provisioning functions that are available with this connector.

- Compiling Adapters
- Enabling Provisioning of Users in Organizations and Organizational Units

Compiling Adapters

Note: You must perform the procedure described in this section if you want to use the provisioning features of the connector.

Adapters are used to implement provisioning functions. The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

> **See Also:** The "Supported Functionality" section on page 1-3 for a listing of the provisioning functions that are available with this connector

- 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
- Update OID Role Details
- Update OID Group Details
- OID Delete Group
- OID Create Group
- Chk Process Parent Org
- OID Create OU
- OID Create Role
- OID Delete Role
- OID Move OU
- OID Change Org Name
- OID Delete OU

You must compile these adapters before they can be used in provisioning operations.

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.

If you want to compile one adapter at a time, then use the Adapter Factory form.

> **See Also:** *Oracle Identity Manager Tools Reference Guide* for information about using the Adapter Factory and Adapter Manager forms

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.

Adding Object Classes for Provisioning

The ldapUserObjectClassSecondary field is one of the fields defined in the AttrName.Prov.Map.OID lookup definition.

By default, this field contains a value that you can change to the name of your object class. If required, you can modify the ldapUserObjectClassSecondary field and add a second object class with a vertical bar (|) separating the two object classes. The following is a sample value that can be assigned to the ldapUserObjectClassSecondary field:

```
objclass1|objClass2
```

You must ensure that the attributes in the new object class are optional, and not mandatory, attributes.

> **Note:** You cannot add more than two object classes in the ldapUserObjectClassSecondary field.

Enabling Provisioning of Users in Organizations and Organizational Units

> **Note:** This section describes an optional procedure. You need not perform this procedure if you do not want to enable provisioning of users in organizations.

In the AttrName.Prov.Map.OID lookup definition, the following are default settings for enabling provisioning of users in organizational units:

- ldapOrgDNPrefix=ou
- ldapOrgUnitObjectClass=OrganizationalUnit

If you want to enable the provisioning of users in organizations, then change these settings as follows:

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

- `ldapOrgDNPrefix=o`
- `ldapOrgUnitObjectClass=organization`

See Also: Appendix A for information about attribute mappings between Oracle Identity Manager and Oracle Internet Directory.

Provisioning Organizational Units, Groups, and Roles

To provision an organizational unit:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. Expand **Organizations**.
3. Click **Create**.
4. Specify a name and the type for the organization that you want to create, and then click **Create Organization**.
5. Select **Resource Profile** from the list.
6. Click **Provision New Resource**.
7. Select the organizational unit option.
8. Click **Continue**, and then click **Continue** again.
9. From the IT server lookup field, select the resource object corresponding to the required IT resource.
10. Click **Continue**, and then click **Continue** again on the Verification page.

To provision a group or role:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. Expand **Organizations**.
3. Click **Manage**.
4. Search for the organizational unit under which you want to provision the group or role.
5. Select **Resource Profile** from the list.
6. Click **Provision New Resource**.
7. On this page, the option that must select depends on what you want to create:
   - Select the group option if you want to create a group.
   - Select the role option if you want to create a group.
8. Click **Continue**, and then click **Continue** again on the Verification page.
9. Enter a name for the group or role.
10. From the IT server lookup field, select the IT resource.
11. Click **Continue**, and then click **Continue** again on the Verification page.

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.

You may want to configure the connector for multiple installations of Oracle Internet Directory. The following example illustrates this requirement:

The Tokyo, London, and New York offices of Acme Multinational Inc. have their own installations of Oracle Internet Directory. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of Oracle Internet Directory.

To meet the requirement posed by such a scenario, you must configure the connector for multiple installations of Oracle Internet Directory.

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

> **See Also:** *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure

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 "Configuring Reconciliation" section on page 3-1 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.

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.

Configuring 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.

4

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 testing 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 testing 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 "Defining IT Resources" 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.

Testing Partial Reconciliation

To test query-based reconciliation, you can specify the following types of query conditions as values for the `CustomizedReconQuery` parameter:

- Query consisting of groups

  Value assigned to the `CustomizedReconQuery` parameter: `group=group1`

  All the users belonging to `group1` are reconciled.

- Query consisting of roles

  Value assigned to the `CustomizedReconQuery` parameter: role=role1

  All the users belonging to role1 are reconciled.

- Query consisting of groups and basic user attributes
  - Value assigned to the `CustomizedReconQuery` parameter: `sn=Doe&group=group1`

    The users with last name Doe and who belong to `group1` are reconciled.
  - Value assigned to the `CustomizedReconQuery` parameter: `sn=Doe&group=group1,group2`

    The users with last name `Doe` and who belong to both the groups `group1` and `group2` are reconciled.
- Query consisting of roles and basic attributes
  - Value assigned to the `CustomizedReconQuery` parameter: `sn=Doe&role=role1`

    The users with last name `Doe` and who belong to `role1` are reconciled.
  - Value assigned to the `CustomizedReconQuery` parameter: `sn=Doe&role=role1,role2`

The users with last name `Doe` and who belong to both the roles `role1` and `role2` are reconciled.

- Query consisting of groups, roles, and basic attributes
  - Value assigned to the `CustomizedReconQuery` parameter: `sn=Doe&group=group1&role=role1`

    The users with last name `Doe` and who belongs to `group1` as well as `role1` are reconciled.

Troubleshooting

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

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. **Returned Error Message:** Connection error encountered **Returned Error Code:** `INVALID_CONNECTION_ERROR`	▪ Ensure that Oracle Internet Directory is running. ▪ Ensure that Oracle Identity Manager is running. ▪ Ensure that all the adapters have been compiled. ▪ Use the IT Resources form to examine the Oracle Identity Manager record. Ensure that the IP address, admin ID, and admin password are correct.
Target not available **Returned Error Message:** Target server not available **Returned Error Code:** `TARGET_UNAVAILABLE_ERROR`	▪ Ensure that Oracle Internet Directory is running. ▪ Ensure that the specified Oracle Internet Directory connection values are correct.
Authentication error **Returned Error Message:** Invalid or incorrect administrator password **Returned Error Code:** `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. **Returned Error Message:** Invalid value specified for an attribute **Returned Error Code:** `INVALID_ATTR_VALUE_ERROR`	Check the values specified during user creation.
Oracle Identity Manager cannot create a user. **Returned Error Message:** Required information missing **Returned Error Code**: `INSUFFICIENT_INFORMATION_PROVIDED`	Ensure that the following information is provided: ■ User ID ■ User password ■ User container ■ User first name ■ User last name
Oracle Identity Manager cannot create a user. **Returned Error Message:** User already exists **Returned Error Code:** `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. **Returned Error Message:** Naming exception encountered **Returned Error Code**: `INVALID_NAMING_ERROR`	Check if the specified user container value already exists in Oracle Internet Directory.
Oracle Identity Manager cannot create a user. **Returned Error Message:** Could not create user **Returned Error Code:** `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. **Returned Error Message:** Required information missing **Returned Error Code:** `INSUFFICIENT_INFORMATION_PROVIDED`	Ensure that the following information is provided: ■ User Container ■ User ID

Problem Description	Solution
Oracle Identity Manager cannot delete a user. **Returned Error Message:** User does not exist **Returned Error Code**: `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. **Returned Error Message:** Attribute does not exist **Returned Error Code:** `ATTRIBUTE_DOESNOT_EXIST`	1. From the corresponding process task, get the value passed for `AttrName` of the connector. 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.
Oracle Identity Manager cannot modify an attribute of a user. **Returned Error Message:** Invalid attribute value or state **Returned Error Code:** `INVALID_ATTR_MODIFY_ERROR`	The attribute ID and value specified may be wrong. Check the specified values.
The Modify User operation failed because a value was being added to an attribute that does not exist in the `AttrName.Prov.Map.OID` lookup definition. **Returned Error Message:** One or more attribute mappings are missing **Returned Error Code**: `ATTR_MAPPING_NOT_FOUND`	1. From the corresponding process task, get the value passed for `AttrName` of the connector. 2. Using the name obtained in the previous step, check if an entry has been made in the `AttrName.Prov.Map.OID` lookup definition.
Oracle Identity Manager cannot update information about a user. **Returned Error Message:** Could not update user **Returned Error Code**: `USER_UPDATE_FAILED`	Generic error. Review the log for more details.
Oracle Identity Manager cannot move a user from one container to another. **Returned Error Message:** Could not move user **Returned Error Code:** `USER_MOVE_FAILED`	Generic error. Review the log for more details.

Child Data Errors

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

Problem Description	Solution
Oracle Identity Manager cannot add a user to a group. **Returned Error Message:** Group does not exist **Returned Error Code:** GROUP_DOESNOT_EXIST	The specified user security group does not exist in Oracle Internet Directory. Check the group name.
Oracle Identity Manager cannot add a role to a user. **Returned Error Message:** Role does not exist **Returned Error Code:** ROLE_DOESNOT_EXIST	The specified role for the user does not exist in Oracle Internet Directory. Check the role name.
The operation failed because a duplicate value was being added to an attribute. **Returned Error Message:** Duplicate value encountered **Returned Error Code:** DUPLICATE_VALUE_ERROR	The user has already been added to the specified group or role.
Oracle Identity Manager cannot add a user to a group. **Returned Error Message:** Could not add user to group **Returned Error Code:** ADD_USER_TO_GROUP_FAILED	Generic error. Review the log for more details.
Oracle Identity Manager cannot remove a user from a group. **Returned Error Message:** Could not remove user from group **Returned Error Code:** REMOVE_USER_FROM_GROUP_FAILED	Generic error. Review the log for more details.
Oracle Identity Manager cannot add a user to a role. **Returned Error Message:** Add user to Role failed **Returned Error Code:** ADD_USER_TO_ROLE_FAILED	Generic error. Review the log for more details.
Oracle Identity Manager cannot remove a user from a role. **Returned Error Message:** Removing assigned role failed **Returned Error Code:** REMOVE_ROLE_FROM_USER_FAILED	Generic error. Review the log for more details.

5

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.

A

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
Organizational 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 `DISABLED`, then it means that the account is locked. If the value is `ENABLED`, 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	Multivalued attribute for the role object, which shows the number of users in the 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

Oracle Identity Manager Attribute	Oracle Internet Directory attribute	Description
ldapGroupDNPrefix	cn	Common name of an entry (for example, organization, user, role, and group)
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 "Step 2: Configuring the Target System" section on page 2-1 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

M

O

P

R

S

T

U

V

X