Oracle® Identity Manager

Connector Guide for Oracle Internet Directory

Release 9.0.4

E10436-07

July 2009

ORACLE®

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

E10436-07

Primary Author: Lyju Vadassery

Contributing Authors: Debapriya Datta, Devanshi Mohan, Alankrita Prakash

Contents

3 Configuring the Connector

4 Testing and Troubleshooting

Preface

This guide provides information about Oracle Identity Manager Connector for Oracle Internet Directory.

Audience

This guide is intended for resource administrators and target system integration teams.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. 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.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of phone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html.

Related Documents

For information about installing and using Oracle Identity Manager, see the Oracle Identity Manager documentation library.

For generic information about connectors, see *Oracle Identity Manager Connector Concepts*.

The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

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

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connectors documentation, 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 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 9.0.4.6.

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

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

- Software Updates

  This section describes updates made to the connector software.

- Documentation-Specific Updates

  This section describes major changes made to this guide. These changes are not related to software updates.

Software Updates

The following sections discuss updates made from release 9.0.4 to the current release of the connector:

- Software Updates in Release 9.0.4.1
- Software Updates in Release 9.0.4.1_6673431
- Software Updates in Release 9.0.4.2
- Software Updates in Release 9.0.4.3
- Software Updates in Release 9.0.4.4
- Software Updates in Release 9.0.4.5
- Software Updates in Release 9.0.4.6

Software Updates in Release 9.0.4.1

The following is a software update in release 9.0.4.1:

- Changes in the Directory Structure of the Connector Files on the Installation Media

Changes in the Directory Structure of the Connector Files on the Installation Media

The `xliOID.jar` file has been split into two files, `OIDProv.jar` and `OIDRecon.jar`. Corresponding changes have been made in the following sections:

Software Updates in Release 9.0.4.1_6673431

The following are resolved issues in release 9.0.4.1_6673431:

Bug Number	Issue	Resolution
6673431	Delete reconciliation was run after trusted source reconciliation. This sequence resulted in deletion of some OIM Users who were not actually deleted on the target system.	This issue has been resolved. During a trusted source reconciliation run, the API that implements Delete reconciliation is called before reconciliation of existing target system records.

Software Updates in Release 9.0.4.2

The following are resolved issues in release 9.0.4.2:

Bug Number	Issue	Resolution
7003824	If you added an object class and its attributes, then subsequent Create User provisioning operations failed. An error message similar to the following one was displayed as the outcome of the provisioning operations: `"Unable to add attributes of the object[LDAP: error code 65 - associatedDomain attribute not found. Mandatory Attribute missing.]"`	This issue has been resolved. You can now add an object class and then perform Create User provisioning operations. See "Adding New Object Classes for Provisioning and Reconciliation" for more information. **Note:** A trusted source reconciliation run fails if it involves user-defined fields (UDFs). This issue is tracked through Bug 7047363.

Software Updates in Release 9.0.4.3

The following is a software update in release 9.0.4.3:

Using the Connector Installer

From Oracle Identity Manager release 9.1.0 onward, the Administrative and User Console provides the Connector Installer feature. This feature can be used to automate the connector installation procedure.

See "Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later" on page 2-2 for details.

Software Updates in Release 9.0.4.4

The following are resolved issues in release 9.0.4.4:

Bug Number	Issue	Resolution
7257647	The connector did not support batched or paged reconciliation. There were performance issues related to this limitation.	The connector now supports paged reconciliation. You can implement this feature if the target system is Oracle Internet Directory 10.1.4.0.1 or later. See "Paged Reconciliation" on page 3-3 for more information.

Bug Number	Issue	Resolution
7306055	There was scope for improvement in the performance of the following provisioning operations: ■ Adding or removing a user from a group ■ Granting or removing a role from a user	The performance of provisioning operations that involve group or role membership changes has been enhanced.

Software Updates in Release 9.0.4.5

The following are resolved issues in release 9.0.4.5:

Bug Number	Issue	Resolution
7564492, 6334595, 6317860	Incremental reconciliation was not supported. If you deleted one user from one organization on the target system and then performed trusted source delete reconciliation, then all users were deleted from all organizations in Oracle Identity Manager. During reconciliation, user data was fetched from the target system, regardless of whether or not it had been modified.	Incremental reconciliation is now supported.
6312504	IT resource parameters for the names of the lookup definitions for reconciliation and provisioning were set to NULL when you restarted Oracle Identity Manager.	The names of the lookup definitions are set as the default values of the IT resource parameters. These parameters are not set to NULL when you restart Oracle Identity Manager.
6168631	In earlier releases, you had to use the orcladmin account on the target system for reconciliation and provisioning operations.	This issue has been resolved. You can now create a user on the target system, assign the minimum required permissions to the user, and then use it for connector operations.
6312344	The default value of the Organization DN field on the Administrative and User Console was cn=user.	The Organization DN field has been changed to a lookup field, and the default value has been removed. You can now select a value in this lookup field.
6804852	The Manager ID field was not available for reconciliation and provisioning.	The Manager ID field has been added to the list of fields that are available for reconciliation and provisioning.
7233799	At the end of a successful provisioning operation, the "Mapping Not Found" message was recorded in the log file. This message has now been removed.	This issue has been resolved. The "Mapping Not Found" message is no longer recorded in the log file at the end of a successful provisioning operation. The following are some of the entries in the AttrName.Prov.Map.OID lookup definition. You must ensure that these entries are not changed. ldapUserID: cn ldapFirstName: givenName ldapLastName: sn ldapPassword: userPassword

Bug Number	Issue	Resolution
6987536	The Start Date and End Date fields of the target system were not used by the connector.	This issue has been resolved. The Start Date and End Date fields have been added for reconciliation and provisioning operations.
7022721	The process form had two fields for two object classes. This imposed a limitation on the number of objectclasses to which a user could be assigned during a Create User provisioning operation.	This issue has been resolved. The Objectclassess field replaces the two fields on the process form. You can enter a list of objectclasses in this field during a provisioning operation. Use the vertical bar (|) as the delimiter character in the list of objectclasses.
7047363	You could not add to the default attribute mappings for reconciliation.	This issue has been resolved. You can now use the AttrName.Recon.Map.OID lookup definition to add attributes for reconciliation. See "Adding the Object Class and its Attributes to the Lookup Definition for Reconciliation" in the connector guide for more information.
6490731	The length of the Password field was 14 bytes.	The length of the Password field has been increased to 30 bytes.
7434067	A reconciliation error was encountered if you applied a custom reconciliation query that filtered user records by both role assignment and group membership. For example, application of the following reconciliation query would result in an error: role=role1&group=group1	This issue has been resolved. Any combination of the following attributes can be used in the query: ■ givenname ■ sn ■ givenname&sn ■ group ■ role ■ givenname&group ■ givenname&role ■ group&role Limitation: The custom reconciliation query must not include field values that contain any of the following characters: ■ & (ampersand) ■ | (vertical bar) ■ = (equal sign) In addition, the field values must not contain the word "group" or "role." The following are examples of query conditions that are invalid: givenname="mary&brown" This value is invalid because it contains the ampersand (&). givenname="johngroup" This value is invalid because it contains the word group.
7360833	The name of the IT resource type for all LDAP-based connectors was LDAP Server.	This issue has been resolved. The IT resource type for the Oracle Internet Directory connector has been renamed to "OID IT Resource."
7308328	A space after a comma in the DN value would cause a reconciliation error.	This issue has been resolved. DN values that have a space after the comma are now correctly reconciled. You implement this solution by copying the JAR files as part of the deployment procedure.

Bug Number	Issue	Resolution
7218933	The "INSUFFICIENT_INFORMATION_PROVIDED" message was displayed if any process form field was left empty during a provisioning operation. The field itself was not pointed out by the message.	This issue has been resolved. The name of the field in which a value has not been provided is included in the message displayed on the console.
7120339	The INSUFFICIENT_INFORMATION_PROVIDED error message was not mapped in the resource bundle.	This issue has been resolved. The error message is now mapped in the resource bundle.
7165810	When you changed the name of an organizational unit through a provisioning operation, the existing OU was deleted and then re-created with the new name that you specified.	This issue has been resolved. The name of the OU is actually changed when you perform the Change OU Name provisioning operation. The OU is not deleted and re-created with the new name. You implement this solution by copying the JAR files as part of the deployment procedure.
6275476	On the target system, DNs of groups are not case-sensitive. In Oracle Identity Manager, group DNs are case-sensitive. This caused problems during reconciliation of group membership details.	■ This issue has been resolved. Group DNs are converted to lowercase before they are reconciled into the group lookup definition in Oracle Identity Manager. In other words, Oracle Identity Manager does not perform a case-sensitive check on group names. ■ You implement this solution by copying the JAR files as part of the deployment procedure.
7423099	Special characters were not supported in the First Name and Last Name fields on the process form.	This issue has been resolved. See "Provisioning Module" in the connector guide for information about the special characters that are supported in process form fields. You implement this solution by copying the JAR files as part of the deployment procedure.
6489877	The connector supported neither Mode 1 nor Mode 2 secure connections to Oracle Internet Directory.	The connector supports Mode 1 secure connections to Oracle Internet Directory. See "Configuring SSL" in the connector guide for detailed information.
7564599	During a Create Group provisioning operation, it was mandatory to specify a parent OU for the group.	This issue has been resolved. If a parent OU is not specified, then the group is created under the DN context.
7601582	The User Deletion Successful message was displayed when the Delete User provisioning operation was performed on a user who had already been deleted on the target system.	The message has been corrected.
7301659	The orclguid field of the target system stores identifier for each LDAP entry in Oracle Internet Directory. The connector did not fetch and store the orclguid of target system users.	This issue has been resolved. The connector now retrieves and stores the orclguid field of target system users.

Software Updates in Release 9.0.4.6

The following are the software updates in release 9.0.4.6:

- Support for Reconciliation and Provisioning of Multivalued Attributes
- Support for New Target System

Support for Reconciliation and Provisioning of Multivalued Attributes

From this release onward, the connector supports the reconciliation and provisioning of multivalued attributes. See "Adding New Multivalued Attributes for Reconciliation and Provisioning" for the procedure to add new multivalued attributes for reconciliation and provisioning.

Support for New Target System

From this release onward, the connector adds support for Oracle Internet Directory 11gR1 as the target system.

This target system is mentioned in the "Verifying Deployment Requirements" section of the connector guide.

Documentation-Specific Updates

The following sections discuss documentation-specific updates in the guide:

- Documentation-Specific Updates in Releases 9.0.4.1 Through 9.0.4.5
- Documentation-Specific Updates in Release 9.0.4.6

Documentation-Specific Updates in Releases 9.0.4.1 Through 9.0.4.5

The following documentation-specific update has been made in releases 9.0.4.1 through 9.0.4.5:

- New points have been added in the "Known Issues" chapter.

Documentation-Specific Updates in Release 9.0.4.6

The following documentation-specific updates have been made in release 9.0.4.6:

- In the "Configuring the Connector" chapter:
  - The "Configuring the Connector for Multiple Installations of the Target System" section has been removed. This feature is not supported by default.
  - The following sections have been added:
    * Adding New Attribute for Target Resource Reconciliation
    * Adding New Attribute for Provisioning
- In the "Lookup Fields Reconciliation Scheduled Task" section:
  - The name of the reconciliation scheduled task has been changed from `OID Group Lookup Reconciliation Task` to `OID Lookup Reconciliation Task`.
  - The `AttrType` attribute has been added to the list of `OID Lookup Reconciliation Task` reconciliation scheduled task attributes.
  - The `LookupCodeName` attribute values for groups, roles, and organization and organization unit have been changed.
- The "Customizing the xlconfig.xml File" section has been moved from the "Configuring the Oracle Identity Manager Server" section to a new location. The instructions described in the "Customizing the xlconfig.xml File" section are now performed before installing the connector.

- In the "Setting Up Lookup Definitions in Oracle Identity Manager" section:
  - The name of the lookup definition has been changed from `global.AttrName.Prov.Map.OID.Preferred-Language` to `Lookup.OID.PrefLang`.
  - The `global.AttrName.Prov.Map.OID.Location` and `global.AttrName.Prov.Map.OID.Time-Zone` definitions have been removed as they have been converted into text fields.
- In the "Deploying the Connector" chapter, the procedure to add custom object classes and custom attributes on the target system has been removed.
- In the "Verifying Deployment Requirements" section, changes have been made in the "Target systems" row.

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. This guide discusses the procedure to deploy the connector that is used to integrate Oracle Identity Manager with Oracle Internet Directory.

This chapter contains the following sections:

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

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

1.1 Reconciliation Module

Reconciliation involves duplicating in Oracle Identity Manager the creation 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 Concepts 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:

1.1.1 Lookup Fields Reconciliation

Lookup fields reconciliation involves reconciling the lookup values for organizations, organizational units, groups, and roles.

1.1.2 User Reconciliation

This section provides information about user reconciliation.

1.1.2.1 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

1.1.2.2 Reconciled Xellerate User (OIM 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

1.2 Provisioning Module

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

> **See Also:** The "Deployment Configurations of Oracle Identity Manager" section in *Oracle Identity Manager Connector Concepts 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.

The following table lists special characters that are supported in process form fields:

Note: The following special characters are *not* supported in process form fields:

- Single quotation mark (')
- Double quotation mark (")

Name of the Character	Character
ampersand	&
asterisk	*
at sign	@
caret	^
comma	,
dollar sign	$
equal sign	=
exclamation point	!
hyphen	-
left brace	{
left bracket	[
left parenthesis	(
number sign	#

Name of the Character	Character
percent sign	%
period	.
plus sign	+
question mark	?
right brace	}
right bracket	]
right parenthesis	)
slash	/
underscore	_

1.3 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
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

Function	Type	Description
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.

1.4 Multilanguage Support

This release of the connector supports the following languages:

- Arabic
- Chinese Simplified
- Chinese Traditional

- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

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

1.5 Files and Directories on the Installation Media

The files and directories on the installation media are listed and described in Table 1–1.

Table 1–1 Files and Directories On the Connector Installation Media

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 "Configuring the Target System" section on page 2-1 for more information.
`configuration/OracleInternetDirectory-CI.xml`	This XML file contains configuration information that is used during connector installation.
`lib/OIDProv.jar`	This JAR file contains the class files required for provisioning. During connector deployment, this file is copied into the following directory: *OIM_HOME*`/xellerate/JavaTasks`
`lib/OIDRecon.jar`	This JAR file contains the class files required for reconciliation. This JAR file contains the class files required for reconciliation. During connector deployment, this file is copied into the following directory: *OIM_HOME*`/xellerate/ScheduleTask`
Files in the `resources` directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, these resource bundles are copied into the following directory: *OIM_HOME*`/xellerate/connectorResources` **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.

Table 1–1 (Cont.) Files and Directories On the Connector Installation Media

File in the Installation Media Directory	Description
Files in the `test/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 ■ Process form ■ Process task and adapters (along with their mappings) ■ Resource object ■ Xellerate User (OIM User) ■ Provisioning process ■ Pre-populate rules ■ Reconciliation process ■ Lookup definitions
`xml/oimUser.xml`	This XML file contains the configuration for the Xellerate User (OIM User). You must import this file only if you plan to use the connector in trusted source reconciliation mode.

Note: The files in the `test/troubleshoot` directory are used only to run tests on the connector.

1.6 Determining the Release Number of the Connector

You might have a deployment of an earlier release of the connector. While deploying the latest release, you might want to know the release number of the earlier release. To determine the release number of the connector that has already been deployed:

1. In a temporary directory, extract the contents of the following JAR file:

   OIM_HOME`/xellerate/JavaTasks/OIDProv.jar`

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

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

2

Deploying the Connector

To deploy the connector, perform the procedures described in the following sections:

- Verifying Deployment Requirements
- Configuring the Target System
- Using External Code Files
- Customizing the xlconfig.xml File
- Depending on the release of Oracle Identity Manager that you use, perform the procedures described in one of the following sections:
  - Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later
  - Installing the Connector on Oracle Identity Manager Release 8.5.3.1 Through 9.0.3.x
- Configuring the Oracle Identity Manager Server
- Configuring SSL

2.1 Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3.1 or later
Target systems	Oracle Internet Directory release 9.x, 10.1.4.x, or 11gR1
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 configuring the IT resource. The procedure is described later in this guide. 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.

2.2 Configuring the Target System

You must configure incremental reconciliation by making the `modifytimestamp` attribute a searchable attribute.

To configure the target system for incremental reconciliation:

1. To make `modifytimestamp` a searchable attribute, use the `catalog.sh` file to index `modifytimestamp`.

   See *Oracle Identity Management User Reference Release 10g (10.1.4.0.1)* for information about the procedure.

2. Restart Oracle Internet Directory for the change to take effect.

2.3 Using External Code Files

The `ldap.jar` file contains APIs that are used to connect to the target system. The `ldapbp.jar` file is used by the connector to enable LDAP-based search of user records on the target system. You must download this file from the Sun Web site and copy it into the `ThirdParty` directory as follows:

1. Log on to the JNDI Downloads section of the Sun Web site at

   `http://java.sun.com/products/jndi/downloads/index.html`

2. On the JNDI Downloads page, click **Download JNDI 1.2.1 & More**.
3. Select the **I agree to the Software License Agreement** check box, and then click **Continue**.
4. Select **LDAP Service Provider, 1.2.4**.
5. Click **jndi-1_2_4.zip**.
6. Specify the temporary directory into which you want to download the `ldap-1_2_4.zip` file.
7. Extract the contents of the `ldap-1_2_4.zip` file.
8. From the `lib` directory inside the `ldap-1_2_4.zip` file, copy the `ldap.jar` and `ldapbp.jar` files into the *`OIM_HOME`*`/xellerate/ThirdParty` directory.

Note: In an Oracle Identity Manager cluster, copy this JAR file into the `ThirdParty` directory on each node of the cluster.

2.4 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.

2.5 Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later

---

Note: In this guide, the term **Connector Installer** has been used to refer to the Connector Installer feature of the Oracle Identity Manager Administrative and User Console.

Installing the connector on Oracle Identity Manager release 9.1.0 or later involves the following procedures:

- Running the Connector Installer

- Configuring the IT Resource

2.5.1 Running the Connector Installer

To run the Connector Installer:

1. Copy the contents of the connector installation media into the following directory:

   OIM_HOME/xellerate/ConnectorDefaultDirectory

2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of *Oracle Identity Manager Administrative and User Console*.
3. Click **Deployment Management**, and then click **Install Connector**.
4. From the Connector List list, select **Oracle Internet Directory 9.0.4.5**. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory:

   OIM_HOME/xellerate/ConnectorDefaultDirectory

   If you have copied the installation files into a different directory, then:

   a. In the **Alternative Directory** field, enter the full path and name of that directory.
   b. To repopulate the list of connectors in the Connector List list, click **Refresh**.
   c. From the Connector List list, select **Oracle Internet Directory 9.0.4.5**.
5. Click **Load**.
6. To start the installation process, click **Continue**.

   The following tasks are performed in sequence:

   a. Configuration of connector libraries
   b. Import of the connector XML files (by using the Deployment Manager)
   c. Compilation of adapters

   On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed. Depending on the reason for the failure, make the required correction and then perform one of the following steps:

   - Retry the installation by clicking **Retry.**
   - Cancel the installation and begin again from Step 1.
7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:

   a. Ensuring that the prerequisites for using the connector are addressed

Note: At this stage, run the `PurgeCache` utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. Refer to "Clearing Content Related to Connector Resource Bundles from the Server Cache" on page 2-10 for information about running the `PurgeCache` utility.

There are no prerequisites for some predefined connectors.

b. Configuring the IT resource for the connector

Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

c. Configuring the scheduled tasks that are created when you installed the connector

Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks is described later in this guide.

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in Table 1–1.

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a clustered environment, you must copy all the JAR files and the contents of the `connectorResources` directory into the corresponding directories on each node of the cluster. See "Files and Directories on the Installation Media" on page 1-6 for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.5.2 Configuring the IT Resource

Note: Perform this procedure if you are installing the connector on Oracle Identity Manager release 9.1.0 or later.

You must specify values for the parameters of the `OID Server` IT resource as follows:

1. Log in to the Administrative and User Console.
2. Expand **Resource Management.**
3. Click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter `OID Server` and then click **Search**.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource. The following table describes each parameter:

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. During provisioning, you can configure the users to be provisioned in a different organization instead of the default Xellerate Users in Oracle Identity Manager. Consider the following example. Suppose a custom organization org1 exists in the target system: ou=org1,dc=corp,dc=company,dc=com In the preceding sample, you can choose org1 from the lookup in the Xellerate form and provision the user to the target system. In the preceding sample, the lookup must be populated with specific organization values. Oracle recommends that you first run a full reconciliation with Use XL Org Structure=true and then provision a user. Once the full reconciliation is run, the data in the target system is replicated in Oracle Identity Manager. As a result lookup gets populated with the organization/organizational unit values automatically during the reconciliation. If you do not run a full reconciliation, then the organization must first be manually created and then the user should be provisioned. The name of the entity should be the same as that in the target system with identical casing. During reconciliation, if this attribute is set to true, then the users are reconciled in the respective organization as specified in the target system. Suppose, a user belongs to ou=org2,dc=corp,dc=company,dc=com in the target system. During reconciliation, the user gets updated in org2 in Oracle Identity Manager. This helps in maintaining the same organization structure in the target system and Oracle Identity Manager. 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. If the value is set to false, then all the users are provisioned and reconciled in the default Oracle Identity Manager organization, Xellerate Users.
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.

8. To save the values, click **Update**.

2.6 Installing the Connector on Oracle Identity Manager Release 8.5.3.1 Through 9.0.3.x

Installing the connector on any Oracle Identity Manager release between releases 8.5.3.1 and 9.0.3.x involves the following procedures:

2.6.1 Copying the Connector Files

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

See Also: "Files and Directories on the Installation Media" section on page 1-6 for more information about these files

File in the Installation Media Directory	Destination Directory
Files in the `Batch/custom` directory	Refer to the "Configuring the Target System" section on page 2-1 for instructions on copying these files.
`lib/OIDProv.jar`	*OIM_HOME*`/xellerate/JavaTasks`
`lib/OIDRecon.jar`	*OIM_HOME*`/xellerate/ScheduleTasks`
Files in the `resources` directory	*OIM_HOME*`/xellerate/connectorResources`
Files in the `test/troubleshoot` directory	*OIM_HOME*`/xellerate/test/troubleshoot`
Files in the `xml` directory	*OIM_HOME*`/xellerate/OID/xml`

Note: In a clustered environment, copy the JAR files and the contents of the `connectorResources` directory to the corresponding directories on each node of the cluster.

2.6.2 Importing the Connector XML File

As mentioned in the "Files and Directories on the Installation Media" section on page 1-6, 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 opening 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 following table for information about the values to be specified:

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. During provisioning, you can configure the users to be provisioned in a different organization instead of the default Xellerate Users in Oracle Identity Manager. Consider the following example. Suppose a custom organization org1 exists in the target system: ou=org1,dc=corp,dc=company,dc=com In the preceding sample, you can choose org1 from the lookup in the Xellerate form and provision the user to the target system. In the preceding sample, the lookup must be populated with specific organization values. Oracle recommends that you first run a full reconciliation with Use XL Org Structure=true and then provision a user. Once the full reconciliation is run, the data in the target system is replicated in Oracle Identity Manager. As a result lookup gets populated with the organization/organizational unit values automatically during the reconciliation. If you do not run a full reconciliation, then the organization must first be manually created and then the user should be provisioned. The name of the entity should be the same as that in the target system with identical casing. During reconciliation, if this attribute is set to true, then the users are reconciled in the respective organization as specified in the target system. Suppose, a user belongs to ou=org2,dc=corp,dc=company,dc=com in the target system. During reconciliation, the user gets updated in org2 in Oracle Identity Manager. This helps in maintaining the same organization structure in the target system and Oracle Identity Manager. 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. If the value is set to false, then all the users are provisioned and reconciled in the default Oracle Identity Manager organization, Xellerate Users.
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.

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.

See Also: If you want to define another IT resource, then refer to *Oracle Identity Manager Administrative and User Console Guide* for instructions.

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.

2.7 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.

- Changing to the Required Input Locale
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Enabling Logging
- Setting Up Lookup Definitions in Oracle Identity Manager

2.7.1 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.

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

While performing the instructions described in the "Copying the Connector Files" section on page 2-7, 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. An exception is thrown if you run the command described in Step 2 as follows:
   >
   > *`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`

2.7.3 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 messages that highlight the progress of the application at a 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 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 Server**

  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, log information is displayed on the server console.

- **IBM WebSphere Application Server**

  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, log information is written to the following file:

  WEBSPHERE_HOME/AppServer/logs/*SERVER_NAME*/SystemOut.log

- **JBoss Application Server**

  To enable logging:

  1. In the *JBOSS_HOME*/server/default/conf/log4j.xml file, add the following lines if they are not already present in the file:

     ```
     <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, log information is written to the following file:

  JBOSS_HOME/server/default/log/server.log

- **Oracle Application Server**

  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, log information is written to the following file:

ORACLE_HOME/opmn/logs/default_group~home~default_group~1.log

2.7.4 Setting Up Lookup Definitions in Oracle Identity Manager

The Lookup.OID.PrefLang lookup definition is created in Oracle Identity Manager when you deploy the connector. During a provisioning operation, you use the Lookup.OID.PrefLang lookup definition to specify a language for the user.

You must enter values in the Lookup.OID.PrefLang lookup definition before you can use it during provisioning operations. To enter values in a lookup definition:

1. Log in to the Design Console.
2. Expand **Administration**, and double-click **Lookup Definition**.
3. Search for and open the lookup definition.
4. Enter Code Key and Decode values for each of entry.

   You can enter any value. However, you must enter the same value in both the Code Key and Decode columns.
5. Click **Save**.

2.7.4.1 Configuring the AttrName.Recon.Map.OID Lookup Definition

To enable incremental reconciliation, you made modifytimestamp a searchable attribute by performing the procedure described in "Configuring the Target System" on page 2-1. In addition, you must modify the AttrName.Recon.Map.OID lookup definition by changing the Decode value of the ldapTargetResourceTimeStampField Code Key from [NONE] to modifytimestamp.

2.8 Configuring SSL

Note:

This is an optional step of the deployment procedure.

The connector supports only Mode 1 secure connections to Oracle Internet Directory.

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

1. Configure SSL on Oracle Internet Directory and then export the Oracle Internet Directory server certificate using Wallet Manager.

   See the "Secure Sockets Layer and the Directory" chapter of *Oracle Internet Directory Administrator's Guide* for detailed instructions.

   Note: For Mode 1 secure connection, you must select SSL Server Authentication as the SSL Authentication.

   The default non-SSL port is 389. The default SSL port is 636. When you create a configuration set of Oracle Internet Directory, it is recommended that you select a different port (for example, 1636) for SSL communication with Oracle Identity 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
- Adding New Multivalued Attributes for Reconciliation and Provisioning
- Adding New Object Classes for Provisioning and Reconciliation
- Configuring the Mapping of the User ID Field

3.1 Configuring Reconciliation

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

- Partial Reconciliation
- Paged Reconciliation
- Configuring Trusted Source Reconciliation
- Configuring the Reconciliation Scheduled Tasks
- Adding New Attribute for Target Resource Reconciliation

3.1.1 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 a value for the `CustomizedReconQuery` IT resource parameter. The procedure to configure the IT resource is described earlier in this guide.

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 configuring the IT resource. The procedure is described earlier in this guide.

3.1.2 Paged Reconciliation

Note: This feature is supported only on Oracle Internet Directory 10.1.4.0.1 or later.

During a reconciliation run, all changes in the target system records are reconciled into Oracle Identity Manager. Depending on the number of records to be reconciled, this process may require a large amount of time. In addition, if the connection breaks during reconciliation, then the process would take longer to complete.

You can configure paged reconciliation to avoid these problems.

To configure paged reconciliation, you specify a value for the `PageSize` user reconciliation scheduled task attribute by following the instructions given in the "User Reconciliation Scheduled Task" section on page 3-7.

3.1.3 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 during a reconciliation run:

- For each newly created user on the target system, an OIM User is created.
- Updates made to each user on the target system are propagated to the corresponding OIM User.

If you designate the target system as a **target resource**, then during a reconciliation run:

- For each account created on the target system, a resource is assigned to the corresponding OIM User.
- Updates made to each account on the target system are propagated to the corresponding resource.

Note: 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 `TrustedSource` 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.

Note: The `OID User Recon delete` task is run with the DN value, which is the value for the `UserContainer` attribute in the User Reconciliation scheduled task. The value of this attribute specifies the organizational unit from where users are reconciled from the target system into Oracle Identity Manager. When you run the `OID User Recon delete` task, all of the users in the other organizational units are deleted in Oracle Identity Manager.

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 opening 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 `TrustedSource` reconciliation scheduled task attribute to `True`. This procedure is described in the "Configuring the Reconciliation Scheduled Tasks" section on page 3-4.

3.1.4 Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in the "Importing the Connector XML File" section on page 2-7, 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 `FAILED` 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 3-5 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 3-10.

3.1.4.1 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

3.1.4.1.1 Lookup Fields Reconciliation Scheduled Task You must specify values for the following attributes of the `OID 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.Group ■ For roles lookup reconciliation: Lookup.OID.Role ■ 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: ■ cn=Groups,dc=mycompany,dc=com ■ cn=Roles,dc=mycompany,dc=com
ObjectClass	Object class name of the master value for which lookup fields reconciliation is being performed	The following are sample values: ■ For groups lookup reconciliation: groupOfUniqueNames ■ For roles lookup reconciliation: OrganizationalRole ■ For organization lookup reconciliation: Organization ■ For organizational unit lookup reconciliation: OrganizationalUnit
CodeKeyLTrimStr	The default value of this attribute is [None]. Do not change this value.	[NONE]
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
AttrType	Attribute type of role, group, or organization	The value can be any one of the following: ■ For role lookup reconciliation: cn ■ For group lookup reconciliation: cn ■ For organization lookup reconciliation: ou

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 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.Group`
   - `SearchContext: cn=Groups,dc=mycompany,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 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: OrganizationalRole`
   - `LookupCodeName: Lookup.OID.Role`
   - `SearchContext: cn=Roles,dc=mycompany,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.

3.1.4.1.2 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`

Attribute	Description	Default/Sample Value
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]
TrustedSource	Specifies whether or not reconciliation is to be performed in trusted mode	True or False
Organization	Default organization of the Xellerate User (OIM User)	Xellerate Users
Xellerate Type	Default xellerate type for the Xellerate User (OIM User) This is a configurable value.	End-User Administrator
Role	Default role for the Xellerate User (OIM User)	Consultant
PageSize	This attribute is used for paged reconciliation. During a reconciliation run, the total set of records to be reconciled is divided into pages and the PageSize attribute specifies the number of records that must constitute one page. It is recommended that you set a page size between 100 and 1000. **See Also:** The "Paged Reconciliation" section on page 3-3	100

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

3.1.5 Adding New Attribute for Target Resource Reconciliation

Note: You must ensure the new attributes that you add for reconciliation contain data in string-format only. Binary attributes must not be introduced into Oracle Identity Manager natively.

By default, the attributes listed in the "Reconciled Resource Object Fields" section of the connector guide are mapped for reconciliation between Oracle Identity Manager

and the target system. If required, you can add new attributes for target resource reconciliation.

To add a new attribute for target resource reconciliation, perform the following procedure:

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new attribute on the OIM User process form as follows:
   a. Expand **Development Tools**.
   b. Double-click **Form Designer**.
   c. Search for and open the **OID User**.
   d. Click **Create New Version**.
   e. In the **Label** field, enter the version name. For example, `version#1`.
   f. Click the **Save** icon.
   g. Select the current version created in Step e from the **Current Version** list.
   h. Click **Add** to create a new attribute, and provide the values for that attribute.

      For example, if you are adding the organization attribute, then enter the following values in the **Additional Columns** tab:

Field	Value
Name	organization
Variant Type	String
Length	100
Field Label	organization
Order	20

   i. Click the **Save** icon.
   j. Click **Make Version Active**.
3. Add the new attribute to the list of reconciliation fields in the resource object as follows:
   a. Expand **Resource Management.**
   b. Double-click **Resource Objects**.
   c. Search for and open the **OID User** resource object.
   d. On the **Object Reconciliation** tab, click **Add Field**, and then enter the following values:

      Field Name: `Organization`

      Field Type: `String`
   e. Click the **Save** icon.
4. Create a reconciliation field mapping for the new attribute in the process definition form as follows:
   a. Expand **Process Management.**
   b. Double-click **Process Definition**.

c. Search for and open the **OID User** process definition.

d. On the **Reconciliation Field Mappings** tab, click **Add Field Map**, and then select the following values:

Field Name: `Organization`

Field Type: `String`

Process Data Field: `Organization`

e. Click the **Save** icon.

5. Create an entry for the attribute in the lookup definition for reconciliation as follows:

a. Expand **Administration**.

b. Double-click **Lookup Definition**.

c. Search for and open the **AttrName.Recon.Map.OID** lookup definition.

d. Click **Add** and enter the **Code Key** and **Decode** values for the attribute. The Code Key value must be the name of the attribute given in the resource object. The Decode value is the name of the attribute in the target system.

For example, enter `organization` in the **Code Key** field and then enter `o` in the **Decode** field.

e. Click the **Save** icon.

3.2 Configuring Provisioning

Note: The following is a guideline that you must apply during provisioning operations:

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 have configured the target system for the Japanese language, then you would not be able to enter more than 25 characters in the same field.

As mentioned earlier in this guide, provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager.

- Compiling Adapters
- Adding Object Classes for Provisioning
- Enabling Provisioning of Users in Organizations and Organizational Units
- Provisioning Organizational Units, Groups, and Roles
- Adding New Attribute for Provisioning

3.2.1 Compiling Adapters

> **Note:** You must perform the procedure described in this section if you want to use the provisioning features of Oracle Identity Manager for this target system.
>
> You need not perform the procedure to compile adapters if you have performed the procedure described in "Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later" on page 2-2.

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 1-4 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.

3.2.2 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 more object classes. Use a vertical bar (`|`) to separate object classes whose names you enter. 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.

3.2.3 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`

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

3.2.4 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.

3.2.5 Adding New Attribute for Provisioning

Note: This section describes an optional procedure. You need not perform this procedure if you do not want to add new attributes for provisioning.

By default, the attributes listed in the "Provisioning Module" section of the connector guide are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning.

To add a new attribute for provisioning, create an entry for the attribute in the lookup definition for provisioning as follows:

1. Expand **Administration.**
2. Double-click **Lookup Definition.**
3. Search for and open the **AttrName.Prov.Map.OID** lookup definition.
4. Click **Add** and enter the **Code Key** and **Decode** values for the attribute. The Code Key value must be the name of the attribute given in the resource object. The Decode value is the name of the attribute in the target system.

   For example, enter `organization` in the **Code Key** field and then enter `o` in the Decode field.
5. Click the Save icon.

3.2.5.1 Enabling Update of New Attributes for Provisioning

After you add an attribute for provisioning, you must enable update operations on the attribute. If you do not perform this procedure, then you will not be able to modify the value of the attribute after you set a value for it during the Create User provisioning operation.

To enable the update of a new attribute for provisioning:

1. Expand **Process Management.**
2. Double-click **Process Definition** and open the **OID User** process definition.
3. In the process definition, add a new task for updating the field as follows:
   a. Click **Add** and enter the task name, for example, `organization Updated` and the task description.
   b. In the Task Properties section, select the following fields:
      – Conditional
      – Required for Completion
      – Allow Cancellation while Pending
      – Allow Multiple Instances
   c. Click on the Save icon.
4. On the Integration tab, click **Add,** and then click **Adapter.**
5. Select the **adpOIDMODIFYUSER** adapter, click **Save,** and then click **OK** in the message that is displayed.
6. To map the adapter variables listed in this table, select the adapter, click **Map,** and then specify the data given in the following table:

   Note: Some of the values in this table are specific to Organization (o value in OID target). These values must be replaced with values relevant to the attributes that you require.

Variable Name	Data Type	Map To	Qualifier	IT Asset Type	IT Asset Property
PDataOrg	String	Process Data	Organization DN	NA	NA
User ID	String	Process Data	User ID	NA	NA
AttrName	String	Literal	String	Literal value :Organization	NA
AttrValue	String	Process Data	Organization Note: The name of the attribute in process form	NA	NA
ProcessInstKey	String	Process Data	Process Instance	NA	NA
Adapter return value	Object	Response Code	NA	NA	NA
SSL FLag	String	IT Resources	Server	OID Server	SSL
Server Address	String	IT Resources	Server	OID Server	Server Address
Server Port	String	IT Resources	Server	OID Server	Port
RootContext	String	IT Resources	Server	OID Server	Root DN
AdminID	String	IT Resources	Server	OID Server	Admin ID
AdminPwd	String	IT Resources	Server	OID Server	Admin Password
AttrLookupCode	String	IT Resources	Server	OID Server	Prov Attribute Lookup Code
OrganizationDN	String	Literal	String	Literal Value:Note: don't specify any value here	NA
XLOrgFlag	String	IT Resources	Server	OID Server	Use XL Org Structure

7. Click the Save icon and then close the dialog box.

3.3 Adding New Multivalued Attributes for Reconciliation and Provisioning

Note: You must ensure that new attributes you add for reconciliation contain only string-format data. Binary attributes must not be brought into Oracle Identity Manager natively.

By default, the multivalued attributes Role and Group are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new multivalued attributes for reconciliation and provisioning.

To add a new multivalued attribute for reconciliation and provisioning:

1. Log in to the Oracle Identity Manager Design Console.
2. Create a form for the multivalued attribute as follows:
   a. Expand **Development Tools**.
   b. Double-click **Form Designer**.

c. Create a form by specifying a table name and description, and then click **Save**.

d. Click **Add** and enter the details of the attribute.

e. Click **Save** and then click **Make Version Active.**

3. Add the form created for the multivalued attribute as a child form of the process form as follows:

a. Search for and open the **UD_OID_USR** process form.

b. Click **Create New Version**.

c. Click the **Child Table(s)** tab.

d. Click **Assign**.

e. In the Assign Child Tables dialog box, select the newly created child form, click the right arrow, and then click **OK**.

f. Click **Save** and then click **Make Version Active.**

4. Add the new attribute to the list of reconciliation fields in the resource object as follows:

a. Expand **Resource Management**.

b. Double-click **Resource Objects**.

c. Search for and open the **OID User** resource object.

d. On the Object Reconciliation tab, click **Add Field**.

e. In the Add Reconciliation Fields dialog box, enter the details of the attribute.

For example, enter `Address` in the **Field Name** field and select **Multi Valued Attribute** from the Field Type list.

f. Click **Save** and then close the dialog box.

g. Right-click the newly created attribute.

h. Select **Define Property Fields**.

i. In the Add Reconciliation Fields dialog box, enter the details of the newly created field.

For example, enter `Mailing Address` in the Field Name field and select **String** from the Field Type list.

j. Click **Save**, and then close the dialog box.

5. Create a reconciliation field mapping for the new attribute as follows:

a. Expand **Process Management**.

b. Double-click **Process Definition**.

c. Search for and open the **OID User** process definition.

d. On the Reconciliation Field Mappings tab of the OID User process definition, click **Add Table Map**.

e. In the Add Reconciliation Table Mapping dialog box, select the field name and table name from the list, click **Save**, and then close the dialog box.

f. Right-click the newly created field, and select **Define Property Field Map**.

g. In the **Field Name** field, select the value for the field that you want to add.

h. Double-click the **Process Data Field** field, and then select the required data field.

i. Select the **Key Field for Reconciliation Mapping** check box, and then click **Save**.

6. Create an entry for the attribute in the lookup definition for reconciliation as follows:

a. Expand **Administration**.

b. Double-click **Lookup Definition.**

c. Search for and open the **AttrName.Recon.Map.OID** lookup definition.

d. Search for the `ldapUserMultiValAttr` Code Key value.

If you do not want to reconcile multivalued attributes, then accept the default Decode value `[NONE]`.

If you want to reconcile a multivalued attribute, then enter a value in the following format:

RECONCILIATION FIELD NAME OF ATTRIBUTE,PROPERTY NAME OF THE RECONCILIATION FIELD

For example: `Address,MailingAddress`

If you want to reconcile more than one multivalued attribute, then enter values in the following format:

RECONCILIATION FIELD NAME OF ATTRIBUTE 1,PROPERTY NAME OF THE RECONCILIATION FIELD 1`|` *RECONCILIATION FIELD NAME OF ATTRIBUTE 2,PROPERTY NAME OF THE RECONCILIATION FIELD 2*`|` *. . .*

For example: `Address,MailingAddress|group,groupname`

e. Search for and open the **Attrname.Prov.Map.OID** lookup definition.

f. In the lookup definition, add an entry for the attribute that you want to add:

– Code Key: Enter the name of the attribute that you add on the process form.

– Decode Key: Enter the name of the attribute displayed on the target system, which you recorded earlier in this procedure.

Enabling Update of New Multivalued Attributes for Provisioning

After you add a multivalued attribute for provisioning, you must enable update operations on the attribute. If you do not perform this procedure, then you will not be able to modify the value of the attribute after you set a value for it during the Create User provisioning operation.

To enable the update of a new multivalued attribute for provisioning:

> **See Also:** *Oracle Identity Manager Design Console Guide* for detailed information about these steps

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Process Management**.
3. Double-click **Process Definition** and open the **OID User** process definition.
4. In the process definition, add a task for setting a value for the attribute:

a. Click **Add**, enter the name of the task for adding multivalued attributes, and enter the task description.

b. In the Task Properties section, select the following fields:

   – Conditional

   – Required for Completion

   – Allow Cancellation while Pending

   – Allow Multiple Instances

   – Select the child table from the list.

     For the example described earlier, select **Mailing Address** from the list.

   – Select **Insert** as the trigger type for adding multivalued data. Alternatively, select **Delete** as the trigger type for removing multivalues data.

c. On the **Integration** tab, click **Add**, and then click **Adapter**.

d. Select the **adpOIDADDMULTIVALUEATTRIBUTE** adapter, click **Save**, and then click OK in the message.

e. To map the adapter variables listed in this table, select the adapter, click **Map**, and then specify the data given in the following table:

Note: Some of the values in this table are specific to the Mailing Address/Postal Address example. These values must be replaced with values relevant to the multivalued attributes that you require.

Variable Name	Data Type	Map To	Qualifier	IT Asset Type	IT Asset Property
SSLFlag	String	IT Resource	Server	OID Server	SSL
Adapter return value	Object	Response Code	NA	NA	NA
UserID	String	Process Data	User ID	NA	NA
userPassword	String	Process Data	Password	NA	NA
rootContext	String	IT Resources	Server	OID Server	Root DN
port	String	IT Resources	Server	OID Server	Port
LDAPServer	String	IT Resources	Server	OID Server	Server Address
AttrLookupCode	String	IT Resources	Server	OID Server	Prov Attribute Lookup Code
PropertyName	String	Literal	String	homePostalAddress **Note:** This is a sample (literal) value.	NA
PropertyValue	String	Select **Process Data** and then select (for example) **OID User Role**.	Address **Note:** This is a sample value.	NA	NA
Admin ID	String	IT Resources	Server	OID Server	Admin Id
AdminPwd	String	IT Resources	Server	OID Server	Admin Password

Variable Name	Data Type	Map To	Qualifier	IT Asset Type	IT Asset Property
organizationDN	String	Literal	String	**Note:** Do not enter a value in the Literal field.	NA
ProcessInstKey	String	Process data	Process Instance	NA	NA
PDataOrg	String	Process data	Organization DN	NA	NA

f. Click the Save icon and then close the dialog box.

5. In the process definition, add a task for removing the value of the attribute by performing Step 4. While performing Step 4.d, select the **adpOIDREMOVEMULTIVALUEATTRIBUTE** adapter.
6. In the process definition, add a task for updating the value of the attribute by performing Step 4.

   While performing Step 4.d select the **adpOIDUPDATEMULTIVALUEATTRIBUTE** adapter. Map the Adapter return Value attribute for this update task by providing the values described in the preceding table.

3.4 Adding New Object Classes for Provisioning and Reconciliation

To add a new object class for provisioning and reconciliation:

- Adding the Attributes of the Object Class to the Process Form
- Adding the Object Class and its Attributes to the Lookup Definition for Provisioning
- Adding the Attributes of the Object Class to the Resource Object
- Adding the Object Class and its Attributes to the Lookup Definition for Reconciliation
- Adding attributes of the Object Class to the Provisioning Process.

3.4.1 Adding the Attributes of the Object Class to the Process Form

To add the attributes of the object class to the process form:

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Development Tools** folder.
3. Double-click **Form Designer.**
4. Search for and open the **UD_OID_USR** process form.
5. Click **Create New Version,** and then click **Add.**
6. Enter the details of the attribute.

   For example, if you are adding the Associated Domain attribute, enter `UD_OID_USR_ASSOCIATEDDOMAIN` in the **Name** field and then enter the other details of this attribute.
7. Click **Save,** and then click **Make Version Active.**

3.4.2 Adding the Object Class and its Attributes to the Lookup Definition for Provisioning

To add the object class and its attributes to the lookup definition for provisioning:

1. Expand the **Administration** folder.
2. Double-click **Lookup Definition.**
3. Search for and open the **AttrName.Prov.Map.OID** lookup definition.
4. Add the object class name to the Decode value of the `ldapUserObjectClass` Code Key.

Note: In the Decode column, use the vertical bar (`|`) as a delimiter when you add the object class name to the existing list of object class names.

For example, if you want to add `domainRelatedObject` in the Decode column then enter the value as follows:

`top|inetorgperson|orclUserV2|`**`domainRelatedObject`**

5. Click **Add** and then enter the Code Key and Decode values for an attribute of the object class. The Code Key value must be the name of the field on the process form and Decode value must be the name of the field on the target system.

   For example, enter `Associated Domain` in the Code Key field and then enter `associatedDomain` in the Decode field.

Note: You must perform this step for all the mandatory attributes of the object class. You can also perform this step for the optional attributes.

6. Click **Save.**

3.4.3 Adding the Attributes of the Object Class to the Resource Object

To add the attributes of the object class to the resource object:

Note: You must perform this step for all the mandatory attributes of the object class. You can also perform this step for the optional attributes.

1. Expand the **Resource Management** folder.
2. Double-click **Resource Objects.**
3. Search for and open the **OID User** resource object.
4. For each attribute of the object class:
   a. On the Object Reconciliation tab, click **Add Field.**
   b. Enter the details of the field.

   For example, enter `Associated Domain` in the **Field Name** field and select **String** from the Field Type list.

5. Click the save icon.

3.4.4 Adding the Object Class and its Attributes to the Lookup Definition for Reconciliation

To add the object class and its attributes to the lookup definition for reconciliation, perform all the instructions given in the "Adding the Object Class and its Attributes to the Lookup Definition for Provisioning" section on the **AttrName.Recon.Map.OID** lookup definition. In other words, while performing Step 3 of the "Adding the Object Class and its Attributes to the Lookup Definition for Provisioning" section, search for and open the **AttrName.Recon.Map.OID** lookup definition instead of the **AttrName.Prov.Map.OID** lookup definition.

While performing Step 5 of the "Adding the Object Class and its Attributes to the Lookup Definition for Provisioning" section, note that the Code Key value must be the name of the reconciliation field in the OID User resource object and Decode value must be the name of the field on the target system. For example, enter `Associated Domain` in the Code Key field and then enter `associatedDomain` in the Decode field.

3.4.5 Adding attributes of the Object Class to the Provisioning Process

To add the attributes of the object class to the provisioning process:

Note: You must perform this step for all the mandatory attributes of the object class. You can also perform this step for the optional attributes.

1. Expand the **Process Management** folder.
2. Double-click **Process Definition.**
3. Search for and open the **OID User** provisioning process.
4. On the Reconciliation Field Mappings tab, click **Add Field Map.**
5. In the **Field Name** field, select the value for the field that you want to add.

   For example, select `Associated Domain = UD_OID_USR_ASSOCIATEDDOMAIN`
6. In the **Field Type** field, select the field type.
7. Click the save icon.

3.5 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. Click Add.
4. In the Code Key column, enter `User ID`.
5. In the Decode column, enter `uid`.
6. 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

4.1 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. Copy the contents of the `test/troubleshoot` directory on the installation media, to the *`OIM_HOME`*`/xellerate/test/troubleshoot` directory.
2. Specify the required values in the `config.properties` file.

   This file is in the *`OIM_HOME`*`/xellerate/test/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 The values that you provide are the same as those provided for the IT resources parameters. The procedure to configure the IT resource is described earlier in this guide.
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

3. Add the following to the `CLASSPATH` environment variable:

   `OIM_HOME``/xellerate/JavaTasks/OIDProv.jar`
   `OIM_HOME``/xellerate/lib/xlLogger.jar`
   `OIM_HOME``/xellerate/ext/log4j-1.2.8.jar`
   `OIM_HOME``/xellerate/lib/xlUtils.jar`

4. 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.

4.1.1 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.

4.2 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

4.2.1 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.

4.2.2 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.

4.2.3 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.

4.2.4 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.

4.2.5 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:

- **Bug 7560319**

  The Time Zone field on the process form can accept invalid values during provisioning operations.

- **Bug 7605087**

  During trusted source reconciliation, if there is a mismatch in the case (uppercase/lowercase) between a user's OU in Oracle Identity Manager and the user's OU on the target system, then the OU field is not populated. This is because the target system is case-sensitive and Oracle Identity Manager is not case-sensitive toward OU names. OU names are converted to lowercase when they are brought to Oracle Identity Manager through reconciliation.

  As a workaround to this problem, it is recommended that you set lowercase names for OUs that you create.

- **Bug 7609477**

  If only the Manager ID field of a user on the target system is modified, then the user is not reconciled during the next reconciliation run.

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:

> **Note:** Apply the following guideline while performing provisioning operations:
>
> 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 have configured the target system for the Japanese language, then you would not be able to enter more than 25 characters in the same field.

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)

Oracle Identity Manager Attribute	Oracle Internet Directory attribute	Description
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	RoleOccupant	Multivalued attribute for the role object, which shows the number of users in the role
UserGroup	groupOfUniqueNames	Object class for the group
UserRole	OrganizationalRole	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)
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	RoleOccupant	Custom object class for the role The "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