Oracle® Identity Manager

Connector Guide for Oracle Internet Directory

Release 9.0.1

B31128-01

June 2006

ORACLE®

Oracle Identity Manager Connector Guide for Oracle Internet Directory, Release 9.0.1

B31128-01

Preface

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

> **Note:** This is a transitional release following Oracle's acquisition of Thor Technologies. Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

Audience

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

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

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

- *Oracle Identity Manager Release Notes*

- *Oracle Identity Manager Installation and Upgrade Guide for JBoss*

- *Oracle Identity Manager Installation and Upgrade Guide for WebLogic*

- *Oracle Identity Manager Installation and Upgrade Guide for WebSphere*

- *Oracle Identity Manager Administrative and User Console Guide*

- *Oracle Identity Manager Administrative and User Console Customization Guide*

- *Oracle Identity Manager Design Console Guide*

- *Oracle Identity Manager Tools Reference Guide*

- *Oracle Identity Manager Audit Report Developer Guide*

- *Oracle Identity Manager Best Practices Guide*

- *Oracle Identity Manager Connector Framework Guide*

- Connector guides for various third-party applications

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.1 connector documentation set, visit Oracle Technology Network at

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

Conventions

The following text conventions are used in this document:

Convention	Meaning
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.

1

About the Connector

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

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

This chapter contains the following sections:

- Supported Functionality
- Reconciliation Module
- Provisioning Module
- Files and Directories That Comprise the Connector

Supported Functionality

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

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

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

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

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

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

Reconciliation Module

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

Reconciliation can be divided into the following types:

- Lookup Fields Reconciliation
- User Reconciliation

Lookup Fields Reconciliation

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

User Reconciliation

This section provides information about user reconciliation.

Reconciled Resource Object Fields

The following fields are reconciled:

- User ID (This is a mandatory field)
- First Name
- Last Name
- Middle Name
- Department
- Location
- Telephone
- Email
- Preferred Language
- Timezone
- Logon Script
- Title
- Organization Unit
- Server Name (IT resource)
- UserGroup
- UserRole

Reconciled Xellerate User Fields

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

- User ID (This is a mandatory field)
- First Name
- Last Name
- Organization
- Xellerate Type
- Password
- Xellerate
- Role

> **Note:** The user search has been modified to fetch all records from the target system, regardless of the `QueryEntryReturnLimit` value set in Oracle Identity Manager. However, this modified functionality works only if the number of Oracle Identity Manager user IDs starting with patterns of `aa`, `ab`, `ac`, and so on is less than or equal to the `QueryEntryReturnLimit` value.

Provisioning Module

The following fields are provisioned:

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

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

Files and Directories That Comprise the Connector

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

```
Directory Servers\Oracle Internet Directory\Oracle Internet Directory Rev
2.0.0.zip
```

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
xml\oimOIDUser.xml	This XML file contains the following components of the connector: ■ IT resource type ■ Custom process form ■ Process task and adapters (along with their mappings) ■ Resource object ■ Xellerate User ■ Provisioning process ■ Pre-populate rules ■ Reconciliation process ■ Lookup definitions
xml\oimUser.xml	This XML file contains the configuration for the Xellerate User. You must import this file only if you plan to use the connector in trusted source reconciliation mode.
lib\xliOID.jar	This JAR file contains the class files required for provisioning and reconciliation.
The following files in the Batch\custom directory: custom.bat customIndex.ldif customOrganizationalRole.ldif customRoleOccupant.ldif readme.txt	When you run the custom.bat file, a required object class and an attribute are added to the existing Oracle Internet Directory schema.
The following files in the troubleshoot directory: config.properties log4j-1.2.9.jar log.properties tcUtilTestOID.class testcreate.bat testdelete.bat testmodify.bat xliOID.jar xlLogger.jar xlUtils.jar	These files are used to perform basic tests on the connector, even before Oracle Identity Manager and the application server are installed.
docs\B31128_01.pdf docs\html	These are PDF and HTML versions of this guide, which provides instructions to deploy the connector.

The "Step 4: Copying the Connector Files and External Code" section on page 2-2 provides instructions to copy these files into the required directories.

2

Deploying the Connector

Deploying the connector involves the following steps:

Step 1: Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3 or later
Target systems	Oracle Internet Directory
Target system host platforms	The target system host platform can be any one of the following: - Red Hat Linux AS 2.1 - Microsoft Windows 2000 - Solaris 9

Step 2: Configuring the Target System

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

To add a custom object class and custom attribute:

1. Ensure that Oracle Internet Directory is running.

2. Copy the contents of the `Batch\custom` directory from the installation media ZIP file to a directory on the target Oracle Internet Directory server. You must ensure that the contents of the `Batch\custom` are kept in the same directory.

3. Using any text editor, open the `custom.bat` file.

4. In the fields indicated in the `custom.bat` file, provide the host name, port, and Oracle Internet Directory superuser DN and password.

The following is the syntax for providing these values:

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

For example:

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

5. Run the `custom.bat` file.

6. Open Oracle Directory Manager and click **Schema Management** in the left pane. The details of all schema elements are displayed in the right pane. You can check if the `customOrganizationalRole` object class and `customRoleOccupant` attributes have been added to their respective categories.

Step 3: Configuring the Oracle Identity Manager Server

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 `xellerate_home\xellerate\config` directory. You must modify the `checkouttimeout` attribute value to ensure that the connector XML files are imported correctly.

Step 4: Copying the Connector Files and External Code

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

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

```
Directory Servers\Oracle Internet Directory\Oracle Internet
Directory Rev 2.0.0.zip
```

Refer to "Files and Directories That Comprise the Connector" on page 1-4 for more information about these files.

File in the Installation Media Directory	Destination Directory
The following files in the `xml` directory:	`xellerate_home\xellerate\OID\xml`
`oimOIDUser.xml` `oimUser.xml`	

File in the Installation Media Directory	Destination Directory
`lib\xliOID.jar`	*xellerate_home*`\Xellerate\JavaTasks`

The following files in the `Batch\custom` directory:
 	
`custom.bat`
`customIndex.ldif`
`customOrganizationalRole.ldif`
`customRoleOccupant.ldif`
`readme.txt`
	If you have performed the procedure in the "Step 2: Configuring the Target System" section, then you have already copied the contents of the `Batch\custom` directory to a directory on the Oracle Internet Directory server.

The following files in the `troubleshoot` directory:
 	
`config.properties`
`log4j-1.2.9.jar`
`log.properties`
`tcUtilTestOID.class`
`testcreate.bat`
`testdelete.bat`
`testmodify.bat`
`xliOID.jar`
`xlLogger.jar`
`xlUtils.jar`
	xellerate_home`\xellerate\troubleshoot`

The following contents of the `docs` directory:
 	
`B31128_01.pdf`
`html`
	xellerate_home`\xellerate\OID\docs`

Step 5: Importing the Connector XML Files

To import the connector XML files:

1. Open the Oracle Identity Manager Administrative and User Console.

2. Click the **Deployment Management** link on the left navigation bar.

3. Click the **Import** link under **Deployment Management.** A dialog box for locating files is displayed.

4. Locate and open the `oimOIDUser.xml` file, which is in the *xellerate_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. Use the table given in the "Defining IT Resources" section on page 2-3 for information about the values to be specified.

9. Click **Next**. The Provide IT Resource Instance Data page for a new instance of the `LDAP Server` IT resource type is displayed.

10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.

11. Click **View Selections.**

The contents of the XML file are displayed on the Import page. You may see a cross-shaped icon along with some nodes. You must remove these nodes. To do this, right-click each such node and then select **Remove.**

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

13. If you plan to use the connector in trusted source reconciliation mode, then perform the same procedure to import the `oimUser.xml` file. This file is in the `xellerate_home`\xellerate\OID\xml directory.

> **Caution:** Only one connector can be configured 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.

After you import the connector XML files, proceed to the "Step 6: Configuring Reconciliation" section on page 2-5.

Defining IT Resources

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

Parameter Name	Parameter Description
`Admin Id`	DN value of the user who has admin rights on the Oracle Internet Directory server Sample value: `cn=Admin,ou=People, o=xyz`
`Admin Password`	Password of the user who has admin 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 the `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 there is no secure communication between Oracle Identity Manager and the Oracle Internet Directory server.
`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`.

Parameter Name	Parameter Description
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`.
Use XL Org Structure	If set to `true`, then the Oracle Identity Manager Organization structure is used during provisioning and reconciliation.
	If set to `false`, then the value of the Organization field in the process form is used for provisioning and the organization or container in the target Oracle Internet Directory is used for reconciliation.
Last Recon TimeStamp	This parameter does not contain a value for the initial load of reconciliation. After the first reconciliation operation is run, the time at which the reconciliation was completed is stored in this parameter. This value is updated each time reconciliation is performed.
	The user does not need provide any value for this parameter. After the first reconciliation, the value is automatically created in its own format.
	Sample value: `20060524110907Z`

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

Step 6: Configuring Reconciliation

Configuring reconciliation involves creating scheduled tasks for lookup fields and user reconciliations. To create 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. Enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager should attempt to complete the task before assigning the ERROR status to the task.

6. Ensure that the **Disabled** and **Stop Execution** check boxes are cleared.

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 appropriate table in the "Specifying Values for the Scheduled Task Attributes"section on page 2-6 for information about the values to be specified.

> **See Also:**   *Oracle Identity Manager Design Console Guide* for
> information about adding and removing task attributes

10. Click **Save**. The scheduled task is created. The `INACTIVE` status is displayed in the
    Status field, because the task is not currently running. The task is run at the date
    and time that you set in Step 7.

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

After you create both scheduled tasks, proceed to the

Specifying Values for the Scheduled Task Attributes

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

■   Lookup Fields Reconciliation Scheduled Tasks

■   User Reconciliation Scheduled Tasks

Lookup Fields Reconciliation Scheduled Tasks

You must specify values for the following attributes of the lookup fields reconciliation
scheduled task.

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

Attribute Name	Description	Default/Sample Value
LookupCodeName	Name of the lookup definition to which the master values are to be reconciled	`Lookup.OID.Groups` (for Groups lookup reconciliation)
		`Lookup.OID.Roles` (for Roles lookup reconciliation)
ITResourceName	Name of the IT resource for setting up the connection to Oracle Internet Directory	`OID Server`
SearchContext	Search context to be used for searching the master values	`DC=mycompany,DC=com`
ObjectClass	Object class name of the master value for which lookup fields reconciliation is being performed	`groupOfUniqueNames` (for Groups lookup reconciliation)
		`customRoleOccupant` (for Roles lookup reconciliation)
CodeKeyLTrimStr	String value for left-trimming the value obtained from the search, such as `cn=`. If there is nothing to be trimmed, then specify the value `[NONE]`.	`[NONE]`
CodeKeyRTrimStr	String value for right-trimming the value obtained from the search, such as `',DC=mycompany,DC=com'`. If there is nothing to be trimmed, then specify the value `[NONE]`.	`,DC=mycompany,DC=com`

Attribute Name	Description	Default/Sample Value
ReconMode	Specify REFRESH to completely refresh the existing lookup.	REFRESH or UPDATE
	Specify UPDATE to update the lookup with the new values.	

> **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.

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

User Reconciliation Scheduled Tasks

You must specify values for the following attributes of the user reconciliation scheduled task.

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

Attribute Name	Description	Default/Sample Value
ITResourceName	Name of the IT resource for setting up a connection to Oracle Internet Directory	OID Server
ResourceObjectName	Name of the resource object into which users are to be reconciled	OID User
XLDeleteUsersAllowed	If this attribute is set to true, then the Delete reconciliation event is started. Users who are deleted from the target system are removed from Oracle Identity Manager. This requires all the users on the target system to be compared with all the users in Oracle Identity Manager. **Note:** This process affects performance.	true or false
UserContainer	DN value from where the users are reconciled from the target system to Oracle Identity Manager	cn=*users*,dc=*hostname*,dc=com Here, *users* is the name of the user container and *hostname* is the host name under which the oracle context is created.
Keystore	Directory path to the Oracle Internet Directory keystore This is required to set up an SSL connection. Specify [NONE] for a non-SSL connection.	C:\j2sdk1.4.2_09\jre\lib\security\cacerts or [NONE]
IsTrusted	Configurable option. Specify True or False.	True or False
Organization	Default organization of the Xellerate User	Xellerate Users

Attribute Name	Description	Default/Sample Value
Xellerate Type	Type of Xellerate User It is a configurable value.	End-User Administrator
Role	Default role of the Xellerate User	Consultant
Password	Default password of the Xellerate User	Admin123

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

Step 7: Compiling Adapters

The following adapters are imported into Oracle Identity Manager when you import the connector XML file. You must compile these adapters before you can use them to provision accounts on the target system.

- 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

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 the **Compile All** option.

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

3. Click **Start.** Oracle Identity Manager compiles the adapters that you specify.

To view detailed information about an adapter:

1. Highlight the adapter in the Adapter Manager form.

2. Double-click the row header of the adapter, or right-click the adapter.

3. Select **Launch Adapter** from the shortcut menu that is displayed. Details of the adapter are displayed.

> **Note:** To compile multiple adapters simultaneously, use the Adapter Manager form. To compile one adapter at a time, use the Adapter Factory form. Refer to *Oracle Identity Manager Tools Reference Guide* for information about how to use these forms.

Step 8: Configuring SSL

> **Note:** If the `SSL` IT resource parameter is set to `False,` then this is an optional step of the deployment procedure.

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

1. Export the Oracle Internet Directory Server certificate using Wallet Manager.

2. Check if the Oracle Internet Directory server is listening on the SSL port. If it is not, then set it to the SSL port (default SSL port is 636), and 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 -file certificate_file_name -alias ndscert -keystore
   java_home\lib\security\cacerts
   ```

4. Restart the Oracle Identity Manager server.

5. In the `OID Server` IT resource:

   - Set the `SSL` parameter value to `true.`

   - Change the `Port` parameter value to the SSL port number. Typically, this number is 636.

3

Testing the Connector

After you deploy the connector, you must test it to ensure that it functions as expected.

This chapter contains the following sections:

- Running Test Cases
- Troubleshooting

Running Test Cases

This section discusses test cases that you can perform by using the troubleshooting utility.

You can use the troubleshooting utility to directly use the connector for identifying the cause of problems associated with connecting to the target system server and performing basic operations on the target system.

Before you can use the troubleshooting utility, you must provide the required values in the `config.properties` file. This file is in the `xellerate_home\xellerate\Troubleshoot` directory. The following table describes the sections of this file.

Section Name	Information
Oracle Internet Directory Connection Parameters	Connection parameters required to connect to the target system
Create User	Values requited to create a user on the target system
Modify User	Values required to modify a user
Delete User	DN of the user to be deleted

After you specify the required values in the `config.properties` file, perform the following tests:

- Create a user.

  Run the `testcreate.bat` file. Then, check if the user is created in Oracle Internet Directory with the details given in the `config.properties` file. If you run this BAT file from the command window, then the `User_Creation_Successful` message is displayed.

- Modify the user.

  Run the `testmodify.bat` file. Then, check if the user is modified in Oracle Internet Directory with the details given in the `config.properties` file. If you

run this BAT file from the command window, the
`User_Modification_Successful` message is displayed.

- Delete the user.

  Run the `testdelete.bat` file. Then, check if the specified user is deleted from
  Oracle Internet Directory. If you run this BAT file from the command window, the
  `User_Deletion_Successful` message is displayed.

Troubleshooting

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

- Connection Errors
- Common LDAP Errors
- Create User Errors
- Delete User Errors
- Modify User Errors
- Child Data Errors

Connection Errors

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

Problem Description	Solution
Oracle Identity Manager cannot establish a connection with Oracle Internet Directory. **Returned Error Message:** LDAP Connection exception **Returned Error Code:** `INVALID_CONNECTION_ERROR`	■ Ensure that the Oracle Internet Directory server is running. ■ Ensure that Oracle Identity Manager is running (that is, the database is running). ■ Ensure that all the adapters have been compiled. ■ Examine the Oracle Identity Manager record (from the IT Resources form). 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 the specified Oracle Internet Directory connection values are correct. ■ Ensure that the Oracle Internet Directory server is running.
Authentication error **Returned Error Message:** Authentication error **Returned Error Code:** `AUTHENTICATION_ERROR`	Ensure that the specified Oracle Internet Directory connection password is correct.

Common LDAP Errors

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

Problem Description	Solution
Trying to add a value to a nonexistent attribute. Therefore, the Modify User operation failed. **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.EDIR lookup definition if the decode value is a valid attribute name in the target.
Trying to add an invalid value. Therefore, the Create User operation failed. **Returned Error Message:** Invalid value specified for an attribute **Returned Error Code:** INVALID_ATTR_VALUE_ERROR	Check the values specified during user creation.

Create User Errors

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

Problem Description	Solution
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 container ▪ User first name ▪ User last name ▪ User ID ▪ User password
Oracle Identity Manager cannot create a user. **Returned Error Message:** User already exists **Returned Error Code:** USER_ALREADY_EXIST	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 **Returned Error Code**: INVALID_NAMING_ERROR	Check if the specified user container value already exists on the target Oracle Internet Directory server.
Oracle Identity Manager cannot create a user. **Returned Error Message:** User creation failed **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 proper and contains all the object classes defined in the lookup definition.

Delete User Errors

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

Problem Description	Solution
Oracle Identity Manager cannot delete a user. **Returned Error Message:** Required information missing **Returned Error Code:** INSUFFICIENT_INFORMATION_PROVIDED	Ensure that the following information is provided: ■ User Container ■ User ID
Oracle Identity Manager cannot delete a user. **Returned Error Message:** User does not exist on the target system. **Returned Error Code**: USER_DOESNOT_EXIST	The specified user ID does not exist in Oracle Internet Directory.

Modify User Errors

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

Problem Description	Solution
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.
Trying to add a value to an attribute that does not exist in the AttrName.Prov.Map.OID lookup definition. Therefore, the Modify User operation failed. **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:** Error while updating user info **Returned Error Code**: USER_UPDATE_FAILED	Generic error. Review the log for more details.

Problem Description	Solution
Oracle Identity Manager cannot move a user from one container to another. **Returned Error Message:** Moving user to different container failed **Returned Error Code:** USER_MOVE_FAILED	Generic error. Review the log for more details.

Child Data Errors

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

Problem Description	Solution
Oracle Identity Manager cannot add a user to a group. **Returned Error Message:** Group does not exist **Returned Error Code:** GROUP_DOESNOT_EXIST	The specified user security group does not exist in Oracle Internet Directory. Check the group name.
Oracle Identity Manager cannot add a role to a user. **Returned Error Message:** Role does not exist **Returned Error Code:** ROLE_DOESNOT_EXIST	The specified role for the user does not exist in Oracle Internet Directory. Check the role name.
Trying to add a duplicate value to an attribute. **Returned Error Message:** Duplicate value **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:** Add user to group failed **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:** Remove user from group failed **Returned Error Code:** REMOVE_USER_FROM_GROUP_FAILED	Generic error. Review the log for more details.

Problem Description	Solution
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:** USER_REMOVE_FROM_ROLE_FAILED	Generic error. Review the log for more details.

4

Known Issues

The following is a known issue associated with this release of the connector:

The default `modifyTimeStamp` field provided by Oracle Internet Directory does not support the search operation. Therefore, all the users are queried for, regardless of the modified timestamp, and the events to be dropped are determined by using the `ignoreEvent` method of the Oracle Identity Manager API.

Index