Oracle® Identity Manager

Connector Guide for Novell eDirectory

Release 9.0.4

E10432-05

July 2009

ORACLE®

Oracle Identity Manager Connector Guide for Novell eDirectory, Release 9.0.4

E10432-05

Primary Author: Alankrita Prakash

Contributing Authors: Debapriya Datta, Devanshi Mohan, Lyju Vadassery

Contents

Preface

This guide provides information about Oracle Identity Manager Connector for Novell eDirectory.

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/oim.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 Novell eDirectory?

This chapter provides an overview of the updates made to the software and documentation for the Novell eDirectory connector in release 9.0.4.4.

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 9.0.4.2
- Software Updates in Release 9.0.4.3
- Software Updates in Release 9.0.4.4

Software Updates in Release 9.0.4.1

The following are software updates 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 `eDirProv.jar` file has been split into two files, `eDirProv.jar` and `eDirRecon.jar`. Corresponding changes have been made in the following sections:

- Files and Directories On the Installation Media on page 1-6
- Determining the Release Number of the Connector on page 1-7
- Using External Code Files on page 2-2
- Running Test Cases on page 4-1

Software Updates in Release 9.0.4.2

The following are software updates in release 9.0.4.2:

- Using the Connector Installer

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 9.0.4.3

The following are issues resolved in release 9.0.4.3:

Bug Number	Issue	Resolution
8433456	During trusted source reconciliation, two reconciliation events were created for each user record fetched from the target system.	This issue has been resolved. Only a single reconciliation event is created for each user record fetched from the target system. The `Last Recon Target TimeStamp` and `Last Recon Trusted TimeStamp` parameters have been added in the IT resource. The `Last Recon TimeStamp` parameter has been removed from the IT resource. See the section on configuring the IT resource for more information. The `TargetResourceObjectName` and `TrustedResourceObjectName` attributes have been added in the scheduled task. See "User Reconciliation Scheduled Task" for more information.

Software Updates in Release 9.0.4.4

The following are software updates in release 9.0.4.4:

- Support for Provisioning Organizational Units, Groups, and Roles Using Multiple Object Classes
- Support for Adding Custom Attributes for Trusted Source Reconciliation
- Resolved Issues

Support for Provisioning Organizational Units, Groups, and Roles Using Multiple Object Classes

By default, newly created organization units, groups, and roles on the target system are assigned to organization unit, group, and role object classes, respectively.

From this release onward, organization units, groups, and roles can be provisioned using multiple object classes.

See the "Adding Custom Object Classes for Provisioning" section for more information.

Support for Adding Custom Attributes for Trusted Source Reconciliation

By default, during trusted source reconciliation, the connector reconciles only the attributes listed in the "Reconciled Xellerate User (OIM User) Fields" section. From this release onward, the connector enables you to add custom attributes for trusted source reconciliation.

See the "Adding Custom Attributes for Trusted Source Reconciliation" section for more information.

Resolved Issues

The following are issues resolved in release 9.0.4.4:

Bug Number	Issue	Resolution
5695644	During a Create eDirectory Group provisioning operation, in the `Organization Unit` process form field, if you entered an organization unit that did not exist in the target system, then an error message was displayed that did not provide sufficient details to identify the cause of the error.	This issue has been resolved. During a Create eDirectory Group provisioning operation, if you do not specify an organization unit that does not exist in the target system, then the following error message is displayed: `Organization unit for new group does not exist in the target system`
8583836	A case-sensitive check was performed on the `ReconMode` attribute in the Code Key column of the `Lookup.EDIR.Organization` and `Lookup.EDIR.UserGroup` lookup definitions. If the case (uppercase or lowercase) of the `ReconMode` attribute did not match the case of the attribute name on the target system, then group and organization lookup reconciliation failed.	This issue has been resolved. A case-sensitive check is not performed on the `ReconMode` attribute in the Code Key column of the `Lookup.EDIR.Organization` and `Lookup.EDIR.UserGroup` lookup definitions.
8583865	By default, during the Create User provisioning operation, the Organization DN process form field displayed the `Regular` value. If you continued with the provisioning operation without specifying the correct value in the Organization DN field, then the provisioning operation failed. The invalid naming exception was thrown.	This issue has been resolved. The Organization DN field on the process form displays no value. Therefore, an appropriate value must be specified to proceed with provisioning operation. If no value is specified for this field, then the following error message is displayed: `Insufficient user information provided`
8586122	The status of the Delete User task was `Rejected` when the connector was configured for identity reconciliation (trusted source) mode. In addition, the status of the user remained at `provisioned` even after the corresponding OIM User was deleted.	This issue has been resolved. After the Delete User operation, the status of the user changes to `Revoked` and Delete User task changes to `Completed`.
8590100	When the password of the OIM User was changed, the Update Password task was not triggered.	This issue has been resolved. The Update Password task is triggered when you change the password of an OIM User.

Bug Number	Issue	Resolution
8597067	A naming exception was encountered if the User ID field contained a special character that was not supported by the target system. This exception did not provide sufficient details to identity the cause of the error.	This issue has been resolved. The following error message is displayed if the User ID field contains a special characters that are not supported by the target system: `The naming attribute contains special characters that are not supported by target`

Documentation-Specific Updates

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

- Documentation-Specific Updates in Releases 9.0.4.1 and 9.0.4.2
- Documentation-Specific Updates in Release 9.0.4.3
- Documentation-Specific Updates in release 9.0.4.4

Documentation-Specific Updates in Releases 9.0.4.1 and 9.0.4.2

The following documentation-specific updates have been made in releases 9.0.4.1 and 9.0.4.2:

- In the "Lookup Fields Reconciliation Scheduled Task" section on page 3-5, the description of the `CodeKeyLTrimStr` attribute has been modified.
- In the "Configuring the Connector for Multiple Installations of the Target System" section, `UD_EDIR_OU`, `UD_EDIR_RL`, and `UD_EDIR_GR` have been added to the list of process forms that are created when you import the connector XML file.
- There are no known issues associated with this release of the connector. Points that were earlier listed in the "Known Issues" chapter have been moved to the "Guidelines to Be Applied While Using the Connector" section on page 3-14.

Documentation-Specific Updates in Release 9.0.4.3

The following documentation-specific updates have been made in release 9.0.4.3:

- The "Configuring the Connector for Multiple Installations of the Target System" section has been removed from the "Configuring the Connector" chapter.

Documentation-Specific Updates in release 9.0.4.4

The following documentation-specific updates have been made in release 9.0.4.4:

- A note has been added in the "Supported Functionality" section.
- In the "Enabling Logging" section, all instances of the `log4j.logger.XL_INTG.eDirectory=` entry have been replaced with `log4j.logger.XL_INTG.EDIRECTORY=`.
- The following sections have been added:
  - Adding Custom Attributes for Trusted Source Reconciliation
  - Adding Custom Object Classes for Provisioning
- In the "Delete User Errors" section, text in the Solution column has been modified.

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 Novell eDirectory.

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, Novell eDirectory 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:

- Lookup Fields Reconciliation
- User Reconciliation

1.1.1 Lookup Fields Reconciliation

Lookup fields reconciliation involves reconciling organization, organizational unit, group, role, domain scope, and profile master data.

1.1.2 User Reconciliation

User reconciliation involves reconciling the fields discussed in this section.

1.1.2.1 Reconciled Resource Object Fields

The following fields are reconciled:

Note: These fields do not have the `ldap` prefix.

- User ID
- First Name
- Last Name
- Middle Name
- Department
- Location
- Telephone
- Email
- Communication Language
- Timezone
- Logon Script
- Title
- Profile
- Organization Unit
- Security Group (multiple group names can be entered)
- Role
  - Role Name
  - Scope
  - Inheritance
- Trustee Rights
  - Property
  - Supervisor
  - Read
  - Write
  - Compare
  - Add Self
- Network Address

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
- Organization
- First Name
- Last Name
- 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
- Timezone
- Logon Script
- Title
- Profile
- Organization Unit
- Server Name
- Security Group
- Role
  - Role Name
  - Scope
  - Inheritance

- Trustee Rights
  - Property
  - Supervisor
  - Read
  - Write
  - Compare
  - Add Self
- Network Address

For provisioning of organizational units, groups, and roles, refer to the "Supported Functionality" section on page 1-4.

1.3 Supported Functionality

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

Process Task	Type	Description
Create User	Provisioning	Creates a user in Novell eDirectory
Delete User	Provisioning	Deletes a user in Novell eDirectory
Enable User	Provisioning	Enables a user in Novell eDirectory
Disable User	Provisioning	Disables a user in Novell eDirectory
Move User	Provisioning	Moves a user from one container to another in Novell eDirectory **Note:** The Move User provisioning operation is not supported when the Novell eDirectory and Novell GroupWise resources are provisioned to an OIM User. This is because the association between the Novell GroupWise mailbox and Novell eDirectory object is lost after the Move User provisioning operation.
Update User Password	Provisioning	Updates the password of a user in Novell eDirectory
Add User to Group	Provisioning	Adds a user to a group in Novell eDirectory
Remove User from Group	Provisioning	Removes a user from a group in Novell eDirectory
Assign Role to User	Provisioning	Assigns a role to a user in Novell eDirectory
Remove Assigned Role from User	Provisioning	Removes a role from a user in Novell eDirectory
Assign Trustee Right to User	Provisioning	Adds a trustee right to a user in Novell eDirectory
Remove Trustee Right from User	Provisioning	Removes a trustee right from a user in Novell eDirectory
Add Network Address Restriction to User	Provisioning	Adds a network address restriction to a user in Novell eDirectory
Remove Network Address Restriction from User	Provisioning	Removes a network address restriction from a user in Novell eDirectory
Create OU	Provisioning	Creates an organizational unit
Change OU Name	Provisioning	Changes an organization name
Delete OU	Provisioning	Deletes an organizational unit

Process Task	Type	Description
Move OU	Provisioning	Moves the organization sub unit to another parent organizational unit
Create eDirectory Group	Provisioning	Creates a Novell eDirectory group
Delete eDirectory Group	Provisioning	Deletes a Novell eDirectory group
New Group Name Updated	Provisioning	Updates the group name
Create eDirectory Role	Provisioning	Creates a Novell eDirectory role
Delete eDirectory Role	Provisioning	Deletes a Novell eDirectory role
New Role Name Updated	Provisioning	Updates a role name
Create User	Reconciliation	Creates a user in 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 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
Assign Trustee Right to User	Reconciliation	Adds a trustee right to a user in Oracle Identity Manager
Remove Trustee Right from User	Reconciliation	Removes a trustee right from a user in Oracle Identity Manager
Add Network Address Restriction to User	Reconciliation	Adds a network address restriction to a user in Oracle Identity Manager
Remove Network Address Restriction from User	Reconciliation	Removes a network address restriction from a user in Oracle Identity Manager
Reconciliation Insert Received	Reconciliation	Inserts a user in Oracle Identity Manager
Reconciliation Update Received	Reconciliation	Updates a user in Oracle Identity Manager

See Also: Appendix A for information about attribute mappings between Oracle Identity Manager and Novell eDirectory

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 in Table 1–1.

Table 1–1 Files and Directories On the Installation Media

File in the Installation Media Directory	Description
`configuration/EDirectory-CI.xml`	This XML file contains configuration information that is used during connector installation.
`lib/eDirProv.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/eDirRecon.jar`	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 Installation Media

File in the Installation Media Directory	Description
Files in the `test/troubleshoot` directory	These files are used to implement test cases that are run by using the testing utility.
`xml/eDirResourceObject.xml`	This XML file contains definitions for the following components of the connector: ■ IT resource type ■ Process form ■ Process tasks and adapters (along with their mappings) ■ Resource object ■ Provisioning process ■ Pre-populate rules ■ Reconciliation process ■ Lookup definitions
`xml/eDirXLResourceObject.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/eDirProv.jar`

2. Open the `manifest.mf` file in a text editor. The `manifest.mf` file is one of the files bundled inside the `eDirProv.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
- Using External Code Files
- 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	Novell eDirectory 8.7.3
External code	`ldap.jar` and `ldapbp.jar` Refer to the "Using External Code Files" section on page 2-2 for information about downloading this JAR file.
Target system user account	Novell eDirectory user account to which the Supervisor right has been assigned You provide the credentials of this user account while performing the procedure in the "Configuring the IT Resource" section on page 2-4. If this target system user account is not assigned the specified rights, then the following error message may be displayed during connector operations: `Transaction is not active (Transaction Manager error)`

2.2 Using External Code Files

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.

The `ldap.jar` file contains APIs that are used to connect to the target system. You must download this file from the Novell Web site and copy it into the `ThirdParty` directory as follows:

1. Log on to the Novell Web site at

   `http://developer.novell.com/wiki/index.php/Special:Downloads/jldap/builds/netware_windows/`

2. Download the following file from the Novell Web site:

   `novell-jldap-devel-2005.10.03-1netware_windows.zip`

   The size of the file is 11.1 MB.

3. Extract the contents of the file that you downloaded in Step 2.

4. Copy the `ldap.jar` file from the `novell-jldap-devel-2005.10.03-1netware_windows\jldap_2005.10.03\lib` directory to the *`OIM_HOME`*`/xellerate/ThirdParty` directory on the Oracle Identity Manager server.

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 the Sun Web site at

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

2. Click **Download JNDI 1.2.1 & More**.

3. From the table on the page that is displayed, select and download the file containing the ldapbp.jar file.

4. Copy the ldapbp.jar file 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.

2.3 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

2.3.1 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 **Novell eDirectory *RELEASE_NUMBER*.** 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 **Novell eDirectory *RELEASE_NUMBER*.**
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 2-9 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 Table 1–1 for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.3.2 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 `eDirectory IT Resource` 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 `eDirectory IT Resource` 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 Novell eDirectory server Default value: cn=Admin,o=PXED-DEV
Admin Password	Password of the administrator
Server Address	Server address of the Novell eDirectory server
Root DN	Base DN on which all user operations are to be carried out Default value: o=PXED-DEV
Port	Port number to connect to the target Novell eDirectory server Default value: 389
SSL	Specifies whether or not SSL is used to secure communication between Oracle Identity Manager and Novell eDirectory The value can be true or false. Default value: false **Note:** It is recommended that you enable SSL to secure communication with the target system.
Last Recon Target TimeStamp	For the first target resource reconciliation run, the time stamp 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.
Last Recon Trusted TimeStamp	For the first trusted source reconciliation run, the time stamp 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.
Prov Attribute Lookup Code	Name of the lookup definition that has the target attribute mappings required for provisioning Default value: AttrName.Prov.Map.EDIR **Note:** This value must not be changed.
Recon Attribute Lookup Code	Name of the lookup definition that has the target attribute mappings required for reconciliation Default value: AttrName.Recon.Map.EDIR **Note:** This value must not be changed.
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 LDAP is used for reconciliation. Default value: false
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: givenname=John For more information about this parameter, refer to the "Partial Reconciliation" section on page 3-1.

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

2.4 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:

- Copying the Connector Files
- Importing the Connector XML File

2.4.1 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" on page 1-6 for more information about these files

File in the Installation Media Directory	Destination Directory
`lib/eDirProv.jar`	*`OIM_HOME`*`/xellerate/JavaTasks`
`lib/eDirRecon.jar`	`OIM_HOME/xellerate/ScheduleTask`
Files in the `resources` directory	*`OIM_HOME`*`/xellerate/connectorResources`
Files in the `test` directory	*`OIM_HOME`*`/xellerate/eDir/test/troubleshoot`
Files in the `xml` directory	*`OIM_HOME`*`/xellerate/eDir/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.

2.4.2 Importing the Connector XML File

> **Note:** Perform this procedure if you are installing the connector on Oracle Identity Manager release 8.5.3.1 through 9.0.3.

As mentioned in "Files and Directories On the Installation Media" 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 into Oracle Identity Manager:

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 `eDirResourceObject.xml` file, which is in the *`OIM_HOME`*`/xellerate/eDir/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 `eDirectory IT Resource` IT resource is displayed.
8. Specify values for the parameters of this IT resource. The following table describes each parameter:

Parameter	Description
`Admin ID`	DN value of the user who has administrator rights on the Novell eDirectory server Default value: `cn=Admin,o=PXED-DEV`
`Admin Password`	Password of the administrator
`Server Address`	Server address of the Novell eDirectory server
`Root DN`	Base DN on which all user operations are to be carried out Default value: `o=PXED-DEV`
`Port`	Port number to connect to the target Novell eDirectory server Default value: `389`
`SSL`	Specifies whether or not SSL is used to secure communication between Oracle Identity Manager and Novell eDirectory The value can be `true` or `false`. Default value: `false` **Note:** It is recommended that you enable SSL to secure communication with the target system.
`Last Recon Target TimeStamp`	For the first target resource reconciliation run, the time stamp 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.
`Last Recon Trusted TimeStamp`	For the first trusted source reconciliation run, the time stamp 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.
`Prov Attribute Lookup Code`	Name of the lookup definition that has the target attribute mappings required for provisioning Default value: `AttrName.Prov.Map.EDIR` **Note:** This value must not be changed.
`Recon Attribute Lookup Code`	Name of the lookup definition that has the target attribute mappings required for reconciliation Default value: `AttrName.Recon.Map.EDIR` **Note:** This value must not be changed.
`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 LDAP is used for reconciliation. Default value: `false`

Parameter	Description
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: givenname=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.

2.5 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

2.5.1 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.

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

While performing the instructions described in the "Using External Code Files" section on page 2-2, you copy files from the `resources` directory on the installation media into the *`OIM_HOME`*`/xellerate/connectorResources` directory. Whenever you add a new resource bundle in the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

1. In a command window, change to the *`OIM_HOME`*`/xellerate/bin` directory.

   Note: You must perform Step 1 before you perform Step 2. 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`

2.5.3 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.EDIRECTORY=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.EDIRECTORY=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.EDIRECTORY=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.EDIRECTORY=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, locate or 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.eDirectory">
   <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.eDirectory">
   <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.EDIRECTORY=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.EDIRECTORY=INFO
```

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

OC4J_home/opmn/logs/default_group~home~default_group~1.log

2.5.4 Setting Up Lookup Definitions in Oracle Identity Manager

The following lookup definitions are created in Oracle Identity Manager when you deploy the connector:

- Lookup.EDIR.NetworkRestriction

  During a provisioning operation, you use this lookup definition to specify the IP addresses of the workstations from which the user can log in. If you do not specify an IP address, then the user can log in from any workstation.

- Lookup.EDIR.CommLang

  During a provisioning operation, you use this lookup definition to specify a language for the user.

You must enter values in these lookup definitions before you can use them 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**.

2.6 Configuring SSL

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

To enable SSL connectivity between Oracle Identity Manager and the target Novell eDirectory:

1. Import the certificate from the target system into the JSDK (the JSDK that is used during installation of Oracle Identity Manager Server) `cacerts` keystore as follows:

   ```
   keytool -import -alias alias_name -file
   certificate_file_name_with_complete_path -keystore
   java_home/jre/lib/security/cacerts
   ```
2. Restart the Oracle Identity Manager server.
3. In the `eDirectory IT Resource` 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
- Guidelines to Be Applied While Using the Connector

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
- Batched Reconciliation
- Configuring Trusted Source Reconciliation
- Configuring the Reconciliation Scheduled Tasks
- Adding Custom Attributes for Trusted Source 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 values for the `CustomizedReconQuery` IT resource parameter while performing the procedure described in the "Configuring the IT Resource" section on page 2-4.

The following table lists the Novell eDirectory 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 Identity Manager Attribute	Novell eDirectory Attribute
User Id	cn
First Name	givenname
Last Name	sn
Email	mail
Middle Name	initials
Title	title
Location	l
Telephone	telephoneNumber
Department	departmentNumber
Language	preferredLanguage

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

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

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

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

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

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

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

You specify a value for the `CustomizedReconQuery` parameter while performing the procedure described in the "Configuring the IT Resource" section on page 2-4.

3.1.2 Batched Reconciliation

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 batched reconciliation to avoid such problems.

To configure batched reconciliation, you must specify values for the following user reconciliation scheduled task attributes:

- `StartRecord`: Use this attribute to specify the record number from which batched reconciliation must begin.
- `BatchSize`: Use this attribute to specify the number of records that must be included in each batch.
- `NumberOfBatches`: Use this attribute to specify the total number of batches that must be reconciled. If you do not want to use batched reconciliation, specify `All Available` as the value of this attribute.

Note: If you specify `All Available` as the value of this attribute, then the values of the `StartRecord` and `BatchSize` attributes are ignored.

You specify values for these attributes by following the instructions described in the "User Reconciliation Scheduled Task" section on page 3-7.

After you configure batched reconciliation, if reconciliation fails during a batched reconciliation run, then refer to the log file for information about the batch at which reconciliation has failed. The log file provides the following information about batched reconciliation:

- Serial numbers of the batches that have been successfully reconciled
- User IDs associated with the records with each batch that has been successfully reconciled
- If the batched reconciliation run fails, then the serial number of the batch that has failed

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, `eDirXLResourceObject.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 `eDirXLResourceObject.xml` file while you have another trusted source configured, then both connector reconciliations would stop working.

2. Set the value of the `TrustedSource` scheduled task attribute to `True`.

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 `eDirXLResourceObject.xml` file, which is in the *`OIM_HOME`*`/xellerate/eDir/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` scheduled task attribute to `True`. See the "Configuring the Reconciliation Scheduled Tasks" section on page 3-4 for more information.

3.1.4 Configuring the Reconciliation Scheduled Tasks

When you run the Connector Installer, the scheduled tasks for lookup fields and user reconciliations are automatically created in Oracle Identity Manager. To configure these scheduled tasks:

1. Log in to the Administrative and User Console.
2. Expand **Resource Management**.
3. Click **Manage Scheduled Task**.
4. Enter the name of the first scheduled task as the search criteria and then click **Search**.
5. In the search results table displaying the list of scheduled tasks, click the edit icon in the Edit column of the table.
6. On the Scheduled Task Details page, you can modify the following details of the scheduled task:
   - **Status:** Specify whether or not you want to leave the task in the enabled state after it is created. In the enabled state, the task is ready for use. If the task is disabled, then you must enable it before you can use it.
   - **Max Retries:** Enter an integer value in this field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the ERROR status to the task. The default value is 1.
   - **Next Start:** Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.
   - **Frequency:** Specify the frequency at which you want the task to run.
7. Click **Continue**.
8. Specify values for the attributes of the scheduled task. Refer to the "Specifying Values for the Scheduled Task Attributes" on page 3-5 for information about the attributes.
9. Click **Save Changes** to commit all the changes to the database.
10. Repeat Steps 3 through 9 for 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 `eDirectory 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.
- You must create a scheduled task for each master lookup data reconciliation: group, role, and profile.
- 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	Sample/Default Value

`AttrTask`	Name of the attribute task	■ For organizations:
		`o`
		■ For domain scope and organizational units:
		`ou`
		■ For groups, roles, and profiles
		`cn`

`LookupCodeName`	Name of the lookup definition to which the values are to be reconciled	■ For organizational units and organizations:
		`Lookup.EDIR.Organization`
		■ For domain scope:
		`Lookup.EDIR.DomainScope`
		■ For groups:
		`Lookup.EDIR.UserGroup`
		■ For roles:
		`Lookup.EDIR.AssignedRole`
		■ For profiles:
		`Lookup.EDIR.Profile`

`ITResourceName`	Name of the IT resource for setting up a connection with Novell eDirectory	`eDirectory IT Resource`
`SearchContext`	Search context to be used for searching for users	`o=PXED-DEV`

`ObjectClass`	Name of the object class	■ For Organizational units and domain scope:
		`OrganizationalUnit`
		■ For groups:
		`group`
		■ For roles:
		`rBSRole`
		■ For profiles:
		`profile`
		■ For organizations:
		`organization`

Attribute	Description	Sample/Default Value
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].	,o=PXED-DEV
ReconMode	Specify REFRESH to completely refresh the existing lookup. Specify UPDATE if you want to update the lookup with new values.	REFRESH or UPDATE

After you specify values for these scheduled task attributes, 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 eDirectory User Recon Task 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	Sample/Default Value
ITResourceName	Name of the IT resource for setting up a connection with Novell eDirectory	eDirectory IT Resource
ResourceObjectName	Name of the resource object into which users need to be reconciled	eDirectory User
XLDeleteUsersAllowed	If this attribute is set to true, then the Delete reconciliation event is started when the scheduled task is run. Users who are deleted from the target system are removed from Oracle Identity Manager. This requires all the users on the target system to be compared with all the users in Oracle Identity Manager. **Note:** This process affects performance.	true
UserContainer	DN value from where users are reconciled into Oracle Identity Manager	o=PXED-DEV
Keystore	Directory path to the Novell eDirectory keystore This is required to make a secure SSL connection. If an SSL connection is not required, then specify the value [NONE].	E:\j2sdk1.4.2_05\jre\lib\security\cacerts or [NONE]

Attribute	Description	Sample/Default Value
TrustedSource	Specifies whether trusted source reconciliation is to be performed If you want to perform target resource reconciliation, then change the value of this attribute to False.	True
TargetResourceObject Name	Specifies the name of the resource object for target resource reconciliation Do not change the value of this attribute.	eDirectory User
TrustedResourceObjec tName	Specifies the name of the resource object (Xellerate User) for trusted source reconciliation Do not change the value of this attribute.	Xellerate User
Xellerate Type	Default xellerate type for the Xellerate User (OIM User)	End-User Administrator
Organization	Default organization for the Xellerate User (OIM User)	Xellerate Users
Role	Default role for the Xellerate User (OIM User)	Consultant
StartRecord	Specifies the start record for batching process This attribute is also discussed in the "Batched Reconciliation" section on page 3-3.	1
BatchSize	Specifies how many records must be there in a batch This attribute is also discussed in the "Batched Reconciliation" section on page 3-3.	1
NumberOfBatches	Specifies the number of batches that must be reconciled This attribute is also discussed in the "Batched Reconciliation" section on page 3-3.	Default value: All Available (for reconciling all the users) Sample value: 50

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

Stopping Reconciliation

Suppose the User Reconciliation Scheduled Task for the connector is running and user records are being reconciled. If you want to stop the reconciliation process:

1. Perform Steps 1 through 4 of the procedure to configure reconciliation scheduled tasks.
2. Select the **Stop Execution** check box in the task scheduler.
3. Click **Save**.

3.1.5 Adding Custom Attributes for Trusted Source Reconciliation

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

By default, the attributes listed in the "Reconciled Xellerate User (OIM User) Fields" section are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new attributes for trusted resource reconciliation.

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 **Administration.**
   b. Double-click **User Defined Field Definition.**
   c. Search for and open the **User** form.
   d. Click **Add.**
   e. In the User Defined Fields dialog box, enter the details of the attribute.

      For example, if you are adding the Title attribute, then enter the following details in the User Defined Fields dialog box:

      – In the **Label** field, enter `Title`.
      – From the Data Type list, select **String.**
      – From the Field Type list, select **Text Field.**
      – In the **Column Name** field, enter `USR_UDF_TITLE`.
      – In the **Field Size** field, enter `100`.

   f. Click **Save.**
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 **Xellerate User** resource object.
   d. On the Object Reconciliation tab, click **Add Field.**
   e. Enter the details of the attribute.

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

   f. Click **Save.**
4. Create a reconciliation field mapping for the new attribute in the process definition as follows:
   a. Expand **Process Management.**
   b. Double-click **Process Definition.**
   c. Search for and open the **Xellerate User** process definition.
   d. On the Reconciliation Field Mappings tab, click **Add Field Map.**
   e. In the Field Name field, select the value for the attribute that you want to add.

      For example, select `Title = Title`.

   f. Click **Save.**
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.EDIR** 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 `Title` in the **Code Key** field and then enter `Title` in the **Decode** field.

e. Click **Save.**

3.2 Configuring Provisioning

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

This section discusses the following topics related to configuring provisioning:

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

- `EDIR Create User`
- `EDIR Delete User`
- `EDIR Modify User`
- `EDIR Move User`
- `EDIR Add User to Group`
- `EDIR Remove User from Group`
- `EDIR Add Trustee Right to User`
- `EDIR Remove Trustee Right from User`

- EDIR Add Assigned Role to User
- EDIR Remove Assigned Role from User
- EDIR Add Network Restriction
- EDIR Remove Network Restriction
- EDIR PP String
- Update eDirectory Role Details
- Update eDirectory Group Details
- EDIR Delete Group
- EDIR Create Group
- EDIR Remove User from Group
- Chk Process Parent Org eDir
- EDIR Create OU
- EDIR Remove User from Role
- EDIR Create Role
- EDIR Delete Role
- EDIR Move OU
- EDIR Change Org Name
- EDIR 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 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.EDIR` lookup definition, the following are default settings for enabling provisioning of users in organizational units:

- `ldapOrgDNPrefix=ou`
- `ldapOrgUnitObjectClass=OrganizationalUnit`

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

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

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

3.2.3 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.

3.2.4 Adding Custom Object Classes for Provisioning

Note: Perform the procedure described in this section only if you want to add custom object classes for provisioning organizational units, groups, or roles.

By default, newly created organizational units, groups, and roles on the target system are assigned to the organizational unit, group, and role object classes, respectively.

The organizational unit object class is the value of the `ldapOrgUnitObjectClass` attribute in the `AttrName.Prov.Map.EDIR` lookup definition. Similarly, the group and role object classes are the values of the `ldapGroupObjectClass` and `ldapRoleObjectClass` attributes in the `AttrName.Prov.Map.EDIR` lookup definition, respectively.

If you want to assign new organizational units, groups, or roles to additional object classes, then enter the list of object classes in the Decode column for their respective attributes in the lookup definition. Use the vertical bar (`|`) to separate the object class names in the value that you specify.

The following are sample values for the ldapGroupObjectClass entry:

- `group`
- `mygroup`
- `group|mygroup`

To add object classes for organizational units, groups, or roles:

1. On the Design Console, expand **Administration,** and then double-click **Lookup Definition.**
2. Search for and open the **AttrName.Prov.Map.EDIR** lookup definition.
3. Perform one of the following:

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.

- To add an object class for an organizational unit, enter the object class name in the Decode column of the `ldapOrgUnitObjectClass` Code Key.
- To add an object class for a group, add the object class name to the Decode value of the `ldapGroupObjectClass` Code Key.
- To add an object class for a role, add the object class name to the Decode value of the `ldapRoleObjectClass` Code Key.

4. Click the save icon.

3.3 Guidelines to Be Applied While Using the Connector

Apply the following guidelines while using the connector:

- 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.

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` directory on the installation media, to the *`OIM_HOME`*`/xellerate/eDir/test/troubleshoot` directory.
2. Specify the required values in the `global.properties` file.

   This file is in the *`OIM_HOME`*`/xellerate/eDir/test/troubleshoot` directory. The following table describes the sections of this file in which you must provide information for running the tests.

Section	Information
Novell eDirectory Server Parameters	Parameters required to connect to Novell eDirectory Refer to the "Configuring the IT Resource" section on page 2-4 for information about the values that you must provide.
Create User Parameters	Values required to create a user on the target system
Modify User Parameters	Values required to modify a user
Delete User Parameters	DN of the user to be deleted

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

   `OIM_HOME``/xellerate/lib/xlLogger.jar`
   `OIM_HOME``/xellerate/lib/xlUtils.jar`
   `OIM_HOME``/xellerate/JavaTasks/eDirProv.jar`
   `OIM_HOME/xellerate/ScheduleTask/eDirRecon.jar`
   `OIM_HOME``/xellerate/ThirdParty/ldapbp.jar`
   `OIM_HOME``/xellerate/ext/log4j-1.2.9.jar`

4. By default, log messages that are generated when you run the testing utility are displayed on the console. If you also want these messages to be recorded in a log file, then:

a. Open the following file in a text editor:

   OIM_HOME/xellerate/eDir/test/troubleshoot/log.properties

b. Search for the following lines, and then uncomment them by removing the number sign (#) at the start of each line:

```
#log4j.appender.logfile=org.apache.log4j.DailyRollingFileAppender
#log4j.appender.logfile.DatePattern='.'yyyy-MM-dd
#log4j.appender.logfile.File=D:/elogfile/edirectory.log
#log4j.appender.logfile.MaxBackupIndex=20
#log4j.appender.logfile.layout=org.apache.log4j.PatternLayout
#log4j.appender.logfile.layout.ConversionPattern=%p %t %c - %m%n
```

c. If required, specify a new date pattern in the following line:

```
log4j.appender.logfile.DatePattern='.'yyyy-MM-dd
```

d. In the following line, specify the directory in which you want the log file to be generated:

```
log4j.appender.logfile.File=D:/elogfile/edirectory.log
```

5. Create an ASCII-format copy of the `global.properties` file as follows:

   Note: You must perform this procedure every time you make a change in the contents of the `global.properties` file.

   a. In a command window, change to the following directory:

      OIM_HOME/xellerate/eDir/test/troubleshoot

   b. Enter the following command:

      ```
      native2ascii global.properties troubleshoot.properties
      ```

      The `troubleshoot.properties` file is created when you run the `native2ascii` command. The contents of this file are an ASCII-format copy of the contents of the `global.properties` file.

6. Run the following tests:

   - Enter the following command to create a Novell eDirectory user:

     ```
     java
     -DpropertyFile=OIM_HOME/xellerate/eDir/test/troubleshoot/troubleshoot.prope
     rties
     -Dlog4j.configuration=file:/OIM_HOME/xellerate/eDir/test/troubleshoot/log.p
     roperties TroubleShootingUtilityLdap createUser
     ```

   - Enter the following command to modify a Novell eDirectory user:

     ```
     java
     -DpropertyFile=OIM_HOME/xellerate/eDir/test/troubleshoot/troubleshoot.prope
     rties
     -Dlog4j.configuration=file:/OIM_HOME/xellerate/eDir/test/troubleshoot/log.p
     roperties TroubleShootingUtilityLdap modifyUser
     ```

   - Enter the following command to delete a Novell eDirectory user:

     ```
     java
     -DpropertyFile=OIM_HOME/xellerate/eDir/test/troubleshoot/troubleshoot.prope
     ```

```
rties
-Dlog4j.configuration=file:/OIM_HOME/xellerate/eDir/test/troubleshoot/log.p
roperties TroubleShootingUtilityLdap deleteUser
```

4.1.1 Testing Partial Reconciliation

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

- Value assigned to the `CustomizedReconQuery` parameter:

  `group=group1`

  Outcome: Records of users belonging to `group1` are reconciled.

- Value assigned to the `CustomizedReconQuery` parameter:

  `sn=Doe&group=group1`

  Outcome: Records of users with last name `Doe` and belonging to `group1` are reconciled.

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

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

    Outcome: Users with last name `Doe` and who belong to both the roles `role1` and `role2` are reconciled.

- Value assigned to the CustomizedReconQuery parameter:

  `sn=Doe&group=group1&role=role1`

  Outcome: Records of users with last name `Doe` and who belong to `group1` as well as `role1` are reconciled.

4.1.2 Testing Batched Reconciliation

You can test reconciliation based on batching and data paging of user records by specifying values for the following user reconciliation scheduled task attributes:

- If you set the value of `StartRecord` to `1`, `BatchSize` to `0`, and `NumberOfBatches` to `All Available`, then all the users are reconciled.
- If you set the value of `StartRecord` to `1`, `BatchSize` to `5`, and `NumberOfBatches` to `50`, then the user records starting from record 1 are reconciled in 50 batches, with 5 records in each batch.
- If you set the value of `StartRecord` to `200`, `BatchSize` to `5`, and `NumberOfBatches` to `50`, then the users starting from record 200 are reconciled in 50 batches, with 5 records in each batch.

The results of batching are displayed in the logger file, which is located in the following path:

`JBOSS_HOME/server/default/log/server.log`

In this file, you can view the batch numbers, the user ids of the users that are reconciled, and whether the reconciliation is successful or not.

4.2 Troubleshooting

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

- Connection Errors
- Create User Errors
- Modify User Errors
- Delete User 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 to Novell eDirectory. **Returned Error Message:** Error encountered while connecting to target server **Returned Error Code:** `INVALID_CONNECTION_ERROR`	■ Ensure that Novell eDirectory 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 is not available **Returned Error Code:** `TARGET_UNAVAILABLE_ERROR`	Ensure that the specified Novell eDirectory connection values are correct.
Returned Error Message: Invalid or incorrect password **Returned Error Code:** `AUTHENTICATION_ERROR`	Ensure that the specified Novell eDirectory connection values are correct.

4.2.2 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 specified IP address, admin ID, and administrator password are correct. ■ Ensure that the following information has been 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 assigned ID already exists in Novell eDirectory.
Oracle Identity Manager cannot create a user. **Returned Error Message:** Naming exception encountered **Returned Error Code:** INVALID_NAMING_ERROR	■ Ensure that the specified Novell eDirectory connection values are correct. ■ Check if the value for an attribute violates the schema definition.
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.
The Create User function failed because a value was being added to a nonexistent attribute. **Returned Error Message:** Attribute does not exist **Returned Error Code:** ATTRIBUTE_DOESNOT_EXIST	In the `AttrName.Prov.Map.EDIR` lookup definition, check if the decode values are valid attribute names in the target system.
The Create User function failed because an invalid value was specified. **Returned Error Message:** Invalid value specified for an attribute **Returned Error Code:** INVALID_ATTR_VALUE_ERROR	Check the values specified during user creation.

4.2.3 Modify User Errors

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

Problem Description	Solution
Oracle Identity Manager cannot modify the value of a user. **Returned Error Message:** Invalid attribute value or state **Returned Error Code:** INVALID_ATTR_MODIFY_ERROR	Check the attribute ID and value that were specified.
The Modify User function 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 specified for AttrName of the connector. 2. Using the name obtained in the previous step, check in the AttrName.Prov.Map.EDIR lookup definition if the decode value is a valid attribute name in the target.
The Modify User function failed because an invalid value was specified. **Returned Error Message:** Invalid value specified for an attribute **Returned Error Code:** INVALID_ATTR_VALUE_ERROR	Check the value entered.
The Modify User function failed because a value was specified for an attribute that does not exist in the AttrName.Prov.Map.EDIR 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 specified 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.EDIR lookup definition.
Error caused because a duplicate value was specified for an attribute. **Returned Error Message:** Duplicate value encountered **Returned Error Code:** DUPLICATE_VALUE_ERROR	The attribute specified already exists for another user in the system.
Oracle Identity Manager cannot move a user from one container to another. **Returned Error Message:** Could not move user to a different container **Returned Error Code:** USER_MOVE_FAILED	Generic error. Review the log for more details.
Oracle Identity Manager cannot add a user to a security group. **Returned Error Message:** Group does not exist **Returned Error Code:** SEC_GROUP_DOESNOT_EXIST	The specified user security group does not exist in Novell eDirectory.

Problem Description	Solution
Oracle Identity Manager cannot add a user to a security group. **Returned Error Message:** Duplicate value encountered **Returned Error Code:** DUPLICATE_VALUE	The user is already a member of the specified security group.
Oracle Identity Manager cannot add the trustee right to a user. **Returned Error Message:** Duplicate value encountered **Returned Error Code:** DUPLICATE_VALUE	Check if the trustee right has already been assigned to the user in Novell eDirectory.
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 in Oracle Identity Manager does not exist in Novell eDirectory. Create the role in Novell eDirectory.
Oracle Identity Manager cannot add a role to 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 add a role to a user. **Returned Error Message:** Duplicate value encountered **Returned Error Code:** DUPLICATE_VALUE	The user has already been assigned this role.
Oracle Identity Manager cannot remove an assigned role from a user. **Returned Error Message:** Could not remove assigned role **Returned Error Code:** USER_DELETE_ASSIGNED_ROLE_FAILED	Generic error. Review the log for more details.
Oracle Identity Manager cannot add a network restriction. **Returned Error Message:** Duplicate value encountered **Returned Error Code:** DUPLICATE_VALUE	The specified network restriction already exists for this user in Novell eDirectory.

4.2.4 Delete User Errors

The following table provides solutions to a commonly encountered Delete User error.

Problem Description	Solution
Oracle Identity Manager cannot delete a user. **Returned Error Message:** User does not exist **Returned Error Code:** `USER_DOESNOT_EXIST`	User is already deleted in the target

5

Known Issues

There are no known issues associated with this release of the connector.

A

Attribute Mappings Between Oracle Identity Manager and Novell eDirectory

The following table discusses attribute mappings between Oracle Identity Manager and Novell eDirectory.

Oracle Identity Manager Attribute	Novell eDirectory Attribute	Description
Logon Script	loginScript	Login script that is used to log in to Novell eDirectory
Communication Language	language	Language of communication
ldapOrgDNPrefix	ou	Organizational unit for organization
ldapPassword	userPassword	Password
ldapOrgPersonObject	OrganizationalPerson	Object class
Timezone	timezone	Time zone of the Novell eDirectory system
ldapRoleObjectClass	rBSRole	Object class of role
ldapRoleDNPrefix	cn	Role object
Profile	profile	Profile
loginDisabled	loginDisabled	Disabled status login
ldapUserUniqueAttr	cn	User name attribute
ldapUserObjectClass	inetOrgPerson	Object class
ldapUserDNPrefix	cn	User object
ldapUserDisableAttr	loginDisabled	Login disable attribute
ldapObjectClass	objectclass	Object class
ldapGroupObjectClass	group	Object class of group
ldapGroupMemberAttr	groupMembership	Group member attribute
ldapGroupDNPrefix	cn	Group object
ldapFirstName	givenName	First name
ldapLastName	sn	Last name
Title	title	Title
Location	l	Location
Telephone	telephoneNumber	Telephone number
Email	mail	Email address

Oracle Identity Manager Attribute	Novell eDirectory Attribute	Description
Department	departmentNumber	Department number
Middle Name	initials	Initials
User ID	cn	User ID
Organization Unit	o	Organizational unit
ldapOrgUnitObjectClass	ldunit	Object class of organizational unit
ldapTargetResourceTimeStampField	modifyTimestamp	Time stamp of the Novell eDirectory system
ldapMultiValAttr	Security Group, Group Name|Trustee Rights, Trustee Rights|Role, Role Name|Network Address, NetAdd	Multivalue attribute
Trustee Rights	ACL	Trustee rights
Role Name	rBSAssignedRoles	User role
NetAdd	networkAddressRestriction	Network address that is restricted for the user
First Name	givenname	First name
Last Name	sn	Last name

Index

M

O

P

R

S

T

U

X