Oracle® Identity Manager

Connector Guide for Novell eDirectory

Release 9.0.4

E10432-14

October 2015

Oracle Identity Manager Connector Guide for Novell eDirectory, Release 9.0.4

E10432-14

Primary Author: Gauhar Khan

Contributing Authors: Alankrita Prakash, Deena Purushothaman

Contents

2 Deploying the Connector

3 Using the Connector

4 Extending the Functionality of the Connector

5 Testing and Troubleshooting

6 Known Issues

Index

List of Figures

List of Tables

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with Novell eDirectory.

Audience

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

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

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 9.0.4.14.

> **Note:** Release 9.0.4.14 of the connector comes after release 9.0.4.12. Release number 9.0.4.13 has not been used.

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 software updates:

- Software Updates in Release 9.0.4.14
- Software Updates in Release 9.0.4.12
- Software Updates in Release 9.0.4.5
- Software Updates in Release 9.0.4.4
- Software Updates in Release 9.0.4.3
- Software Updates in Release 9.0.4.2
- Software Updates in Release 9.0.4.1

Software Updates in Release 9.0.4.14

The following are resolved issues in release 9.0.4.14:

Bug Number	Issue	Resolution
13253177	The connector revoked all net addresses restrictions of a user during provisioning operations.	This issue has been resolved.

Bug Number	Issue	Resolution
9824698	When attempting to disable or modify a user, the updates were not made in Novell eDirectory due to LDAP error code.	This issue has been resolved.
10199421	When a provisioned attribute value is set to empty string in Oracle Identity Manager, the attribute value was also nullified on the target system. There was no option to remove the attribute from the user on the target system.	This issue has been resolved.
10357910	If the eDirectory Organization Lookup Reconciliation Task scheduled task was run, the task was indicated as success without any error/exception. However, the result was empty, it was not populating any entries.	This issue has been resolved.
16484995	Provisioning groups in LDAP containing large number of users took a very long time to complete.	This issue has been resolved.
16623193	When attempting to revoke an account from an eDirectory configured with Org DN prefix "o", the operation failed with an error.	This issue has been resolved.
9258623	You specify the port number of the target system host computer as the value of the Port IT resource parameter. The following issues were related to this feature: ■ The connector did not work if a port other than 389 was specified as the value of the Port parameter. ■ In a high-availability environment, if the primary server fails, then the connector automatically switches to a secondary server based on the entry in the Lookup.EDIR.BackupServers lookup definition. However, the connector failed if the port for connector operations on the secondary server was not the same as the port specified in the IT resource.	Both issues have been resolved: ■ You can now specify any port as the value of the Port parameter. ■ In the Lookup.EDIR.BackupServers lookup definition, you now specify the port for connector operations for each secondary server.
9667788 and 9772198	The Move User provisioning operation did not work correctly.	This issue has been resolved. The Move User provisioning operation now works as expected.

Bug Number	Issue	Resolution

9504505	The Add User to Group and Remove User from Group provisioning operations failed if the domain name was in the format shown in the following example:
	`o=ts-bec,st=qc,c=ca`
	The operation did not fail if the domain name was in a format such as the following:
	`o=Company`
		This issue has been resolved. The Add User to Group and Remove User from Group provisioning operations work for both formats of the domain name.

9675680	The AttrTask attribute of the scheduled tasks for lookup field synchronization is used to hold the naming attribute of the object on the target system. During lookup field synchronization, a NullPointerException was encountered if the object (specified as the value of the AttrTask attribute) was not present in the target system.	This issue has been resolved.

Software Updates in Release 9.0.4.12

The following are the software updates in release 9.0.4.12:

- Support for New Oracle Identity Manager Release
- Support for Request-Based Provisioning

Support for New Oracle Identity Manager Release

From this release onward, the connector can be installed and used on Oracle Identity Manager 11*g* release 1 (11.1.1). Where applicable, instructions specific to this Oracle Identity Manager release have been added in the guide.

See Section 1.1, "Certified Components" for the full list of certified Oracle Identity Manager releases.

Support for Request-Based Provisioning

From this release onward, the connector provides support for request-based provisioning on Oracle Identity Manager 11*g* release 1 (11.1.1).

See Section 3.6.1.2, "Request-Based Provisioning" for more information.

Software Updates in Release 9.0.4.5

The following are software updates in release 9.0.4.5:

- Addition to the List of Certified Target System Versions
- Change in the Minimum Oracle Identity Manager Release Requirement
- Support for Reconciliation and Provisioning of Groups and Roles
- Support for Reconciliation and Provisioning of Custom Single-valued and Multivalued Attributes of Users, Groups, and Roles

- Separate Scheduled Tasks for User, Group and Role Reconciliation and Lookup Field Synchronization
- Support for High Availability Target System Environments
- Support for Paged Reconciliation
- Support for Transformation of Data During Reconciliation
- Support for Reconciliation and Provisioning of Home Directories
- Enhanced Logging
- Addition of the GUID to the Standard Set of User, Group, and Role Attributes
- Inclusion of Javadocs in the Connector Deployment Package
- Resolved Issues

Addition to the List of Certified Target System Versions

From this release onward, Novell eDirectory 8.8 has been added to the list of certified target system versions. This version is mentioned in Section 1.1, "Certified Components."

Change in the Minimum Oracle Identity Manager Release Requirement

In earlier releases, the minimum Oracle Identity Manager release requirement was release 8.5.3.1. From this release onward, the minimum requirement is Oracle Identity Manager release 9.0.3.2. This change has been made in Section 1.1, "Certified Components."

Support for Reconciliation and Provisioning of Groups and Roles

From this release onward, the connector supports reconciliation and provisioning of groups and roles from the target system. This is in addition to support for single-valued and multivalued user attributes.

See the following sections for information about the group and role object attributes that are mapped by the connector:

- Section 1.6.2, "Group Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6.3, "Role Attributes for Target Resource Reconciliation and Provisioning"

Support for Reconciliation and Provisioning of Custom Single-valued and Multivalued Attributes of Users, Groups, and Roles

In earlier releases, the connector supported reconciliation and provisioning of only standard single-valued and multivalued user attributes. From this release onward, the connector can be configured to reconcile from and provision to custom single-valued and multivalued attributes of users, groups, and roles.

See Chapter 4, "Extending the Functionality of the Connector" for more information.

Separate Scheduled Tasks for User, Group and Role Reconciliation and Lookup Field Synchronization

Separate scheduled tasks have been introduced for lookup field synchronization and user, group, and role reconciliation. See the following sections for more information:

- Section 3.2, "Lookup Field Synchronization"
- Section 3.3.4, "Reconciliation Scheduled Tasks"

Support for High Availability Target System Environments

From this release onward, the connector can be configured to work with high-availability target system environments.

See Section 1.4.10, "Support for High-Availability Configuration of the Target System" for more information.

Support for Paged Reconciliation

From this release onward, you can use the PageSize entry in the Lookup.EDIR.Configuration lookup definition to implement paged reconciliation.

See Section 1.4.4, "Support for Paged Reconciliation" for more information.

Support for Transformation of Data During Reconciliation

From this release onward, you can configure transformation of data during reconciliation.

See Section 1.4.8, "Support for Transformation of Data During Reconciliation" for more information.

Support for Reconciliation and Provisioning of Home Directories

From this release onward, the connector supports reconciliation and provisioning of Home directories for users. The procedure to enable and use this feature is optional.

See Section 1.4.9, "Support for Reconciliation and Provisioning of Home Directories" for more information.

Introduction of New Lookup Definitions

New lookup definitions have been introduced in this release. These lookup definitions are described in Section 1.5, "Lookup Definitions Used During Reconciliation and Provisioning."

Enhanced Logging

The logging feature has been enhanced in this release.

See Section 2.3.6, "Enabling Logging" for information about this feature.

Addition of the GUID to the Standard Set of User, Group, and Role Attributes

From this release onward, the GUID attribute has been added to the standard set of user, group, and role attributes. This attribute is used to uniquely identify a user, group, or role record during reconciliation and provisioning operations.

See Section 1.5, "Connector Objects Used During Reconciliation and Provisioning" for information about attribute mappings.

Inclusion of Javadocs in the Connector Deployment Package

To facilitate reuse and customization of some parts of the connector code, Javadocs are included in the connector deployment package.

Resolved Issues

The following are issues resolved in release 9.0.4.5:

Bug Number	Issue	Resolution

8495610 and 8687094	During a provisioning operation, a user's home directory could not be created on a computer running Novell Netware.	This issue has been resolved. A user's home directory can be created on a computer running Novell Netware.
		Note: In the Home Directory Name field on the Administrative and User Console, you can enter either the name of the home directory or the full path and name of the home directory. The directory path that you specify must exist on the target system.
		The following are sample values for the Home Directory Name field:
		`jdoe_home`
		`accounts/north_east/jdoe_home`

8602804	The Disable User operation did not work as expected.	This issue has been resolved. Provisioning and reconciliation of user status data now works as expected.
8608914	In earlier releases, the reconciliation query that you set as the value of the CustomizedReconQuery parameter of the IT resource was not correctly applied.	This issue has been resolved. The CustomizedReconQuery parameter of the IT resource has been replaced by the SearchFilter attribute of the scheduled task. See Section 3.3.2, "Limited Reconciliation" for information about the SearchFilter attribute.
8686335	The full DN was not provided for selection of the OU while setting or modifying an access policy. The outcome was that users were sometimes provisioned to an OU different from the one selected in the access policy.	This issue has been resolved. The full DN is displayed for selection of the OU while setting or modifying access policies. The OU you select is the OU that is used for the provisioning operation.
8703234	The Create User provisioning operation failed if you tried to provision users in an organization object. The operation was successful if you created users in an organizational unit object.	This issue has been resolved. Through Create User provisioning operations, you can create users in both organizations and organizational units.
8864051	A Create User provisioning operation could not be performed if you were also trying to assign the user to a group that had the backslash (\) character in its name.	This issue has been resolved. You can now assign users to groups that contain the backslash character in their names.

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 New 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`

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 9.0.4.2

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.x and Release 11.1.x" on page 2-5 for details.

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 5-1

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- Documentation-Specific Updates in Release 9.0.4.14
- Documentation-Specific Updates in Release 9.0.4.12
- Documentation-Specific Updates in Release 9.0.4.5
- Documentation-Specific Updates in Release 9.0.4.4
- Documentation-Specific Updates in Release 9.0.4.3
- Documentation-Specific Updates in Releases 9.0.4.1 and 9.0.4.2

Documentation-Specific Updates in Release 9.0.4.14

The following documentation-specific update has been made in revision "14" of release 9.0.4.14:

The names of properties listed in Step 12 of Section 2.3.1.1, "Tagging Form Fields" have been modified.

The following documentation-specific update has been made in revision "13" of release 9.0.4.14:

In Table 1–1, " Certified Components" the "Oracle Identity Manager" row has been modified.

The following are documentation-specific updates in revision "12" of release 9.0.4.14:

- Information regarding logger name has been updated in Section 2.3.6.2, "Enabling Logging on Oracle Identity Manager Release 11.1.x"
- The Destination Directory path to import XML files for trusted source reconciliation has been updated in Section 2.3.10, "Configuring Trusted Source Reconciliation"
- Information about the attributes that are added when a user is assigned a role has been updated in Section 1.6.1, "User Attributes for Target Resource Reconciliation and Provisioning"

The following are documentation-specific updates in revision "11" of release 9.0.4.14:

- The "Oracle Identity Manager" row in Table 1–1, " Certified Components" has been modified.
- The following sections have been added:
  - Section 2.3.1, "Configuring Oracle Identity Manager 11.1.2 or Later"
  - Section 2.3.2, "Localizing Field Labels in UI Forms"
  - Section 3.7, "Configuring Provisioning in Oracle Identity Manager Release 11.1.2"
- Instructions specific to Oracle Identity Manager release 11.1.2.*x* have been added in the following sections:
  - Section 2.2.1.1, "Running the Connector Installer"
  - Section 2.2.1.2, "Configuring the IT Resource"
  - Section 3.4, "Configuring Scheduled Tasks"

The following are documentation-specific updates in earlier revisions of release 9.0.4.14:

- The structure of Section 2.1, "Preinstallation" has been changed to include Section 2.1.1, "Preinstallation on Oracle Identity Manager" and Section 2.1.2, "Preinstallation on the Target System." In addition, Section 2.1.2.1, "Installing Role Based Services" has been added.
- In Section 3.3.1, "Full Reconciliation vs. Incremental Reconciliation," the value to be set to the time-stamp parameter to perform full reconciliation has been changed.
- In Chapter 6, "Known Issues," issues tracked by bugs 11802703 and 11821981 have been added.

Documentation-Specific Updates in Release 9.0.4.12

The following documentation-specific updates have been made in release 9.0.4.12:

- The "Description" column has been removed from Table 1–9, " Provisioning Functions".
- Section 3.4.1, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.0.1 through 9.0.3.2" has been added.

Documentation-Specific Updates in Release 9.0.4.5

Major changes have been made in the structure of the guide. The objective of these changes is to improve the usability of the guide.

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 "Provisioning Functions" 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 New 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.

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 "Extending the Functionality of the Connector" chapter.

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 "Lookup Fields Reconciliation Scheduled Task" on page 4-5, 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 "Guidelines to Be Applied While Using the Connector" on page 3-14.

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 external, identity-aware applications. This guide discusses the connector that enables you to use Novell eDirectory either as a managed (target) resource or as an authoritative (trusted) source of identity data for Oracle Identity Manager.

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

In the account management (target resource) mode of the connector, information about users created or modified directly on the target system can be reconciled into Oracle Identity Manager. In addition, you can use Oracle Identity Manager to perform provisioning operations on the target system.

In the identity reconciliation (trusted source) configuration of the connector, users are created or modified only on the target system and information about these users is reconciled into Oracle Identity Manager.

> **Note:** It is recommended that you do not configure the target system as both an authoritative (trusted) source and a managed (target) resource.

This chapter contains the following sections:

- Section 1.1, "Certified Components"
- Section 1.2, "Certified Languages"
- Section 1.3, "Connector Architecture"
- Section 1.4, "Features of the Connector"
- Section 1.5, "Lookup Definitions Used During Reconciliation and Provisioning"
- Section 1.6, "Connector Objects Used During Target Resource Reconciliation and Provisioning"
- Section 1.7, "Connector Objects Used During Trusted Source Reconciliation"
- Section 1.8, "Roadmap for Deploying and Using the Connector"

1.1 Certified Components

Table 1–1 lists the certified components for this connector.

Table 1–1 Certified Components

Item	Requirement
Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager: ■ Oracle Identity Manager release 9.0.1 through 9.0.3.2 ■ Oracle Identity Manager release 9.1.0.1 and any later BP in this release track **Note:** In this guide, **Oracle Identity Manager release 9.1.0.*x*** has been used to denote Oracle Identity Manager release 9.1.0.1 and future releases in the 9.1.0.*x* series that the connector supports. ■ Oracle Identity Manager 11*g* release 1 (11.1.1.3.0) and any later BP in this release track **Note:** In this guide, **Oracle Identity Manager release 11.1.1** has been used to denote Oracle Identity Manager 11*g* release 1 (11.1.1) and future releases in this release track. ■ Oracle Identity Manager 11g Release 1 PS1 (11.1.1.5.0) and any later BP in this release track ■ Oracle Identity Manager 11g Release 1 PS2 (11.1.1.7.0) and any later BP in this release track ■ Oracle Identity Manager 11*g* release 2 BP04 (11.1.2.0.4) and any later BP in this release track **Note:** In this guide, **Oracle Identity Manager release 11.1.2** has been used to denote Oracle Identity Manager 11*g* release 2 BP04 (11.1.2) and future releases in this release track.
Target systems	Novell eDirectory 8.7.3 and 8.8
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 configuring the IT resource. The procedure is described later in this guide. 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)`
JDK	The JDK version can be one of the following: ■ For Oracle Identity Manager release Oracle Identity Manager release 9.0.1 through 9.0.3.2, use JDK 1.4.2 or a later release in the 1.4.2 series. ■ For Oracle Identity Manager release 9.1.0.*x*, use JDK 1.5 or a later release in the 1.5 series. ■ For Oracle Identity Manager release 11.1.*x*, use JDK 1.6 update 18 or later, or JRockit JDK 1.6 update 17 or later.

1.2 Certified Languages

This release of the connector supports the following languages:

- Arabic
- Chinese Simplified
- Chinese Traditional
- Danish

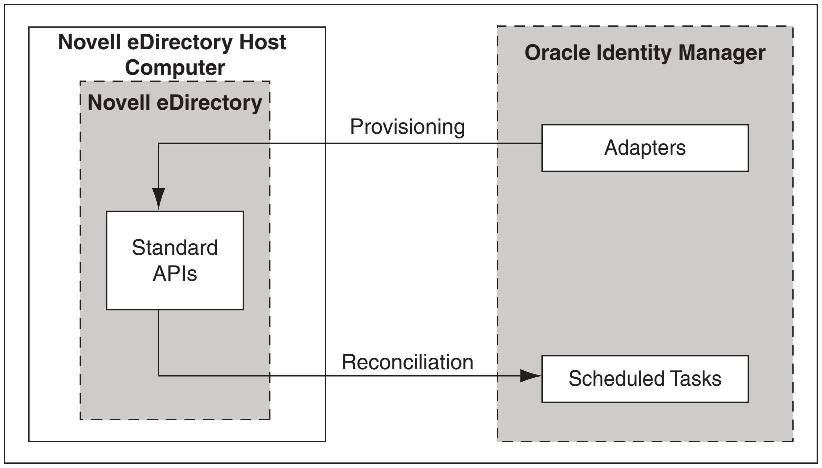
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

> **See Also:** For information about supported special characters:
>
> - For Oracle Identity Manager release from 9.0.1 through 9.0.3.2 and release 9.1.0.*x*, see *Oracle Identity Manager Globalization Guide*.
> - For Oracle Identity Manager release 11.1.*x*, see *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

1.3 Connector Architecture

Figure 1–1 shows the connector integrating Novell eDirectory with Oracle Identity Manager.

Figure 1–1 Connector Architecture



Novell eDirectory is configured as a target resource of Oracle Identity Manager. Through provisioning operations performed on Oracle Identity Manager, accounts are created and updated on the target system for OIM Users. Through reconciliation, account data that is created and updated on the target system is fetched into Oracle Identity Manager and stored against the corresponding OIM Users.

During provisioning, adapters carry provisioning data submitted through the process form to the target system. APIs on the target system accept provisioning data from the adapters, carry out the required operation on the target system, and return the response from the target system to the adapters. The adapters return the response to Oracle Identity Manager.

During reconciliation, a scheduled task establishes a connection with the target system and sends reconciliation criteria to the APIs. The APIs extracts user records that match the reconciliation criteria and hand them over to the scheduled task, which brings the records to Oracle Identity Manager.

Each record fetched from the target system is compared with Novell eDirectory resources that are already provisioned to OIM Users. If a match is found, then the update made to the record on the target system is copied to the Novell eDirectory resource in Oracle Identity Manager. If no match is found, then the user ID of the record is compared with the user ID of each OIM User. If a match is found, then data in the target system record is used to provision a Novell eDirectory resource to the OIM User.

1.4 Features of the Connector

- Section 1.4.1, "Support for Both Target Resource and Trusted Source Reconciliation"
- Section 1.4.2, "Support for Limited Reconciliation"
- Section 1.4.3, "Support for Batched Reconciliation"
- Section 1.4.4, "Support for Paged Reconciliation"
- Section 1.4.5, "Support for Reconciliation of Deleted User Records"
- Section 1.4.6, "Support for Both Full and Incremental Reconciliation"
- Section 1.4.7, "Support for Adding New Single-Valued and Multivalued Attributes for Reconciliation and Provisioning"
- Section 1.4.8, "Support for Transformation of Data During Reconciliation"
- Section 1.4.9, "Support for Reconciliation and Provisioning of Home Directories"
- Section 1.4.10, "Support for High-Availability Configuration of the Target System"

1.4.1 Support for Both Target Resource and Trusted Source Reconciliation

You can use the connector to configure Novell eDirectory as either a target resource or trusted source of Oracle Identity Manager.

See Section 3.3, "Configuring Reconciliation" for more information.

1.4.2 Support for Limited Reconciliation

You can set a reconciliation filter as the value of the SearchFilter attribute of the scheduled tasks. This filter specifies the subset of newly added and modified target system records that must be reconciled.

See Section 3.3.2, "Limited Reconciliation" for more information.

1.4.3 Support for Batched Reconciliation

You can break down a reconciliation run into batches by specifying the number of records that must be included in each batch.

See Section 3.3.3, "Batched Reconciliation" for more information.

1.4.4 Support for Paged Reconciliation

Paged reconciliation is the reconciliation of a specified set of target system records at a time, within a reconciliation run. Multiple pages of records are fetched to complete the reconciliation run. This feature helps reduce memory issues that might arise when there are a large number of records to be reconciled.

> **Note:** Only Novell eDirectory 8.8 and later versions support paged reconciliation.

Paged reconciliation is implemented using the PageSize entry in the Lookup.EDIR.Configuration lookup definition.

See Section 2.3.7.1, "Setting Up the Lookup.EDIR.Configuration Lookup Definition" for information about this lookup definition.

1.4.5 Support for Reconciliation of Deleted User Records

You can configure scheduled tasks for reconciliation of deleted user records. In target resource mode, if a record is deleted on the target system, then the corresponding Novell eDirectory resource is revoked from the OIM User. In trusted source mode, if a record is deleted on the target system, then the corresponding OIM User is deleted.

The scheduled tasks for reconciliation of deleted user records are described in Section 3.3.4, "Reconciliation Scheduled Tasks."

1.4.6 Support for Both Full and Incremental Reconciliation

After you deploy the connector, you can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Manager. After the first full reconciliation run, change-based or incremental reconciliation is automatically enabled from the next run of the user reconciliation.

You can perform a full reconciliation run at any time.

See Section 3.3.1, "Full Reconciliation vs. Incremental Reconciliation" for more information.

1.4.7 Support for Adding New Single-Valued and Multivalued Attributes for Reconciliation and Provisioning

If you want to add to the standard set of single-valued and multivalued attributes for reconciliation and provisioning, then perform the procedures described in Chapter 4, "Extending the Functionality of the Connector".

1.4.8 Support for Transformation of Data During Reconciliation

You can configure transformation of data during reconciliation. For example, you can automate the look up of the field name from an external system and set the value based on the field name.

See Section 4.10, "Configuring Transformation of Data During Reconciliation" for more information.

1.4.9 Support for Reconciliation and Provisioning of Home Directories

From this release onward, the connector supports reconciliation and provisioning of Home directories for users. The procedure to enable and use this feature is optional. This feature makes use of the transformation feature.

See Section 4.9, "Linking the Home Directory Provisioning Operation with the Create User Provisioning Operation" for more information.

1.4.10 Support for High-Availability Configuration of the Target System

The connector can be configured to work with high-availability target system environments. If the primary installation becomes unavailable, then the connector reads information about backup target system installations from the Lookup.EDIR.BackupServers lookup definition and uses this information to switch to a backup target system installation. The timeout interval stored in the LDAPConnectTimeOut entry of the Lookup.EDIR.Configuration lookup definition is used to determine when to switch to the backup target system installation.

See Section 2.3.9, "Configuring High Availability of the Target System" for more information.

1.5 Lookup Definitions Used During Reconciliation and Provisioning

Lookup definitions used during connector operations can be divided into the following categories:

- Section 1.5.1, "Lookup Definitions Synchronized with the Target System"
- Section 1.5.2, "Other Lookup Definitions"

1.5.1 Lookup Definitions Synchronized with the Target System

The following lookup definitions are populated with values fetched from the target system by the scheduled tasks for lookup field synchronization:

> **See Also:** Section 3.2, "Lookup Field Synchronization" for information about these scheduled tasks

- For organizations and organization units: Lookup.EDIR.Organization
- For groups: Lookup.EDIR.UserGroup
- For roles: Lookup.EDIR.AssignedRole
- For domain scopes: Lookup.EDIR.DomainScope
- For profiles: Lookup.EDIR.Profile

1.5.2 Other Lookup Definitions

Table 1–2 describes the other lookup definitions that are created in Oracle Identity Manager when you deploy the connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed.

Table 1–2 Other Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.EDIR.Configuration	This lookup definition holds connector configuration entries that are used during reconciliation and provisioning.	Some of the entries in this lookup definition are preconfigured. See Section 2.3.7.1, "Setting Up the Lookup.EDIR.Configuration Lookup Definition" for information about the entries for which you can set values.
Lookup.EDIR.Constants	This lookup definition stores values that are used internally by the connector. The connector development team can use this lookup definition to make minor configuration changes in the connector.	You must not modify the entries in this lookup definition.
Lookup.EDIR.Transformation	This lookup definition is used to configure transformation of attribute values fetched from the target system during reconciliation.	It is optional to enter values in this lookup definition. Section 4.10, "Configuring Transformation of Data During Reconciliation" provides information about this lookup definition.
AttrName.Recon.Map.EDIR	This lookup definition holds mappings between the eDirectory User resource object fields and target system attributes.	This lookup definition is preconfigured. Table 1–3 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new target system attributes for user reconciliation. Chapter 4, "Extending the Functionality of the Connector" provides more information.
AttrName.Prov.Map.EDIR	This lookup definition holds mappings between eDirectory User process form fields and target system attributes.	This lookup definition is preconfigured. Table 1–3 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new target system attributes for user provisioning. Chapter 4, "Extending the Functionality of the Connector" provides more information.
AttrName.ReconGroup.Map.EDIR	This lookup definition holds mappings between eDirectory Group resource object fields and target system attributes.	This lookup definition is preconfigured. Table 1–6 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new target system attributes for group reconciliation. Chapter 4, "Extending the Functionality of the Connector" provides more information.
AttrName.ProvGroup.EDIR.Map	This lookup definition holds mappings between eDirectory Group process form fields and target system attributes.	This lookup definition is preconfigured. Table 1–6 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new target system attributes for group provisioning. Chapter 4, "Extending the Functionality of the Connector" provides more information.
AttrName.ReconRole.Map.EDIR	This lookup definition holds mappings between eDirectory Role resource object fields and target system attributes.	This lookup definition is preconfigured. Table 1–7 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new target system attributes for role reconciliation. Chapter 4, "Extending the Functionality of the Connector" provides more information.

Table 1–2 (Cont.) Other Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
AttrName.ProvRole.EDIR.Map	This lookup definition holds mappings between eDirectory Role process form fields and target system attributes.	This lookup definition is preconfigured. Table 1–7 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new target system attributes for group provisioning. Chapter 4, "Extending the Functionality of the Connector" provides more information.
Lookup.EDIR.BackupServers	This lookup definition holds mappings between primary Novell eDirectory servers and secondary Novell eDirectory servers.	It is optional to enter values in this lookup definition. Section 2.3.9, "Configuring High Availability of the Target System" provides information about this lookup definition
Lookup.EDIR.Volume	This lookup definition holds the names of volume objects created on the target system. Home directories that you provision are created on these volume objects.	You enter the names of the volume objects in this lookup definition. Section 2.3.7, "Setting Up Lookup Definitions in Oracle Identity Manager" provides more information.
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.	Section 2.3.7, "Setting Up Lookup Definitions in Oracle Identity Manager" provides information about creating entries in this lookup definition.
Lookup.EDIR.CommLang	During a provisioning operation, you use this lookup definition to specify a language for the user.	Section 2.3.7, "Setting Up Lookup Definitions in Oracle Identity Manager" provides information about creating entries in this lookup definition.
Lookup.EDIR.TrusteeProperty	During a provisioning operation, you use this lookup definition to specify trustee rights on the property for the user.	Section 2.3.7, "Setting Up Lookup Definitions in Oracle Identity Manager" provides information about creating entries in this lookup definition.

1.6 Connector Objects Used During Target Resource Reconciliation and Provisioning

The following sections provide information about connector objects used during target resource reconciliation and provisioning:

> **See Also:** The "Reconciliation" section in *Oracle Identity Manager Connector Concepts* for conceptual information about reconciliation

- Section 1.6.1, "User Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6.2, "Group Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6.3, "Role Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6.4, "Reconciliation Rule for Target Resource Reconciliation"
- Section 1.6.5, "Reconciliation Action Rules for Target Resource Reconciliation"
- Section 1.6.6, "Provisioning Functions"

1.6.1 User Attributes for Target Resource Reconciliation and Provisioning

Table 1–3 provides information about user attribute mappings for target resource reconciliation and provisioning.

Note: When a user is assigned a role, the equivalentToMe, securityEquals, and rBSAssignedRoles attributes are added to the user object.

Table 1–3 User Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	Novell eDirectory Attribute	Description
Guid	GUID	GUID **Note:** This is a hidden field.
User ID	cn	User ID
First Name	givenname	First name
Last Name	sn	Last name
Middle Name	initials	Middle name
Department	departmentNumber	Department
Location	l	Location
Telephone	telephoneNumber	Telephone
Email	mail	Email
Communication Language	preferredLanguage	Communication language
Timezone	timezone	Timezone
Logon Script	loginScript	Logon script
Title	title	Title
Profile	profile	Profile
Container DN	NA	Container in which the user is present on the target system For example: `o=abc,dc=Company`
Security Group (multiple group names can be entered)	GroupMembership	List of groups of which the user is a member
Network Address	networkAddressRestriction	Network address
Volume Name	NA	Name of the volume object in Novell Netware
Home Directory Name	NA	Name of the user's Home directory

Table 1–4 lists the role attributes of the user record for target resource reconciliation and provisioning.

Note: When a role is assigned to a user, the equivalentToMe and rBSTrusteeOf attributes are added to the role object.

Table 1–4 Role (Child Form) Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	Novell eDirectory Role Attribute	Description
Role Name	rBSMember	Role name
Scope	Scope	Scope
Inheritance	Inheritable	Inheritance

Table 1–5 lists the trustee rights attributes of the user record for target resource reconciliation and provisioning.

Table 1–5 Trustee Rights (Child Form) Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	Novell eDirectory Trustee Rights Attribute	Description
Property	Property	Property
Supervisor	Supervisor	Supervisor
Read	Read	Read permission
Write	Write	Write permission
Compare	Compare	Compare permission
Add Self	Add Self	Add Self permission

1.6.2 Group Attributes for Target Resource Reconciliation and Provisioning

Note: If you are using Oracle Identity Manager release 11.1.*x*, then you cannot reconcile data from group attributes of the target system. This is tracked by Bug 9799541 in Chapter 6, "Known Issues."

Table 1–6 provides information about group attribute mappings for target resource reconciliation and provisioning.

Table 1–6 Group Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	Novell eDirectory Group Attribute	Description
Group Name	cn	Group name
Organization	NA	Container in which the group object is located on the target system
Guid	GUID	GUID

1.6.3 Role Attributes for Target Resource Reconciliation and Provisioning

Note: If you are using Oracle Identity Manager release 11.1.*x*, then you cannot reconcile data from role attributes of the target system. This is tracked by Bug 9799541 in Chapter 6, "Known Issues."

Table 1–7 provides information about role attribute mappings for target resource reconciliation and provisioning.

Table 1–7 Role Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	Novell eDirectory Role Attribute	Description
Role Name	cn	Role name
Organization	NA	Container in which the role object is located on the target system
Guid	GUID	GUID

1.6.4 Reconciliation Rule for Target Resource Reconciliation

> **See Also:** *Oracle Identity Manager Connector Concepts* for generic information about reconciliation matching and action rules

The following is the process matching rule:

Rule name: eDir Recon User

Rule element: (GUID Equals GUID) OR (User Login Equals User ID)

In the first rule component:

- GUID to the left of "Equals" is the GUID of the resource assigned to the OIM User.
- GUID to the right of "Equals" is the GUID of the resource on the target system.

In the second rule component:

- User Login is one of the following:
  - For Oracle Identity Manager Release 9.0.1 through 9.0.3.2:

    User ID field on the Xellerate User form.
  - For Oracle Identity Manager release 9.1.0.*x* or release 11.1.*x*:

    User ID field on the OIM User form.
- User ID is the cn field on the target system.

This rule supports the following scenarios:

- You can provision multiple Novell eDirectory resources to the same OIM User, either on Oracle Identity Manager or directly on the target system.
- You can change the user ID of a user on the target system.

This is illustrated by the following use cases:

- Use case 1: You provision a Novell eDirectory account for an OIM User, and you also create an account for the user directly on the target system.

  When the first rule condition is applied, no match is found. Then, the second rule condition is applied and it is determined that a second account has been given to the user on the target system. The second account is linked with the OIM User at the end of the reconciliation run.
- Use case 2: An OIM User has a Novell eDirectory account. You then change the user ID of the user on the target system.

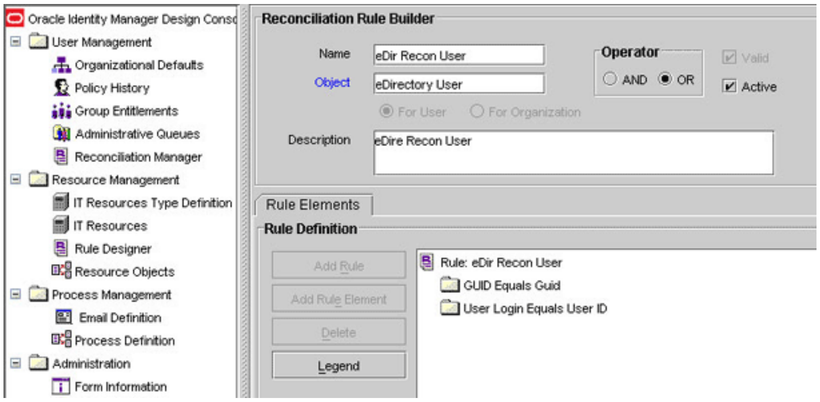
  During the next reconciliation run, application of the first rule condition helps match the resource with the record.

After you deploy the connector, you can view the reconciliation rule for target resource reconciliation by performing the following steps:

> **Note:** Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **eDir Recon User**. Figure 1–2 shows the reconciliation rule for target resource reconciliation.

Figure 1–2 Reconciliation Rule for Target Resource Reconciliation



Name: eDir Recon User

Object: eDirectory User

Operator: ○ AND ● OR

☑ Valid

☑ Active

● For User ○ For Organization

Description: eDire Recon User

Rule: eDir Recon User
- GUID Equals Guid
- User Login Equals User ID

1.6.5 Reconciliation Action Rules for Target Resource Reconciliation

Table 1–8 lists the action rules for target resource reconciliation.

Table 1–8 Action Rules for Target Resource Reconciliation

Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

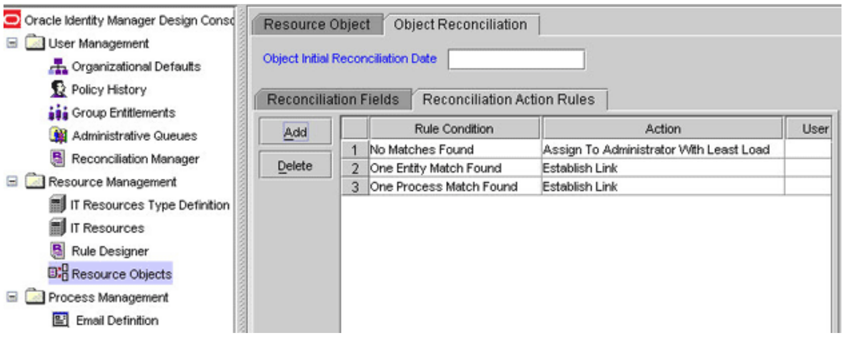
> **Note:** No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See *Oracle Identity Manager Design Console Guide* for information about modifying or creating reconciliation action rules.

After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.

3. Double-click **Resource Objects**.
4. Search for and open the **eDirectory User** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–3 shows the reconciliation action rule for target resource reconciliation.

Figure 1–3 Reconciliation Action Rules for Target Resource Reconciliation



	Rule Condition	Action	User
1	No Matches Found	Assign To Administrator With Least Load	
2	One Entity Match Found	Establish Link	
3	One Process Match Found	Establish Link	

1.6.6 Provisioning Functions

Table 1–9 lists the provisioning functions that are supported by the connector. The Adapter column gives the name of the adapter that is used when the function is performed.

Table 1–9 Provisioning Functions

Function	Adapter
Create a user	EDIR Create User
Delete a user	EDIR Delete User
Enable a user	EDIR Modify User
Disable a user	EDIR Modify User
Move 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.	EDIR Move User
Update user password	EDIR Modify User
Add user to a group	EDIR Add user to Group
Remove User from Group	EDIR Remove user from Group
Assign a role to a user	EDIR Add Assigned Role to User
Remove assigned role from user	EDIR Remove Assigned Role from User
Assign trustee right to a user	EDIR Add Trustee Right to User
Remove trustee right from a user	EDIR Remove Trustee Right from User

Table 1–9 (Cont.) Provisioning Functions

Function	Adapter
Add network address restriction to user	EDIR Add Network Restriction
Remove network address restriction from user	EDIR Remove Network Restriction
Create OU	EDIR Create OU
Change OU name	EDIR Change Org Name
Delete OU	EDIR Delete OU
Move an organization sub unit to another parent organizational unit	EDIR Move OU
Create eDirectory group	EDIR Create Group
Delete eDirectory group	EDIR Delete Group
Update group name	Update eDirectory Group Details
Create eDirectory role	EDIR Create Role
Delete eDirectory role	EDIR Delete Role
Update role name	Update eDirectory Role Details
Create Home directory	EDIR Create Home Directory

1.7 Connector Objects Used During Trusted Source Reconciliation

The following sections provide information about connector objects used during trusted source reconciliation:

- Section 1.7.1, "User Attributes for Trusted Source Reconciliation"
- Section 1.7.2, "Reconciliation Rule for Trusted Source Reconciliation"
- Section 1.7.3, "Reconciliation Action Rules for Trusted Source Reconciliation"

1.7.1 User Attributes for Trusted Source Reconciliation

Table 1–10 lists user attributes for trusted source reconciliation.

Table 1–10 User Attributes for Trusted Source Reconciliation

OIM User Form Field	Novell eDirectory Attribute	Description
User ID	cn	Common name
First Name	givenname	Given name
Last Name	sn	Last name
Employee Type	NA	Default value: `Consultant`
User Type	NA	Default value: `End-User Administrator`
Organization	NA	Default value: `Xellerate Users`

1.7.2 Reconciliation Rule for Trusted Source Reconciliation

See Also: *Oracle Identity Manager Connector Concepts* for generic information about reconciliation matching and action rules

The following is the process matching rule:

Rule name: eDir Trusted Recon Rule

Rule element: User Login Equals User ID

In this rule element:

- User Login is one of the following:
  - For Oracle Identity Manager Release 9.0.1 through 9.0.3.2:

    User ID field on the Xellerate User form.
  - For Oracle Identity Manager release 9.1.0.*x* or release 11.1.*x*:

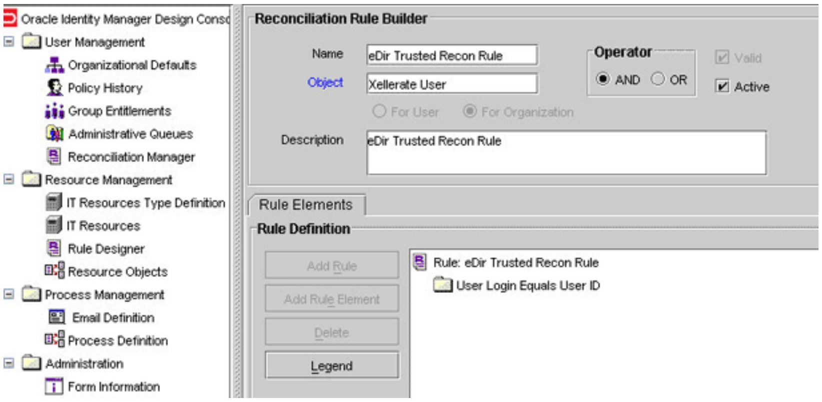
    User ID field on the OIM User form.
- User ID is the cn field of Novell eDirectory.

After you deploy the connector, you can view the reconciliation rule for target resource reconciliation by performing the following steps:

> **Note:** Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **eDir Trusted Recon Rule**. Figure 1–4 shows the reconciliation rule for trusted source reconciliation.

Figure 1–4 Reconciliation Rule for Trusted Source Reconciliation



Name: eDir Trusted Recon Rule

Object: Xellerate User

Operator: ● AND ○ OR

☑ Valid

☑ Active

○ For User ● For Organization

Description: eDir Trusted Recon Rule

Rule: eDir Trusted Recon Rule

User Login Equals User ID

1.7.3 Reconciliation Action Rules for Trusted Source Reconciliation

Table 1–11 lists the action rules for trusted source reconciliation.

Table 1–11 Action Rules for Trusted Source Reconciliation

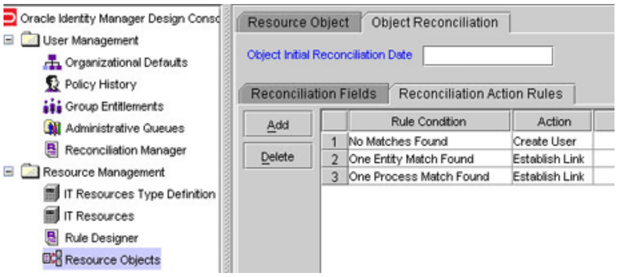
Rule Condition	Action
No Matches Found	Create User
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

> **Note:** No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See *Oracle Identity Manager Design Console Guide* for information about modifying or creating reconciliation action rules.

After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **Xellerate User** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–5 shows the reconciliation action rules for trusted source reconciliation.

Figure 1–5 Reconciliation Action Rules for Trusted Source Reconciliation



	Rule Condition	Action
1	No Matches Found	Create User
2	One Entity Match Found	Establish Link
3	One Process Match Found	Establish Link

1.8 Roadmap for Deploying and Using the Connector

The following is the organization of information in the rest of this guide:

- Chapter 2, "Deploying the Connector" describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Chapter 3, "Using the Connector" describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- Chapter 4, "Extending the Functionality of the Connector" describes procedures that you can perform if you want to extend the functionality of the connector.

- Chapter 5, "Testing and Troubleshooting" describes the procedure to use the connector testing utility for testing the connector.
- Chapter 6, "Known Issues" lists known issues associated with this release of the connector.

2

Deploying the Connector

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

- Section 2.1, "Preinstallation"
- Section 2.2, "Installation"
- Section 2.3, "Postinstallation"

2.1 Preinstallation

Preinstallation information is divided across the following sections:

- Section 2.1.1, "Preinstallation on Oracle Identity Manager"
- Section 2.1.2, "Preinstallation on the Target System"

2.1.1 Preinstallation on Oracle Identity Manager

This section contains the following topics:

- Section 2.1.1.1, "Files and Directories On the Installation Media"
- Section 2.1.1.2, "Determining the Release Number of the Connector"
- Section 2.1.1.3, "Using External Code Files"

2.1.1.1 Files and Directories On the Installation Media

Table 2–1 describes the files and directories on the installation media.

Table 2–1 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 installation, this file is copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/JavaTasks ■ For Oracle Identity Manager release 11.1.*x*: Oracle Identity Manager database
lib/eDirRecon.jar	This JAR file contains the class files required for reconciliation. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/ScheduleTask ■ For Oracle Identity Manager release 11.1.*x*: Oracle Identity Manager database
lib/eDirRemote.jar	This JAR file contains the class file required for creation of a user's Home directory. During connector deployment, this file is copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/JavaTasks ■ For Oracle Identity Manager release 11.1.*x*: Oracle Identity Manager database
lib/eDirRM.jar	This JAR file contains the class file required to check the Remote Manger connections. During connector deployment, this file is copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/JavaTasks ■ For Oracle Identity Manager release 11.1.*x*: Oracle Identity Manager database
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/connectorResources ■ For Oracle Identity Manager release 11.1.*x*: Oracle Identity Manager database **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
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 of the various connector components.
xml/eDirXLResourceObject.xml	This XML file contains the configuration for the Xellerate User (OIM User). You 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.

2.1.1.2 Determining the Release Number of the Connector

Note: If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then the procedure described in this section is optional.

If you are using Oracle Identity Manager release 11.1.*x,* then skip this section.

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.

2.1.1.3 Using External Code Files

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

Copy the following code files into the specified directories:

- **ldap.jar**

  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 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 this ZIP file.

  4. Copy the ldap.jar file from the novell-jldap-devel-2005.10.03-1netware_windows\jldap_2005.10.03\lib directory to the following directory:

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

- For Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*:

  OIM_HOME/xellerate/ThirdParty

- For Oracle Identity Manager release 11.1.*x*:

  OIM_HOME/server/ThirdParty

- **ldapbp.jar**

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

  1. Log on to the 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 following directory:

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

     - For Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*:

       OIM_HOME/xellerate/ThirdParty

     - For Oracle Identity Manager release 11.1.*x*:

       OIM_HOME/server/ThirdParty

- **njclv2.jar**

  The njclv2.jar file contains APIs that are used to create the home directory on Novell eDirectory. This file is in the lib directory inside the Novell eDirectory installation directory. The following is a sample path:

  NOVELL_CONSOLE_HOME\ndk\nocell-njclc-devel-2008.02.29-1windows\lib\njclv2.jar

  Copy the njclv2.jar file into the following directory:

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

  - For Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*:

    OIM_HOME/xellerate/ThirdParty

  - For Oracle Identity Manager release 11.1.*x*:

    OIM_HOME/server/ThirdParty

2.1.2 Preinstallation on the Target System

Preinstallation on the target system involves performing the procedure described in the following section:

2.1.2.1 Installing Role Based Services

> **Note:** Perform the procedure described in this section *only* if your target system does not contain the RBS:Role schema.

To support provisioning of roles, you must perform the following procedure:

1. Log in to Novell ConsoleOne.
2. From the **Tools** menu, select **Install . . . .**
3. In the Installation Wizard dialog box, click **Next** to proceed with installing Role Based Services.
4. On the Select the desired products to install page, from the Product name region, select **Role Based Services,** and then click **Next.**
5. On the Select the desired NDS trees to install to page, from the Authenticated trees region, select the tree (for example, **EDIR_88SP6**) in which the Role Based Services must be installed, and then click **Next.**
6. On the Summary of services to be installed page, verify the services and the trees into which these services are being installed, and then click **Finish.**

   Installation of Role Based Services is complete.

2.2 Installation

Depending on the Oracle Identity Manager release that you are using, perform the procedure described in one of the following sections:

- Section 2.2.1, "Installing the Connector on Oracle Identity Manager Release 9.1.0.x and Release 11.1.x"
- Section 2.2.2, "Installing the Connector on Oracle Identity Manager Release 9.0.1 Through 9.0.3.2"

2.2.1 Installing the Connector on Oracle Identity Manager Release 9.1.0.*x* and Release 11.1.x

> **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.*x* and release 11.1.*x* involves the following procedures:

- Section 2.2.1.1, "Running the Connector Installer"
- Section 2.2.1.2, "Configuring the IT Resource"

2.2.1.1 Running the Connector Installer

To run the Connector Installer:

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

   > **Note:** In an Oracle Identity Manager cluster, copy this JAR file to each node of the cluster.

   - For Oracle Identity Manager release 9.1.0.*x*:
     OIM_HOME/xellerate/ConnectorDefaultDirectory
   - For Oracle Identity Manager release 11.1.*x*:
     OIM_HOME/server/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 the following guide:

   - For Oracle Identity Manager release 9.1.0.*x*:

     Oracle Identity Manager Administrative and User Console Guide

   - For Oracle Identity Manager release 11.1.*x*:

     Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager

3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

   - For Oracle Identity Manager release 9.1.0.*x*:

     Click **Deployment Management**, and then click **Install Connector**.

   - For Oracle Identity Manager release 11.1.1:

     On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Install Connector**.

   - For Oracle Identity Manager release 11.1.2:

     In the left pane, under System Management, click **Manage Connector.** In the Manage Connector page, click **Install.**

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 in Step 1.

   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 file (through 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 Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Section 2.3.5, "Clearing Content Related to Connector Resource Bundles from the Server Cache" 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

   > **Note:** In Oracle Identity Manager release 11.1.*x*, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.*x*.
   >
   > See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

   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 2–1.

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 Section 2.1.1.1, "Files and

Directories On the Installation Media" for information about the files that you must copy and their destination locations on the Oracle Identity Manager host computer.

2.2.1.2 Configuring the IT Resource

You must specify values for the parameters of the eDirectory IT Resource IT resource as follows:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 9.*x* or 11.1.1:

     Log in to the Administrative and User Console
   - For Oracle Identity Manager release 11.1.2:

     Log in to Oracle Identity System Administration
2. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.*x*, expand **Resource Management,** and then click **Manage IT Resource.**
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced.**
     b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the **Configuration** region, click **Manage IT Resource.**
   - If you are using Oracle Identity Manager release 11.1.2, then in the left pane under Configuration, click **IT Resource**.
3. In the IT Resource Name field on the Manage IT Resource page, enter `eDirectory IT Resource` and then click **Search**.
4. Click the edit icon for the IT resource.
5. From the list at the top of the page, select **Details and Parameters**.
6. Specify values for the parameters of the IT resource. Table 2–2 describes the parameters of the IT resource.

Table 2–2 Parameters of the IT Resource

Parameter	Description
Admin ID	Enter the DN of the user who has administrator rights on the Novell eDirectory server. Sample value: `cn=Admin,o=PXED-DEV`
Admin Password	Enter the password of the user whose DN you enter as the value of the Admin ID parameter.
Server Address	Enter the server address of the Novell eDirectory host computer.
Root DN	Enter the base DN on which all user operations must be carried out. Sample value: `o=PXED-DEV`
Port	Enter the port number to connect to Novell eDirectory. Default value: `636`

Table 2–2 (Cont.) Parameters of the IT Resource

Parameter	Description
SSL	Enter `true` if you plan to configure SSL to secure communication between Novell eDirectory and Oracle Identity Manager. Otherwise, enter `false`. Default value: `true` **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, this parameter does not hold any value. For subsequent rounds of reconciliation, the time at which the previous reconciliation run was completed is stored in this parameter. See Section 3.3.1, "Full Reconciliation vs. Incremental Reconciliation" for information about using this parameter to switch from incremental to full reconciliation.
Last Recon Trusted TimeStamp	For the first trusted source reconciliation run, this parameter does not hold any value. For subsequent rounds of reconciliation, the time at which the previous reconciliation run was completed is stored in this parameter. See Section 3.3.1, "Full Reconciliation vs. Incremental Reconciliation" for information about using this parameter to switch from incremental to full reconciliation.
Prov Attribute Lookup Code	This parameter holds the name of the lookup definition that stores attribute mappings for provisioning. Default value: `AttrName.Prov.Map.EDIR` **Note:** This value must not be changed.
Recon Attribute Lookup Code	This parameter holds the name of the lookup definition that stores attribute mappings for reconciliation. Default value: `AttrName.Recon.Map.EDIR` **Note:** This value must not be changed.
Role Reconciliation TimeStamp	For the first role resource reconciliation run, this parameter does not hold any value. For subsequent rounds of reconciliation, the time at which the previous reconciliation run was completed is stored in this parameter automatically.
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`
Group Reconciliation TimeStamp	For the first group resource reconciliation run, the time stamp value is not set. For subsequent rounds of reconciliation, the time at which the previous reconciliation run was completed is stored in this parameter.
Tree name	Enter the name of the tree of the domain in which you want to let users create home directories. Sample Value: `MY_TREE`
Server Name	Enter the host name of the target system host computer.

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

2.2.2 Installing the Connector on Oracle Identity Manager Release 9.0.1 Through 9.0.3.2

Installing the connector on any Oracle Identity Manager release between releases 9.0.1 and 9.0.3.2 involves the following procedures:

- Section 2.2.2.1, "Copying the Connector Files"
- Section 2.2.2.2, "Importing the Connector XML File"
- Section 2.2.2.3, "Compiling Adapters"

2.2.2.1 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:** Section 2.1.1.1, "Files and Directories On the Installation Media" for more information about these files

File in the Installation Media Directory	Destination Directory
lib/eDirProv.jar	*OIM_HOME*/xellerate/JavaTasks
lib/eDirRemote.jar	*OIM_HOME*/xellerate/JavaTasks
lib/eDirRM.jar	*OIM_HOME*/xellerate/JavaTasks **Note:** Copy this file only if you want to enable provisioning of Home directories.
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.

2.2.2.2 Importing the Connector XML File

Perform this section only if you are using Oracle Identity Manager 9.*x* versions. As mentioned in Section 2.1.1.1, "Files and Directories On the Installation Media," 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. Table 2–2 describes the parameters of the IT resource.
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 might 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.

2.2.2.3 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.

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:** Section 1.6.6, "Provisioning Functions" 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
- EDIR Add MultiValAttr
- EDIR Remove MultiValAttr
- EDIR Update MultiValAttr
- EDIR Create Home Directory
- EDIR Modify Home Directory

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.

2.3 Postinstallation

The following sections discuss postinstallation procedures:

- Section 2.3.1, "Configuring Oracle Identity Manager 11.1.2 or Later"
- Section 2.3.2, "Localizing Field Labels in UI Forms"
- Section 2.3.3, "Copying Files to the Oracle Identity Manager Host Computer"
- Section 2.3.4, "Changing to the Required Input Locale"
- Section 2.3.5, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 2.3.6, "Enabling Logging"
- Section 2.3.7, "Setting Up Lookup Definitions in Oracle Identity Manager"
- Section 2.3.8, "Installing and Configuring the Remote Manager"
- Section 2.3.9, "Configuring High Availability of the Target System"
- Section 2.3.10, "Configuring Trusted Source Reconciliation"
- Section 2.3.11, "Enabling Provisioning of Users in Organizations and Organizational Units"
- Section 2.3.12, "Configuring Oracle Identity Manager for Request-Based Provisioning"
- Section 2.3.13, "Configuring SSL"

2.3.1 Configuring Oracle Identity Manager 11.1.2 or Later

If you are using Oracle Identity Manager release 11.1.2 or later, you must create additional metadata such as a UI form and an application instance. In addition, you must run entitlement and catalog synchronization jobs. These procedures are described in the following sections:

- Section 2.3.1.1, "Tagging Form Fields"
- Section 2.3.1.2, "Creating and Activating a Sandbox"
- Section 2.3.1.3, "Creating a New UI Form"
- Section 2.3.1.4, "Creating an Application Instance"
- Section 2.3.1.5, "Publishing a Sandbox"
- Section 2.3.1.6, "Harvesting Entitlements and Sync Catalog"
- Section 2.3.1.7, "Updating an Existing Application Instance with a New Form"

2.3.1.1 Tagging Form Fields

You must add properties to certain form fields. To do so:

1. Log in to Oracle Identity Manager Design Console.
2. Open Novell eDirectory child form (UD_EDIR_ROL).
3. Create a new form version.
4. In the **Properties** tab, for the **Role Name** field, add `Entitlement = true` property.
5. Click **Make Version Active.**
6. Open Novell eDirectory child form (UD_EDIR_GRP).
7. Create a new form version.
8. In the **Properties** tab, for the **Group Name** field, add `Entitlement = true` property.
9. Click **Make Version Active.**
10. Open Novell eDirectory user form (UD_EDIR_USR).
11. Create a new form version.
12. In the **Properties** tab, add the following properties:

    For the **Novell Server (ITResourceLookupField)** field, add `ITResource = true` property.

    For the **User ID** field, add `AccountName = true` property.

    For the **Guid** field, add `AccountId = true` property.
13. Click **Make Version Active.**

2.3.1.2 Creating and Activating a Sandbox

Create and activate a sandbox as follows. For detailed instructions, see the "Managing Sandboxes" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

1. On the upper navigation bar, click **Sandboxes.** The Manage Sandboxes page is displayed.
2. On the toolbar, click **Create Sandbox.** The Create Sandbox dialog box is displayed.
3. In the Sandbox Name field, enter a name for the sandbox. This is a mandatory field.
4. In the Sandbox Description field, enter a description of the sandbox. This is an optional field.
5. Click **Save and Close.** A message is displayed with the sandbox name and creation label.
6. Click **OK.** The sandbox is displayed in the Available Sandboxes section of the Manage Sandboxes page.
7. Select the sandbox that you created.
8. From the table showing the available sandboxes in the Manage Sandboxes page, select the newly created sandbox that you want to activate.
9. On the toolbar, click **Activate Sandbox.**

The sandbox is activated.

2.3.1.3 Creating a New UI Form

Create a new UI form as follows. For detailed instructions, see the "Managing Forms" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

1. In the left pane, under Configuration, click **Form Designer.**
2. Under Search Results, click **Create.**
3. Select the resource type for which you want to create the form, for example, `Novell eDirectory IT resource.`
4. Enter a form name and click **Create.**

2.3.1.4 Creating an Application Instance

Create an application instance as follows. For detailed instructions, see the "Managing Application Instances" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

1. In the System Administration page, under Configuration in the left pane, click **Application Instances.**
2. Under Search Results, click **Create.**
3. Enter appropriate values for the fields displayed on the Attributes form and click **Save.**
4. In the Form drop-down list, select the newly created form and click **Apply.**
5. Publish the application instance for a particular organization.

2.3.1.5 Publishing a Sandbox

To publish the sandbox that you created in Section 2.3.1.2, "Creating and Activating a Sandbox":

1. Close all the open tabs and pages.
2. From the table showing the available sandboxes in the Manage Sandboxes page, select the sandbox that you created in Section 2.3.1.2, "Creating and Activating a Sandbox."
3. On the toolbar, click **Publish Sandbox.** A message is displayed asking for confirmation.
4. Click **Yes** to confirm. The sandbox is published and the customizations it contained are merged with the main line.

2.3.1.6 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in Section 3.2, "Lookup Field Synchronization."
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table. See the "Predefined Scheduled Tasks" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for more information about this scheduled job.

3. Run the Catalog Synchronization Job scheduled job. See the "Predefined Scheduled Tasks" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for more information about this scheduled job.

2.3.1.7 Updating an Existing Application Instance with a New Form

For any changes you do in the Form Designer, you must create a new UI form and update the changes in an application instance. To update an existing application instance with a new form:

1. Create a sandbox and activate it as described in Section 2.3.1.2, "Creating and Activating a Sandbox."
2. Create a new UI form for the resource as described in Section 2.3.1.3, "Creating a New UI Form."
3. Open the existing application instance.
4. In the **Form** field, select the new UI form that you created.
5. Save the application instance.
6. Publish the sandbox as described in Section 2.3.1.5, "Publishing a Sandbox."

> **Note:** If you are using Oracle Identity Manager 11*g* Release 2 (11.1.2.0.4) or later, and if the eDirectory connector 9.*x* is configured on Remote Manger, then you must perform the steps mentioned in MetaLink note 1535369.1 to ensure provisioning operations work as expected.

2.3.2 Localizing Field Labels in UI Forms

> **Note:** Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.2 or later and you want to localize UI form field labels.

To localize field label that you add to in UI forms:

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear.**
3. In the right pane, from the Application Deployment list, select **MDS Configuration.**
4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
5. Extract the contents of the archive, and open the following file in a text editor:

   SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf
6. Edit the BizEditorBundle.xlf file in the following manner:

   a. Search for the following text:

      ```
      <file source-language="en"
      original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
      datatype="x-oracle-adf">
      ```

b. Replace with the following text:

   ```
   <file source-language="en" target-language="LANG_CODE"
   original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
   datatype="x-oracle-adf">
   ```

   In this text, replace LANG_CODE with the code of the language that you want to localize the form field labels. The following is a sample value for localizing the form field labels in Japanese:

   ```
   <file source-language="en" target-language="ja"
   original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
   datatype="x-oracle-adf">
   ```

c. Search for the application instance code. This procedure shows a sample edit for Novell eDirectory application instance. The original code is:

   ```
   <trans-unit
   id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
   ndle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.use
   rEO.UD_EDIR_USR_LOCATION__c_description']}">
   <source>Location</source>
   <target/>
   </trans-unit>
   <trans-unit
   id="sessiondef.oracle.iam.ui.runtime.form.model.EDIRFORM.entity.EDIREO.UD_E
   DIR_USR_LOCATION__c_LABEL">
   <source>Location</source>
   <target/>
   </trans-unit>
   ```

d. Open the resource file from the connector package, for example eDirectory_ja.properties, and get the value of the attribute from the file, for example, global.udf.UD_EDIR_USR_LOCATION=\u5834\u6240.

e. Replace the original code shown in Step 6.c with the following:

   ```
   <trans-unit
   id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
   ndle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.use
   rEO.UD_EDIR_USR_LOCATION__c_description']}">
   <source>Location</source>
   <target>\u5834\u6240</target>
   </trans-unit>
   <trans-unit
   id="sessiondef.oracle.iam.ui.runtime.form.model.EDIR.entity.EDIREO.UD_EDIR_
   USR_LOCATION__c_LABEL">
   <source>Location</source>
   <target>\u5834\u6240</target>
   </trans-unit>
   ```

f. Repeat Steps 6.a through 6.d for all attributes of the process form.

g. Save the file as BizEditorBundle_*LANG_CODE*.xlf. In this file name, replace LANG_CODE with the code of the language to which you are localizing.

   Sample file name: BizEditorBundle_ja.xlf.

7. Repackage the ZIP file and import it into MDS.

See Also: The "Deploying and Undeploying Customizations" chapter in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager,* for more information about exporting and importing metadata files

8. Log out of and log in to Oracle Identity Manager.

2.3.3 Copying Files to the Oracle Identity Manager Host Computer

You must manually copy the files listed in Table 2–3.

Note: If a particular destination directory does not exist on the Oracle Identity Manager host computer, then create it.

Table 2–3 Files to Be Copied to the Oracle Identity Manager Host Computer

Files on the Installation Media	Destination Directory on the Oracle Identity Manager Release 9.0.1 through Release 9.1.0.*x* Host Computer	Destination Directory on the Oracle Identity Manager Release 11.1.*x* Host Computer
Files in the test/troubleshoot directory	*OIM_HOME*/xellerate/eDir/test/troubleshoot	*OIM_HOME*/server/eDir/test/troubleshoot
Files in the xml directory	*OIM_HOME*/xellerate/eDir/xml	*OIM_HOME*/server/ eDir/xml

2.3.4 Changing to the Required Input Locale

Note: In an Oracle Identity Manager cluster, you must perform this step on each node of the cluster. Then, restart each node.

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.

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

Note: In an Oracle Identity Manager cluster, you must perform this step on each node of the cluster. Then, restart each node.

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the *OIM_HOME*/xellerate/connectorResources directory for Oracle Identity Manager release 9.0.1 through 9.0.3.2 and release 9.1.0.*x*, and Oracle Identity Manager database for Oracle Identity Manager release 11.1.*x.* Whenever you add a new resource bundle to 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, perform one of the following steps:

- If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then switch to the *OIM_HOME*/xellerate/bin directory.
- If you are using Oracle Identity Manager release 11.1.*x*, then switch to the *OIM_HOME*/server/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:

For Oracle Identity Manager release 9.0.3.2 or release 9.1.0.*x*:

```
OIM_HOME/xellerate/bin/SCRIPT_FILE_NAME
```

For Oracle Identity Manager release 11.1.*x*:

```
OIM_HOME/server/bin/SCRIPT_FILE_NAME
```

---

2. Enter one of the following commands:

Note: You can use the PurgeCache utility to purge the cache for any content category. Run `PurgeCache.bat` *`CATEGORY_NAME`* on Microsoft Windows or `PurgeCache.sh` *`CATEGORY_NAME`* on UNIX. The *`CATEGORY_NAME`* argument represents the name of the content category that must be purged.

For example, the following commands purge Metadata entries from the server cache:

```
PurgeCache.bat MetaData
```

```
PurgeCache.sh MetaData
```

- For Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*:

  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. This exception is different from the one mentioned in Step 1.

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

  OIM_HOME/xellerate/config/xlconfig.xml

- For Oracle Identity Manager release 11.1.*x*:

  On Microsoft Windows: `PurgeCache.bat All`

  On UNIX: `PurgeCache.sh All`

  When prompted, enter the user name and password of an account belonging to the SYSTEM ADMINISTRATORS group. In addition, you are prompted to enter the service URL in the following format:

```
t3://OIM_HOST_NAME:OIM_PORT_NUMBER
```

In this format:

- Replace *OIM_HOST_NAME* with the host name or IP address of the Oracle Identity Manager host computer.
- Replace *OIM_PORT_NUMBER* with the port on which Oracle Identity Manager is listening.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

2.3.6 Enabling Logging

Depending on the Oracle Identity Manager release you are using, perform the procedure described in one of the following sections:

- Section 2.3.6.1, "Enabling Logging on Oracle Identity Manager Release 9.0.1 through 9.0.3.2 or Release 9.1.0.x"
- Section 2.3.6.2, "Enabling Logging on Oracle Identity Manager Release 11.1.x"

2.3.6.1 Enabling Logging on Oracle Identity Manager Release 9.0.1 through 9.0.3.2 or Release 9.1.0.x

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 might 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:

- **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:

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

- **Oracle 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.

2.3.6.2 Enabling Logging on Oracle Identity Manager Release 11.1.*x*

> **Note:** In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster. Then, restart each node.

Oracle Identity Manager release 11.1.*x* uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on java.util.logger. 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:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

  This level enables logging of information about errors that might allow Oracle Identity Manager to continue running.

- WARNING

  This level enables logging of information about potentially harmful situations.

- INFO

  This level enables logging of messages that highlight the progress of the application.

- CONFIG

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

- FINE, FINER, FINEST

These levels enable logging of information about fine-grained events, where FINEST logs information about all events.

These log levels are mapped to ODL message type and level combinations as shown in Table 2–4.

Table 2–4 Log Levels and ODL Message Type:Level Combinations

Log Level	ODL Message Type:Level
SEVERE.intValue()+100	INCIDENT_ERROR:1
SEVERE	ERROR:1
WARNING	WARNING:1
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

The configuration file for OJDL is logging.xml, which is located at the following path:

DOMAIN_HOME/config/fmwconfig/servers/*OIM_SERVER*/logging.xml

Here, *DOMAIN_HOME* and *OIM_SERVER* are the domain name and server name specified during the installation of Oracle Identity Manager.

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

   a. Add the following blocks in the file:

```
<log_handler name='edir-handler' level='[LOG_LEVEL]'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path' value='[FILE_NAME]'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
   </log_handler>

<logger name="XL_INTG.EDIRECTORY" level="[LOG_LEVEL]"
useParentHandlers="false">
     <handler name="edir-handler"/>
     <handler name="console-handler"/>
   </logger>
```

   b. Replace both occurrences of **`[LOG_LEVEL]`** with the ODL message type and level combination that you require. Table 2–4 lists the supported message type and level combinations.

   Similarly, replace **`[FILE_NAME]`** with the full path and name of the log file in which you want log messages to be recorded.

   The following blocks show sample values for **`[LOG_LEVEL]`** and **`[FILE_NAME]`**:

```
<log_handler name='edir-handler' level='NOTIFICATION:1'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1\servers\o
im_server1\logs\oim_server1-diagnostic-1.log'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
   </log_handler>

<logger name="XL_INTG.EDIRECTORY" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="edir-handler"/>
     <handler name="console-handler"/>
   </logger>
```

With these sample values, when you use Oracle Identity Manager, all messages generated for this connector that are of a log level equal to or higher than the `NOTIFICATION:1` level are recorded in the specified file.

2. Save and close the file.
3. Set the following environment variable to redirect the server logs to a file:

   For Microsoft Windows:

   ```
   set WLS_REDIRECT_LOG=FILENAME
   ```

   For UNIX:

   ```
   export WLS_REDIRECT_LOG=FILENAME
   ```

   Replace ***FILENAME*** with the location and name of the file to which you want to redirect the output.
4. Restart the application server.

2.3.7 Setting Up Lookup Definitions in Oracle Identity Manager

You must enter values in some of the lookup definitions that are created when you install the connector. 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 definitions described in the following sections. After you enter values in each lookup definitions, save the changes.

- Section 2.3.7.1, "Setting Up the Lookup.EDIR.Configuration Lookup Definition"
- Section 2.3.7.2, "Setting Up Other Lookup Definitions"

2.3.7.1 Setting Up the Lookup.EDIR.Configuration Lookup Definition

You can specify values for the following entries in the Lookup.EDIR.Configuration lookup definition:

- TimeStampFormat

  Enter the time-stamp format that must be used for connector operations.

  Default value: `yyyyMMddHHmmss'Z'`

- Special Characters

  Enter the list of special characters that must not be modified in any way during connector operations. To add a special character to the default value, append the character to the default value without adding a space or any other delimiter.

  Default value: `+=\<>%;#`

- PageSize

  Enter the page size that must be used during reconciliation. This entry enables the reconciliation of a specified set of target system records at a time, within a reconciliation run. Multiple pages of records are fetched to complete the reconciliation run.

  > **Note:** Only Novell eDirectory 8.8 and later versions support paged reconciliation.

  Default value: `100`

- LDAPConnectTimeOut

  Enter the timeout interval (in milliseconds) after which the connector must start trying to establish a connection with the backup target system installations.

  Default value: `3000`

2.3.7.2 Setting Up Other Lookup Definitions

The following are other lookup definitions in which you must manually create entries:

> **See Also:** Section 1.5.2, "Other Lookup Definitions" for the descriptions of these lookup definitions

- **Lookup.EDIR.NetworkRestriction**

  Table 2–5 shows the default entries in the Lookup.EDIR.NetworkRestriction lookup definition.

  > **Note:** If you want to add entries in this lookup definition, then ensure that the entries are in the format used for the default values.

Table 2–5 Entries in the Lookup.EDIR.NetworkRestriction Lookup Definition

Code Key	Decode
IP:123.124.35.36	IP:123.124.35.36
IPX:AAAAAAAA:BBBBBBBBBBBB:CCCC	IPX:AAAAAAAA:BBBBBBBBBBBB:CCCC
OSI:1234567890	OSI:1234567890
SDLC:2222:222222:2222222222	SDLC:2222:222222:2222222222

Table 2–5 (Cont.) Entries in the Lookup.EDIR.NetworkRestriction Lookup Definition

Code Key	Decode
SDLC:3434:343434:3434343434	SDLC:3434:343434:3434343434
TCP:255.0.255.255	TCP:255.0.255.255
TCP:164.164.164.164	TCP:164.164.164.164
UDP:121.121.121.121	UDP:121.121.121.121
UDP:255.255.255.255	UDP:255.255.255.255
ETHERNET_TOKENRING:2222:333333:5555555555	ETHERNET_TOKENRING:2222:333333:5555555555
IP:300.34.35.26	IP:300.34.35.26

- **Lookup.EDIR.CommLang**

  Table 2–6 shows the default entries in the Lookup.EDIR.CommLang lookup definition.

  > **Note:** If you want to add entries in this lookup definition, then ensure that the entries are in the format used for the default values.

Table 2–6 Entries in the Lookup.EDIR.CommLang Lookup Definition

Code Key	Decode
ENGLISH	ENGLISH
FRENCH	FRENCH
GERMAN	GERMAN
ITALIAN	ITALIAN
JAPANESE	JAPANESE
KOREAN	KOREAN
SPANISH	SPANISH
SIMPLIFIED CHINESE	SIMPLIFIED CHINESE
TRADITIONAL CHINESE	TRADITIONAL CHINESE
BRAZILIAN PORTUGUESE	BRAZILIAN PORTUGUESE

- **Lookup.EDIR.TrusteeProperty**

  Table 2–7 shows the default entries in the Lookup.EDIR.TrusteeProperty lookup definition.

  > **Note:** If you want to add entries in this lookup definition, then ensure that the entries are in the format used for the default values.

Table 2–7 Entries in the Lookup.EDIR.TrusteeProperty Lookup Definition

Code Key	Decode
[All Attributes Rights]	All Attributes Rights
sn	sn

Table 2–7 (Cont.) Entries in the Lookup.EDIR.TrusteeProperty Lookup Definition

Code Key	Decode
givenName	givenName
title	title

2.3.8 Installing and Configuring the Remote Manager

To enable the creation of home directories for users on the target system, you must install a Remote Manager on a computer running Microsoft Windows in the domain. In addition, you must install Novell Console One Application on the same computer.

Note:

- Perform the procedure described in this section only if you want to include the Home Directory field in provisioning operations.
- The directory in which you install the Remote Manager is referred to as *RM_HOME*.
- The directory in which you install the Novell Console One Application is referred to as *NOVELL_CONSOLE_HOME*.
- See Novell documentation for information about installing Novell Console One Application.

Installing and configuring the Remote Manager involves performing the following procedures:

- Section 2.3.8.1, "Installing the Remote Manager"
- Section 2.3.8.2, "Enabling Logging in the Remote Manager"
- Section 2.3.8.3, "Configuring the IT Resource for the Remote Manager"
- Section 2.3.8.4, "Configuring Oracle Identity Manager Release 9.0.1 through 9.0.3.2 or Release 9.1.0.x to Trust the Remote Manager"
- Section 2.3.8.5, "Configuring Oracle Identity Manager Release 11.1.x to Trust the Remote Manager"
- Section 2.3.8.6, "Verifying That the Remote Manager Is Running"

2.3.8.1 Installing the Remote Manager

Note: You can install the Remote Manager only if you are using Oracle Identity Manager release 9.0.3.*x*, release 9.1.0.*x*, or release 11.1.*x*.

If you are using an Oracle Identity Manager release earlier than 9.0.3.*x*, then skip this section.

To install the Remote Manager:

1. The Remote Manager installation files are shipped along with the Oracle Identity Manager installation files. You can install the Remote Manager on any computer that is a part of the domain.

If you are using Oracle Identity Manager release 11.1.*x*, then see the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* guide for instructions on installing the Remote Manager.

If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then depending on the application server that you use, perform the procedure to install the Remote Manager by following the instructions given in one of the following guides:

- *Oracle Identity Manager Installation and Configuration Guide for Oracle WebLogic Server*
- *Oracle Identity Manager Installation and Configuration Guide for IBM WebSphere Application Server*
- *Oracle Identity Manager Installation and Configuration Guide for JBoss Application Server*
- *Oracle Identity Manager Installation and Configuration Guide for Oracle Application Server*

2. If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then copy the following JAR files into the *RM_HOME*\xlremote\JavaTasks directory:

   - *OIM_HOME*\xellerate\lib\xlVO.jar
   - *OIM_HOME*\xellerate\lib\xlScheduler.jar
   - *OIM_HOME*\xellerate\lib\xlAPI.jar
   - *NOVELL_CONSOLE_HOME*\ndk\nocell-njclc-devel-2008.02.29-1windows\lib\njclv2.jar (sample path)
   - *INSTALL_MEDIA*\lib\eDirRemote.jar

   Note: In this guide, the connector installation media is referred to as *INSTALL_MEDIA*.

   - *INSTALL_MEDIA*\lib\eDirRM.jar
   - *INSTALL_MEDIA*\lib\eDirProv.jar

3. If you are using Oracle Identity Manager release 11.1.*x*, then copy the following JAR files into the *RM_HOME*\xlremote\JavaTasks directory:

   - *OIM_HOME*\server\lib\xlVO.jar
   - *OIM_HOME*\server\lib\xlScheduler.jar
   - *OIM_HOME*\server\lib\xlAPI.jar
   - *OIM_HOME*\server\lib\xlUtils.jar
   - *OIM_HOME*\server\lib\xlRemoteManager.jar
   - *INSTALL_MEDIA*\lib\ eDirRecon.jar
   - *INSTALL_MEDIA*\lib\ eDirProv.jar

4. Copy the following file into the C:\WINDOWS\system32 directory:

   NOVELL_CONSOLE_HOME\consoleone\1.2\bin\jncpv2.dll

5. Use the following script to start the Remote Manager:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.2 and release 9.1.0.*x*:

  RM_HOME\xlremote\remotemanager.bat

- For Oracle Identity Manager release 11.1.*x*:

  RM_HOME\remote_manager\remotemanager.bat

6. Note the Remote Manager service name and URL. These values are displayed in the Remote Manager command window. You will need these values while creating the IT resource for the Remote Manager. The default values are `RManager` and `rmi://`*`HOST_NAME`*`:12346`. For example, for a Remote Manager running on ten.mydomain.com, the default values will be `RManager` and `rmi://ten.mydomain.com:12346`.

2.3.8.2 Enabling Logging in the Remote Manager

To enable logging in the Remote Manager:

1. Add the `log4j.logger.XL_INTG.EDIRECTORY=`*`LOG_LEVEL`* line in one of the following files:

   - For Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*:

     RM_HOME\xlremote\config\log.properties

   - For Oracle Identity Manager release 11.1.*x*:

     OIM_HOME\remote_manager\config\log.properties

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

   For example:

   ```
   log4j.logger.XL_INTG.EDIRECTORY=INFO
   ```

3. In the log.properties file, use the following parameter to specify the name and location of the file in which you want log information to be recorded:

   ```
   log4j.appender.logfile.File
   ```

2.3.8.3 Configuring the IT Resource for the Remote Manager

Table 2–8 describes the parameters of the IT resource for the Remote Manager. Enter values for these parameters.

> **See Also:** Section 2.2.1.2, "Configuring the IT Resource" for information about the procedure to set values for parameters of IT resources

Table 2–8 Parameters of the IT Resource for the Remote Manager

Parameter	Description
service name	Enter a name for the Remote Manager. Sample value: `RManager`
url	Enter the IP address of the target system host computer and the port number at which the Remote Manager is listening. Sample value: `rmi://10.0.0.1:12346`

2.3.8.4 Configuring Oracle Identity Manager Release 9.0.1 through 9.0.3.2 or Release 9.1.0.*x* to Trust the Remote Manager

To configure Oracle Identity Manager to trust the Remote Manager:

1. From the computer hosting the Remote Manager, copy the *RM_HOME*/xlremote/config/xlserver.cert file to a temporary directory on the Oracle Identity Manager host computer.

   > **Note:** The server certificate in the *OIM_HOME* directory is also named xlserver.cert. Ensure that you do not overwrite that certificate.

2. To import the certificate by using the keytool utility, run the following command:

   ```
   JAVA_HOME/jre/bin/keytool -import -alias ALIAS -file
   RM_CERT_LOCATION/xlserver.cert -keystore OIM_HOME/xellerate/config/.xlkeystore
   -storepass PASSWORD
   ```

   In the preceding command, replace:

   – *JAVA_HOME* with the location of the Java directory for your application server.

   – *ALIAS* with an alias for the certificate in the store.

   – *RM_CERT_LOCATION* with the full path of the temporary directory where you copied the certificate.

   – *PASSWORD* with the password of the keystore.

3. Copy the *OIM_HOME*/xellerate/config/xlserver.cert file to a temporary directory on the Remote Manager host computer.

4. To import the certificate by using the keytool utility on the Remote Manager host computer, run the following command:

   ```
   JAVA_HOME/jre/bin/keytool -import -alias ALIAS -file
   OIM_CERT_LOCATION/xlserver.cert -keystore RM_HOME/xlremote/config/.xlkeystore
   -storepass PASSWORD
   ```

   In the preceding command, replace:

   – *JAVA_HOME* with the location of the Java directory for your application server.

   – *ALIAS* with an alias for the certificate in the store.

   – *OIM_CERT_LOCATION* with the full path of the temporary directory where you copied the certificate.

   – *PASSWORD* with the password of the keystore.

   > **Note:** It is recommended that you follow security best practices and change the default passwords used for the Remote Manager keystore. To change the Remote Manager keystore password, follow the instructions given in *Oracle Identity Manager Installation and Configuration Guide* for your application server.

2.3.8.5 Configuring Oracle Identity Manager Release 11.1.x to Trust the Remote Manager

To configure Oracle Identity Manager to trust the Remote Manager:

1. On the computer hosting Oracle Identity Manager, export the certificate by running the following command:

   ```
   keytool -export -keystore KEYSTORE_FILE -storepass KEYSTORE_PASSWORD -alias
   ALIAS -file CERT_FILE_NAME
   ```

   In this command:

   - *KEYSTORE_FILE* is the complete path and name of the keystore.
   - *KEYSTORE_PASSWORD* is the password of the keystore.
   - *ALIAS* is the alias of the certificate to be exported.
   - *CERT_FILE_NAME* is the file name containing the exported certificate

   The following is a sample command:

   ```
   keytool -export -keystore
   D:\March11g\Middleware\user_projects\domains\MARCHWIN\config\fmwconfig\default-
   keystore.jks -storepass MyPa55word -alias xell -file oim.cer
   ```

2. Copy the exported certificate to any directory on the target system.
3. To import the certificate, run the following command:

   ```
   keytool -import -keystore KEYSTORE_FILE -storepass KEYSTORE_PASSWORD -alias
   ALIAS -file CERT_FILE_NAME
   ```

   In this command:

   - *KEYSTORE_FILE* is the complete path and name of the keystore.
   - *KEYSTORE_PASSWORD* is the password of the keystore.
   - *ALIAS* is the alias of the certificate to be imported.
   - *CERT_FILE_NAME* is the file name containing the imported certificate

   The following is a sample command:

   ```
   keytool -import -keystore
   C:\Oracle\Middleware1\Oracle_IDM1\remote_manager\config\default-keystore.jks
   -storepass MyPa55word -alias oimserver -file
   C:\Oracle\Middleware1\OIMCert\oim.cer
   ```

4. Copy the *OIM_HOME*\server\config\xlserver.cert file from the Remote Manager host computer to a temporary directory on the Oracle Identity Manager host computer.
5. To import the certificate, run the following command:

   ```
   keytool -import -keystore KEYSTORE_FILE -storepass KEYSTORE_PASSWORD -alias
   ALIAS -file CERT_FILE_NAME
   ```

   In this command:

   - *KEYSTORE_FILE* is the complete path and name of the keystore.
   - *KEYSTORE_PASSWORD* is the password of the keystore.
   - *ALIAS* is the alias of the certificate to be imported.
   - *CERT_FILE_NAME* is the file name containing the imported certificate

   The following is a sample command

```
keytool -import -keystore
D:\March11g\Middleware\user_projects\domains\MARCHWIN\config\fmwconfig\default_
keystore.jks -storepass Welcome1 -alias rmcert -file
D:\March11g\Middleware\RMCert146\xlserver.cert
```

2.3.8.6 Verifying That the Remote Manager Is Running

To verify that the Remote Manager is running:

1. Use one of the following scripts to start the Remote Manager:
   - For Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*:

     RM_HOME\xlremote\remotemanager.bat
   - For Oracle Identity Manager release 11.1.*x*:

     OIM_HOME\remote_manager\remotemanager.bat
2. Log in to the Design Console.
3. Expand **Administration**, and double-click **Remote Manager**.
4. Search for and open the Remote Manager that you have created.
5. Click the Refresh icon. The screen displays details of the Remote Manager that you have configured. The Running check box should be selected for the Remote Manager. This implies that the status of the Remote Manager is active.

2.3.9 Configuring High Availability of the Target System

Suppose you have set up multiple, replicated installations of the target system for high availability. You can use the Lookup.EDIR.BackupServers lookup definition to ensure that if the primary target system installation becomes unavailable, then Oracle Identity Manager switches to one of the secondary target system installations. The Lookup.EDIR.BackupServers lookup definition is one of the lookup definitions created when you deploy the connector.

For a single primary installation, you can have any number of secondary installations. In addition, if you configure the connector to work with multiple primary installations, then you can specify secondary installations for each primary installation.

To use the Lookup.EDIR.BackupServers lookup definition, open it in the Design Console and enter Code Key and Decode values for each combination of primary and secondary target system installations.

> **Note:** In addition, set the timeout interval as the value of the LDAPConnectTimeOut entry of the Lookup.EDIR.Configuration lookup definition. See Section 2.3.7, "Setting Up Lookup Definitions in Oracle Identity Manager" for more information.

Table 2–9 shows samples entries for the Lookup.EDIR.BackupServers lookup definition.

Table 2–9 Samples Entries for the Lookup.EDIR.BackupServers Lookup Definition

Code Key	Decode
172.20.55.64	172.20.55.65
172.20.55.64	172.20.55.66
172.20.55.97	172.20.55.98

In this table, the first two entries represent two secondary installations (172.20.55.65 and 172.20.55.66) for one primary installation (172.20.55.64). The third entry shows a one-to-one combination of primary (172.20.55.97) and secondary (172.20.55.98) installations.

2.3.10 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 importing the XML file for trusted source reconciliation, eDirXLResourceObject.xml, by using the Deployment Manager.

> **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.

To import the XML file for trusted source reconciliation:

1. Open the Oracle Identity Manager Administrative and User Console.
2. If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
   a. Click the **Deployment Management** link on the left navigation bar.
   b. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
3. If you are using Oracle Identity Manager release 11.1.*x*, then:

   a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Import Deployment Manager File**. A dialog box for opening files is displayed.

4. Locate and open the eDirXLResourceObject.xml file located in the following directory:

   - For Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*:

     OIM_HOME/xellerate/ConnectorDefaultDirectory/eDirectory_9.0.4.14.0/xml

   - For Oracle Identity Manager release 11.1.*x*:

     OIM_HOME/server/ConnectorDefaultDirectory/eDirectory_9.0.4.14.0/xml

   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**.

2.3.11 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 Lookup.EDIR.Configuration 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`

2.3.12 Configuring Oracle Identity Manager for Request-Based Provisioning

> **Note:** Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.1 and you want to configure request-based provisioning.

In request-based provisioning, an end user creates a request for a resource by using the Administrative and User Console. Administrators or other users can also create requests for a particular user. Requests for a particular resource on the resource can be viewed and approved by approvers designated in Oracle Identity Manager.

The following are features of request-based provisioning:

- A user can be provisioned only one resource (account) on the target system.

> **Note:** Direct provisioning allows the provisioning of multiple target system accounts on the target system.

- Direct provisioning cannot be used if you enable request-based provisioning.

To configure request-based provisioning, perform the following procedures:

- Section 2.3.12.1, "Copying Predefined Request Datasets"
- Section 2.3.12.2, "Importing Request Datasets into MDS"
- Section 2.3.12.3, "Enabling the Auto Save Form Feature"
- Section 2.3.12.4, "Running the PurgeCache Utility"

2.3.12.1 Copying Predefined Request Datasets

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. Predefined request datasets are shipped with this connector. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation. The following is the predefined request dataset available in the DataSets directory on the installation media:

- ProvisionResourceeDirectory User.xml
- ModifyResourceeDirectory User.xml

Copy the files from the DataSets directory on the installation media to the *OIM_HOME*/DataSet/file directory.

Depending on your requirement, you can modify the file names of the request datasets. In addition, you can modify the information in the request datasets. See *Oracle Fusion Middleware Developer's Guide* for Oracle Identity Manager for information on modifying request datasets.

2.3.12.2 Importing Request Datasets into MDS

> **Note:** In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster.

All request datasets must be imported into the metadata store (MDS), which can be done by using the Oracle Identity Manager MDS Import utility.

To import a request dataset definition into MDS:

1. Ensure that you have set the environment for running the MDS Import utility. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about setting up the environment for MDS utilities.

2. In a command window, change to the *OIM_HOME*\server\bin directory.
3. Run one of the following commands:
   - On Microsoft Windows

     ```
     weblogicImportMetadata.bat
     ```

   - On UNIX

     ```
     weblogicImportMetadata.sh
     ```

4. When prompted, enter the following values:
   - `Please enter your username [weblogic]`

     Enter the username used to log in to the WebLogic server

     Sample value: `WL_User`

   - `Please enter your password [weblogic]`

     Enter the password used to log in to the WebLogic server.

   - `Please enter your server URL [t3://localhost:7001]`

     Enter the URL of the application server in the following format:

     `t3://`*`HOST_NAME_IP_ADDRESS`*`:`*`PORT`*

     In this format, replace:

     – *HOST_NAME_IP_ADDRESS* with the host name or IP address of the computer on which Oracle Identity Manager is installed.

     – *PORT* with the port on which Oracle Identity Manager is listening.

   The request dataset is imported into MDS.

2.3.12.3 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

1. Log in to the Design Console.
2. Expand **Process Management,** and then double-click **Process Definition.**
3. Search for and open the **eDirectory User PD** process definition.
4. Select the **Auto Save Form** check box.
5. Click the Save icon.

2.3.12.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.3.5, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

The procedure to configure request-based provisioning ends with this step.

2.3.13 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 Using the Connector

This chapter is divided into the following sections:

3.1 Performing First-Time Reconciliation

First-time reconciliation involves synchronizing lookup definitions in Oracle Identity Manager with the lookup fields of the target system, and performing full reconciliation. In full reconciliation, all existing user records from the target system are brought into Oracle Identity Manager.

The following is the sequence of steps involved in reconciling all existing user records:

> **Note:** In Oracle Identity Manager release 11.1.*x*, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.*x*.
>
> See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

1. Perform lookup field synchronization by running the scheduled tasks provided for this operation.

   See Section 3.2, "Lookup Field Synchronization" for information about the attributes of the scheduled tasks for lookup field synchronization.

   See Section 3.4, "Configuring Scheduled Tasks" for information about running scheduled tasks.

2. Perform user reconciliation by running the scheduled task for user reconciliation.

See Section 3.3.4, "Reconciliation Scheduled Tasks" for information about the attributes of this scheduled task.

See Section 3.4, "Configuring Scheduled Tasks" for information about running scheduled tasks.

After first-time reconciliation, depending on the mode in which you configure the connector, one of the following parameters of the eDirectory IT Resource IT resource is automatically set to the time stamp at which the reconciliation run began:

- For trusted source reconciliation, the Last Recon Trusted TimeStamp parameter is set.
- For target resource reconciliation, the Last Recon Target TimeStamp parameter is set.

> **See Also:** Section 2.2, "Installation" for information about the parameters of the IT resource

From the next reconciliation run onward, only target system user records that are added or modified after the time stamp stored in the IT resource are considered for incremental reconciliation. These records are brought to Oracle Identity Manager when you configure and run the user reconciliation scheduled task.

3.2 Lookup Field Synchronization

The following scheduled tasks are used for lookup fields reconciliation:

- eDirectory Organization Lookup Reconciliation Task
- eDirectory Role Lookup Reconciliation Task
- eDirectory Group Lookup Reconciliation Task
- eDirectory Profile Lookup Reconciliation Task
- eDirectory DomainScope Lookup Reconciliation Task

You must specify values for the attributes of these scheduled tasks. Table 3–1 describes the attributes of these scheduled tasks. Section 3.4, "Configuring Scheduled Tasks" describes the procedure to configure scheduled tasks.

> **Note:** This table describes the attributes of all the scheduled tasks for lookup field synchronization. Some of these attributes are not common to all the scheduled tasks.

Table 3–1 Attributes of the Scheduled Tasks for Lookup Field Synchronization

Attribute	Description
ConfigurationLookup	This attribute holds the name of the configuration lookup definition, which contains values that are used during connector operations. Default value: `Lookup.EDIR.Configuration`

AttrTask	The attribute holds the naming attribute of the object on the target system.
	- Default value for organizations:
	`o`
	- Default value for domain scope and organizational units:
	`ou`
	- Default value for groups, roles, and profiles
	`cn`

LookupCodeName	This attribute holds the name of the lookup definition with which the values are to be synchronized.
	- Default value for organizational units and organizations:
	`Lookup.EDIR.Organization`
	- Default value for domain scope:
	`Lookup.EDIR.DomainScope`
	- Default value for groups:
	`Lookup.EDIR.UserGroup`
	- Default value for roles:
	`Lookup.EDIR.AssignedRole`
	- Default value for profiles:
	`Lookup.EDIR.Profile`

ITResourceName	This attribute holds the name of the IT resource for setting up a connection with Novell eDirectory. Default value: `eDirectory IT Resource`
SearchContext	Enter the search context (DN of the user container) to be used for fetching lookup field values from the target system. Default value: `o=PXED-DEV,dc=Company`

ObjectClass	This attribute holds the name of the object class.
	- Default value for organizational units and domain scope:
	`OrganizationalUnit`
	- Default value for groups:
	`group`
	- Default value for roles:
	`rBSRole`
	- Default value for profiles:
	`profile`
	- Default value for organizations:
	`organization`

CodeKeyLTrimStr	The default value of this attribute is `[None]`. Do not change this value.

Table 3–1 (Cont.) Attributes of the Scheduled Tasks for Lookup Field Synchronization

Attribute	Description
CodeKeyRTrimStr	Enter the string value that must be right-trimmed from each value returned by the scheduled task. Sample value: `,o=PXED-DEV` If there is nothing to be trimmed, then enter `[NONE]`.
ReconMode	Enter `REFRESH` to completely refresh the existing lookup. Existing values in the lookup definition are deleted and then new values are added. Enter `UPDATE` if you want to update the lookup definition with new values. Existing values in the lookup definition are left untouched.
SearchFilter	Enter the query or filter that must be applied during a reconciliation run. See Section 3.3.2, "Limited Reconciliation" for more information. You can enter one of the following values: For organizational units and domain scope: `(objectClass=OrganizationalUnit)` For groups: `(objectClass=Group)` For roles: `(objectClass=RBS:Role)` For profiles: `(objectClass=Profile)` For organizations: `(objectClass=organization)`

3.3 Configuring Reconciliation

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:

- Section 3.3.1, "Full Reconciliation vs. Incremental Reconciliation"
- Section 3.3.2, "Limited Reconciliation"
- Section 3.3.3, "Batched Reconciliation"
- Section 3.3.4, "Reconciliation Scheduled Tasks"

3.3.1 Full Reconciliation vs. Incremental Reconciliation

The Last Recon Trusted TimeStamp and Last Recon Target TimeStamp parameters of the IT resource store the time stamp at which a reconciliation run begins. During the next reconciliation run, the scheduled task fetches only target system records that are added or modified after the time stamp stored in the parameter for reconciliation. This is incremental reconciliation.

In full reconciliation, all existing target system records are fetched into Oracle Identity Manager for reconciliation. If you want to run full reconciliation, then ensure that no value is entered for the time-stamp parameter. In other words, the time-stamp parameter must be empty.

You can switch from incremental to full reconciliation at any time by not setting any value for the time-stamp parameter. If you want to continue with incremental reconciliation, then accept the default value of the time-stamp parameter.

3.3.2 Limited 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 a reconciliation filter.

For this connector, you create a filter by specifying a query condition as the value of the SearchFilter attribute of the scheduled tasks. The query condition must be in the LDAP format, as shown in the following sample value:

```
(objectclass=inetOrgPerson)
```

With this query condition, only records for users whose objectclass is inetOrgPerson are considered for reconciliation.

You can add multiple query conditions by using the ampersand (&) as the AND operator and the vertical bar (|) as the OR operator. For example, the following query condition is used to limit reconciliation to records of those users whose first name is John and objectclass is inetOrgPerson:

> **Note:** As shown in this sample value, you must enclose the query condition in parentheses.

```
(&(objectClass=inetOrgPerson)(givenname=John))
```

The following are sample query conditions that can be specified as the value of the SearchFilter attribute:

```
(&(objectClass=inetOrgPerson)(givenname=John))
(&(objectClass=inetOrgPerson)(sn=Doe))
(&(&(sn=Doe)(givenname=John))(objectClass=inetOrgPerson))
(|(|(sn=lastname)(givenname=firstname))(objectClass=inetOrgPerson))
```

The SearchFilter attribute is also present in the scheduled tasks for lookup field synchronization. You can select one of the following values in one of those scheduled tasks:

- For organizational units and domain scope: `(objectClass=OrganizationalUnit)`
- For groups: `(objectClass=Group)`
- For roles: `(objectClass=RBS:Role)`
- For profiles: `(objectClass=Profile)`
- For organizations: `(objectClass=organization)`

3.3.3 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 Section 3.3.4, "Reconciliation Scheduled Tasks."

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

3.3.4 Reconciliation Scheduled Tasks

This section discusses the following topics:

- Section 3.3.4.1, "User Reconciliation Scheduled Tasks"
- Section 3.3.4.2, "Group and Role Reconciliation Scheduled Task"

3.3.4.1 User Reconciliation Scheduled Tasks

The following scheduled tasks are used for user reconciliation:

- eDirectory User Trusted Recon Task
- eDirectory User Target Recon Task
- eDirectory User Trusted Delete Recon Task
- eDirectory User Target Delete Recon Task

You must specify values for the set of scheduled tasks that are used for the mode (target resource or trusted source) in which you are using the connector. Table 3–2 describes the attributes of these scheduled tasks.

> **Note:**
>
> This table describes the attributes of all the scheduled tasks for user reconciliation. Some of these attributes are not common to all the scheduled tasks.
>
> Section 3.4, "Configuring Scheduled Tasks" describes the procedure to configure scheduled tasks.

Table 3–2 Attributes of the User Reconciliation Scheduled Tasks

Attribute	Description
UseTransformMapping	Enter yes to specify that you want to configure transformation of attributes during reconciliation. Otherwise, enter no. See Section 4.10, "Configuring Transformation of Data During Reconciliation" for more information. In the eDirectory User Target Recon Task scheduled task, set this attribute to yes if you want to enable provisioning of the Home directories. See Step 6 of Section 4.9, "Linking the Home Directory Provisioning Operation with the Create User Provisioning Operation" for more information. Default value: no
Keystore	If you are planning to configure SSL communication between Oracle Identity Manager and the target system, then enter the name and full path of the Novell eDirectory keystore directory. If you are not planning to configure an SSL connection, then enter [NONE]. Sample value: E:\j2sdk1.4.2_05\jre\lib\security\cacerts
UserContainer	Enter the DN value of the organization from where users must be reconciled into Oracle Identity Manager. Default value: o=PXED-DEV,dc=Company
Organization	Enter the default organization for the OIM User. Default value: Xellerate Users
Role	Enter the default role for the OIM User. Default value: Consultant
StartRecord	Enter the number of the record from which the batched reconciliation process must begin. Default value: 1 See Section 3.3.3, "Batched Reconciliation" for information about batched reconciliation.
Batch Size	Enter the number of records that must be included in each batch fetched from the target system during a reconciliation run. Default value: 100 See Section 3.3.3, "Batched Reconciliation" for information about batched reconciliation.
NumberOfBatches	Enter the number of batches that must be reconciled. Default value: All Available (for reconciling all the users) Sample value: 50 See Section 3.3.3, "Batched Reconciliation" for information about batched reconciliation.
ConfigurationLookup	This attribute holds the name of the lookup definition that stores the configurable attributes used for connector operations. Value: Lookup.EDIR.Configuration
TransformLookupName	This attribute holds the name of the lookup definition that is used for transformation mapping. Value: Lookup.EDIR.Transformation
IT Resource	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: eDirectory IT Resource

Table 3–2 (Cont.) Attributes of the User Reconciliation Scheduled Tasks

Attribute	Description
Xellerate Type	This attribute holds the default employee type for the OIM User. Default value: `End-User Administrator`
TrustedResourceObjectName	This attribute holds the name of the resource object that is used in trusted reconciliation. Default value: `Xellerate User`
SearchFilter	Enter the search filter in LDAP format for fetching records from the target system during the reconciliation run. Default value: `(objectclass=inetOrgPerson)`
TargetResourceObjectName	This attribute holds the name of the resource object that is used in target reconciliation. Default value: `eDirectory User`
SearchBase	Enter the DN value of the user container from which users must be reconciled into Oracle Identity Manager. Default value: `o=PXED-DEV,dc=Company`

3.3.4.2 Group and Role Reconciliation Scheduled Task

Note: You cannot reconcile group data and role data from the target system if you are using Oracle Identity Manager release 11.1.*x*. This issue is tracked by Bug 9799541 in Chapter 6, "Known Issues."

The eDirectory GroupOrRole Recon Task scheduled task is used for group or role reconciliation. Table 3–3 describes the attributes of this scheduled task.

Table 3–3 Attributes of the eDirectory GroupOrRole Recon Task Scheduled Task

Attribute	Description
ConfigurationLookup	This attribute holds the name of the lookup definition that stores configuration information used during connector operations. Default value: `Lookup.EDIR.Configuration`
Field Lookup Code	This attribute holds the name of the lookup definition that stores reconciliation field mappings for group or role connector operations. Provide the corresponding reconciliation look up mappings Default value: For group reconciliation: `AttrName.ReconGroup.Map.EDIR` For role reconciliation: `AttrName.ReconRole.Map.EDIR`
isRoleRecon	Enter `yes` if you want role reconciliation to be performed. Enter `no` if you want group reconciliation to be performed. Default value: `yes`
ITResourceName	This attribute holds the name of the IT resource that contains connection information to connect to Novell eDirectory. Default value: `eDirectory IT Resource`

Table 3–3 (Cont.) Attributes of the eDirectory GroupOrRole Recon Task Scheduled Task

Attribute	Description
MultiValued Attributes	Enter the list of multivalued attributes that you add for reconciliation and provisioning. See Section 4.2, "Adding New Multivalued Attributes for Target Resource Reconciliation" for information about adding multivalued attributes. The default value of this attribute is `[NONE]` . Sample value: `owner|description`
ResourceObjectName	Enter the name of the resource object into which groups or roles are to be reconciled. The value can be one of the following: ■ For group reconciliation: `eDirectory Group` ■ For role reconciliation: `eDirectory Role`
SearchBase	Enter the DN value from where the groups or roles are reconciled from the target system to Oracle Identity Manager. Sample value: `ou=myou,dc=corp,dc=com` or `dc=corp,dc=com`

SearchFilter	Enter the LDAP search filter that is used to locate groups or roles.
	See Section 3.3.2, "Limited Reconciliation" for more information.
	Sample values:
	`(objectClass=Group)`
	`(objectClass=RBS:Role)`

3.4 Configuring Scheduled Tasks

You can apply the procedure described in this section to configure the scheduled tasks for lookup field synchronization and reconciliation.

Table 3–4 lists the scheduled tasks that form part of the connector.

Table 3–4 Scheduled Tasks for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
eDirectory Organization Lookup Reconciliation Task	This scheduled task is used for organization lookup field synchronization. See Section 3.2, "Lookup Field Synchronization" for information about this scheduled task.
eDirectory Role Lookup Reconciliation Task	This scheduled task is used for role lookup field synchronization. See Section 3.2, "Lookup Field Synchronization" for information about this scheduled task.
eDirectory Group Lookup Reconciliation Task	This scheduled task is used for group lookup field synchronization. See Section 3.2, "Lookup Field Synchronization" for information about this scheduled task.
eDirectory DomainScope Lookup Reconciliation Task	This scheduled task is used for domain lookup field synchronization. See Section 3.2, "Lookup Field Synchronization" for information about this scheduled task.
eDirectory Profile Lookup Reconciliation Task	This scheduled task is used for profile lookup field synchronization. See Section 3.2, "Lookup Field Synchronization" for information about this scheduled task.
eDirectory User Trusted Recon Task	This scheduled task is used for user reconciliation when the target system is configured as a trusted source. See Section 3.3.4, "Reconciliation Scheduled Tasks" for information about this scheduled task.

Table 3–4 (Cont.) Scheduled Tasks for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
eDirectory User Target Recon Task	This scheduled task is used for user reconciliation when the target system is configured as a target resource. See Section 3.3.4, "Reconciliation Scheduled Tasks" for information about this scheduled task.
eDirectory User Trusted Delete Recon Task	This scheduled task is used for reconciliation of deleted users when the target system is configured as a trusted source. See Section 3.3.4, "Reconciliation Scheduled Tasks" for information about this scheduled task.
eDirectory User Target Delete Recon Task	This scheduled task is used for reconciliation of deleted users when the target system is configured as a target resource. See Section 3.3.4, "Reconciliation Scheduled Tasks" for information about this scheduled task.
eDirectory GroupOrRole Recon Task	This scheduled task is used for reconciliation of groups and roles from the target system. See Section 3.3.4, "Reconciliation Scheduled Tasks" for information about this scheduled task.

Depending on the Oracle Identity Manager release that you are using, perform the procedure described in one of the following sections:

- Section 3.4.1, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.0.1 through 9.0.3.2"
- Section 3.4.2, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.x or Release 11.1.x"

3.4.1 Configuring Scheduled Tasks on Oracle Identity Manager Release 9.0.1 through 9.0.3.2

To configure the reconciliation scheduled task:

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.
5. Enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the `FAILED` status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.
7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, select the date and time at which you want the task to run.
8. In the Interval region, set the following schedule parameters:
   - To set the task to run on a recurring basis, select the **Daily**, **Weekly**, **Recurring Intervals**, **Monthly**, or **Yearly** option.

     If you select the **Recurring Intervals** option, then you must also specify the time interval at which you want the task to run on a recurring basis.
   - To set the task to run only once, select the **Once** option.
9. Provide values for the user-configurable attributes of the scheduled task. See Section 3.3.4, "Reconciliation Scheduled Tasks" 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.

3.4.2 Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.x or Release 11.1.x

To configure a scheduled task:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 9.*x* or 11.1.1:
     a. Log in to the Administrative and User Console.
     b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
   - For Oracle Identity Manager release 11.1.2:
     a. Log in to Oracle Identity System Administration.
     b. In the left pane, under System Management, click **Scheduler.**
2. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.*x*, expand **Resource Management,** and then click **Manage Scheduled Task.**
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced.**
     b. Click the **System Management** tab, and then click **Scheduler.**
     c. On the left pane, click **Advanced Search**.
3. On the page that is displayed, you can use any combination of the search options provided to locate a scheduled task. Click **Search** after you specify the search criteria.

   The list of scheduled tasks that match your search criteria is displayed in the search results table.
4. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then in the search results table, click the Edit icon in the Edit column for the scheduled task.
   - If you are using Oracle Identity Manager release 11.1.*x*, then select the link for the scheduled task from the list of scheduled tasks displayed in the search results table.
5. Modify the details of the scheduled task. To do so:

   a. If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Edit Scheduled Task Details page, modify the following parameters, and then click **Continue**:

- **Status:** Specify whether you want to leave the task in the enabled state. In the enabled state, the task is ready for use.
- **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.

b. If you are using Oracle Identity Manager release 11.1.*x*, then on the Job Details tab, you can modify the following parameters:

- **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
- **Schedule Type:** Depending on the frequency at which you want the job to run, select the appropriate schedule type.

Note: See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for detailed information about schedule types.

In addition to modifying the job details, you can enable or disable a job.

6. Specify values for the attributes of the scheduled task. To do so:

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 is left empty, then reconciliation is not performed.
- Attributes of the scheduled task are discussed in Section 3.3.4, "Reconciliation Scheduled Tasks."

- If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Attributes page, select the attribute from the Attribute list, specify a value in the field provided, and then click **Update**.
- If you are using Oracle Identity Manager release 11.1.*x,* then on the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.

7. After specifying the attributes, perform one of the following:

- If you are using Oracle Identity Manager release 9.1.0.*x*, then click **Save Changes** to save the changes.

Note: The Stop Execution option is not available in the Administrative and User Console. If you want to stop a task, then click **Stop Execution** on the Task Scheduler form of the Design Console.

- If you are using Oracle Identity Manager release 11.1.*x*, then click **Apply** to save the changes.

Note: The Stop Execution option is available in the Administrative and User Console. You can use the Scheduler Status page to either start, stop, or reinitialize the scheduler.

3.5 Guidelines on Performing Provisioning

Apply the following guideline while performing provisioning operations:

- While provisioning a Home directory, you must select the Container DN value on the Administrative and User Console.

3.6 Performing Provisioning Operations

See Also: Section 3.7, "Configuring Provisioning in Oracle Identity Manager Release 11.1.2"

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:

- Section 3.6.1, "Provisioning Users"
- Section 3.6.2, "Provisioning Organizational Units, Groups, and Roles"
- Section 3.6.3, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1"

3.6.1 Provisioning Users

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create a target system account for the user.

When you install the connector on Oracle Identity Manager release 11.1.1, the direct provisioning feature is automatically enabled. This means that the process form is enabled when you install the connector.

If you have configured the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then perform the steps described in Section 3.6.3, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1."

The following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning

- Provisioning triggered by policy changes

> **See Also:** *Oracle Identity Manager Connector Concepts* for information about the types of provisioning

This section discusses the following topics:

- Section 3.6.1.1, "Direct Provisioning"
- Section 3.6.1.2, "Request-Based Provisioning"

3.6.1.1 Direct Provisioning

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. If you want to first create an OIM User and then provision a target system account, then:
   - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
     a. From the Users menu, select **Create**.
     b. On the Create User page, enter values for the OIM User fields and then click **Create User**.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Identity Administration page, in the Users region, click **Create User**.
     b. On the Create User page, enter values for the OIM User fields, and then click **Save**.
3. If you want to provision a target system account to an existing OIM User, then:
   - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
     a. From the Users menu, select **Manage**.
     b. Search for the OIM User and select the link for the user from the list of users displayed in the search results.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Identity Administration page, search for the OIM User by selecting **Users** from the list on the left pane.
     b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.
4. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
     a. On the User Detail page, select **Resource Profile** from the list at the top of the page.
     b. On the Resource Profile page, click **Provision New Resource**.
   - If you are using Oracle Identity Manager release 11.1.1, then:

   a. On the user details page, click the **Resources** tab.

   b. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.

5. On the Step 1: Select a Resource page, select **eDirectory User** from the list and then click **Continue**.

6. On the Step 2: Verify Resource Selection page, click **Continue**.

7. On the Step 5: Provide Process Data for eDirectory User Details page, enter the details of the account that you want to create on the target system and then click **Continue**.

8. On the Step 5: Provide Process Data for User Role page, search for and select a role for the user on the target system and then click **Continue**.

9. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.

10. The "Provisioning has been initiated" message is displayed. Perform one of the following steps:

    - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, click **Back to User Resource Profile.** The Resource Profile page shows that the resource has been provisioned to the user.

    - If you are using Oracle Identity Manager release 11.1.1, then:

      a. Close the window displaying the "Provisioning has been initiated" message.

      b. On the Resources tab, click **Refresh** to view the newly provisioned resource.

3.6.1.2 Request-Based Provisioning

> **Note:** The information provided in this section is applicable only if you are using Oracle Identity Manager release 11.1.1.

A request-based provisioning operation involves both end users and approvers. Typically, these approvers are in the management chain of the requesters. The following sections discuss the steps to be performed by end users and approvers during a request-based provisioning operation:

> **Note:** The procedures described in these sections are built on an example in which the end user raises or creates a request for provisioning a target system account. This request is then approved by the approver.

- Section 3.6.1.2.1, "End User's Role in Request-Based Provisioning"
- Section 3.6.1.2.2, "Approver's Role in Request-Based Provisioning"

3.6.1.2.1 End User's Role in Request-Based Provisioning The following steps are performed by the end user in a request-based provisioning operation:

See Also: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for detailed information about these steps

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Advanced** in the upper-right corner of the page.
3. On the Welcome to Identity Administration page, click the **Administration** tab, and then click the **Requests** tab.
4. From the Actions menu on the left pane, select **Create Request**.

   The Select Request Template page is displayed.
5. From the Request Template list, select **Provision Resource** and click **Next**.
6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click **Search**. A list of users that match the search criterion you specify is displayed in the Available Users list.
7. From the **Available Users** list, select the user to whom you want to provision the account.

   If you want to create a provisioning request for more than one user, then from the **Available Users** list, select users to whom you want to provision the account.
8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next**.
9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.
10. From the Available Resources list, select **eDirectory User**, move it to the Selected Resources list, and then click **Next**.
11. On the Resource Details page, enter details of the account that must be created on the target system, and then click **Next**.
12. On the Justification page, you can specify values for the following fields, and then click **Finish**.
    - Effective Date
    - Justification

    On the resulting page, a message confirming that your request has been sent successfully is displayed along with the Request ID.
13. If you click the request ID, then the Request Details page is displayed.
14. To view details of the approval, on the Request Details page, click the **Request History** tab.

3.6.1.2.2 Approver's Role in Request-Based Provisioning The following are steps performed by the approver in a request-based provisioning operation:

The following are steps that the approver can perform:

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Self-Service** in the upper-right corner of the page.
3. On the Welcome to Identity Manager Self Service page, click the **Tasks** tab.
4. On the **Approvals** tab, in the first section, you can specify a search criterion for request task that is assigned to you.

5. From the search results table, select the row containing the request you want to approve, and then click **Approve Task**.

   A message confirming that the task was approved is displayed.

3.6.2 Provisioning Organizational Units, Groups, and Roles

> **See Also:**
>
> For Oracle Identity Manager release 9.0.1 through 9.0.3.2 or 9.1.0.x, see *Oracle Identity Manager Administrative and User Console Guide* for detailed information about these steps.
>
> For Oracle Identity Manager release 11.1.1, see *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for detailed information about these steps.

To provision an organizational unit:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. Create an organization. To do so:
   - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
     a. Expand **Organizations,** and then click **Create**.
     b. Specify a name and the type for the organization that you want to create, and then click **Create Organization**.

        The organization is created.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome page, click **Administration** in the upper-right corner of the page.
     b. On the Welcome to Identity Administration page, from the Organizations section, click **Create Organization**.
     c. On the Create Organization page, enter values for the Name, Type, and Parent Organization (optional) fields, and then click **Save.**

        The organization is created.
3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
     a. Select **Resource Profile** from the list.
     b. Click **Provision New Resource**.

        The Provision Resource to Organization page is displayed.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the organization details page, click the **Resources** tab.
     b. From the Actions menu, select **Provision.** Alternatively, click **Provision** on the toolbar. The Provision Resource to Organization page is displayed in a new window.

4. On the Step 1: Select a Resource page, search for and select the organizational unit you want to provision, and then click **Continue.**
5. On the Step 2: Verify Resource Selection page, verify the data that you provided, and then click **Continue.**
6. On the Step 5: Provide Process Data page, enter the details of the organizational unit that you want to provision and then click **Continue.**
7. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue.**
8. The "Provisioning has been initiated" message is displayed. Perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, click **Back to User Resource Profile.** The Resource Profile page shows that the organizational unit has been provisioned to the organization.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. Close the window displaying the "Provisioning has been initiated" message.
     b. On the Resources tab, click **Refresh** to view the newly provisioned organizational unit.

To provision a group or role:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. Search for and open the organization to which you want to provision a group or role by performing one of the following steps:
   - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
     a. From the Organizations menu, select **Manage.**
     b. Search for the organization and select the link for the organization from the list of organizations displayed in the search results.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Identity Administration page, in the Organizations section, click **Advanced Search - Organizations,** provide a search criterion, and then click **Search.**

        Alternatively, search for the organization by selecting Organizations from the list on the left pane.
     b. From the organizations displayed in the search results table, click the row containing the organization to which to want to provision a group or role.

        The organization details page is displayed.
3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
     a. On the Organization Detail page, select **Resource Profile** from the list at the top of the page.
     b. On the Resource Profile page, click **Provision New Resource.**

The Provision Resource to Organization page is displayed.

- If you are using Oracle Identity Manager release 11.1.1, then:

    a. On the organization details page, click the **Resources** tab.

    b. From the Actions menu, select **Provision.** Alternatively, click **Provision** on the toolbar. The Provision Resource to Organization page is displayed in a new window.

4. On the Step 1: Select a Resource page, select one of the following options, and then click **Continue:**

    - Select the group option if you want to create a group.

      The default settings to enable provisioning of groups in organizational units in the AttrName.ProvGroup.EDIR.Map lookup definition are listed in the following table:

      Code key: Group Name

      Decode: cn

    - Select the role option if you want to create a role.

      The default settings to enable provisioning of roles in organizational units in the AttrName.ProvRole.EDIR.Map lookup definition are listed in the following table:

      Code key: Role Name

      Decode: cn

5. On the Step 2: Verify Resource Selection page, verify the data that you provided, and then click **Continue.**

6. On the Step 5: Provide Process Data page, depending on whether you have selected a group or role while performing Step 4, enter the group or role details, and then click **Continue.**

7. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue.**

8. The "Provisioning has been initiated" message is displayed. Perform one of the following steps:

    - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, click **Back to User Resource Profile.** The Resource Profile page shows that the group or role has been provisioned to the organization.

    - If you are using Oracle Identity Manager release 11.1.1, then:

        a. Close the window displaying the "Provisioning has been initiated" message.

        b. On the Resources tab, click **Refresh** to view the newly provisioned group or role.

3.6.3 Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1

> **Note:** It is assumed that you have performed the procedure described in Section 2.3.12, "Configuring Oracle Identity Manager for Request-Based Provisioning."

On Oracle Identity Manager release 11.1.1, if you want to switch from request-based provisioning to direct provisioning, then:

1. Log in to the Design Console.
2. Disable the Auto Save Form feature as follows:
    a. Expand **Process Management**, and then double-click **Process Definition**.
    b. Search for and open the **eDirectory User PD** process definition.
    c. Deselect the **Auto Save Form** check box.
    d. Click the Save icon.
3. If the Self Request Allowed feature is enabled, then:
    a. Expand **Resource Management**, and then double-click **Resource Objects**.
    b. Search for and open the **eDirectory User** resource object.
    c. Deselect the **Self Request Allowed** check box.
    d. Click the Save icon.

On Oracle Identity Manager release 11.1.1, if you want to switch from direct provisioning back to request-based provisioning, then:

1. Log in to the Design Console.
2. Enable the Auto Save Form feature as follows:
    a. Expand **Process Management**, and then double-click **Process Definition**.
    b. Search for and open the **eDirectory User PD** process definition.
    c. Select the **Auto Save Form** check box.
    d. Click the Save icon.
3. If you want to enable end users to raise requests for themselves, then:
    a. Expand **Resource Management**, and then double-click **Resource Objects**.
    b. Search for and open the **eDirectory User** resource object.
    c. Select the **Self Request Allowed** check box.
    d. Click the Save icon.

3.7 Configuring Provisioning in Oracle Identity Manager Release 11.1.2

To configure provisioning operations in Oracle Identity Manager release 11.1.2:

> **Note:** The time required to complete a provisioning operation that you perform the first time by using this connector takes longer than usual.

1. Log in to Oracle Identity Administrative and User console.
2. Create a user. See the "Managing Users" chapter in *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for more information about creating a user.
3. On the Account tab, click **Request Accounts.**
4. In the Catalog page, search for and add to cart the application instance, and then click **Checkout.**
5. Specify values for fields in the application form and then click **Ready to Submit.**
6. Click **Submit.**
7. If you want to provision a resource to an existing OIM User, then:
   a. On the Users page, search for the required user.
   b. On the user details page, click **Accounts.**
   c. Click the **Request Accounts** button.
   d. Search for the Novell eDirectory application instance in the catalog search box and select it.
   e. Click **Add to Cart.**
   f. Click **Checkout.**
   g. Specify values for fields in the application form and then click **Ready to Submit.**
   h. Click **Submit.**

4

Extending the Functionality of the Connector

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

> **Note:** If you are using Oracle Identity Manager 11.1.2 or later and modify the parent form (add or delete an attribute), then edit the application instance in usage and create a new form and make it active.

- Section 4.1, "Adding New Attributes for Target Resource Reconciliation"
- Section 4.2, "Adding New Multivalued Attributes for Target Resource Reconciliation"
- Section 4.3, "Adding New Attributes for Trusted Source Reconciliation"
- Section 4.4, "Adding New Attributes for Provisioning Users"
- Section 4.5, "Adding New Attributes for Provisioning Groups and Roles"
- Section 4.6, "Adding New Multivalued Attributes for Provisioning"
- Section 4.7, "Adding Custom Object Classes for Provisioning"
- Section 4.8, "Adding New Object Classes for Provisioning and Reconciliation"
- Section 4.9, "Linking the Home Directory Provisioning Operation with the Create User Provisioning Operation"
- Section 4.10, "Configuring Transformation of Data During Reconciliation"

4.1 Adding New Attributes for Target Resource Reconciliation

> **Note:** This section describes an optional procedure. Perform this procedure only if you want to add new attributes for target resource reconciliation.
>
> You must ensure that new attributes you add for reconciliation contain only string-format data. Binary attributes must not be brought into Oracle Identity Manager natively.

By default, the attributes listed in Section 1.6, "Connector Objects Used During Target Resource Reconciliation and Provisioning" are mapped for reconciliation between

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

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

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

     For example, if you are adding the Car License attribute, then enter the following values on the **Additional Columns** tab:

Field	Value
Name	Car License
Variant Type	String
Length	100
Field Label	Car License
Order	20

The following screenshot shows this form:

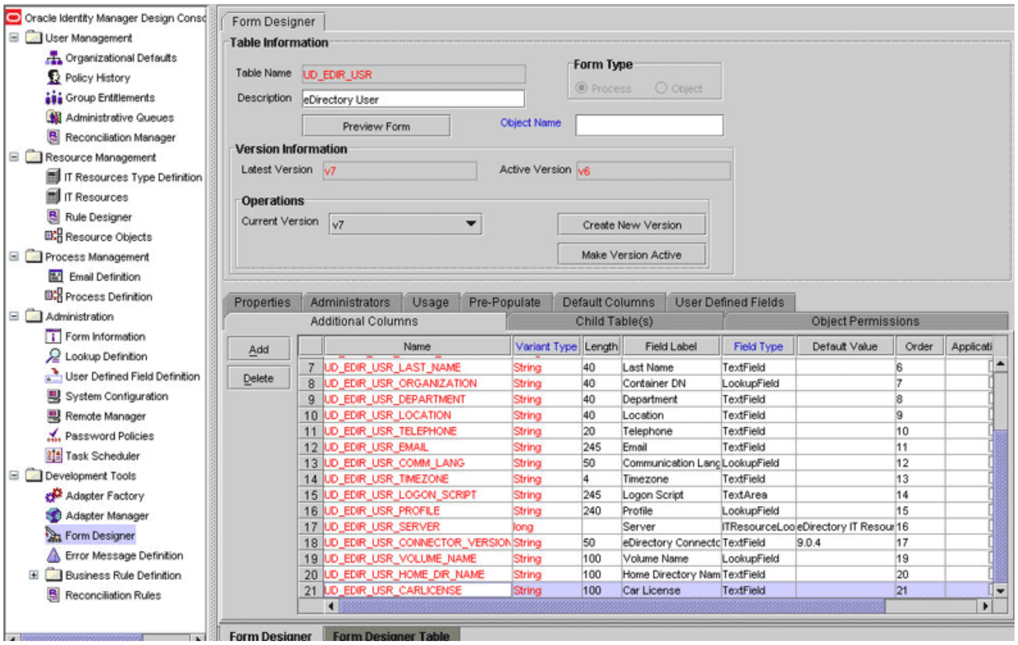


Table Information

Table Name: UD_EDIR_USR

Description: eDirectory User

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: v7

Active Version: v6

Operations

Current Version: v7

	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Applicati
7	UD_EDIR_USR_LAST_NAME	String	40	Last Name	TextField		6	
8	UD_EDIR_USR_ORGANIZATION	String	40	Container DN	LookupField		7	
9	UD_EDIR_USR_DEPARTMENT	String	40	Department	TextField		8	
10	UD_EDIR_USR_LOCATION	String	40	Location	TextField		9	
11	UD_EDIR_USR_TELEPHONE	String	20	Telephone	TextField		10	
12	UD_EDIR_USR_EMAIL	String	245	Email	TextField		11	
13	UD_EDIR_USR_COMM_LANG	String	50	Communication Lang	LookupField		12	
14	UD_EDIR_USR_TIMEZONE	String	4	Timezone	TextField		13	
15	UD_EDIR_USR_LOGON_SCRIPT	String	245	Logon Script	TextArea		14	
16	UD_EDIR_USR_PROFILE	String	240	Profile	LookupField		15	
17	UD_EDIR_USR_SERVER	long		Server	ITResourceLoo	eDirectory IT Resour	16	
18	UD_EDIR_USR_CONNECTOR_VERSION	String	50	eDirectory Connecto	TextField	9.0.4	17	
19	UD_EDIR_USR_VOLUME_NAME	String	100	Volume Name	LookupField		19	
20	UD_EDIR_USR_HOME_DIR_NAME	String	100	Home Directory Nam	TextField		20	
21	UD_EDIR_USR_CARLICENSE	String	100	Car License	TextField		21	

i. Click the **Save** icon.

j. Click **Make Version Active**.

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

a. Expand **Resource Management.**

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

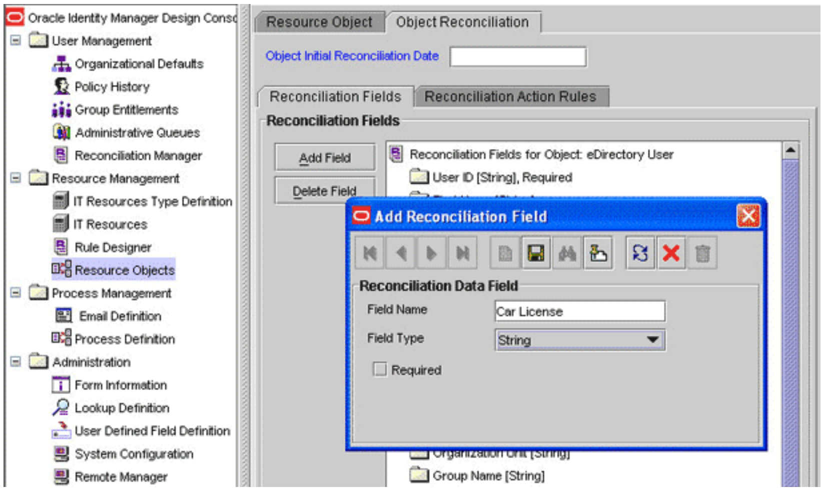
c. Search for and open the **eDirectory User** resource object.

d. On the **Object Reconciliation** tab, click **Add Field**, and then enter the following values:

Field Name: `Car License`

Field Type: `String`

The following screenshot shows this form:



Field Name: Car License

Field Type: String

□ Required

e. If you are using Oracle Identity Manager release 11.1.*x*, then click **Create Reconciliation Profile.** This copies changes made to the resource object into the MDS.

f. Click the **Save** icon.

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 **eDirectory User PD** process definition.

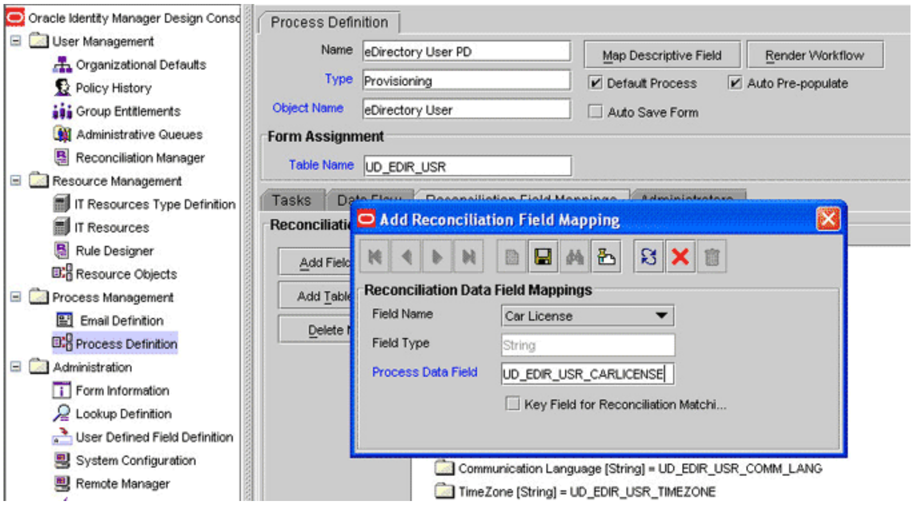
d. On the **Reconciliation Field Mappings** tab, click **Add Field Map**, and then select the following values:

Field Name: `Car License`

Field Type: `String`

Process Data Field: `carLicense`

The following screenshot shows this form:



Name: eDirectory User PD

Type: Provisioning

Object Name: eDirectory User

☑ Default Process ☑ Auto Pre-populate

□ Auto Save Form

Form Assignment

Table Name: UD_EDIR_USR

Reconciliation Data Field Mappings

Field Name: Car License

Field Type: String

Process Data Field: UD_EDIR_USR_CARLICENSE

□ Key Field for Reconciliation Matchi...

Communication Language [String] = UD_EDIR_USR_COMM_LANG

TimeZone [String] = UD_EDIR_USR_TIMEZONE

e. Click the **Save** icon.

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

   a. Expand **Administration**.

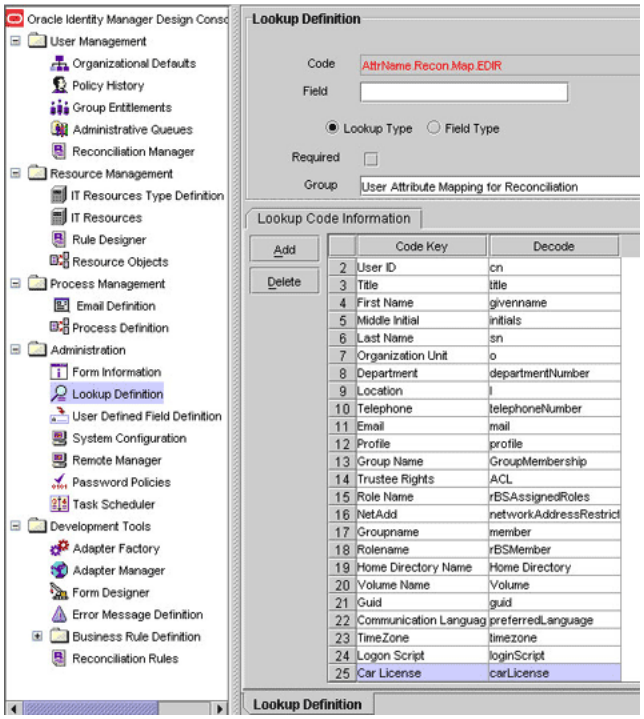
   b. Double-click **Lookup Definition**.

   c. Search for and open the **AttrName.Recon.Map.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 `Car License` in the **Code Key** field and then enter `carLicense` in the **Decode** field.

   The following screenshot shows this form:



Code: AttrName.Recon.Map.EDIR

Field:

● Lookup Type ○ Field Type

Required □

Group: User Attribute Mapping for Reconciliation

	Code Key	Decode
2	User ID	cn
3	Title	title
4	First Name	givenname
5	Middle Initial	initials
6	Last Name	sn
7	Organization Unit	o
8	Department	departmentNumber
9	Location	l
10	Telephone	telephoneNumber
11	Email	mail
12	Profile	profile
13	Group Name	GroupMembership
14	Trustee Rights	ACL
15	Role Name	rBSAssignedRoles
16	NetAdd	networkAddressRestrict
17	Groupname	member
18	Rolename	rBSMember
19	Home Directory Name	Home Directory
20	Volume Name	Volume
21	Guid	guid
22	Communication Languag	preferredLanguage
23	TimeZone	timezone
24	Logon Script	loginScript
25	Car License	carLicense

   e. Click the **Save** icon.

6. If you are using Oracle Identity Manager release 11.1.2 or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Section 2.3.1.3, "Creating a New UI Form" and Section 2.3.1.7, "Updating an Existing Application Instance with a New Form" for the procedures.

4.2 Adding New Multivalued Attributes for Target Resource Reconciliation

> **Note:** This section describes an optional procedure. Perform this procedure only if you want to add new multivalued fields for reconciliation. This procedure can be applied to add user, group, or role attributes.
>
> You must ensure that new attributes you add for reconciliation contain only string-format data. Binary attributes must not be brought into Oracle Identity Manager natively.

By default, only the UserGroup, UserRole, Trustee Rights, and Network Address Restriction multivalued attributes are mapped for user reconciliation between Oracle Identity Manager and the target system. If required, you can add new multivalued attributes for user reconciliation.

By default, no multivalued attributes are mapped for reconciliation between Oracle Identity Manager and the target system for groups and roles. If required, you can add new multivalued attributes for reconciliation of groups or roles.

To add a new multivalued attribute for target resource reconciliation:

1. Log in to the Oracle Identity Manager Design Console.
2. Create a form for the multivalued attribute as follows:
   a. Expand **Development Tools**.
   b. Double-click **Form Designer**.
   c. Create a form by specifying a table name and description, and then click **Save**.
   d. Click **Add** and enter the details of the attribute.

      The following screenshot shows this form:

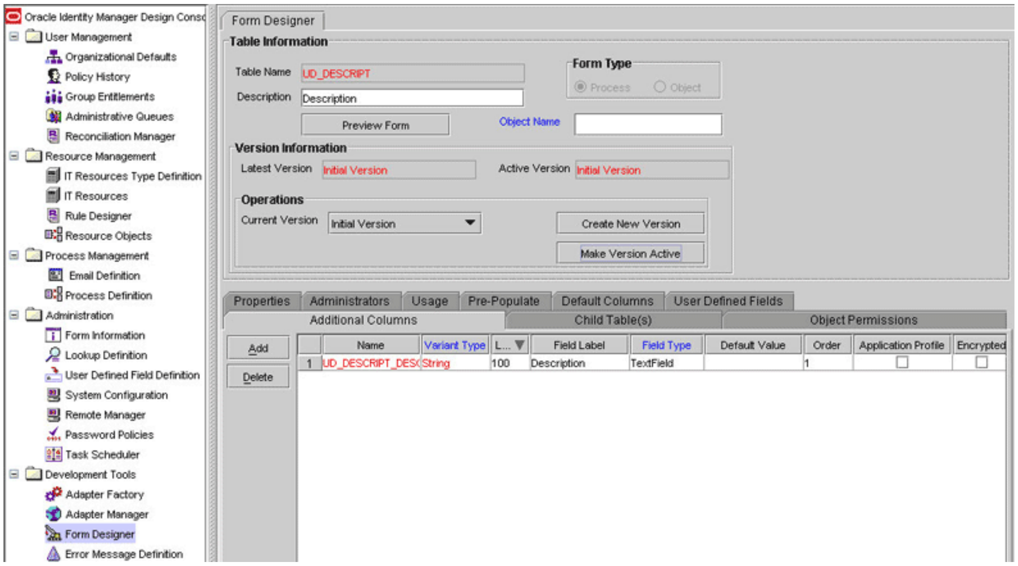


Table Name: UD_DESCRIPT

Description: Description

Object Name:

Form Type: ● Process ○ Object

Latest Version: Initial Version

Active Version: Initial Version

Current Version: Initial Version

	Name	Variant Type	L...	Field Label	Field Type	Default Value	Order	Application Profile	Encrypted
1	UD_DESCRIPT_DESC	String	100	Description	TextField		1	□	□

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

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

   a. Perform one of the following steps:

      – For users, search for and open the **UD_EDIR_USR** process form.

      – For groups, search for and open the **UD_EDIR_GR** process form.

      – For roles, search for and open the **UD_EDIR_RL** process form.

   b. Click **Create New Version**.

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

   d. Click **Assign**.

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

      The following screenshot shows this form:

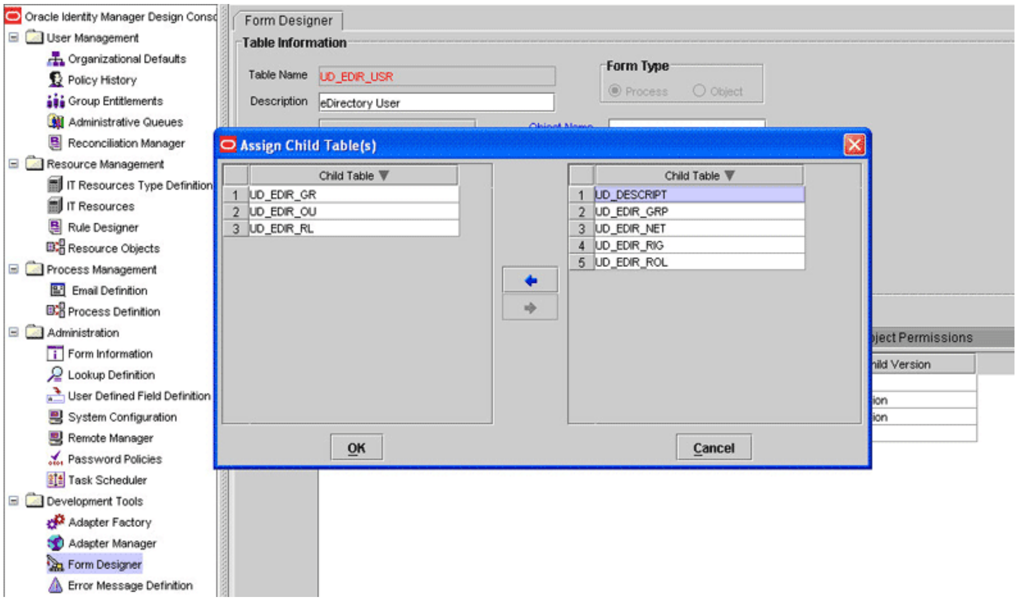


Table Name: UD_EDIR_USR

Description: eDirectory User

	Child Table
1	UD_EDIR_GR
2	UD_EDIR_OU
3	UD_EDIR_RL

	Child Table
1	UD_DESCRIPT
2	UD_EDIR_GRP
3	UD_EDIR_NET
4	UD_EDIR_RIG
5	UD_EDIR_ROL

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

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

   a. Expand **Resource Management**.

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

   c. Perform one of the following steps:

      – For users, search for and open the **eDirectory User** resource object.

      – For groups, search for and open the **eDirectory Group** resource object.

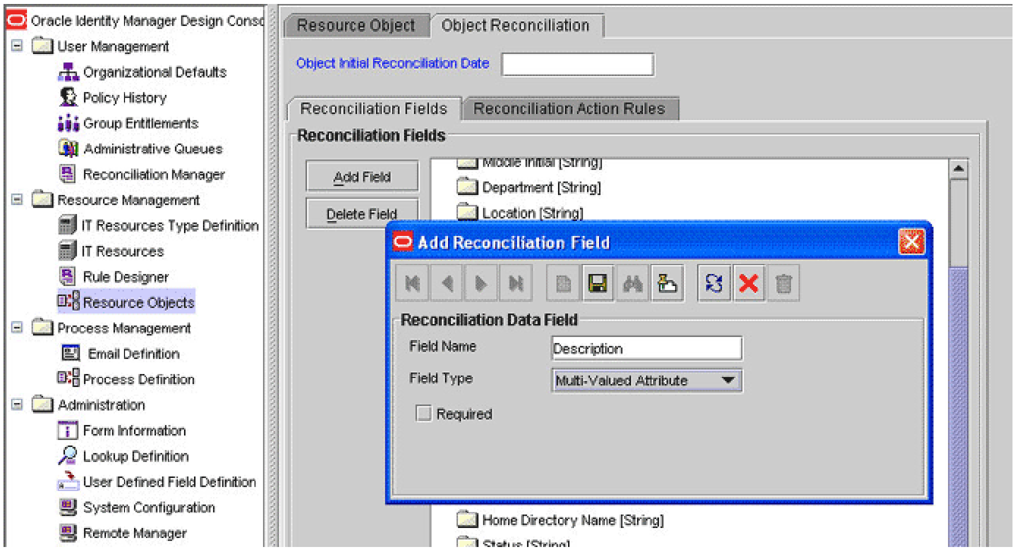
      – For roles, search for and open the **eDirectory Role** resource object.

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

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

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

   The following screenshot shows this form:



Field Name: Description

Field Type: Multi-Valued Attribute

□ Required

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

g. Right-click the newly created attribute.

h. Select **Define Property Fields**.

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

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

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

k. If you are using Oracle Identity Manager release 11.1.*x*, then click **Create Reconciliation Profile.** This copies changes made to the resource object into the MDS.

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

a. Expand **Process Management**.

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

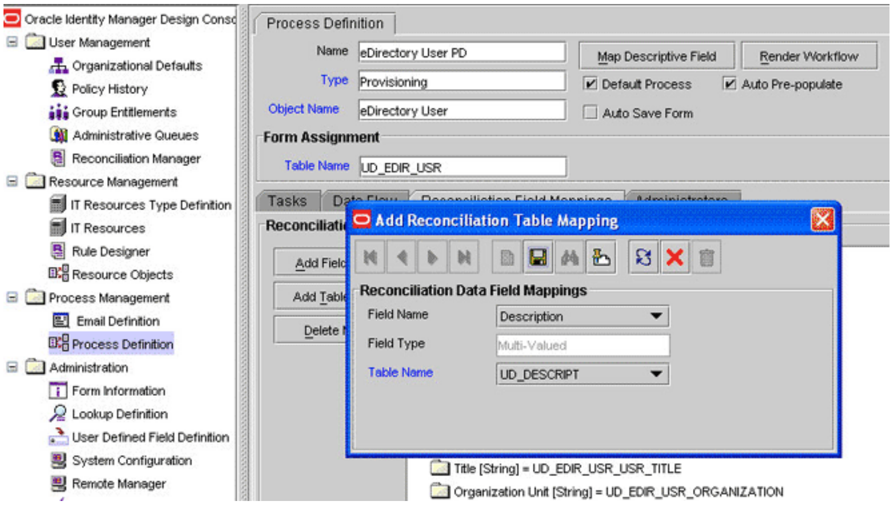
c. Perform one of the following steps:

- For users, search for and open the **eDirectory User PD** process form.
- For groups, search for and open the **eDirectory Group** process form.
- For roles, search for and open the **eDirectory Role** process form.

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

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

The following screenshot shows this form:



Name: eDirectory User PD

Type: Provisioning

Object Name: eDirectory User

☑ Default Process

☑ Auto Pre-populate

□ Auto Save Form

Form Assignment

Table Name: UD_EDIR_USR

Field Name: Description

Field Type: Multi-Valued

Table Name: UD_DESCRIPT

Title [String] = UD_EDIR_USR_USR_TITLE

Organization Unit [String] = UD_EDIR_USR_ORGANIZATION

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

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

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

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

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

   a. Expand **Administration**.

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

   c. For a user attribute, search for and open the **Lookup.EDIR.Configuration** lookup definition. Then, search for the `ldapMultiValAttr` Code Key value.

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

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

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

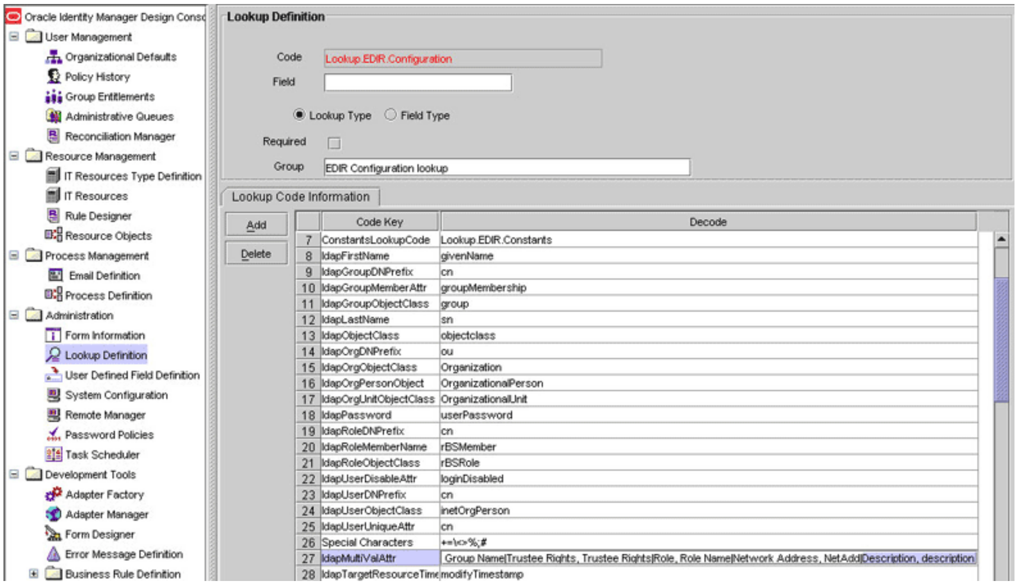
      For example: `Description,description`

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

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

      For example: `Description,description|group,groupname`

      The following screenshot shows this form:



Lookup Definition

Code: Lookup.EDIR.Configuration

Field:

● Lookup Type ○ Field Type

Required □

Group: EDIR Configuration lookup

Lookup Code Information

	Code Key	Decode
7	ConstantsLookupCode	Lookup.EDIR.Constants
8	ldapFirstName	givenName
9	ldapGroupDNPrefix	cn
10	ldapGroupMemberAttr	groupMembership
11	ldapGroupObjectClass	group
12	ldapLastName	sn
13	ldapObjectClass	objectclass
14	ldapOrgDNPrefix	ou
15	ldapOrgObjectClass	Organization
16	ldapOrgPersonObject	OrganizationalPerson
17	ldapOrgUnitObjectClass	OrganizationalUnit
18	ldapPassword	userPassword
19	ldapRoleDNPrefix	cn
20	ldapRoleMemberName	rBSMember
21	ldapRoleObjectClass	rBSRole
22	ldapUserDisableAttr	loginDisabled
23	ldapUserDNPrefix	cn
24	ldapUserObjectClass	inetOrgPerson
25	ldapUserUniqueAttr	cn
26	Special Characters	+=\<>%;#
27	ldapMultiValAttr	Group Name|Trustee Rights, Trustee Rights|Role, Role Name|Network Address, NetAdd|Description, description
28	ldapTargetResourceTim	modifyTimestamp

d. If you are adding a group or role multivalued attribute, then perform one of the following steps:

– For groups, search for and open the **AttrName.ReconGroup.Map.EDIR** lookup definition.

– For roles, search for and open the **AttrName.ReconGroup.Map.EDIR** lookup definition.

e. In the lookup definition, add an entry for the multivalued attribute:

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

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

f. Perform one of the following steps:

– For users, search for and open the **AttrName.Prov.Map.EDIR** lookup definition.

– For groups, search for and open the **AttrName.ProvGroup.EDIR.Map** lookup definition.

– For roles, search for and open the **AttrName.ProvRole.EDIR.Map** lookup definition.

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

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

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

7. If you are using Oracle Identity Manager release 11.1.2 or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Section 2.3.1.3, "Creating a New UI Form" and Section 2.3.1.7, "Updating an Existing Application Instance with a New Form" for the procedures.

If you have added multivalued group or role attributes, then you must specify the Decode values of the newly added attributes as a value of the Multivalue Attribute

attribute of the scheduled task. See Section 3.3.4.2, "Group and Role Reconciliation Scheduled Task" for more information.

4.3 Adding New Attributes for Trusted Source Reconciliation

> **Note:** This section describes an optional procedure. Perform this procedure only if you want to add new multivalued attributes for target resource reconciliation.
>
> You must ensure that new attributes you add for reconciliation contain only string-format data. Binary attributes must not be brought into Oracle Identity Manager natively.

By default, the attributes listed in Section 1.7.1, "User Attributes for Trusted Source Reconciliation" are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new attributes for trusted resource reconciliation as follows:

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new attribute on the Xellerate User process form as follows:
   a. Expand **Administration.**
   b. Double-click **User Defined Field Definition.**
   c. Search for and open the **Users** 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`.

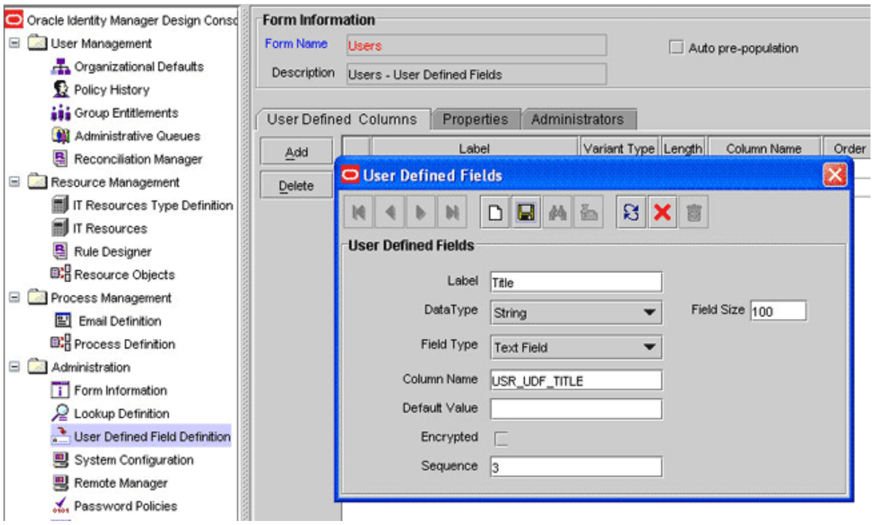
      – From the Data Type list, select **String.**

      – From the Field Type list, select **Text Field.**

      – In the **Column Name** field, enter `USR_UDF_TITLE`.

      – In the **Field Size** field, enter `100`.

      The following screenshot shows this form:



Form Information

Form Name: Users

Description: Users - User Defined Fields

□ Auto pre-population

User Defined Fields

User Defined Fields

Label: Title

DataType: String

Field Size: 100

Field Type: Text Field

Column Name: USR_UDF_TITLE

Default Value:

Encrypted: □

Sequence: 3

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.**

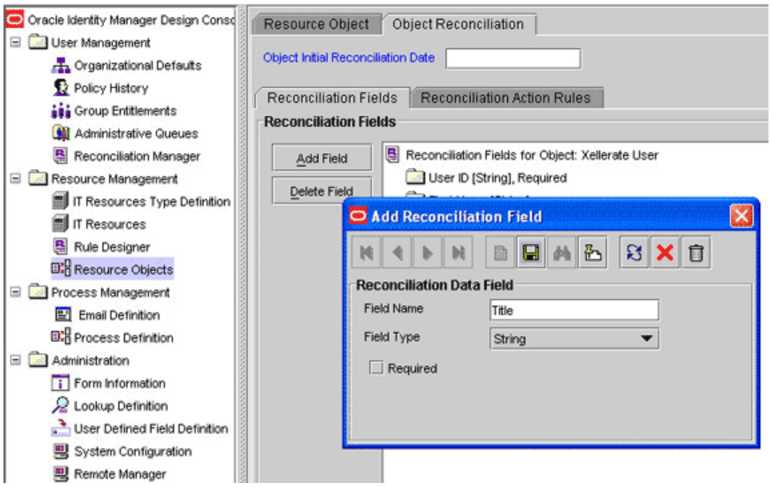
   c. Search for and open the **Xellerate User** resource object.

   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.

      The following screenshot shows this form:



Object Initial Reconciliation Date:

Reconciliation Fields

Reconciliation Fields for Object: Xellerate User

User ID [String], Required

Add Reconciliation Field

Reconciliation Data Field

Field Name: Title

Field Type: String

□ Required

   f. If you are using Oracle Identity Manager release 11.1.*x*, then click **Create Reconciliation Profile.** This copies changes made to the resource object into the MDS.

   g. 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.**

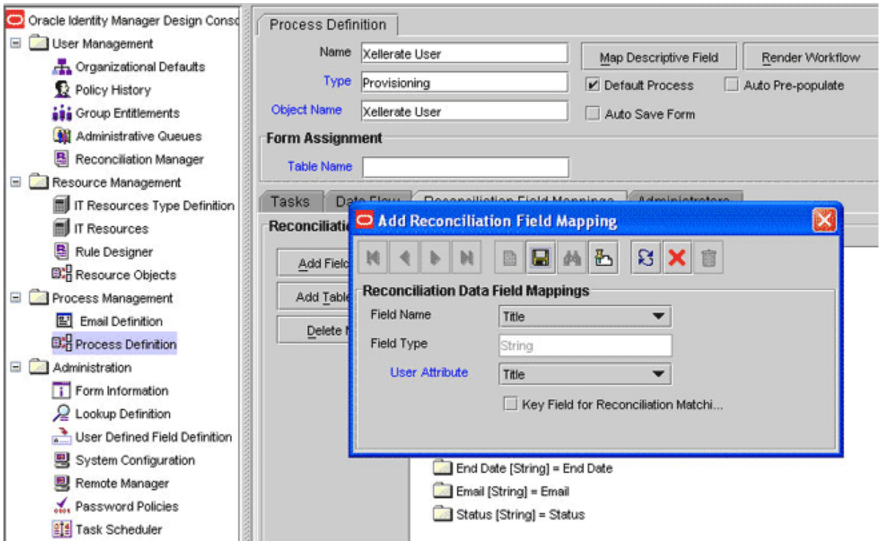
   c. Search for and open the **Xellerate User** process definition.

   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.`

      The following screenshot shows this form:



Name: Xellerate User
Type: Provisioning
Object Name: Xellerate User
☑ Default Process
□ Auto Pre-populate
□ Auto Save Form
Table Name:

Field Name: Title
Field Type: String
User Attribute: Title
□ Key Field for Reconciliation Matchi...

End Date [String] = End Date
Email [String] = Email
Status [String] = Status

   f. Click **Save.**

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

   a. Expand **Administration.**

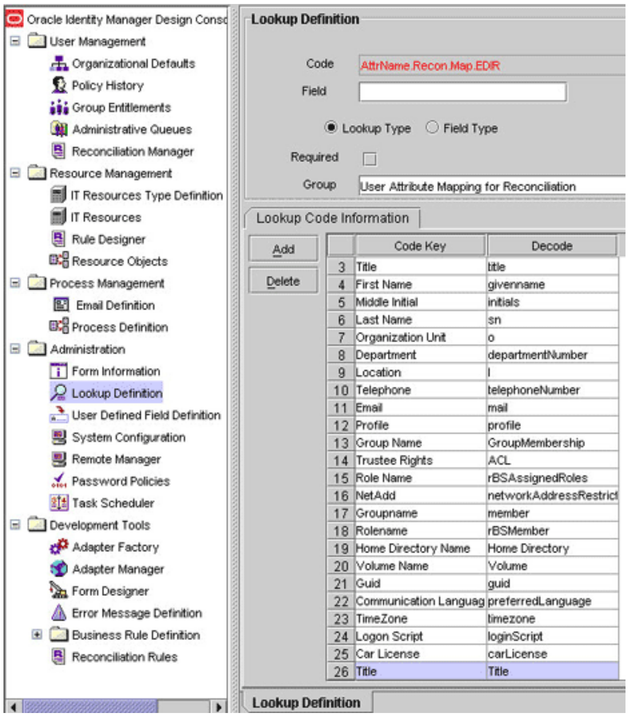
   b. Double-click **Lookup Definition.**

   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.

      The following screenshot shows this form:



Lookup Definition

Code: AttrName.Recon.Map.EDIR

Field:

● Lookup Type ○ Field Type

Required □

Group: User Attribute Mapping for Reconciliation

Lookup Code Information

	Code Key	Decode
3	Title	title
4	First Name	givenname
5	Middle Initial	initials
6	Last Name	sn
7	Organization Unit	o
8	Department	departmentNumber
9	Location	l
10	Telephone	telephoneNumber
11	Email	mail
12	Profile	profile
13	Group Name	GroupMembership
14	Trustee Rights	ACL
15	Role Name	rBSAssignedRoles
16	NetAdd	networkAddressRestrict
17	Groupname	member
18	Rolename	rBSMember
19	Home Directory Name	Home Directory
20	Volume Name	Volume
21	Guid	guid
22	Communication Languag	preferredLanguage
23	TimeZone	timezone
24	Logon Script	loginScript
25	Car License	carLicense
26	Title	Title

e. Click **Save.**

6. If you are using Oracle Identity Manager release 11.1.2 or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Section 2.3.1.3, "Creating a New UI Form" and Section 2.3.1.7, "Updating an Existing Application Instance with a New Form" for the procedures.

4.4 Adding New Attributes for Provisioning Users

Note:

- This section describes an optional procedure. You need not perform this procedure if you do not want to add new user attributes for provisioning.
- Before starting the following procedure, perform Steps 1 and 2 as described in Section 4.1, "Adding New Attributes for Target Resource Reconciliation." If these steps have been performed while adding new attributes for target resource reconciliation, then you need not repeat the steps.

By default, the attributes listed in Section 1.6.1, "User Attributes for Target Resource Reconciliation and Provisioning" are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning.

To add a new attribute for provisioning users:

1. Create an entry for the attribute in the lookup definition for provisioning as follows:

   a. Expand **Administration.**

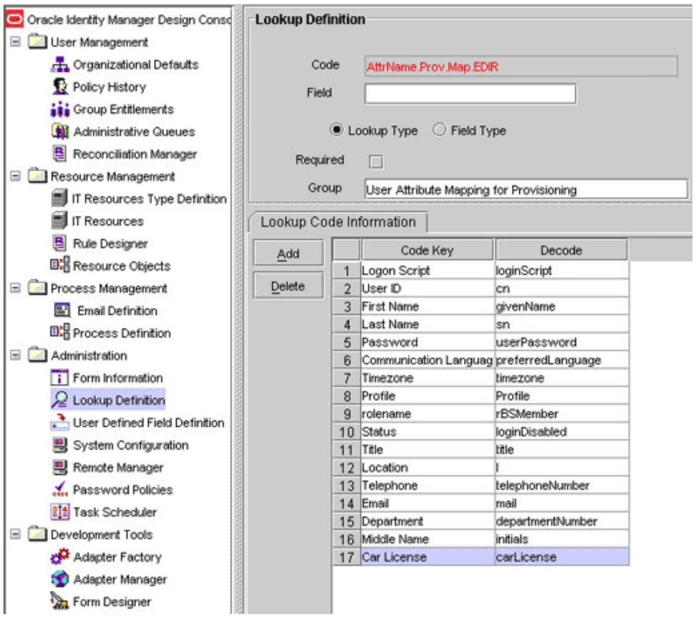
b. Double-click **Lookup Definition.**

c. Search for and open the **AttrName.Prov.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 on the target system.

For example, enter `Car License` in the **Code Key** field and then enter `carLicense` in the **Decode** field.

The following screenshot shows this form:



Code: AttrName.Prov.Map.EDIR

Field:

● Lookup Type ○ Field Type

Required □

Group: User Attribute Mapping for Provisioning

	Code Key	Decode
1	Logon Script	loginScript
2	User ID	cn
3	First Name	givenName
4	Last Name	sn
5	Password	userPassword
6	Communication Languag	preferredLanguage
7	Timezone	timezone
8	Profile	Profile
9	rolename	rBSMember
10	Status	loginDisabled
11	Title	title
12	Location	l
13	Telephone	telephoneNumber
14	Email	mail
15	Department	departmentNumber
16	Middle Name	initials
17	Car License	carLicense

e. Click the Save icon.

2. To enable the update of a new attribute for provisioning a user, create a process task for the new attribute as follows:

a. Expand **Process Management.**

b. Double-click **Process Definition** and open the **eDirectory User PD** process definition.

c. In the process definition, add a new task for updating the field as follows:

– Click **Add** and enter the task name (for example, `Car License Updated`) and the task description.

– In the Task Properties section, select the following fields:

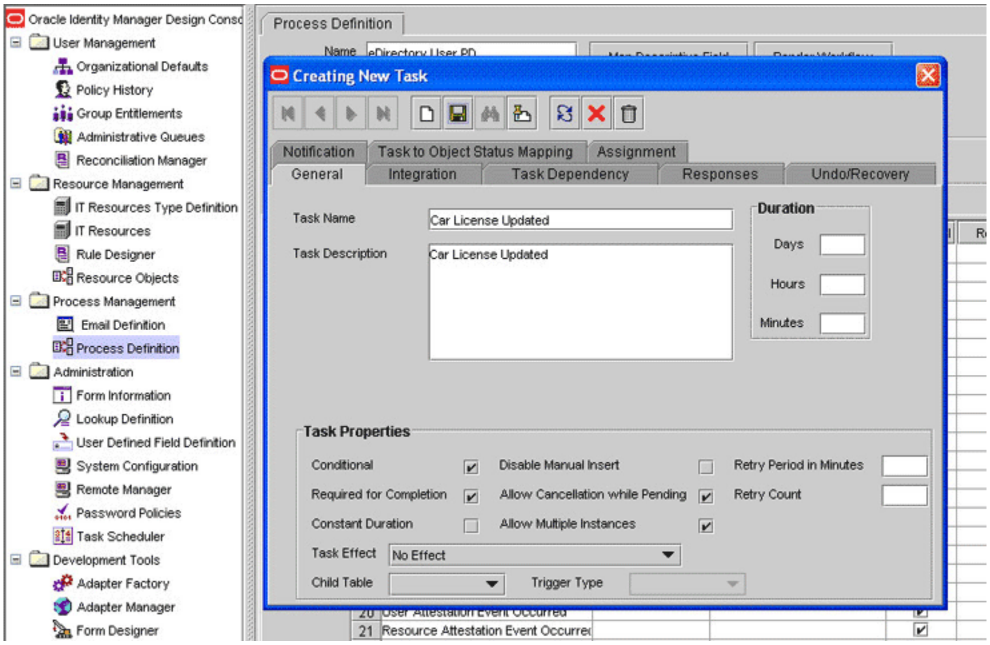
Conditional

Required for Completion

Allow Cancellation while Pending

Allow Multiple Instances

The following screenshot shows this form:



Name: eDirectory User PD

Task Name: Car License Updated

Task Description: Car License Updated

Conditional ☑ Disable Manual Insert ☐

Required for Completion ☑ Allow Cancellation while Pending ☑

Constant Duration ☐ Allow Multiple Instances ☑

Task Effect: No Effect

– Click the Save icon.

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

e. Select the **adpEDIRMODIFYUSER** adapter, click **Save,** and then click **OK** in the message that is displayed.

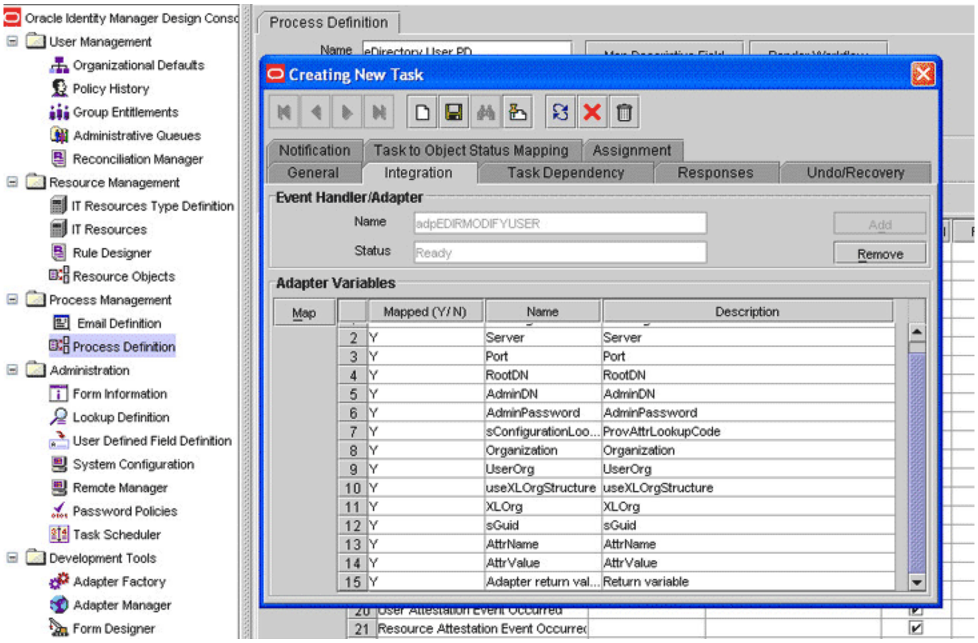
f. To map the adapter variables listed in this table, select the adapter, click **Map,** and then enter the data given in the following table:

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

Variable Name	Data Type	Map To	Qualifier	IT Asset Type	IT Asset Property
Adapter return value	Object	Response code	NA	NA	NA
UserID	String	Process Data	User ID	NA	NA
SGuid	String	Process Data	Guid	NA	NA
AttrName	String	Literal	String	Literal value :carLicense	NA
AttrValue	String	Process Data	Car License **Note:** This is the name of the attribute on the process form.	NA	NA
SSL FLag	String	IT Resources	Server	LDAP Server	SSL
Server	String	IT Resources	Server	LDAP Server	Server Address
RootDN	String	IT Resources	Server	LDAP Server	RootDN

Variable Name	Data Type	Map To	Qualifier	IT Asset Type	IT Asset Property
useXLOrgStructure	String	IT Resources	Server	LDAP Server	Use XL Org Structure
AdminDN	String	IT Resources	Server	LDAP Server	Admin ID
AdminPassword	String	IT Resources	Server	LDAP Server	Admin Password
Port	String	IT Resources	Server	LDAP Server	Port
Organization	String	Literal	String	LiteralValue:null	NA
sConfigurationLookup	String	Literal	String	LiteralValue: Lookup.EDIR.Configuration	NA
UseOrg	String	Process Data	Container DN	NA	NA
XLOrg	String	User Definition	Organization	NA	NA

The following screenshot shows this form:



Name eDirectory User PD

Event Handler/Adapter

Name adpEDIRMODIFYUSER

Status Ready

Adapter Variables

	Mapped (Y/N)	Name	Description
2	Y	Server	Server
3	Y	Port	Port
4	Y	RootDN	RootDN
5	Y	AdminDN	AdminDN
6	Y	AdminPassword	AdminPassword
7	Y	sConfigurationLoo...	ProvAttrLookupCode
8	Y	Organization	Organization
9	Y	UserOrg	UserOrg
10	Y	useXLOrgStructure	useXLOrgStructure
11	Y	XLOrg	XLOrg
12	Y	sGuid	sGuid
13	Y	AttrName	AttrName
14	Y	AttrValue	AttrValue
15	Y	Adapter return val...	Return variable

20 User Attestation Event Occurred ☑
21 Resource Attestation Event Occurre ☑

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

3. Update the request dataset.

> **Note:** Perform steps 3 through 5 only if you want to perform request-based provisioning.

When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:

a. In a text editor, open the XML file located in the *OIM_HOME*/DataSet/file directory for editing.

b. Add the AttributeReference element and specify values for the mandatory attributes of this element.

See Also: The "Configuring Requests" chapter of the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* guide for more information about creating and updating request datasets

For example, if you added Car License as an attribute on the process form, then enter the following line:

```
<AttributeReference
name = "Car License"
attr-ref = "Car License"
type = "String"
widget = "text"
length = "100"
available-in-bulk = "false"/>
```

In this AttributeReference element:

– For the name attribute, enter the value in the Name column of the process form without the tablename prefix.

  For example, if UD_EDIR_USR_CARLICENSE is the value in the Name column of the process form, then you must specify `Car License` as the value of the name attribute in the AttributeReference element.

– For the attr-ref attribute, enter the value that you entered in the Field Label column of the process form.

– For the type attribute, enter the value that you entered in the Variant Type column of the process form.

– For the widget attribute, enter the value that you entered in the Field Type column of the process form.

– For the length attribute, enter the value that you entered in the Length column of the process form.

– For the available-in-bulk attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

If you add more than one attribute on the process form, then repeat this step for each attribute that you add.

c. Save and close the XML file.

4. Run the PurgeCache utility to clear content related to request datasets from the server cache.

   See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

5. If you are using Oracle Identity Manager release prior to 11.1.2, import into MDS, the request dataset definitions in XML format.

   See Section 2.3.12.2, "Importing Request Datasets into MDS" for detailed information about the procedure.

6. If you are using Oracle Identity Manager release 11.1.2 or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Section 2.3.1.3, "Creating a New UI Form" and Section 2.3.1.7, "Updating an Existing Application Instance with a New Form" for the procedures.

4.5 Adding New Attributes for Provisioning Groups and Roles

By default, the attributes listed in Section 1.6.2, "Group Attributes for Target Resource Reconciliation and Provisioning" are mapped for provisioning of groups between Oracle Identity Manager and the target system. Similarly, by default, the attributes listed in Section 1.6.3, "Role Attributes for Target Resource Reconciliation and Provisioning" are mapped for provisioning of roles between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning groups and roles.

To add a new attribute for provisioning a group or role:

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new attribute on the process form as follows:

   a. Open the Form Designer form.

   b. Perform one of the following steps:

   Search for and open the **UD_EDIR_GR** form.

   Search for and open the **UD_EDIR_RL** form.

   c. Create another version of the form.

   d. Add the new attribute on the form.

   The following screenshot shows this form:

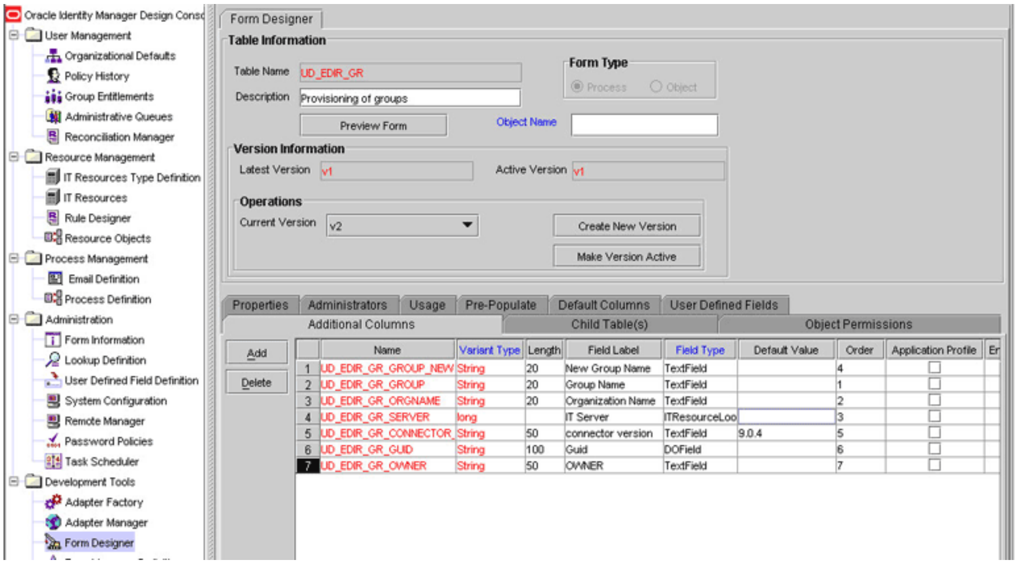


Table Information

Table Name: UD_EDIR_GR

Description: Provisioning of groups

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: v1

Active Version: v1

Operations

Current Version: v2

	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Application Profile	Er
1	UD_EDIR_GR_GROUP_NEW	String	20	New Group Name	TextField		4	□	
2	UD_EDIR_GR_GROUP	String	20	Group Name	TextField		1	□	
3	UD_EDIR_GR_ORGNAME	String	20	Organization Name	TextField		2	□	
4	UD_EDIR_GR_SERVER	long		IT Server	ITResourceLoo		3	□	
5	UD_EDIR_GR_CONNECTOR_	String	50	connector version	TextField	9.0.4	5	□	
6	UD_EDIR_GR_GUID	String	100	Guid	DOField		6	□	
7	UD_EDIR_GR_OWNER	String	50	OWNER	TextField		7	□	

   e. Save the form.

   f. Make the version active, and then close the form.

3. In the lookup definition for provisioning, create an entry for the new attribute as follows:

   a. Open the Lookup Definition form.

   b. Perform one of the following steps:

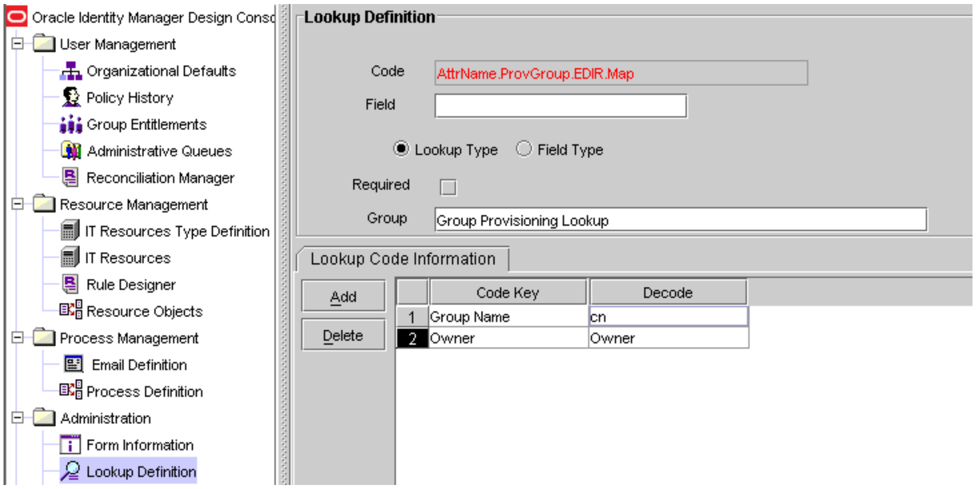
   – Search for and open the **AttrName.ProvGroup.EDIR.Map** lookup definition.

- Search for and open the **AttrName.ProvRole.EDIR.Map** lookup definition.

c. In the lookup definition, create an entry for the new attribute:

- **Code Key:** Enter the name of the attribute that you add on the process form.
- **Decode:** Enter the name of the attribute displayed on the target system, which you recorded earlier in this procedure.

The following screenshot shows this form:



Lookup Definition

Code: AttrName.ProvGroup.EDIR.Map

Field:

● Lookup Type ○ Field Type

Required □

Group: Group Provisioning Lookup

Lookup Code Information

	Code Key	Decode
1	Group Name	cn
2	Owner	Owner

4. To test whether or not you can use the newly added attribute for provisioning, log in to the Oracle Identity Manager Administrative and User Console and perform a provisioning operation in which you specify a value for the newly added attribute.

5. To create a process task for the new multivalued attribute:

a. Log in to the Oracle Identity Manager Design Console.

b. Expand **Process Management**.

c. Perform one of the following steps:

- Double-click **Process Definition** and open the **eDirectory Group** process definition.
- Double-click **Process Definition** and open the **eDirectory Role** process definition.

d. In the process definition, add a task for setting a value for the attribute:

- Click **Add**, enter the name of the task for adding multivalued attributes, and then enter the task description.
- In the Task Properties section, select the following fields:

Conditional

Required for Completion

Allow Cancellation while Pending

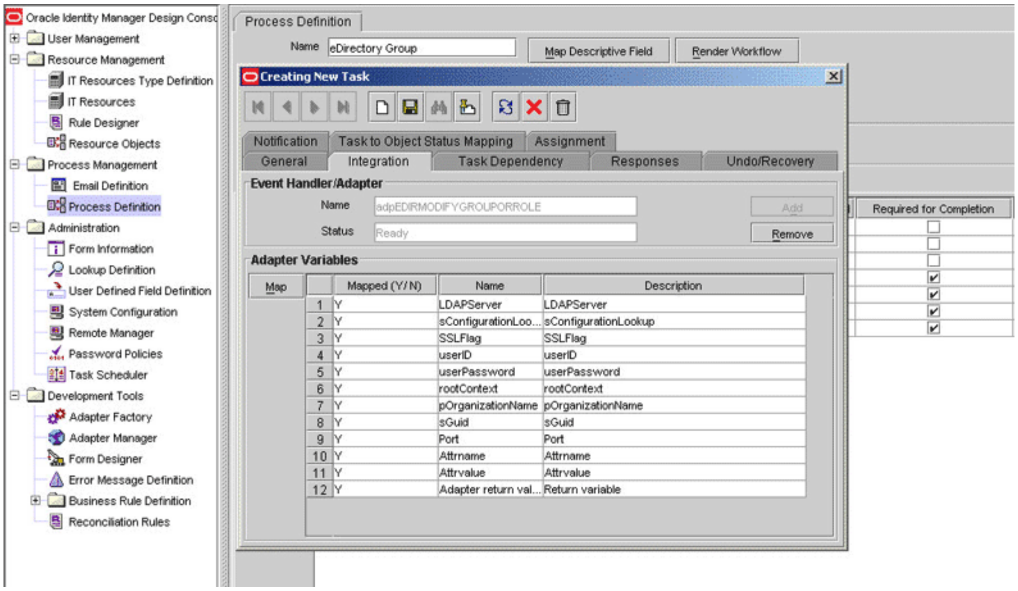
Allow Multiple Instances

Select the child table from the list.

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

- On the Integration tab, click **Add**, and then click **Adapter**.
- Select the **adpEDIRMODIFYGROUPORROLE** adapter, click **Save**, and then click **OK** in the message.
- To map the adapter variables listed in this table, select the adapter, click **Map**, and then enter the data given in the following table:

Variable Name	Data Type	Map To	Qualifier	IT Asset Type	IT Asset Property
Adapter return value	Object	Response code	NA	NA	NA
UserID	String	Process Data	User ID	NA	NA
SGuid	String	Process Data	Guid	NA	NA
AttrName	String	Literal	String	Literal value :carLicense	NA
AttrValue	String	Process Data	Owner **Note:** The name of the attribute in the process form	NA	NA
SSL FLag	String	IT Resources	Server	LDAP Server	SSL
Server	String	IT Resources	Server	LDAP Server	Server Address
RootDN	String	IT Resources	Server	LDAP Server	RootDN
useXLOrgStructure	String	IT Resources	Server	LDAP Server	Use XL Org Structure
AdminDN	String	IT Resources	Server	LDAP Server	Admin ID
AdminPassword	String	IT Resources	Server	LDAP Server	Admin Password
Port	String	IT Resources	Server	LDAP Server	Port
Organization	String	Literal	String	LiteralValue:null	NA
sConfigurationLookup	String	Literal	String	LiteralValue: Lookup.EDIR.Configuration	NA
UseOrg	String	Process Data	Container DN	NA	NA
XLOrg	String	User Definition	Organization	NA	NA



Name: eDirectory Group

Creating New Task

Event Handler/Adapter

Name: adpEDIRMODIFYGROUPORROLE

Status: Ready

Adapter Variables

	Mapped (Y/N)	Name	Description
1	Y	LDAPServer	LDAPServer
2	Y	sConfigurationLoo...	sConfigurationLookup
3	Y	SSLFlag	SSLFlag
4	Y	userID	userID
5	Y	userPassword	userPassword
6	Y	rootContext	rootContext
7	Y	pOrganizationName	pOrganizationName
8	Y	sGuid	sGuid
9	Y	Port	Port
10	Y	Attrname	Attrname
11	Y	Attrvalue	Attrvalue
12	Y	Adapter return val...	Return variable

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

Note: Perform steps 6 through 8 only if you want to perform request-based provisioning.

6. Update the request dataset.

   When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:

   a. In a text editor, open the XML file located in the *OIM_HOME*/DataSet/file directory for editing.

   b. Add the AttributeReference element and specify values for the mandatory attributes of this element.

      See Also: The "Configuring Requests" chapter of the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* guide for more information about creating and updating request datasets

      For example, while performing Step 2 of this procedure, if you added Owner as an attribute on the process form, then enter the following line:

```
<AttributeReference
name = "Owner"
attr-ref = "Owner"
type = "String"
widget = "text"
length = "50"
available-in-bulk = "false"/>
```

      In this AttributeReference element:

      – For the name attribute, enter the value in the Name column of the process form without the tablename prefix.

For example, if UD_EDIR_GR_OWNER is the value in the Name column of the process form, then you must specify `Owner` as the value of the name attribute in the AttributeReference element.

- For the attr-ref attribute, enter the value that you entered in the Field Label column of the process form while performing Step 2.
- For the type attribute, enter the value that you entered in the Variant Type column of the process form while performing Step 2.
- For the widget attribute, enter the value that you entered in the Field Type column of the process form, while performing Step 2.
- For the length attribute, enter the value that you entered in the Length column of the process form while performing Step 2.
- For the available-in-bulk attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

While performing Step 2, if you added more than one attribute on the process form, then repeat this step for each attribute added.

c. Save and close the XML file.

7. Run the PurgeCache utility to clear content related to request datasets from the server cache.

   See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

8. If you are using Oracle Identity Manager release prior to 11.1.2, import into MDS, the request dataset definitions in XML format.

   See Section 2.3.12.2, "Importing Request Datasets into MDS" for detailed information about the procedure.

9. If you are using Oracle Identity Manager release 11.1.2 or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Section 2.3.1.3, "Creating a New UI Form" and Section 2.3.1.7, "Updating an Existing Application Instance with a New Form" for the procedures.

4.6 Adding New Multivalued Attributes for Provisioning

Note: This section describes an optional procedure. Perform this procedure only if you want to add new multivalued fields for provisioning. This procedure can be applied to add user, group, or role attributes.

By default, only the UserGroup, UserRole, User Profile, and Network Address Restriction multivalued attributes are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can add new multivalued attributes for provisioning.

By default, no multivalued attributes are mapped for provisioning between Oracle Identity Manager and the target system for groups and roles. If required, you can add new multivalued group or role attributes for reconciliation and provisioning.

To add a new multivalued attribute for provisioning:

> **Note:** If you have already performed Steps 1 through 3 of Section 4.2, "Adding New Multivalued Attributes for Target Resource Reconciliation," then you need not repeat the steps in the following procedure. Perform only the remaining steps of this procedure.

1. Log in to the Oracle Identity Manager Design Console.
2. Create a form for the multivalued attribute as follows:
   a. Expand **Development Tools**.
   b. Double-click **Form Designer**.
   c. Create a form by specifying a table name and description, and then click **Save**.
   d. Click **Add** and enter the details of the attribute.

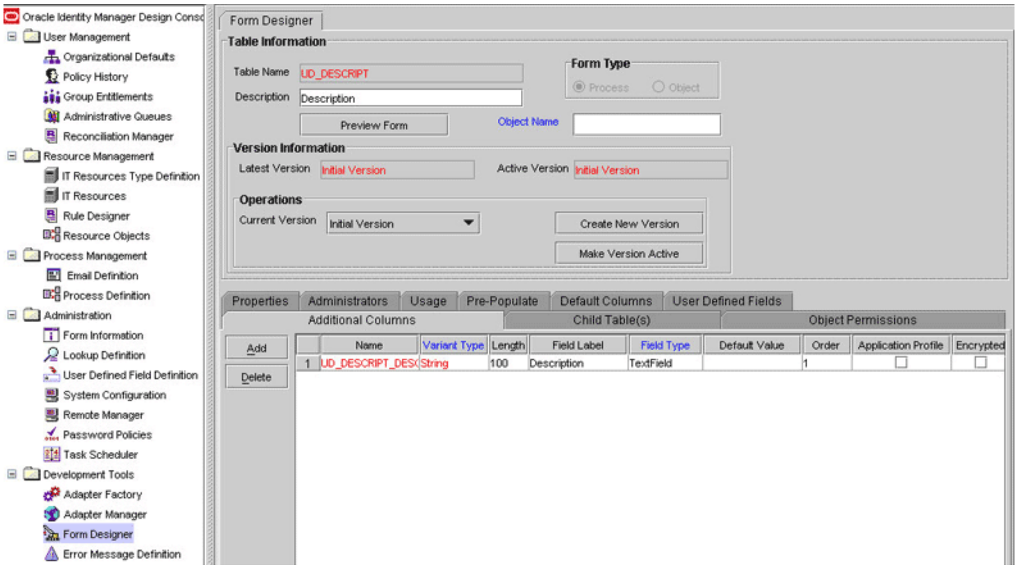


Table Name: UD_DESCRIPT
Description: Description
Object Name:
Latest Version: Initial Version
Active Version: Initial Version
Current Version: Initial Version

	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Application Profile	Encrypted
1	UD_DESCRIPT_DES(	String	100	Description	TextField		1	□	□

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

3. Add the form created for the multivalued attribute as a child form of the process form as follows:
   a. Perform one of the following steps:
      – For users, search for and open the **UD_EDIR_USR** process form.
      – For groups, search for and open the **UD_EDIR_GR** process form.
      – For roles, search for and open the **UD_EDIR_RL** process form.
   b. Click **Create New Version**.
   c. Click the **Child Table(s)** tab.
   d. Click **Assign**.
   e. In the Assign Child Tables dialog box, select the newly created child form, click the right arrow, and then click **OK**.

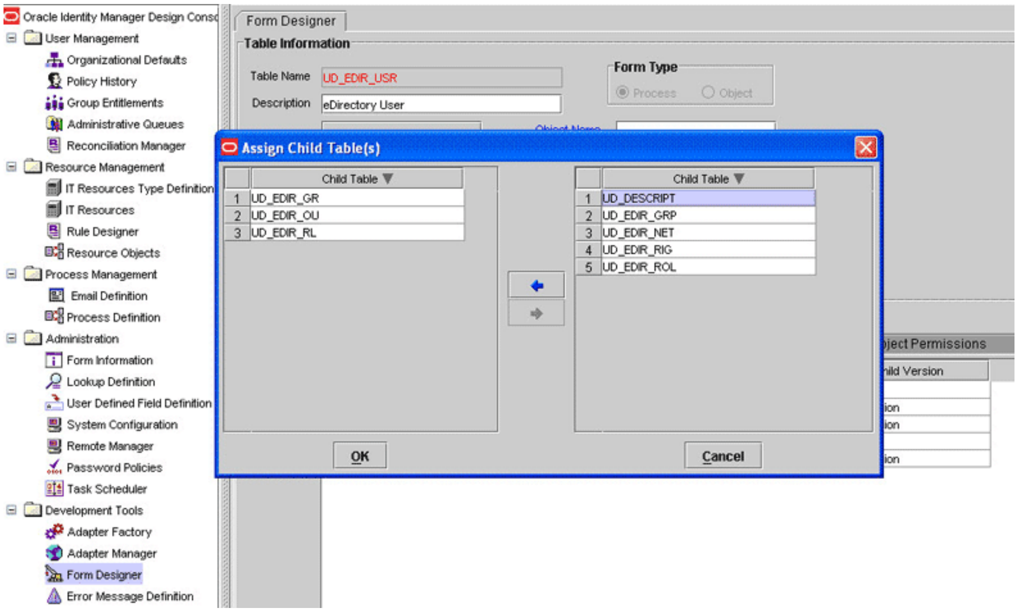


Table Name: UD_EDIR_USR

Description: eDirectory User

Form Type: ● Process ○ Object

	Child Table
1	UD_EDIR_GR
2	UD_EDIR_OU
3	UD_EDIR_RL

	Child Table
1	UD_DESCRIPT
2	UD_EDIR_GRP
3	UD_EDIR_NET
4	UD_EDIR_RIG
5	UD_EDIR_ROL

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

4. To create a process task for the new multivalued attribute:

   a. Expand **Process Management**.

   b. Double-click **Process Definition**, and then perform one of the following steps:

      – For users, open the **eDirectory User PD** process definition.

      – For groups, open the **eDirectory Group** process definition.

      – For roles, open the **eDirectory Role** process definition.

   c. In the process definition, add a task for setting a value for the attribute:

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

      – In the Task Properties section, select the following fields:

        Conditional

        Required for Completion

        Allow Cancellation while Pending

        Allow Multiple Instances

        Select the child table from the list.

        For the example described earlier, select **Description** from the list.

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

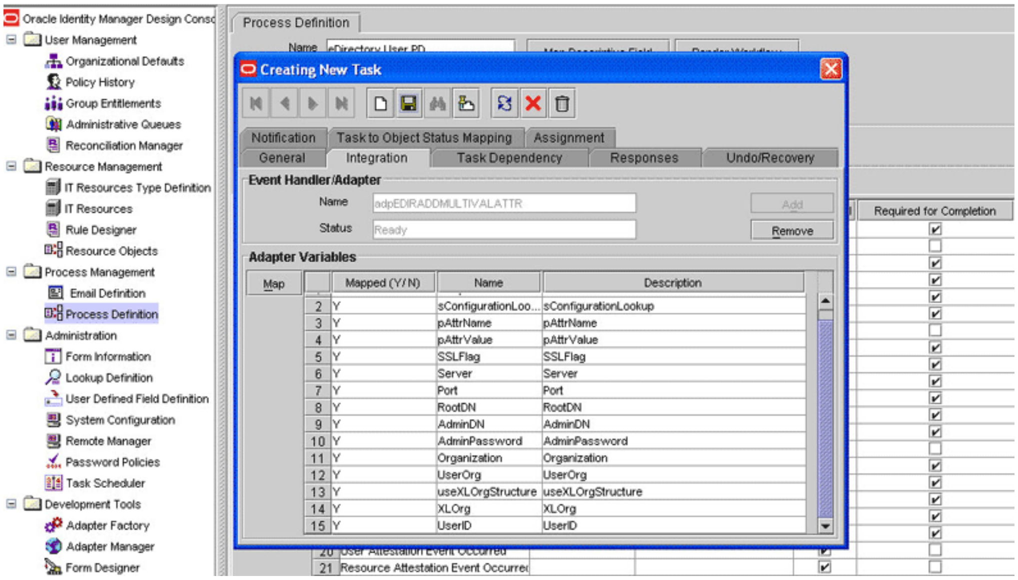
      – On the **Integration** tab, click **Add**, and then click **Adapter**.

      – Select the **adpEDIRADDMULTIVALATTR** adapter, click **Save**, and then click **OK** in the message.

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

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

Variable Name	Data Type	Map To	Qualifier	IT Asset Type	IT Asset Property
Adapter return value	Object	Response code	NA	NA	NA
UserID	String	Process Data	User ID	NA	NA
SGuid	String	Process Data	Guid	NA	NA
pAttrName	String	Literal	String	Literal value :description	NA
pAttrValue	String	Process Data	Description Note: the name of the attribute in the process form	NA	NA
SSL FLag	String	IT Resources	Server	LDAP Server	SSL
Server	String	IT Resources	Server	LDAP Server	Server Address
RootDN	String	IT Resources	Server	LDAP Server	RootDN
useXLOrgStructure	String	IT Resources	Server	LDAP Server	Use XL Org Structure
AdminDN	String	IT Resources	Server	LDAP Server	Admin ID
AdminPassword	String	IT Resources	Server	LDAP Server	Admin Password
Port	String	IT Resources	Server	LDAP Server	Port
Organization	String	Literal	String	LiteralValue:null	NA
sConfigurationLookup	String	Literal	String	LiteralValue: Lookup.EDIR.Configuration	NA
UseOrg	String	Process Data	Container DN	NA	NA
XLOrg	String	User Definition	Organization	NA	NA



Name eDirectory User PD

Event Handler/Adapter

Name adpEDIRADDMULTIVALATTR

Status Ready

Adapter Variables

	Mapped (Y/N)	Name	Description
2	Y	sConfigurationLoo...	sConfigurationLookup
3	Y	pAttrName	pAttrName
4	Y	pAttrValue	pAttrValue
5	Y	SSLFlag	SSLFlag
6	Y	Server	Server
7	Y	Port	Port
8	Y	RootDN	RootDN
9	Y	AdminDN	AdminDN
10	Y	AdminPassword	AdminPassword
11	Y	Organization	Organization
12	Y	UserOrg	UserOrg
13	Y	useXLOrgStructure	useXLOrgStructure
14	Y	XLOrg	XLOrg
15	Y	UserID	UserID

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

d. In the process definition, add a task for removing the value of the attribute by performing Step c. While performing Step c, select the **adpEDIRREMOVEMULTIVALATTR** adapter.

e. In the process definition, add a task for updating the value of the attribute by performing Step c.

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

Note: Perform steps 5 through 7 only if you want to perform request-based provisioning.

---

5. Update the request dataset.

When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:

a. In a text editor, open the XML file located in the *OIM_HOME*/DataSet/file directory for editing.

b. Add the AttributeReference element and specify values for the mandatory attributes of this element.

See Also: The "Configuring Requests" chapter of the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* guide for more information about creating and updating request datasets

For example, while performing Step 2 of this procedure, if you added Description as an attribute on the process form, then enter the following line:

```
<AttributeReference
name = "Description"
attr-ref = "Description"
type = "String"
```

```
widget = "text"
length = "100"
available-in-bulk = "false"/>
```

In this AttributeReference element:

- For the name attribute, enter the value in the Name column of the process form without the tablename prefix.

  For example, if UD_DESCRIPT_DESCRIPTION is the value in the Name column of the process form, then you must specify `Description` as the value of the name attribute in the AttributeReference element.
- For the attr-ref attribute, enter the value that you entered in the Field Label column of the process form while performing Step 2.
- For the type attribute, enter the value that you entered in the Variant Type column of the process form while performing Step 2.
- For the widget attribute, enter the value that you entered in the Field Type column of the process form while performing Step 2.
- For the length attribute, enter the value that you entered in the Length column of the process form while performing Step 2.
- For the available-in-bulk attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

While performing Step 2, if you add more than one attribute on the process form, then repeat this step for each attribute that you add.

c. Save and close the XML file.

6. If you are using Oracle Identity Manager release prior to 11.1.2, import into MDS, the request dataset definitions in XML format.

   See Section 2.3.12.2, "Importing Request Datasets into MDS" for detailed information about the procedure.

7. If you are using Oracle Identity Manager release 11.1.2 or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Section 2.3.1.3, "Creating a New UI Form" and Section 2.3.1.7, "Updating an Existing Application Instance with a New Form" for the procedures.

4.7 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 Lookup.EDIR.Configuration lookup definition. Similarly, the group and role object classes are the values of the ldapGroupObjectClass and ldapRoleObjectClass attributes in the Lookup.EDIR.Configuration 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 **Lookup.EDIR.Configuration** 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 column value of the ldapGroupObjectClass Code Key.
   - To add an object class for a role, add the object class name to the Decode column value of the ldapRoleObjectClass Code Key.
4. Click the Save icon.

4.8 Adding New Object Classes for Provisioning and Reconciliation

To add a new object class for provisioning and reconciliation:

- Section 4.8.1, "Adding the Attributes of the Object Class to the Process Form"
- Section 4.8.2, "Adding the Object Class and its Attributes to the Lookup Definition for Provisioning"
- Section 4.8.3, "Adding the Attributes of the Object Class to the Resource Object"
- Section 4.8.4, "Adding Attributes of the Object Class to the Provisioning Process".
- Section 4.8.5, "Adding Custom Object Classes for Provisioning Organization, Groups, and Roles"

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

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

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Development Tools** folder.
3. Double-click **Form Designer.**
4. Search for and open the **UD_EDIR_USR** process form.

5. Click **Create New Version,** and then click **Add.**

6. Enter the details of the attribute.

   For example, if you are adding the Associated Domain attribute, enter UD_EDIR_USR_ASSOCIATEDDOMAIN in the **Name** field and then enter the other details of this attribute.

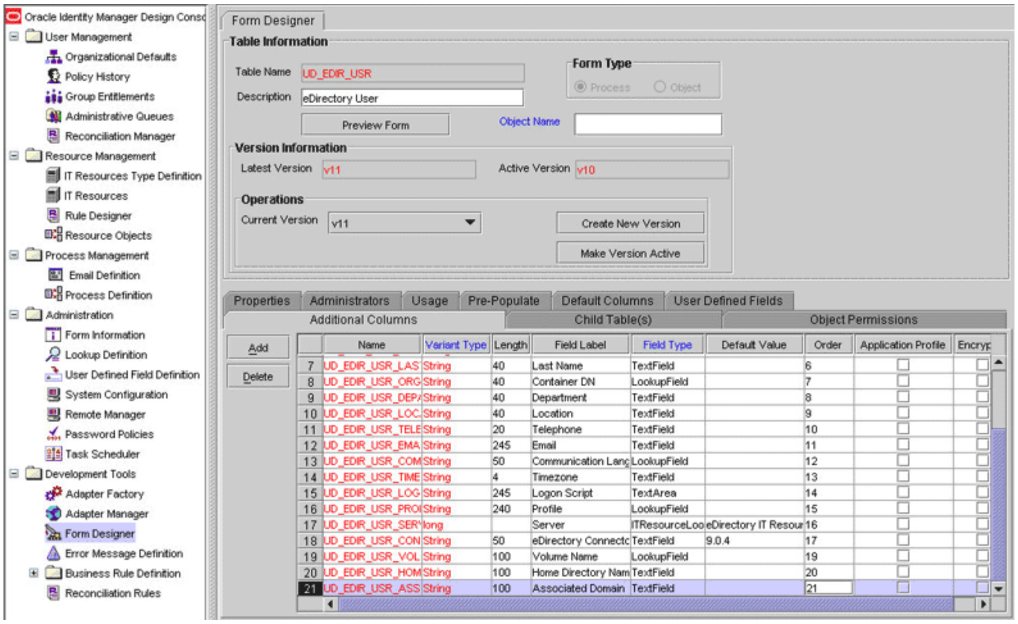


Table Information

Table Name: UD_EDIR_USR

Description: eDirectory User

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: v11

Active Version: v10

Operations

Current Version: v11

	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Application Profile	Encryp
7	UD_EDIR_USR_LAS	String	40	Last Name	TextField		6	□	□
8	UD_EDIR_USR_ORG	String	40	Container DN	LookupField		7	□	□
9	UD_EDIR_USR_DEP/	String	40	Department	TextField		8	□	□
10	UD_EDIR_USR_LOC	String	40	Location	TextField		9	□	□
11	UD_EDIR_USR_TELE	String	20	Telephone	TextField		10	□	□
12	UD_EDIR_USR_EMA	String	245	Email	TextField		11	□	□
13	UD_EDIR_USR_COM	String	50	Communication Lang	LookupField		12	□	□
14	UD_EDIR_USR_TIME	String	4	Timezone	TextField		13	□	□
15	UD_EDIR_USR_LOG	String	245	Logon Script	TextArea		14	□	□
16	UD_EDIR_USR_PRO	String	240	Profile	LookupField		15	□	□
17	UD_EDIR_USR_SER	long		Server	ITResourceLoo	eDirectory IT Resour	16	□	□
18	UD_EDIR_USR_CON	String	50	eDirectory Connectc	TextField	9.0.4	17	□	□
19	UD_EDIR_USR_VOL	String	100	Volume Name	LookupField		19	□	□
20	UD_EDIR_USR_HOM	String	100	Home Directory Nam	TextField		20	□	□
21	UD_EDIR_USR_ASS	String	100	Associated Domain	TextField		21	□	□

7. Click the Save icon, and then click **Make Version Active.**

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

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

1. Expand the **Administration** folder.

2. Double-click **Lookup Definition.**

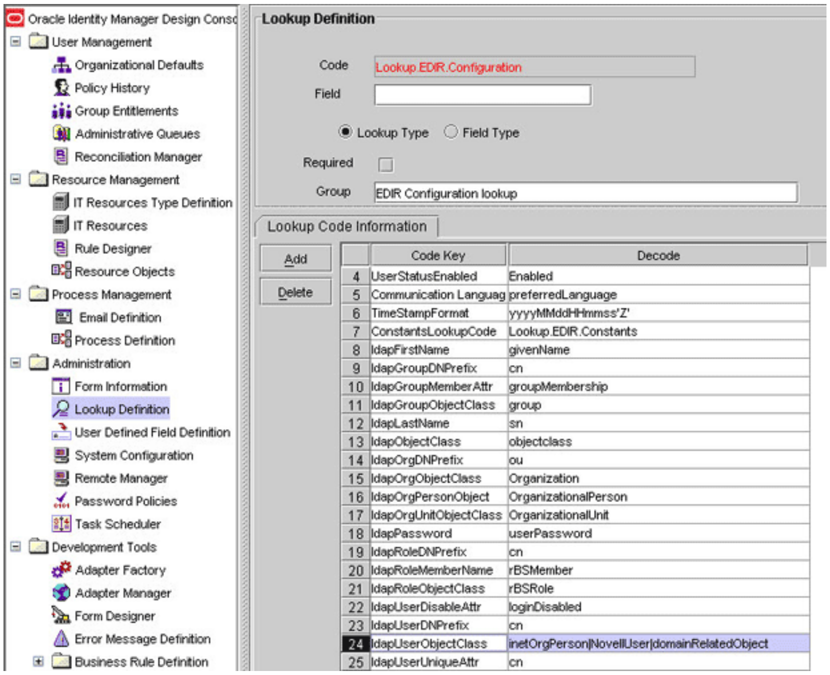
3. Search for and open the **Lookup.EDIR.Configuration** lookup definition.

4. Add the object class name to the Decode value of the ldapUserObjectClass Code Key.

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

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

   ```
   top|inetorgperson|NovellUser|domainRelatedObject
   ```



Lookup Definition

Code: Lookup.EDIR.Configuration

Field:

● Lookup Type ○ Field Type

Required □

Group: EDIR Configuration lookup

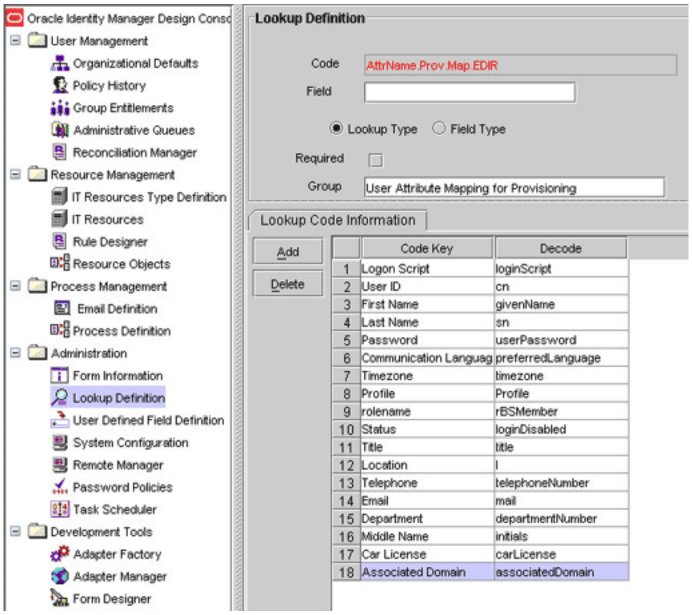
Lookup Code Information

	Code Key	Decode
4	UserStatusEnabled	Enabled
5	Communication Languag	preferredLanguage
6	TimeStampFormat	yyyyMMddHHmmss'Z'
7	ConstantsLookupCode	Lookup.EDIR.Constants
8	ldapFirstName	givenName
9	ldapGroupDNPrefix	cn
10	ldapGroupMemberAttr	groupMembership
11	ldapGroupObjectClass	group
12	ldapLastName	sn
13	ldapObjectClass	objectclass
14	ldapOrgDNPrefix	ou
15	ldapOrgObjectClass	Organization
16	ldapOrgPersonObject	OrganizationalPerson
17	ldapOrgUnitObjectClass	OrganizationalUnit
18	ldapPassword	userPassword
19	ldapRoleDNPrefix	cn
20	ldapRoleMemberName	rBSMember
21	ldapRoleObjectClass	rBSRole
22	ldapUserDisableAttr	loginDisabled
23	ldapUserDNPrefix	cn
24	ldapUserObjectClass	inetOrgPerson|NovellUser|domainRelatedObject
25	ldapUserUniqueAttr	cn

5. Expand the **Administration** folder.
6. Double-click **Lookup Definition**.
7. Search for and open the **AttrName.Prov.Map.EDIR** lookup definition.
8. Click **Add** and then enter the Code Key and Decode values for an attribute of the object class. The Code Key value must be the name of the field on the process form and Decode value must be the name of the field on the target system.

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

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



Lookup Definition

Code: AttrName.Prov.Map.EDIR

Field:

● Lookup Type ○ Field Type

Required □

Group: User Attribute Mapping for Provisioning

Lookup Code Information

	Code Key	Decode
1	Logon Script	loginScript
2	User ID	cn
3	First Name	givenName
4	Last Name	sn
5	Password	userPassword
6	Communication Languag	preferredLanguage
7	Timezone	timezone
8	Profile	Profile
9	rolename	rBSMember
10	Status	loginDisabled
11	Title	title
12	Location	l
13	Telephone	telephoneNumber
14	Email	mail
15	Department	departmentNumber
16	Middle Name	initials
17	Car License	carLicense
18	Associated Domain	associatedDomain

9. Click **Save.**

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

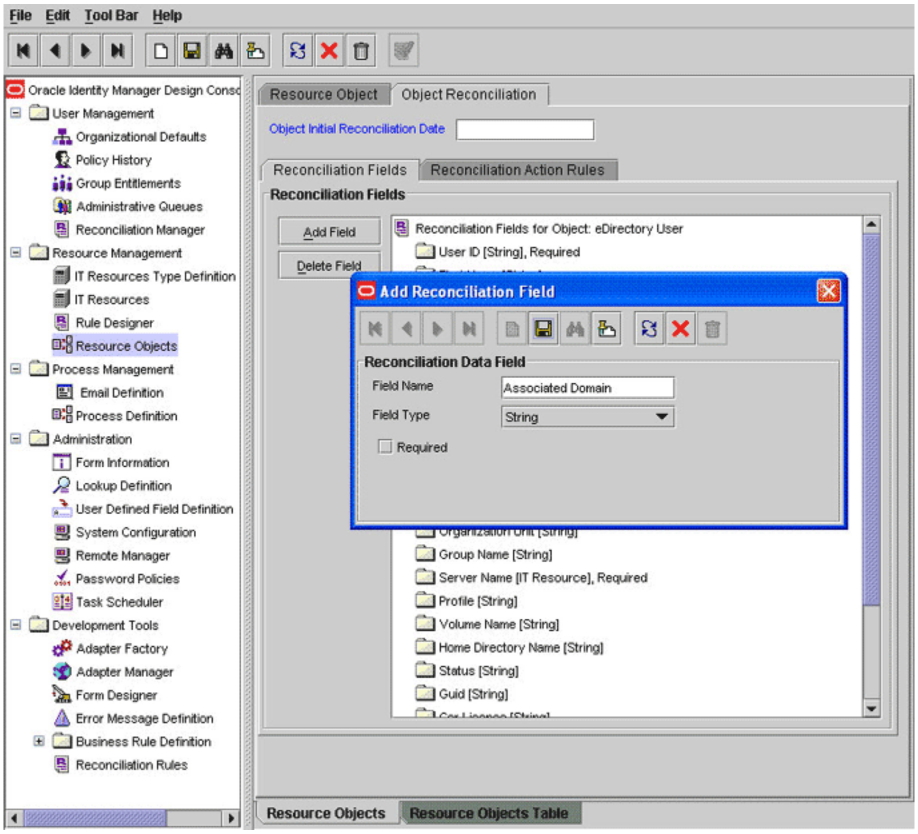
To add the attributes of the object class to the resource object:

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

---

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

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



Reconciliation Fields

Reconciliation Fields for Object: eDirectory User
User ID [String], Required
Organization Unit [String]
Group Name [String]
Server Name [IT Resource], Required
Profile [String]
Volume Name [String]
Home Directory Name [String]
Status [String]
Guid [String]
Car License [String]

Reconciliation Data Field

Field Name: Associated Domain

Field Type: String

☐ Required

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

6. If you are using Oracle Identity Manager release 11.1.*x*, then click **Create Reconciliation Profile.** This copies changes made to the resource object into the MDS.

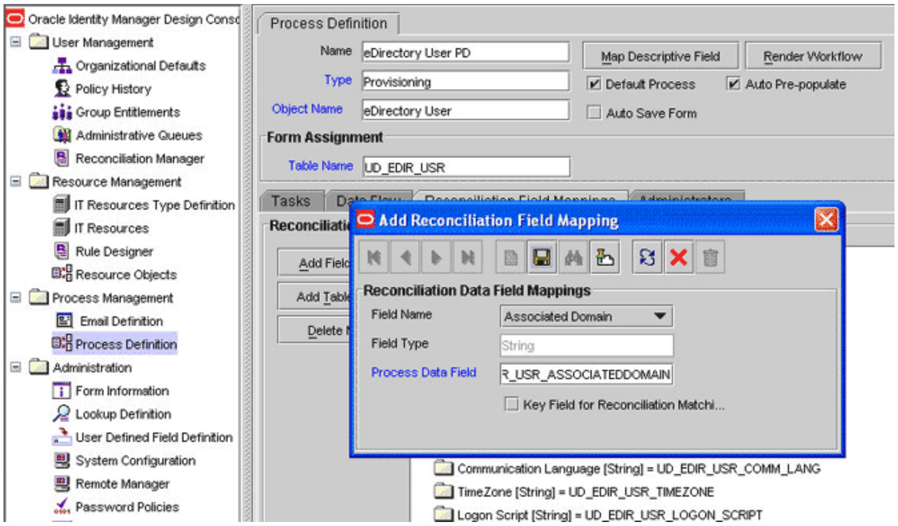
4.8.4 Adding Attributes of the Object Class to the Provisioning Process

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

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

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

   For example, select `Associated Domain = UD_EDIR_USR_ASSOCIATEDDOMAIN`



Name: eDirectory User PD

Type: Provisioning

Object Name: eDirectory User

☑ Default Process ☑ Auto Pre-populate

□ Auto Save Form

Form Assignment

Table Name: UD_EDIR_USR

Reconciliation Data Field Mappings

Field Name: Associated Domain

Field Type: String

Process Data Field: R_USR_ASSOCIATEDDOMAIN

□ Key Field for Reconciliation Matchi...

Communication Language [String] = UD_EDIR_USR_COMM_LANG

TimeZone [String] = UD_EDIR_USR_TIMEZONE

Logon Script [String] = UD_EDIR_USR_LOGON_SCRIPT

6. In the **Field Type** field, select the field type.
7. Click the Save icon.

4.8.5 Adding Custom Object Classes for Provisioning Organization, Groups, and Roles

> **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 RBS:Role object classes, respectively.

The Organizational Unit object class is the value of the ldapOrgUnitObjectClass attribute in the Lookup.EDIR.Configuration lookup definition. Similarly, the group and RBS:Role object classes are the values of the ldapGroupObjectClass and ldapRoleObjectClass attributes in the Lookup.EDIR.Configuration 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 **Lookup.EDIR.Configuration** lookup definition.
3. Perform one of the following steps:

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.

Note: If you want to reconcile a record (group or role) that is created with these object classes, then include these object classes in the SearchFilter attribute of the GrouporRole Recon Scheduled task. See Section 3.3.2, "Limited Reconciliation" for more information.

4.9 Linking the Home Directory Provisioning Operation with the Create User Provisioning Operation

By default, the Create Home Directory provisioning operation is not linked with the Create User provisioning operation. If you want to link the Create User and Create Home Directory operations, then:

1. If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then copy the eDirRemote.jar and eDirRM.jar files from the lib directory on the installation media to the *OIM_HOME*\xellerate\JavaTasks directory.
2. If you are using Oracle Identity Manager release 11.1.*x*, then run the Oracle Identity Manager Upload JARs utility to post the eDirRemote.jar and eDirRM.jar files (located in the lib directory on the installation media) to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

   Note: Verify that the WL_HOME environment variable is set to the directory in which Oracle WebLogic Server is installed.

   For Microsoft Windows:

   OIM_HOME/server/bin/UploadJars.bat

   For UNIX:

   OIM_HOME/server/bin/UploadJars.sh

   When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify `1` as the value of the JAR type.

> **See Also:** *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about the Upload JARs utility

3. Log in to the Design Console.
4. In the Lookup.EDIR.Volume lookup definition, enter the names of volume objects created on the target system. Home directories that you provision are created on these volume objects.

   To create entries in the Lookup.EDIR.Volume lookup definition:

   a. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.

   b. Search for and open the **Lookup.EDIR.Volume** lookup definition.

   c. Click **Add**.

   d. The Lookup.EDIR.Volume lookup definition does not contain any entries by default. You must create entries in this lookup definition based on the volumes defined on the target system.

   The following is a sample entry:

   Code key: mph_vol_10

   Decode: mph_vol_10

   > **Note:** As shown in this sample value, Code Key and Decode values in this lookup definition must be the same.

   e. Click the Save icon to save the entries that you create.
5. Modify the process task for the Create User operation as follows:

   a. Expand **Process Management**, and open the **eDirectory User PD** process definition.

   b. Search for and open the process task for the **Create User** operation.

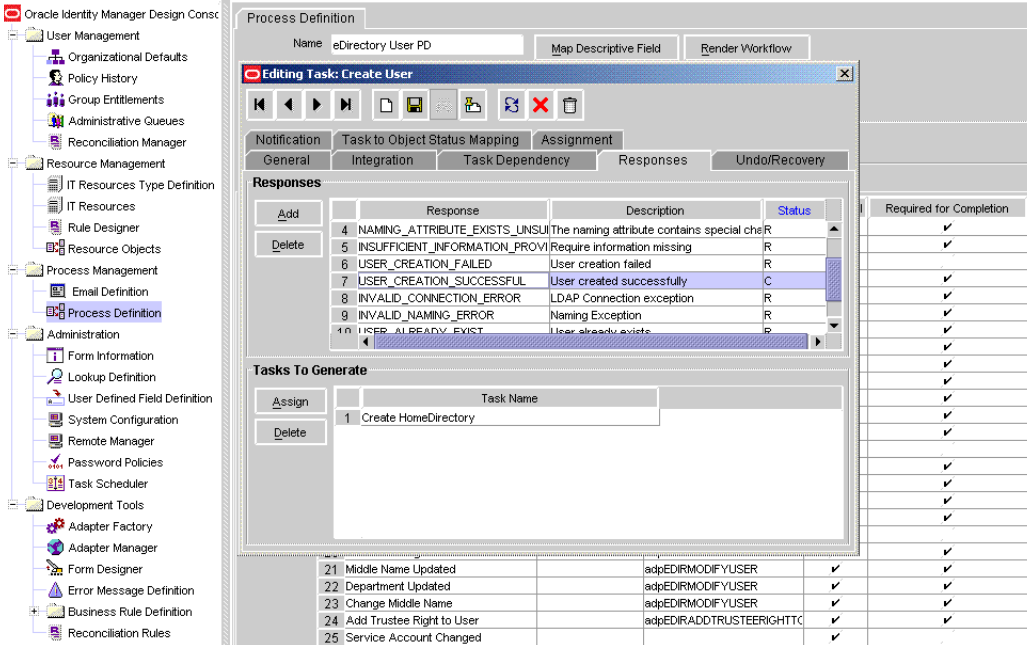
   c. On the Responses tab, and select the response with the status C.

   d. In the Tasks To Generate region, click Assign.

   e. Select the Create Home Directory task from the list, and then click the right arrow.

   f. Click **OK**.

   The following screenshot shows this form:



Name eDirectory User PD

Responses

	Response	Description	Status
4	NAMING_ATTRIBUTE_EXISTS_UNSUI	The naming attribute contains special cha	R
5	INSUFFICIENT_INFORMATION_PROVI	Require information missing	R
6	USER_CREATION_FAILED	User creation failed	R
7	USER_CREATION_SUCCESSFUL	User created successfully	C
8	INVALID_CONNECTION_ERROR	LDAP Connection exception	R
9	INVALID_NAMING_ERROR	Naming Exception	R
10	USER_ALREADY_EXIST	User already exists	R

Tasks To Generate

	Task Name
1	Create HomeDirectory

21	Middle Name Updated		adpEDIRMODIFYUSER	✓	✓
22	Department Updated		adpEDIRMODIFYUSER	✓	✓
23	Change Middle Name		adpEDIRMODIFYUSER	✓	✓
24	Add Trustee Right to User		adpEDIRADDTRUSTEERIGHTT(	✓	✓
25	Service Account Changed			✓	

g. Click the Save icon.

6. Reconciliation of Home directories involves the use of the transformation feature. See Section 1.4.8, "Support for Transformation of Data During Reconciliation" for information about this feature.

> **Note:** Perform this step only if you want to configure reconciliation of Home directory values.

To enable this feature, set the UseTransformMapping attribute of the eDirectory User Target Recon Task scheduled task to `yes`. See Section 3.3.4, "Reconciliation Scheduled Tasks" for more information.

4.10 Configuring Transformation of Data During Reconciliation

> **Note:** This section describes an optional procedure. Perform this procedure only if you want to configure transformation of data during reconciliation.
>
> The default entry in the Lookup.EDIR.Transformation lookup definition is used for reconciliation of Home directories. Do not modify or remove this entry.

You can configure transformation of reconciled data according to your requirements. For example, you can automate the look up of the field name from an external system and set the value based on the field name.

To configure transformation of data:

1. Incorporate the required logic in a Java class.

This transformation class must implement the com.thortech.xl.schedule.tasks.AttributeTransformer interface and the transform method.

The following is one such sample class:

```
package com.thortech.xl.schedule.tasks;
public class AppendTransformer implements AttributeTransformer {
/**
* @param inValue: This is the input string to be transformed.
* @return String: This is the string that is returned.
*/
public String transform(String value) {
   return value;

}
```

2. Create a JAR file to hold the Java class.

3. If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then copy the JAR file into the following directory:

   OIM_HOME/xellerate/ScheduleTask

4. If you are using Oracle Identity Manager release 11.1.*x*, then run the Oracle Identity Manager Upload JARs utility to post the JAR file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

   > **Note:** Verify that the WL_HOME environment variable is set to the directory in which Oracle WebLogic Server is installed.

   For Microsoft Windows:

   OIM_HOME/server/bin/UploadJars.bat

   For UNIX:

   OIM_HOME/server/bin/UploadJars.sh

   When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify `2` as the value of the JAR type.

   > **See Also:** *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about the Upload JARs utility

5. Add an entry in the Lookup.EDIR.Transformation lookup definition.

   Code Key: Enter the name of the attribute on which you want to apply the transformation. For example: `FirstName`

   Decode: Enter the name of the class file. For example: `com.thortech.xl.schedule.tasks.AppendTransformer`

6. Enter `yes` as the value of the Use Transform Mapping attribute of the eDirectory User Trusted Recon Task and eDirectory User Target Recon Task scheduled tasks. See Section 3.3.4, "Reconciliation Scheduled Tasks" for more information.

5

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:

- Section 5.1, "Running Test Cases"
- Section 5.2, "Troubleshooting"

5.1 Running Test Cases

To use the testing utility for running basic tests on the connector:

1. Specify the required values in the global.properties file, which is located in one of the following directories:

   - For Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*:

     OIM_HOME/xellerate/eDir/test/troubleshoot

   - For Oracle Identity Manager release 11.1.*x*:

     OIM_HOME/xellerate/eDir/test/troubleshoot

   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 See Section 2.2.1.2, "Configuring the IT Resource" 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

2. Add the following to the CLASSPATH environment variable:

   - For Oracle Identity Manager release 9.0.1 through 9.0.3.2 or 9.1.0.*x*:

     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

- For Oracle Identity Manager release 11.1.*x*:

  OIM_HOME/server/lib/xlLogger.jar

  OIM_HOME/server/lib/xlUtils.jar

  OIM_HOME/server/JavaTasks/eDirProv.jar

  OIM_HOME/server/ScheduleTask/eDirRecon.jar

  OIM_HOME/server/ThirdParty/ldapbp.jar

  OIM_HOME/server/ext/log4j-1.2.9.jar

3. 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 one of the following files in a text editor:

      – For Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*:

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

      – For Oracle Identity Manager release 11.1.*x*:

        OIM_HOME/server/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
```

4. 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:

      – For Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*:

        OIM_HOME/xellerate/eDir/test/troubleshoot

      – For Oracle Identity Manager release 11.1.*x*:

        OIM_HOME/server/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.

5. Run the following tests:

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

     ```
     java
     -DpropertyFile=OIM_HOME/Server/eDir/test/troubleshoot/troubleshoot.properti
     es
     -Dlog4j.configuration=file:/OIM_HOME/Server/eDir/test/troubleshoot/log.prop
     erties TroubleShootingUtilityLdap createUser
     ```

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

     ```
     java
     -DpropertyFile=OIM_HOME/Server/eDir/test/troubleshoot/troubleshoot.properti
     es
     -Dlog4j.configuration=file:/OIM_HOME/Server/eDir/test/troubleshoot/log.prop
     erties TroubleShootingUtilityLdap modifyUser
     ```

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

     ```
     java
     -DpropertyFile=OIM_HOME/Server/eDir/test/troubleshoot/troubleshoot.properti
     es
     -Dlog4j.configuration=file:/OIM_HOME/Server/eDir/test/troubleshoot/log.prop
     erties TroubleShootingUtilityLdap deleteUser
     ```

5.2 Troubleshooting

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

- Section 5.2.1, "Connection Errors"
- Section 5.2.2, "Create User Errors"
- Section 5.2.3, "Modify User Errors"
- Section 5.2.4, "Delete User Errors"

5.2.1 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.

Problem Description	Solution
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.

5.2.2 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.

Problem Description	Solution
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.

5.2.3 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.

Problem Description	Solution
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.
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.

Problem Description	Solution
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.

5.2.4 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

6 Known Issues

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

- **Bug 7207232**

  Some Asian languages use multibyte character sets. If the character limit for fields on 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 point:

  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.

The following issues are observed when you deploy this release of the connector on Oracle Identity Manager release 9.0.3.2:

- **Bug 8880450**

  If you install this release of the connector on top of an earlier release of the connector, then some error messages are displayed in the server console. However, the connector works as expected.

- **Bug 8294433**

  During trusted source reconciliation, the Enable User operation performed on the target system is correctly propagated to the OIM User but not to the resource assigned to the OIM User. The resource remains in the Disabled state.

The following issues are observed when you deploy this release of the connector on Oracle Identity Manager release 11.1.2:

- **Bug 16519747**

  The Novell eDirectory connector has a child form where values can be provided for role name, scope, and inheritable attributes. During entitlement provisioning, the values to these attributes cannot be provided. A value can only be provided to role name.

The following issues are observed when you deploy this release of the connector on Oracle Identity Manager release 11.1.1:

- **Bug 7627046**

  Reconciliation of organization data is not supported.

- **Bug 9799541**

  Reconciliation of group data and role data is not supported.

- **Bug 11802703**

  During the Change OU Name provisioning operation, the Change Organization Name task is not invoked. Therefore, the name of an organizational unit is not updated.

  As a workaround, perform the following steps:

  > **See Also:** *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about these steps

  1. In the Design Console, search for and open the **eDirectory Organisation unit** process definition.
  2. Rename the **Change Organisation Name** process task to `Organisation Unit Name Updated.`
  3. In the Organisation Unit Name Updated process task, create the following mapping for OrgOrganisationName variable:

     Map To: Process Data

     Qualifier: Organisation Unit Name
  4. Click the Save icon.

- **Bug 11821981**

  A trusted source reconciliation run fails if both the following scenarios are true:

  – The target system is configured to use a port other than the default port (389).

  – The NumberOfBatches attribute of the eDirectory User Trusted Recon Task scheduled job contains a value other than the default value (`All Available`).

  In other words, if you perform a trusted source reconciliation run in the preceding scenario, then reconciliation fails because the connector tries to connect to the target system by using the default port.

Index