

Bidirectional eDirectory Driver Implementation Guide

Identity Manager 4.0.2

January 2014

Novell.



Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. For more information on exporting Novell software, see the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/). Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2011-2012 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see [Novell Documentation \(http://www.novell.com/documentation/\)](http://www.novell.com/documentation/).

Novell Trademarks

For a list of Novell trademarks, see [Trademarks \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide	5
1 Understanding the Bidirectional eDirectory Driver	7
1.1 Driver Concepts	8
1.1.1 Key Terms	8
1.1.2 Data Flow	10
1.1.3 How the Bidirectional eDirectory Driver Works	10
1.2 Standard Driver Features	11
1.2.1 Local Platforms	11
1.2.2 Entitlements	12
1.2.3 Password Synchronization	12
1.2.4 Driver Packages	12
2 Installing the Driver Files	13
3 Preparing the Connected System	15
3.1 Preventing Loopback on the Publisher Channel	15
3.2 Installing Change-Log module on a connected eDirectory server	15
3.2.1 Installing the Change-Log Module on Linux	16
3.2.2 Installing the Change-Log Module on Solaris	16
3.2.3 Installing the Change-Log Module on Windows	16
4 Creating a New Driver Object	17
4.1 Creating the Driver Object in Designer	17
4.1.1 Importing the Current Driver Packages	17
4.1.2 Installing the Driver Packages	18
4.1.3 Configuring the Driver Object	23
4.1.4 Deploying the Driver Object	23
4.1.5 Starting the Driver	24
4.2 Activating the Driver	24
4.3 Adding Packages to an Existing Driver	25
5 Configuring SSL Connections	27
5.1 Importing the Certificate into the Client's Certificate Store	27
5.2 Configuring Mutual Authentication	28
5.3 Security Considerations	29
6 Synchronizing Passwords	31
7 Managing the Driver	33
8 Troubleshooting	35
8.1 Troubleshooting Driver Processes	35

9	Known Issues	37
9.1	NDSTrace displays unable to load dxdap extension module error message	37
9.2	The structured attributes are not properly converted	37
9.3	The users are not correctly synchronized	37
9.4	The NDS password does not synchronize on the Subscriber Channel with Read-Only, Filter Read-Only, and Filter Read/Write replicas	38
9.5	Importing the driver causes change of the driver icon	38
9.6	The Account Tracking GCV is not upgraded with Designer AU2	38
A	Driver Properties	39
A.1	Driver Configuration	39
A.1.1	Driver Module	40
A.1.2	Driver Object Password	40
A.1.3	Authentication	40
A.1.4	Startup Option	40
A.1.5	Driver Parameters	41
A.1.6	ECMAScript	43
A.1.7	Global Configurations	43
A.2	Global Configuration Values	43
A.2.1	eDirectory Base Container	44
A.2.2	Default Configuration	44
A.2.3	Password Synchronization	45
A.2.4	Account Tracking	45
A.2.5	Entitlements	46
A.2.6	Managed System Information	48
A.3	Trace Levels	49
B	Synchronized Attributes	51
B.1	Default Attributes	51
B.2	Creating Home Directories	52

About This Guide

This guide explains how to install and configure the Identity Manager Bidirectional Driver for eDirectory.

- ◆ Chapter 1, “Understanding the Bidirectional eDirectory Driver,” on page 7
- ◆ Chapter 2, “Installing the Driver Files,” on page 13
- ◆ Chapter 3, “Preparing the Connected System,” on page 15
- ◆ Chapter 4, “Creating a New Driver Object,” on page 17
- ◆ Chapter 5, “Configuring SSL Connections,” on page 27
- ◆ Chapter 6, “Synchronizing Passwords,” on page 31
- ◆ Chapter 7, “Managing the Driver,” on page 33
- ◆ Chapter 8, “Troubleshooting,” on page 35
- ◆ Chapter 9, “Known Issues,” on page 37
- ◆ Appendix A, “Driver Properties,” on page 39
- ◆ Appendix B, “Synchronized Attributes,” on page 51

Audience

This guide is for Novell eDirectory and Identity Manager administrators who are using the Identity Manager Bidirectional Driver for eDirectory.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation and add your comments there.

Documentation Updates

For the most recent version of this document, see the [Identity Manager 4.0.2 Drivers Documentation Web site](http://www.netiq.com/documentation/idm402drivers/index.html) (<http://www.netiq.com/documentation/idm402drivers/index.html>).

Additional Documentation

For information on Identity Manager 4.0.2 and other Identity Manager 4.0.2 drivers, see the [Identity Manager 4.0.2 Documentation Web site](http://www.netiq.com/documentation/idm402drivers/index.html) (<http://www.netiq.com/documentation/idm402drivers/index.html>).

1 Understanding the Bidirectional eDirectory Driver

The Identity Manager bidirectional eDirectory driver synchronizes data between the Identity Vault and eDirectory.

The traditional Identity Manager driver for eDirectory synchronizes objects and attributes between two eDirectory trees. This requires Identity Manager to be configured on both eDirectory servers. It also requires two instances of the eDirectory driver configuration.

Another way of connecting to eDirectory is by using the LDAP driver. However, connecting to eDirectory driver through an LDAP driver has the following limitations:

- ♦ The LDAP driver uses LDAP Search method to synchronize eDirectory data because eDirectory doesn't provide a change-log functionality. The LDAP Search method is not as efficient as the change-log method.
- ♦ The LDAP driver doesn't support universal password synchronization on the Publisher channel.

The bidirectional eDirectory driver was designed to make the connection between two connected trees easier in cases where one of the trees did not have an Identity Manager server. This also reduces the licencing burden for customers who do not need Identity Manager in multiple trees.

If you are connecting two Identity Manager enabled trees, it is recommended to use the traditional eDirectory driver. The traditional eDirectory driver and the new bidirectional eDirectory driver are mutually exclusive. The bidirectional eDirectory driver's change-log cannot be installed on an Identity Manager server. [Table 1-1](#) contains details about the features of the two drivers.

Table 1-1 Traditional NDS-to-NDS Driver Compared to the Bidirectional eDirectory Driver

Features	Bidirectional eDirectory Driver	Traditional NDS-to-NDS Driver
Installation	The change-log module is installed on the connected eDirectory.	Identity Manager is installed on the connected eDirectory.
Configuration	One driver is configured for achieving data synchronization between Identity Vault and eDirectory.	Two drivers are configured for achieving synchronization. The configuration is split across the Identity Vault and eDirectory.
Communication	LDAP/TLS is used for communication.	TCP/SSL is used for communication.
NDS Password Sync	Available	Available
Distribution Password Sync	Available	Available
Driver Package	Available	Available
Account Tracking	Available	Available
Entitlements	Available	Available
Data Collection Service	Available	

- ♦ [Section 1.1, “Driver Concepts,” on page 8](#)
- ♦ [Section 1.2, “Standard Driver Features,” on page 11](#)

1.1 Driver Concepts

- ♦ [Section 1.1.1, “Key Terms,” on page 8](#)
- ♦ [Section 1.1.2, “Data Flow,” on page 10](#)
- ♦ [Section 1.1.3, “How the Bidirectional eDirectory Driver Works,” on page 10](#)

1.1.1 Key Terms

Identity Manager: Novell Identity Manager is a service that synchronizes data among servers in a set of connected systems by using a robust set of configurable policies. Identity Manager uses the Identity Vault to store shared information, and uses the Metadirectory engine for policy-based management of the information as it changes in the vault or connected system. Identity Manager runs on the server where the Identity Vault and the Metadirectory engine are located.

Connected System: Any system that can share data with Identity Manager through a driver.

Identity Vault: A hub, with applications and directories publishing their changes to it. The Identity Vault then sends changes to the applications and directories that have subscribed for them. This results in two main flows of data: the Publisher channel and the Subscriber channel.

Metadirectory Engine: The core server that implements the event management and policies of Identity Manager. The engine runs on the Java Virtual Machine in eDirectory.

Driver: A set of policies, filters, and objects that act as the connector between an Identity Vault and the driver shim.

This software enables an application to publish events from an application to the directory, enables an application to subscribe to events from the directory, and synchronizes data between the directory and applications.

Driver Object: A collection of channels, policies, rules, and filters that connect an application to an Identity Vault that is running Identity Manager.

Each driver performs different tasks. Policies, rules, and filters tell the driver how to manipulate the data to perform those tasks.

The Driver object displays information about the driver's configuration, policies, and filters. This object enables you to manage the driver and provide eDirectory management of the driver shim parameters.

Driver Shim: The driver shim handles communication between the eDirectory and the Metadirectory engine. A driver shim can be implemented either in Java class or as a native Windows DLL file.

The driver shim filename for the bidirectional eDirectory driver is `EdirDriverShim.jar`.

Remote Loader: Enables a driver shim to execute outside of the Metadirectory engine (perhaps remotely on a different machine). The Remote Loader is typically used when the Identity Manager server does not meet the requirements of the driver shim.

The Remote Loader executes the driver shim and passes information between the shim and the Metadirectory engine. When you use a Remote Loader, you install the driver shim on the server where the Remote Loader is running, not on the server where the Metadirectory engine is running. You can choose to use SSL to encrypt the connection between the Metadirectory engine and the Remote Loader. For more information, see the [Identity Manager 4.0.2 Remote Loader Guide](#).

NOTE: The bidirectional eDirectory driver does not support the Remote Loader.

TAO: A TAO (Timing Analysis Output) file is an ASCII text file with the `.TAO` extension. The file contains the results of a timing analysis. In the current context, the TAO file refers to the event cache file used by Identity Manager.

LDAP: The Lightweight Directory Access Protocol. An Internet protocol for accessing distributed directory services that act in accordance with X.500 data and service models.

SSL: Secure Sockets Layer. A protocol for managing the security of the messages transmitted on the Internet. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

TLS: Transport Layer Security. A protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that there is no tampering with any message. TLS is the successor of the Secure Sockets Layer (SSL).

Keystore: A keystore contains private keys and certificates with their corresponding public keys required by a server for client authentication.

1.1.2 Data Flow

The Identity Manager bidirectional eDirectory driver synchronizes data between the Identity Vault and eDirectory. The driver can run anywhere that a Metadirectory server is running. The driver uses the Lightweight Directory Access Protocol to bidirectionally synchronize changes between an Identity Vault and the connected system (eDirectory).

The driver uses the change-log publication method to recognize data changes and communicates them to an Identity Vault. The Subscriber channel sends the Identity Vault changes to the connected system (eDirectory) through LDAP/LDAPS.

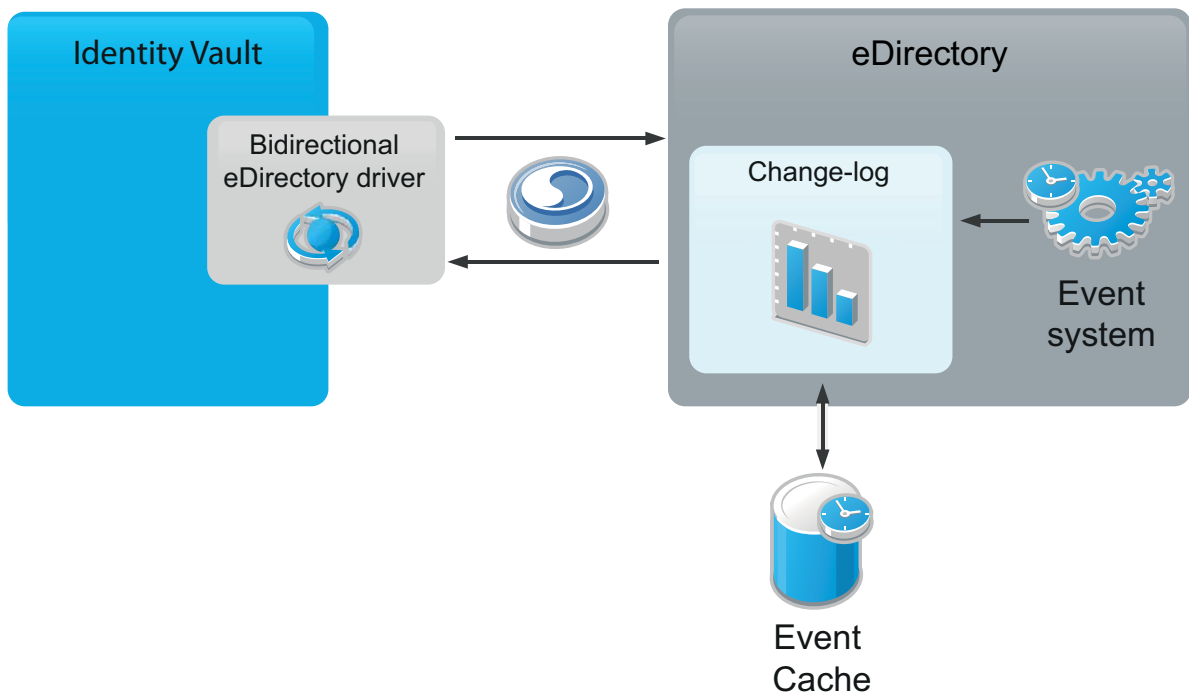
1.1.3 How the Bidirectional eDirectory Driver Works

The bidirectional eDirectory driver requires a change-log module to be present in the eDirectory server. The change-log module cannot coexist with the Identity Manager engine.

The change-log module provides change notification for the driver's Publisher channel. The data flow between the bidirectional eDirectory driver and the Identity Vault is controlled by filters and policies that are in place for the bidirectional eDirectory driver.

If you need to connect to an Identity Manager server, you must use the traditional eDirectory driver.

Figure 1-1 Bidirectional eDirectory Driver Functionality



- ◆ **Driver:** The bidirectional driver has Subscriber and Publisher channels:
 - ◆ **Subscriber Channel:** The Subscriber channel watches for additions and modifications to Identity Vault objects and issues LDAP commands that make changes to the connected system (eDirectory).
 - ◆ **Publisher Channel:** The Publisher channel reads information from the change-log and submits that information to an Identity Vault via the Metadirectory engine. By default, the Publisher channel checks the log every 10 seconds. The Metadirectory engine applies policies, takes the appropriate actions, and posts the events to the Identity Vault.

- ♦ **Filters:** Identity Manager uses filters to control which objects and attributes are shared. The default filter configuration for the bidirectional eDirectory driver allows objects and attributes to be shared.
- ♦ **Policies:** Policies are used to control data synchronization between the driver and the Identity Vault.
- ♦ **Change-log Module:** The change-log module has the following components:
 - ♦ **Change Cache:** The event logger logs eDirectory events into a change cache, which is a TAO file that has the same structure as the Identity Manager engine. A unique change cache is associated with a registered driver instance. Every successful new driver registration creates a new change cache that is associated with that driver. The TAO files have a proprietary format and are designed to reduce the disk usage for storing the change information. The change cache files are local to the eDirectory server on which they are created, because they refer to several server-specific details in the logged events.
 - ♦ **Event Logger:** The event logger is an Identity Manager dxevent module with a limited functionality. It registers event handlers for the eDirectory events. The event handler uses the filter information that is passed to the change-log when an eDirectory driver is registered. The filters determine events that the driver can consume from the change-log. The event handler filters events based on the driver filter. All filtered events are logged by the event logger.
 - ♦ **Change-log Extension Handler:** The change-log module provides LDAP extensions for changes to the eDirectory driver. The LDAP extension handler exposes the extension for registering an eDirectory driver instance and for initiating and stopping a change publication to the eDirectory driver. The driver registration information is stored in the `driver data` configuration file, which resides in the DIB directory of eDirectory. The event logger module provides changes to the change-log. The changes are stored in the TAO file format of the Identity Manager engine.

The LDAP extension handler is a limited version of the `dxldap` module, whose only job is to expose extensions for the change-log. Other Identity Manager extensions are not present in the change-log module.

There are four change-log operations: `InitRequest`, `GetChangesRequest`, `SendChangesResponse`, and `EndRequest`. The `clientID` is the GUID of the eDirectory driver in the Identity Vault. The GUID is used to uniquely identify the registered eDirectory driver instances.

1.2 Standard Driver Features

The following sections provide information about how the bidirectional eDirectory driver supports standard driver features:

- ♦ [Section 1.2.1, “Local Platforms,” on page 11](#)
- ♦ [Section 1.2.2, “Entitlements,” on page 12](#)
- ♦ [Section 1.2.3, “Password Synchronization,” on page 12](#)
- ♦ [Section 1.2.4, “Driver Packages,” on page 12](#)

1.2.1 Local Platforms

The bidirectional eDirectory driver runs in any Identity Manager installation. See “[System Requirements](#)” in the *Identity Manager 4.0.2 Integrated Installation Guide*.

1.2.2 Entitlements

Entitlements standardize a method of recording this information on objects in the Identity Vault. The bidirectional eDirectory driver implements entitlements. You can use entitlements to grant or revoke rights to an account in the driver. The driver is unaware of the User Application or Role-Based Entitlements. It depends on the User Application server or the Entitlements driver to grant or revoke the entitlement for a user based upon its own rules.

You should enable entitlements for the driver only if you plan to use the User Application or Role-Based Entitlements with the driver. For more information about entitlements, see the [Identity Manager 4.0.2 Entitlements Guide](#).

1.2.3 Password Synchronization

The bidirectional eDirectory driver supports password synchronization via Universal Password. You can also use the older form of password synchronization (a public/private key pair or NDS password). For more information, see [Chapter 6, "Synchronizing Passwords," on page 31](#).

1.2.4 Driver Packages

The Identity Manager content is now delivered in packages. The packages are included with Identity Manager 4.0 and later. For more information about Identity Manager packages, see "[Configuring Packages](#)" in the [Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide](#).

There are multiple packages for the bidirectional eDirectory driver. The packages create a driver with a set of policies suitable for synchronizing data with the Identity Vault.

2 Installing the Driver Files

By default, the bidirectional eDirectory driver files are installed on the Metadirectory server at the same time as the Metadirectory engine. The installation program extends the Identity Vault's schema and installs the driver shim. It does not create the driver in the Identity Vault (see [Chapter 4, "Creating a New Driver Object,"](#) on page 17).

If you performed a custom installation and did not install the bidirectional eDirectory driver on the Metadirectory server, you must install the files on the Metadirectory server, using the instructions in "Installing Identity Manager" in the *Identity Manager 4.0.2 Integrated Installation Guide*.

For the bidirectional eDirectory driver to work, you must also install the change?log module on the connected system (eDirectory). For information on change-log installation, see "[Installing Change-Log module on a connected eDirectory server](#)" on page 15.

3 Preparing the Connected System

You need to do the following tasks to prepare the connected system (eDirectory server) to which you are connecting:

- ♦ Create a user account through which the bidirectional eDirectory driver can authenticate to the connected eDirectory.
- ♦ Install the change-log module on the connected eDirectory server for synchronization of data from the connected eDirectory server to the Identity Vault (Publisher channel).

The following sections provide instructions for creating an eDirectory user object and installing the change-log module on a connected eDirectory server:

- ♦ [Section 3.1, “Preventing Loopback on the Publisher Channel,” on page 15](#)
- ♦ [Section 3.2, “Installing Change-Log module on a connected eDirectory server,” on page 15](#)

3.1 Preventing Loopback on the Publisher Channel

The change-log mechanism implements loopback detection by ignoring events that are detected in the connected system made by the account that is used in the driver configuration. All changes made in the connected system by the account used in the driver configuration are not published in the Identity Vault on the Publisher channel. For example, if the driver is configured with user account as “jdoe”, use any other user account except “jdoe” to make changes on the connected system. To create an account with proper rights to be used in the driver configuration, see, see [“Security Considerations” on page 29](#).

3.2 Installing Change-Log module on a connected eDirectory server

For the bidirectional eDirectory driver to work, you must install the change-log module on the connected eDirectory server. The change-log enables the driver to recognize changes that require publication from the connected eDirectory to the Identity Vault. The change-log module is supported on eDirectory version 8.8.5 and later versions.

The change-log module is provided on the Identity Manager media for both 32-bit and 64-bit platforms. Based on your architecture, copy the change-log module from the `/products/IDM/Dirxml-ChangeLog` directory of your installation folder and install it on the connected eDirectory server.

The following sections provide instructions to install the change-log module on Linux, Solaris, and Windows platforms:

- ♦ [Section 3.2.1, “Installing the Change-Log Module on Linux,” on page 16](#)
- ♦ [Section 3.2.2, “Installing the Change-Log Module on Solaris,” on page 16](#)
- ♦ [Section 3.2.3, “Installing the Change-Log Module on Windows,” on page 16](#)

3.2.1 Installing the Change-Log Module on Linux

To install the change-log module on Linux platforms,

- 1 Stop eDirectory.
- 2 Navigate to the directory containing the change-log RPM.
- 3 Install the change-log RPM.
 - ♦ **For a 64-bit platform:** Run the following command:

```
rpm -ivh ./novell-DXMLChlgx-4.0.1-0.x86_64.rpm
```
 - ♦ **For a 32-bit platform:** Run the following command:

```
rpm -ivh ./novell-DXMLChlg-4.0.1-0.i586.rpm
```
- 4 Start eDirectory.

3.2.2 Installing the Change-Log Module on Solaris

To install the change-log on Solaris,

- 1 Stop eDirectory.
- 2 Navigate to the directory containing the change-log package.
- 3 Install the change-log package.
 - ♦ **For a 64-bit platform:** Run the following command:

```
pkgadd -d ./DXMLChlgx.pkg
```
 - ♦ **For a 32-bit platform:** Run the following command:

```
pkgadd -d ./DXMLChlg.pkg
```
- 4 Start eDirectory.

3.2.3 Installing the Change-Log Module on Windows

To install the change-log module on Windows,

- 1 Shutdown the eDirectory service.
- 2 Depending on your platform, navigate to a 32-bit or 64-bit folder containing the following DLLs, then copy them to the eDirectory install location. The default install location is `C:\novell\nds`.
 - ♦ `dirxmllib.dll`
 - ♦ `dxevent.dll`
 - ♦ `xcldap.dll`
- 3 Start the eDirectory service.

4 Creating a New Driver Object

After the bidirectional eDirectory driver files are installed on the server where you want to run the driver (see [Chapter 2, “Installing the Driver Files,” on page 13](#)), you can create the driver in the Identity Vault. You do so by installing the driver packages and then modifying the driver configuration to suit your environment.

- ♦ [Section 4.1, “Creating the Driver Object in Designer,” on page 17](#)
- ♦ [Section 4.2, “Activating the Driver,” on page 24](#)
- ♦ [Section 4.3, “Adding Packages to an Existing Driver,” on page 25](#)

4.1 Creating the Driver Object in Designer

To create the bidirectional eDirectory driver object, install the driver packages and then modify the configuration to suit your environment. After you create and configure the driver object, you need to deploy it to the Identity Vault and start it.

To synchronize data between the eDirectory connected system and the Identity Vault, you need to complete the following procedures for the drivers that are installed in each Identity Vault:

- ♦ [Section 4.1.1, “Importing the Current Driver Packages,” on page 17](#)
- ♦ [Section 4.1.2, “Installing the Driver Packages,” on page 18](#)
- ♦ [Section 4.1.3, “Configuring the Driver Object,” on page 23](#)
- ♦ [Section 4.1.4, “Deploying the Driver Object,” on page 23](#)
- ♦ [Section 4.1.5, “Starting the Driver,” on page 24](#)

NOTE: You should not create driver objects using the new Identity Manager 4.0 and later configuration files through iManager. This method of creating driver objects is no longer supported. To create drivers, you now need to use the new package management features provided in Designer.

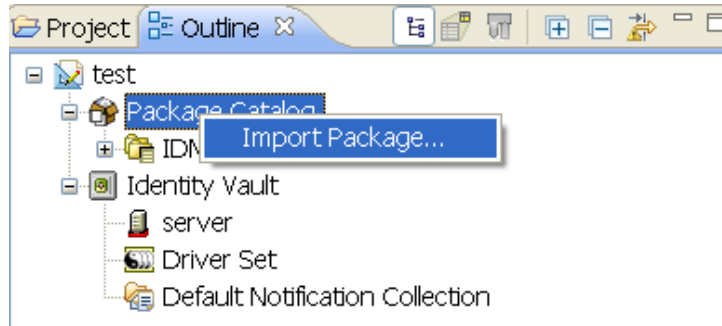
4.1.1 Importing the Current Driver Packages

The driver packages contain the items required to create a driver, such as policies, entitlements, filters, and Schema Mapping policies. These packages are only available in Designer. You can upgrade any package that is installed if there is a newer version of the package available. Before creating a driver object in Designer, it is recommended to have the latest packages in the Package Catalog. Designer prompts you for importing the required packages when it creates the driver object. For more information on upgrading packages, see [“Upgrading Installed Packages” in the *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*](#).

To verify that you have the most recent version of the driver packages imported into the Package Catalog:

- 1 Open Designer.
- 2 In the toolbar, click *Help > Check for Package Updates*.

- 3 Click *OK* to update the packages
or
Click *OK* if the packages are up-to-date.
- 4 In the Outline view, right-click the Package Catalog.
- 5 Click *Import Package*.



In the Select Package window, browse to the installation folder and select bidirectional eDirectory driver packages. These packages are added to the list of packages for this driver.

- 6 Click *Select All* to import all of the packages displayed.
By default, only the base packages are displayed. Deselect *Show Base Packages Only* to display all packages.
- 7 Click *OK* to import the selected packages, then click *OK* in the successfully imported packages message.
- 8 After the current packages are imported, restart Designer.
Continue with [Section 4.1.2, “Installing the Driver Packages,”](#) on page 18.

4.1.2 Installing the Driver Packages

After you import the current driver packages into the Package Catalog, you can install the driver packages to create a new driver.

- 1 In Designer, open your project.
- 2 In the Modeler, right-click the driver set where you want to create the driver, then click *New > Driver*.
- 3 Select *eDir2eDir Base*, then click *Next*.
- 4 Select the optional packages to install for the bidirectional eDirectory driver. All options are selected by default. The options are:

Default Configuration: These packages contain the default configuration information for the bidirectional eDirectory driver. Always leave this option selected.

Entitlements: These packages contain the policies and entitlements required to enable the driver for account creation and management with entitlements. For more information, see the [Identity Manager 4.0.2 Entitlements Guide](#).

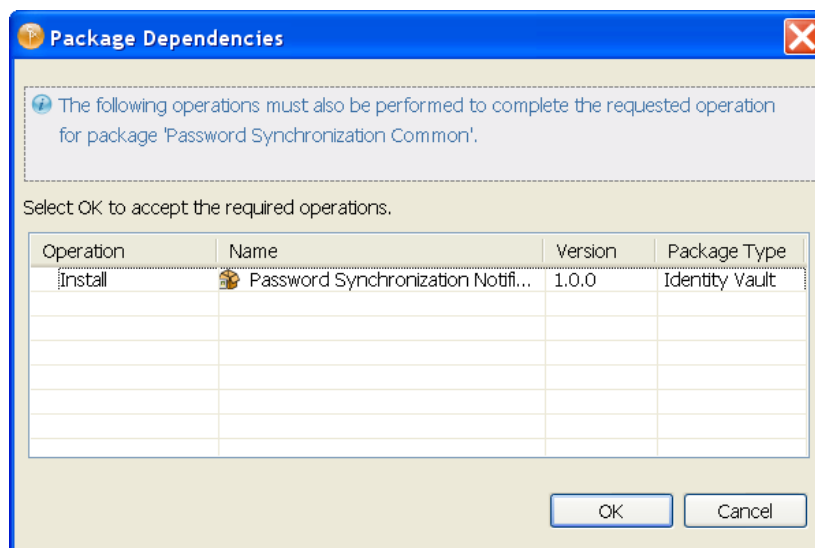
Password Synchronization: These packages contain the policies required to enable password synchronization. Leave this option selected if you want to synchronize passwords between the Identity Vault and the eDirectory server.

Data Collection: These packages contain the policies that enable the driver to collect data for reports. If you are using the Identity Reporting Module, verify that this option is selected. For more information, see the [Using Identity Manager 4.0.2 Reports](#).

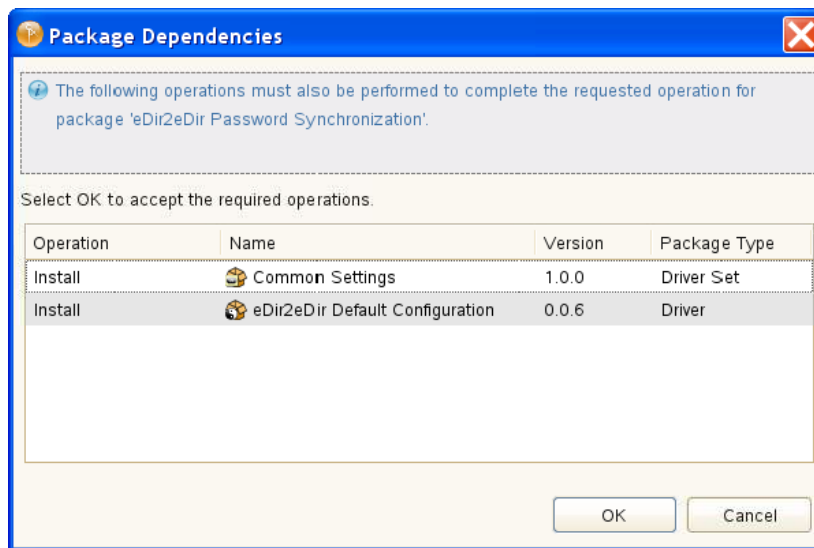
Account Tracking: These packages contain the policies that enable account tracking information for reports. If you are using the Identity Reporting Module, verify that this option is selected. For more information, see the [Using Identity Manager 4.0.2 Reports](#).

Account Tracking feature was introduced with Novell Compliance Management Platform. The Compliance Management Platform helps you mitigate risk, simplify business governance, and ensures compliance throughout the enterprise. The platform enables you to provision users based on how you do business, secure both Web and Client applications by granting access to users based upon provisioning policy, and monitor and validate user and system activity in real time with automated, policy-based corrective actions for non-compliant activities. For more information, see [Novell Compliance Management Platform product page \(http://www.novell.com/products/compliancemanagementplatform/\)](http://www.novell.com/products/compliancemanagementplatform/).

- 5 After selecting the optional packages, click *Next*.
- 6 If there is a package dependency, install the dependent package. For example, Password Synchronization Notification Packages.



- 7 (Conditional) Click *OK* to install the Common Settings package and the edir2eDir Default Configuration package, if you have not installed any other packages into the selected driver set.



- 8 (Conditional) Fill in the following fields on the Common Settings page, then click *Next*:

The Common Settings page is displayed only if the Common Settings package is installed as a dependency.

User Container: Select the container where the users are added if they don't already exist in the Identity Vault. This value becomes the default value for all drivers in the driver set. It is in slash format, such as `netiq/users`, where `ou=users.o=netiq`.

If you want a unique location for this driver, set the value for all drivers on this page. After the driver is created, change the value on the driver's Global Configuration Values page.

Group Container: Select the container where the groups are added if they don't already exist in the Identity Vault. This value becomes the default value for all drivers in the driver set.

If you want a unique location for this driver, set the value for all drivers on this page. After the driver is created, change the value on the driver's Global Configuration Values page.

- 9 On the Driver Information page, specify a name for the driver, then click *Next*.

- 10 On the Application Authentication page, fill in the following fields, then click *Next*:

Authentication ID: Specify the DN of the LDAP account in full LDAP DN format that the driver will use to authenticate to connected eDirectory.

For information, see [Chapter 5, "Configuring SSL Connections," on page 27](#).

Connection Information: Specify the hostname or IP address of the eDirectory server as well as the decimal port number (for example, `187.168.1.1:389`).

Port 389 uses the TLS protocol for clear text transfer and port 636 uses the SSL protocol. For more information, see [Chapter 5, "Configuring SSL Connections," on page 27](#).

Password: Specify the password for the LDAP account that the driver will use to authenticate to connected eDirectory.

Use SSL: Select *Yes* to use SSL to secure communication between the bidirectional eDirectory driver and the eDirectory server. If you use SSL, fill in the following parameters:

- ♦ **Always Accept Server Certificate:** Select *Yes* for the driver to accept the LDAP server's certificate for establishing the SSL connection with the eDirectory server. To use the keystore, select this option to *No*. For more information on setting up SSL connections, see [Chapter 5, "Configuring SSL Connections," on page 27](#).
- ♦ **Keystore Path for SSL Certs:** Specify the full path to the keystore file containing the SSL certificates.

- ◆ **Use Mutual Authentication:** Select *Yes* if you want the driver to use SSL mutual authentication (both client and server), or select *No* for server authentication only. If you select *Yes*, you must have the appropriate certificates configured in your keystore.
- ◆ **Key Alias:** Specify the alias of the key.
- ◆ **Keystore Password:** Specify the keystore password for accessing the keystore file containing the SSL certificates.

eDirectory Base Container: Specify the base container in the slash format. This is the container in the Identity Vault where objects are synchronized. If you are using a flat Placement rule, this is the container where the users are placed. If you are using a mirrored Placement rule, this is the base container. For example, `netiq/users`, where `ou=users.o=netiq` or `ou=people,ou=example,o=com`.

- 11 On the Remote Loader page, do not fill any fields. Click *Next*.

NOTE: The bidirectional eDirectory driver does not support the Remote Loader. This option does not apply.

- 12 (Conditional) Fill in the following fields to define your connected eDirectory system, then click *Next*.

This page is displayed only if you selected to install the Data Collection and Account Tracking packages.

Name: Specify a descriptive name for this connected eDirectory system. The name is displayed in the reports.

Description: Specify a brief description of the connected eDirectory system. The description is displayed in the reports.

Location: Specify the physical location of the connected eDirectory system. The location is displayed in the reports.

Vendor: Select Novell as the vendor of the connected eDirectory system. The vendor information is displayed in the reports.

Version: Specify the version of the connected eDirectory system. The version is displayed in the reports.

- 13 (Conditional) Fill in the following fields to define the ownership of the connected eDirectory system, then click *Next*.

This page is displayed only if you selected to install the Data Collection and Account Tracking packages.

Business Owner: Select a user object in the Identity Vault that is the business owner of the connected eDirectory system. This can only be a user object, not a role, group, or container.

Application Owner: Select a user object in the Identity Vault that is the application owner of the connected eDirectory system. This can only be a user object, not a role, group, or container.

- 14 (Conditional) Fill in the following fields to define the classification of the connected eDirectory system, then click *Next*.

This page is displayed only if you selected to install the Data Collection and Account Tracking packages.

Classification: Select the classification of the connected eDirectory system. This information is displayed in the reports. The options are:

- ◆ Mission-Critical
- ◆ Vital
- ◆ Not-Critical

- ◆ Other

If you select *Other*, you must specify a custom classification for the Identity Vault.

Environment: Select the type of environment the connected eDirectory system provides. The options are:

- ◆ Development
- ◆ Test
- ◆ Staging
- ◆ Production
- ◆ Other

If you select *Other*, you must specify a custom classification for the connected eDirectory system.

- 15** Fill in the following fields on the bidirectional eDirectory Default Configuration page, then click *Next*:

Publisher Placement type: Select the desired form of placement for the Publisher channel. This option determines the Publisher Channel Placement policies. The options are:

- ◆ **Mirrored:** Mirrors the structure between the Identity Vault and eDirectory.
This option in the driver configuration synchronizes User, Group, Organization, Country, and Organizational Unit objects.
- ◆ **Flat:** All of the objects are placed into a single (base) container.
This option synchronizes User, Group, Organization, and Organizational Unit objects.

Subscriber Channel Placement Type: Select the desired form of placement for the Subscriber channel. This option determines the Subscriber Channel Placement policies. The options are:

- ◆ **Mirrored:** Mirrors the structure between the Identity Vault and the connected eDirectory server. It places objects hierarchically within the base container.
This option in the driver configuration synchronizes User, Group, Organization, Country, and Organizational Unit objects.
- ◆ **Flat:** All of the objects are placed within the base container.
This option synchronizes User, Group, Organization, and Organizational Unit objects.

- 16** On the Password Sync Settings page, specify a password for the user, then click *Next*.
This option in the driver configuration assumes a default password if you don't specify the password for the user.

- 17** (Conditional) On the Account Tracking page, specify the name of the realm which uniquely identifies the location of the users in the connected eDirectory.

- 18** Review the summary of tasks, then click *Finish*.

- 19** After the driver packages are installed, there is additional configuration required for the bidirectional eDirectory driver. Continue to [Section 4.1.3, "Configuring the Driver Object,"](#) on [page 23](#) to configure the driver.

4.1.3 Configuring the Driver Object


The bidirectional eDirectory driver is operational after the driver packages are installed. However, the basic configuration might not meet the requirements for your environment. You should complete the following tasks to configure the driver object:

- ♦ **Secure the driver connection:** The bidirectional eDirectory driver communicates through LDAP protocols via SSL, using digital certificates for authentication. You need to set up this secure connection. See [Chapter 5, “Configuring SSL Connections,” on page 27](#).
- ♦ **Configure the driver filter:** Modify the driver filter to include the object classes and attributes you want synchronized between the eDirectory connected system and the Identity Vault. For information about the classes and attributes included in the filter for the basic configuration, see [Appendix B, “Synchronized Attributes,” on page 51](#).
- ♦ **Configure policies:** Modify the policies as needed for your driver.
- ♦ **Configure password synchronization:** The basic driver configuration is set up to support bidirectional password synchronization through Universal Password and NDS password. By default, Universal Password is configured. For more information, see [Chapter 6, “Synchronizing Passwords,” on page 31](#).

After completing the configuration tasks, continue with the next section, [Deploying the Driver Object \(page 23\)](#).

4.1.4 Deploying the Driver Object

After the driver object is created in Designer, it must be deployed into the Identity Vault.

- 1 In Designer, open your project.
- 2 In the Modeler, right-click the driver icon  or the driver line, then select *Live > Deploy*.
- 3 If you are authenticated to the Identity Vault, skip to [Step 5](#); otherwise, specify the following information:

Host: Specify the IP address or DNS name of the server hosting the Identity Vault.

Username: Specify the DN of the user object used to authenticate to the Identity Vault.

IMPORTANT: The *Username* specified in the driver properties should be an `admin` type user that is only used by the Bidirectional eDirectory driver for authentication and rights to the connected eDirectory tree. Create an `admin` user in the connected eDirectory that is solely used by the Bidirectional eDirectory driver for authentication.

If you are authenticating to the Bidirectional eDirectory driver as the same user that you used to administer the connected eDirectory tree, the change-log filter fails to pick and synchronize changes that you made to the connected eDirectory because the loopback protection disregards the changes. For the driver to pick the changes, you must connect to the Bidirectional eDirectory driver as a different user.

Password: Specify the user's password.

- 4 Click *OK*.
- 5 Read through the deployment summary, then click *Deploy*.
- 6 Read the message indicating that the deployment was successful, then click *OK*.
- 7 Click *Define Security Equivalence* to assign rights to the driver.

The driver requires rights to objects within the Identity Vault. The Admin user object is most often used to supply these rights. However, you might want to create a DriversUser (for example) and assign security equivalence to that user.

For receiving events from the Identity Vault, ensure that the driver's *Security Equals DN* has the following rights in the Identity Vault:

- ◆ **Entry:** Browse rights.
- ◆ **Attributes:** Read rights.

For more information, see [Section 5.3, “Security Considerations,” on page 29](#).

7a Click *Add*, then browse to and select the object with the correct rights.

7b Click *OK* twice.

8 Click *Exclude Administrative Roles* to exclude users that should not be synchronized.

You should exclude any administrative User objects (for example, Admin and DriversUser) from synchronization.

8a Click *Add*, then browse to and select the user object you want to exclude, then click *OK*.


8b Repeat [Step 8a](#) for each object you want to exclude, then click *OK*.

9 Click *OK*.

4.1.5 Starting the Driver

When a driver is created, it is stopped by default. To make the driver work, you must start the driver. Identity Manager is an event-driven system, so after the driver is started, it won't do anything until an event occurs. You can use `iManager` or `dxevent` commands to start the driver.

To start the driver by using Designer:

- 1** Launch Designer, then open your project.
- 2** In the Modeler, right-click the driver icon  or the driver line, then select *Live > Start Driver*.

For information about management tasks with the driver, see [Chapter 7, “Managing the Driver,” on page 33](#).

4.2 Activating the Driver

If you created the driver in a driver set that has not been activated, you must activate the driver within 90 days. Otherwise, the driver stops working.

To activate the bidirectional eDirectory driver, activate the Metadirectory engine, then activate the driver by using the separate bidirectional eDirectory activation key.

For information on activation, refer to “[Activating Novell Identity Manager Products](#)” in the *Identity Manager 4.0.2 Integrated Installation Guide*.

If driver activation has expired, the following error message is displayed in the `ndstrace` window:

```
DirXML Log Event -----
Driver:   \META-RHEL6\system\DriverSet\eDirDriver-BulkOperations
Channel:  Subscriber
Status:   Error
Message:  Code(-9075) Shutting down because DirXML engine evaluation period
has expired. Activation is required for further use.
```

To use the driver, you must reactivate it.

Package Management ← - → ▾

Installed Packages + 🗑️

Package	Versi...	Upgra...	Operation
🟢 Password Synchronization Notificatio...	0.2.0		Select Operation...
🟡 Provisioning Notification Templates	0.2.0		Install
🟡 Password Management Notification T...	0.2.0		Install
🟡 Password Expiration Notification Tem...	0.2.0		Install
🟡 Job Default Notification Templates	0.2.0		Install

- 6 (Conditional) Fill in the fields with appropriate information to install the package you selected for the driver, then click *Next*.
- 7 Read the summary of the installation, then click *Finish*.
- 8 Click *OK* to close the Package Management page after you have reviewed the installed packages.

Package Management ← - → ▾

Installed Packages + 🗑️

Package	Versi...	Upgra...	Operation
🟢 Job Default Notification Templates	0.2.0		Select Operation...
🟢 Password Expiration Notification Tem...	0.2.0		Select Operation...
🟢 Password Management Notification T...	0.2.0		Select Operation...
🟢 Password Synchronization Notificatio...	0.2.0		Select Operation...
🟢 Provisioning Notification Templates	0.2.0		Select Operation...

- 9 Repeat [Step 1](#) through [Step 8](#) for each driver where you want to add the new packages.

5 Configuring SSL Connections

The bidirectional eDirectory driver uses the LDAP protocol to communicate with the eDirectory servers. SSL connections encrypt all traffic on the TCP/IP socket by using a public/private key pair.

The bidirectional eDirectory driver supports mutual authentication to support secure data transfer and data integrity. You can establish mutual authentication on the Identity Manager side for the bidirectional eDirectory driver to authenticate to the Identity Vault.

- ♦ [Section 5.1, “Importing the Certificate into the Client’s Certificate Store,” on page 27](#)
- ♦ [Section 5.2, “Configuring Mutual Authentication,” on page 28](#)
- ♦ [Section 5.3, “Security Considerations,” on page 29](#)

5.1 Importing the Certificate into the Client’s Certificate Store

You need to import the trusted root certificate into a certificate store (also called a keystore) that the driver can use.

- 1 Import the trusted root certificate from the connected eDirectory server and save it to a file in `der` format.
 - 1a In iManager, log in to the connected eDirectory server with administrator rights.
 - 1b In the left pane of the *Roles and Tasks* tab, select *Novell Certificate Access > Server Certificates*, then select any server certificate.
 - 1c Click *Export*.
 - 1d Select *OU=Organizational CA* certificate from drop down menu for the *Certificate* option.
 - 1e Select `der` as the *Export* format, then click *Next*.
 - 1f Save the file to a local file system.
- 2 Add the `.der` file to the keystore by using the following command at the command line:

```
keytool -import -file PATH_OF_DERFile\PublicKeyCert.der -keystore  
KEYSTOERPATH\NAME.keystore -storepass keystorepass
```

You are recommended to use Java 1.6 keytool. The command might not work with versions earlier than Java 1.6.

- 3 When you are asked to trust this certificate, select *Yes*, then click *Enter*.
- 4 Copy the `.keystore` file to any directory on the same file system that has the Identity Vault files.
- 5 In iManager, select *Identity Manager > Identity Manager Overview*.
- 6 Search for drivers.
- 7 Click the bidirectional eDirectory driver object, then click it again in the *Identity Manager Driver Overview* page.
- 8 In the *Keystore Path* parameter, enter the complete path to the `keystore` file.
- 9 Enable the driver’s SSL parameter and adjust the other SSL parameters as needed.
For information, see [Section A.1.5, “Driver Parameters,” on page 41](#).

Continue with [Section 5.2, “Configuring Mutual Authentication,”](#) on page 28.

5.2 Configuring Mutual Authentication

Use the following procedure to configure mutual authentication between the bidirectional eDirectory driver and the Identity Vault:

- 1 Complete [Step 1](#) through [Step 9](#) in [Section 5.1, “Importing the Certificate into the Client’s Certificate Store,”](#) on page 27.
- 2 Create a user certificate that the driver can use:
 - 2a In iManager, log in to the connected eDirectory server with administrator rights.
 - 2b In the left pane of the *Roles and Tasks* tab, select *Novell Certificate Server > Create User Certificate > Browse > Driver Authenticate User* option, then click *Next*.
 - 2c Specify the *Nickname* and leave other settings as the defaults.
 - 2d Click *Finish*.
- 3 Import the user `cert.pfx` file:
 - 3a In iManager, log in to the connected eDirectory server as the driver’s authenticated user.
 - 3b In the left pane of the *Roles and Tasks* tab, select *Novell Certificate Access > User Certificates > Nickname*, then click *Export*.

The *Nickname* must be same as the one specified in [Step 2](#).

You are recommended to use Java 1.6 keytool. The command might not work with versions earlier than Java 1.6.
 - 3c Specify the private key password for the certificate, then click *Next*.
 - 3d Save the `cert.pfx` file to a local file system.
- 4 Copy the `cert.pfx` file to any directory on the same file system that has the Identity Vault files.
- 5 Add the private key to the keystore by using the following command at the command line:

```
keytool -importkeystore -srckeystore cert.pfx -srcstoretype PKCS12 -  
destkeystore mykeystore -alias AliasName
```

The *AliasName* must be the same as *Nickname* that you specified for the user certificate. Ensure that you use the same keystore file that you used for the SSL configuration in [Step 2 on page 27](#).
- 6 Adjust the driver’s configuration as needed.
- 7 Change the LDAP options of the connected eDirectory server to enable mutual authentication with the Identity Vault:
 - 7a In iManager, log in to the connected eDirectory server with administrator rights.
 - 7b In the left pane of the *Roles and Tasks* tab, select *LDAP > LDAP Options > View LDAP Server*, then select the connected eDirectory server from the list of servers with which you want to enable mutual authentication
 - 7c In the *Connections* tab, specify the connection information, then click *OK*.
 - 7d Change the *Set Client Certificate* option to *Requested*, then click *OK*. Leave other settings as the defaults.

To communicate only with mutual authentication, set this option to *Required*.
 - 7e Click *Apply*, then click *OK*.
- 8 Start the driver.

5.3 Security Considerations

- ♦ The bidirectional eDirectory driver requires appropriate read/write rights in the container on which it operates. The eDirectory servers where you install the driver must hold master or read/write replicas of the objects you want synchronized between eDirectory and Identity Vault. The following permissions are required for synchronizing changes with the connected system and the Identity Vault:

- ♦ **Rights Required on the Connected System:** For receiving events from the connected system, the driver's *Authentication DN* must have the following rights in the connected system (eDirectory):
 - ♦ **Entry Rights:** Browse permission.
 - ♦ **Attributes Rights:** Read permission.

For synchronizing the NDS password, ensure that the driver's *Authentication DN* has Read and Write permissions on the ACLs of the objects.

For synchronizing changes to the connected system, ensure that the driver's *Authentication DN* has the following rights in the connected system (eDirectory).

- ♦ **Entry Rights:** The rights to create entries in the connected system. Supervisor rights on the objects for synchronizing NDS passwords.
- ♦ **Attributes Rights:** The rights to modify the attributes in the connected system.

For modifying the write-managed attributes, the driver's *Authentication DN* must have the management rights on the objects whose DN is being modified.

- ♦ **Rights Required on the Identity Vault:** To synchronize changes to the Identity Vault, ensure that the driver's *Security Equals DN* has the following rights in the Identity Vault:
 - ♦ **Entry Rights:** The rights to create entries in the Identity Vault.
 - ♦ **Attributes Rights:** The rights to modify the attributes in the Identity Vault.

For modifying the write-managed attributes, the driver's *Security Equals DN* must have management rights on the objects whose DN is being modified.

For receiving events from the Identity Vault, the driver's *Security Equals DN* must have the following rights in the Identity Vault.

- ♦ **Entry Rights:** Browse permission.
- ♦ **Attributes Rights:** Read permission.

- ♦ The change-log file contains information about events on the connected eDirectory servers and passwords. It is encrypted, but it should be protected against access by unauthorized users. The change-log file is located in the DIB directory of eDirectory. The name of the change-log file is based on the GUID of the driver and has a *.TAO* extension. The change-log file can only be accessed by the owner of the eDirectory instance.
- ♦ Sensitive data like passwords and encrypted attributes is encrypted before writing it to the change-log cache file.

6 Synchronizing Passwords

The following list contains information that is specific to setting up password synchronization with the bidirectional eDirectory driver. Use it to supplement the information in the [Identity Manager 4.0.2 Password Management Guide](#).

Universal Password is the standard method to synchronize passwords with Identity Manager. Ensure that the Password policy has Universal Password enabled for synchronizing passwords with Identity Manager. The bidirectional eDirectory driver's configuration policies and filters in the basic configuration file are set up to support the Universal Password method.

To synchronize UP passwords from a Read-only replica on the Publisher Channel, ensure that the following mandatory attributes are enabled on the filter for the user object:

- ◆ CN
- ◆ Surname
- ◆ nspmDistributionPassword
- ◆ nspmPasswordKey

To synchronize the NDS password between the Identity Vault and the connected eDirectory by using the bidirectional eDirectory driver, in the [Driver Configuration](#) section, set the *Password Sync Type* to NDS password.

Password transfer over a clear-text connection is disabled by default. Password transfer is allowed over a secure connection only. The default behavior for transferring passwords can be changed by setting the *Allow password on clear-text connection* driver configuration parameter to *True*. However, this is not a recommended configuration.

7 Managing the Driver

As you work with the bidirectional eDirectory driver, there are several management tasks you might need to perform, including the following:

- ♦ Starting, stopping, and restarting the driver
- ♦ Viewing driver version information
- ♦ Using Named Passwords to securely store passwords associated with the driver
- ♦ Monitoring the driver's health status
- ♦ Backing up the driver
- ♦ Inspecting the driver's cache files
- ♦ Viewing the driver's statistics
- ♦ Using the DirXML Command Line utility to perform management tasks through scripts
- ♦ Securing the driver and its information
- ♦ Synchronizing objects
- ♦ Migrating and resynchronizing data
- ♦ Activating the driver

Because these tasks, as well as several others, are common to all Identity Manager drivers, they are included in one reference, the [NetIQ Identity Manager 4.0.2 Common Driver Administration Guide](#).

8 Troubleshooting

This section provides information about troubleshooting problems you might encounter with the bidirectional eDirectory driver:

- ♦ [Section 8.1, “Troubleshooting Driver Processes,” on page 35](#)

8.1 Troubleshooting Driver Processes

Viewing driver processes is necessary to analyze unexpected behavior. To view the driver processing events, use DSTrace. You should only use it during testing and troubleshooting the driver. Running DSTrace while the drivers are in production increases the utilization on the Identity Manager server and can cause events to process very slowly. For more information, see “[Viewing Identity Manager Processes](#)” in the *NetIQ Identity Manager 4.0.2 Common Driver Administration Guide*.

The following articles provide more information about the Identity Manager trace:

- ♦ [Capturing and Reading Novell Identity Manager Traces \(http://www.novell.com/communities/node/5681/capturing-and-reading-novell-identity-manager-traces\)](http://www.novell.com/communities/node/5681/capturing-and-reading-novell-identity-manager-traces)
- ♦ [Comprehending Identity Manager Traces - Part 1 \(http://www.novell.com/communities/node/9677/comprehending-idm-traces-part-1\)](http://www.novell.com/communities/node/9677/comprehending-idm-traces-part-1)
- ♦ [Comprehending Identity Manager Traces - Part 2 \(http://www.novell.com/communities/node/11166/comprehending-idm-traces-part-2\)](http://www.novell.com/communities/node/11166/comprehending-idm-traces-part-2)

9 Known Issues

The following known issues exist for this version of the driver:

- ♦ [Section 9.1, “NDSTrace displays unable to load dxldap extension module error message,” on page 37](#)
- ♦ [Section 9.2, “The structured attributes are not properly converted,” on page 37](#)
- ♦ [Section 9.3, “The users are not correctly synchronized,” on page 37](#)
- ♦ [Section 9.4, “The NDS password does not synchronize on the Subscriber Channel with Read-Only, Filter Read-Only, and Filter Read/Write replicas,” on page 38](#)
- ♦ [Section 9.5, “Importing the driver causes change of the driver icon,” on page 38](#)
- ♦ [Section 9.6, “The Account Tracking GCV is not upgraded with Designer AU2,” on page 38](#)

9.1 NDSTrace displays unable to load dxldap extension module error message

Sometimes NDSTrace displays the following error message when you refresh the LDAP server object or restart eDirectory on a computer that has change-log installed and had Identity Manager installed on it earlier:

```
Unable to load extension module dxldap, err = -5984 (0xffffffffffffe8a0)
```

When the LDAP server tries to load the `dxldap` handlers that were registered earlier with Identity Manager installation, it doesn't find them because `dxldap` module which has those handlers no longer exists on the computer.

It is safe to ignore this error.

9.2 The structured attributes are not properly converted

The driver does not support the syntax of ACL, Octet List, and SYN_HOLD attributes.

9.3 The users are not correctly synchronized

If you add a user on the connected eDirectory system by using the same *Authentication ID* that was specified in the driver configuration, the newly created user might be synchronized with Identity manager without password.

If the loopback detection is enabled, the change-log fails to pick any changes when you create or modify an object with the same credentials as used in *Authentication ID*. *Authentication ID* should be a unique ID in the connected eDirectory that is not used by any users for object creation, modification, or deletion.

9.4 The NDS password does not synchronize on the Subscriber Channel with Read-Only, Filter Read-Only, and Filter Read/Write replicas

The driver fails to synchronize NDS passwords on the Subscriber Channel because changes cannot be written to the replicas enabled with Read-Only, Filter Read-Only, or Filter Read/Write setting. If *Prefer Chaining* setting is enabled on the replica server, though users are synchronized on the Subscriber channel over the LDAP protocol, the NDS passwords are not synchronized.

9.5 Importing the driver causes change of the driver icon


When the bidirectional eDirectory driver is imported into Designer, the driver icon changes to the legacy eDirectory driver icon.

9.6 The Account Tracking GCV is not upgraded with Designer AU2

To work around this issue, add LDAP DN to the existing set of Account Tracking GCV identifiers.

A Driver Properties


This section provides information about the Driver Configuration, Global Configuration Values properties, and Trace Levels for the bidirectional eDirectory driver. These are the only unique properties for the bidirectional eDirectory driver. All other driver properties (Named Password, Engine Control Values, Log Level, and so forth) are common to all drivers. Refer to “[Driver Properties](#)” in the *NetIQ Identity Manager 4.0.2 Common Driver Administration Guide* for information about the common properties.

The information is presented from the viewpoint of iManager. If a field is different in Designer for Identity Manager, it is marked with a Designer  icon.

- ◆ [Section A.1, “Driver Configuration,” on page 39](#)
- ◆ [Section A.2, “Global Configuration Values,” on page 43](#)
- ◆ [Section A.3, “Trace Levels,” on page 49](#)

A.1 Driver Configuration

In iManager:

- 1 Click  to display the Identity Manager Administration page.
- 2 Open the driver set that contains the driver whose properties you want to edit:
 - 2a In the *Administration* list, click *Identity Manager Overview*.
 - 2b If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.
 - 2c Click the driver set to open the Driver Set Overview page.
- 3 Locate the driver icon, then click the upper right corner of the driver icon to display the *Actions* menu.
- 4 Click *Edit Properties* to display the driver’s properties page.

In Designer:

- 1 Open a project in the Modeler, then right-click the driver line and click *Properties > Driver Configuration*.

The Driver Configuration options are divided into the following sections:

- ◆ [Section A.1.1, “Driver Module,” on page 40](#)
- ◆ [Section A.1.2, “Driver Object Password,” on page 40](#)
- ◆ [Section A.1.3, “Authentication,” on page 40](#)
- ◆ [Section A.1.4, “Startup Option,” on page 40](#)
- ◆ [Section A.1.5, “Driver Parameters,” on page 41](#)
- ◆ [Section A.1.6, “ECMAScript,” on page 43](#)
- ◆ [Section A.1.7, “Global Configurations,” on page 43](#)

A.1.1 Driver Module

The driver module changes the driver from running locally to running remotely or the reverse.

Java: Used to specify the name of the Java class that is instantiated for the shim component of the driver. This class can be located in the `classes` directory as a class file, or in the `lib` directory as a `.jar` file. If this option is selected, the driver is running locally. By default, the Java class name is `com.novell.nds.dirxml.driver.edir.EDIRDriverShim`. The class path is case-sensitive.

Native: This option is not used with the bidirectional eDirectory driver.

Connect to Remote Loader: The Remote Loader is not used with the bidirectional eDirectory driver.

A.1.2 Driver Object Password

This option is not used with the bidirectional eDirectory driver.

A.1.3 Authentication

The Authentication section stores the information required to authenticate to the connected system. For the bidirectional eDirectory driver, it stores the information required to authenticate to the eDirectory server that the driver is associated with.

Authentication ID: Specify the DN of the LDAP account that the driver will use to authenticate to connected eDirectory. For information, see [Chapter 5, “Configuring SSL Connections,” on page 27](#).

Connection Context: Specify the hostname or IP address of the eDirectory server as well as the decimal port number (for example, 187.168.1.1:389).

Port 389 uses the TLS protocol for a clear text connection, and port 636 uses the SSL protocol. For more information, see [Chapter 5, “Configuring SSL Connections,” on page 27](#).

Remote Loader Connection Parameters: The bidirectional eDirectory driver does not support the use of the Remote Loader for a local driver. These options do not apply.

Driver Cache Limit (KB): Specify the maximum event cache file size (in KB). If the value is set to zero, the file size is unlimited. Click *Unlimited* to set the file size to unlimited in Designer.

Application Password: Specify the password for the user object listed in the *Authentication ID* option.

For more information, see [Chapter 5, “Configuring SSL Connections,” on page 27](#).

Remote Loader Password: This option is not used with the bidirectional eDirectory driver.

A.1.4 Startup Option

The Startup Option section enables you to set the driver state when the Identity Manager server is started.

Auto start: The driver starts every time the Identity Manager server is started.

Manual: The driver does not start when the Identity Manager server is started. The driver must be started through Designer or iManager.

Disabled: The driver has a cache file that stores all of the events. When the driver is set to *Disabled*, this file is deleted and no new events are stored in the file until the driver state is changed to *Manual* or *Auto Start*.

If the driver is *Disabled* and then changed to *Auto start* or *Manual*, you can select the *Do Not Automatically Synchronize the Driver* check box. This prevents the driver from synchronizing objects automatically when it loads. To synchronize objects manually, use the *Synchronize* button on the Driver Overview page.

A.1.5 Driver Parameters

The Driver Parameters section lets you configure the driver-specific parameters. When you change driver parameters, you tune driver behavior to align with your network environment.

The parameters are divided into the following categories:

- ◆ “[Driver Settings](#)” on page 41
- ◆ “[Subscriber Settings](#)” on page 42
- ◆ “[Publisher Settings](#)” on page 42

Driver Settings

Use SSL: Select *Yes* to use SSL to secure communication between the bidirectional eDirectory driver and the eDirectory server. If you use SSL, fill in the following parameters:

- ◆ **Always Accept Server Certificate:** Select *Yes* if you want the driver to accept the LDAP server's certificate for establishing SSL connection with the eDirectory server. To use the keystore, select this option to *No*. For more information on setting up SSL connections, see [Chapter 5, “Configuring SSL Connections,” on page 27](#).
- ◆ **Keystore Path for SSL Certificates:** Specify the full path to the keystore file containing the SSL certificates.
- ◆ **Use Mutual Authentication:** Select *Yes* if you want the driver to use SSL mutual authentication (both client and server), or select *No* for server authentication only. If you select *Yes*, you must have the appropriate certificates configured in your keystore.
- ◆ **Key Alias:** Specify the alias of the key.
- ◆ **Keystore Password:** Specify the password for accessing the keystore file containing the SSL certificates.
- ◆ **Reenter Keystore Password:** Specify the password again.
- ◆ **Remove Existing Password:** Enable this option if you do not want to specify the keystore password. If you select this option, the *Keystore Password* option is automatically disabled.

Password Sync Type: Specifies which password sync type to use. By default, this option is set to *Sync UP password*. To sync NDS password, select *Sync NDS password* option and enable the public/private key pair in the driver filter for both Publisher and Subscriber channels.

User Container: Specifies the container where the users are added if they do not already exist in the Identity Vault. This value becomes the default value for all drivers in the driver set. It is in slash format, such as `netiq/users`, where `ou=users.o=netiq`.

Subscriber Settings

Show Default Configuration: This option applies to the connected eDirectory server. Select *Show* to display the following option:

- ♦ **eDirectory Port Number:** Specify the port number of the connected eDirectory server. This port number is used for creating home directories. The default value is 524. For more information, see [Section B.2, “Creating Home Directories,”](#) on page 52.

Publisher Settings

Show Default Configuration: This option applies to the connected eDirectory server. Select *Show* to display the following options:

- ♦ **eDirectory Base Container:** Specifies the connected eDirectory container in the slash format where objects are synchronized. If you are using a flat Placement rule, this is the container where the users are placed. If you are using a mirrored Placement rule, this is the base container. For example, `netiq/users`, where `ou=users.o=netiq` or `ou=people,ou=example,o=com`.
- ♦ **Polling Interval in Seconds:** Specifies the number of seconds that the Publisher channel waits after running the polling script and sending eDirectory events from the change-log to the Metadirectory engine.
- ♦ **Heartbeat Interval in Minutes:** Specifies how often, in minutes, the driver shim contacts the Metadirectory engine when there has not been any traffic during the interval time. Specify 0 to disable the heartbeat.
- ♦ **Allow Loop-back Detection:** When this option is set to *True*, the driver avoids event loopback. However, the passwords still loopback into the Publisher channel since passwords are always modified by the server object. When the option is set to *False*, the Subscriber channel events might loop into the Publisher channel.

The default behavior of the Publisher channel is to avoid sending changes that the Subscriber channel makes. The Publisher channel detects Subscriber channel changes by looking at the `creatorsName` or `modifiersName` attribute to see whether the authenticated entry that made the change is the same entry that the driver uses to authenticate to the eDirectory server. If the entry is the same, the Publisher channel assumes that this change was made by the driver's Subscriber channel and doesn't synchronize the change.

Show Change-log Plug-in Configuration: This setting applies to the configuration of the change-log plug-in. Select *Show* to display the following options:

- ♦ **Maximum Days without Reconnect:** Specify the number of days after which driver change cache and registration information is deleted if the driver does not connect. The default value is 30.
- ♦ **Ignore Processing Errors:** Specify if the change-log should ignore any error codes that it receives during `SendChangesResponse` operation. If the value is set to *true*, the errors are ignored and the next event is processed. By default, the value is set to *false*, which means the same event might be resent.
- ♦ **Allow Password on Clear-text Connection:** By default, the value is *false*, which means that the password is sent over a secure channel. You can change the value to *true* to send the password in clear text, but this is not a recommended setting.
- ♦ **Change-log Trace Level:** Specify the change-log trace level. There are three trace levels: `ERROR`, `INFO`, and `DEBUG`. Detailed messages are logged if you select `INFO`. `DEBUG` logs debugging data along with detailed messages. The default trace level is `ERROR`.

To view the change-log trace on the remote eDirectory server, enable the DVRS and DXML flags of the DSTrace utility.

- ♦ **Change-log Preferred Maximum Batch-size:** Specify the maximum number of events that the change-log module sends in a batch between a range of 1 to 500.

A.1.6 ECMAScript

The ECMAScript section enables you to add ECMAScript resource files. The resources extend the driver's functionality when Identity Manager starts the driver.


A.1.7 Global Configurations

The Global Configurations section displays an ordered list of Global Configuration objects. The objects contain extension GCV definitions for the driver that Identity Manager loads when the driver is started. You can add or remove the Global Configuration objects, and you can change the order in which the objects are executed.

A.2 Global Configuration Values


Global configuration values (GCVs) are values that can be used by the driver to control functionality. GCVs are defined on the driver or on the driver set. Driver set GCVs can be used by all drivers in the driver set. Driver GCVs can be used only by the driver on which they are defined.

The bidirectional eDirectory driver includes several GCVs that are created from information supplied during importing the driver configuration file (see [Chapter 4, "Creating a New Driver Object," on page 17](#)) and one that is not.

The driver also includes the GCVs that are used with password synchronization. In Designer, you must click the  icon next to a password synchronization GCV to edit it. This displays the Password Synchronization Options dialog box that has a better view of the relationship between the different settings. In iManager, you should edit the password synchronization settings on the *Server Variables* tab rather than under the GCVs. The Server Variables page has a better view of the relationship between the different GCVs.

You can add your own GCVs if you discover you need additional ones as you implement policies in the driver.


To access the driver's GCVs in iManager:

- 1 Click  to display the Identity Manager Administration page.
- 2 Open the driver set that contains the driver whose properties you want to edit:
 - 2a In the *Administration* list, click *Identity Manager Overview*.
 - 2b If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.
 - 2c Click the driver set to open the Driver Set Overview page.
- 3 Locate the driver icon, click the upper right corner of the driver icon to display the *Actions* menu, then click *Edit Properties*.

or

To add a GCV to the driver set, click *Driver Set*, then click *Edit Driver Set properties*.

To access the driver's GCVs in Designer:

- 1 Open a project in the Modeler.
 - 2 Right-click the driver icon  or line, then select *Properties > Global Configuration Values*.
- or

To add a GCV to the driver set, right-click the driver set icon , then click *Properties > GCVs*.

The Global Configuration Values are divided into following categories:

- ♦ [Section A.2.1, “eDirectory Base Container,” on page 44](#)
- ♦ [Section A.2.2, “Default Configuration,” on page 44](#)
- ♦ [Section A.2.3, “Password Synchronization,” on page 45](#)
- ♦ [Section A.2.4, “Account Tracking,” on page 45](#)
- ♦ [Section A.2.5, “Entitlements,” on page 46](#)
- ♦ [Section A.2.6, “Managed System Information,” on page 48](#)

A.2.1 eDirectory Base Container

The eDirectory Base Container section specifies the container where user objects reside in the connected eDirectory server. If you are using a Flat Placement rule, this is the container where the users are placed. If you are using a Mirrored Placement rule, this is the base container. For example, `OU=People,DC=example,DC=com`.

A.2.2 Default Configuration

The following GCVs define control the default configuration of the bidirectional eDirectory driver:

Subscriber Channel Placement type: Controls how the objects are placed in the base container of the connected eDirectory server. The options are:

- ♦ **Mirrored:** Mirrors the structure between the Identity Vault and the connected eDirectory server. It places objects hierarchically within the base container.

This option in the driver configuration synchronizes User, Group, Organization, Country, and Organizational Unit objects.

- ♦ **Flat:** All of the objects are placed within the base container.

This option synchronizes User, Group, Organization, and Organizational Unit objects.

Publisher Channel Placement Type: Controls how the objects are placed in the Identity Vault. The options are:

- ♦ **Mirrored:** Mirrors the structure between the Identity Vault and the connected eDirectory server. It places objects hierarchically within the base container.


This option in the driver configuration synchronizes User, Group, Organization, Country, and Organizational Unit objects.

- ♦ **Flat:** All of the objects are placed within the base container.

This option synchronizes User, Group, Organization, and Organizational Unit objects.

A.2.3 Password Synchronization

The following GCVs control password synchronization for the bidirectional eDirectory driver. For more information, see the [Identity Manager 4.0.2 Password Management Guide](#).

In Designer, you must click the  icon next to a GCV to edit it. This displays the Password Synchronization Options dialog box for a better view of the relationship between the different GCVs.

In iManager, you should edit the Password Management Options on the *Server Variables* tab rather than under the GCVs. The Server Variables page has a better view of the relationship between the different GCVs.

Connected System Name or Driver Name: Specify the name of the driver. The e-mail notification template uses this value to identify the source of the notification message.

Application accepts passwords from Identity Manager: If this option is set to *True*, it allows passwords to flow from the Identity Manager data store to the connected eDirectory server.

Identity Manager accepts passwords from application: If this option is set to *True*, it allows passwords to flow from the connected system to Identity Manager.

Publish passwords to NDS password: Use the password from the connected system to set the non-reversible NDS password in eDirectory.

Publish passwords to Distribution Password: Use the password from the connected system to set the NMAS Distribution Password used for Identity Manager password synchronization.

Require password policy validation before publishing passwords: If this option is set to *True*, it applies NMAS password policies during publish password operations. The password is not written to the data store if it does not comply.

Reset user's external system password to the Identity Manager password on failure: If this option is set to *True*, and the Distribution Password fails to distribute, attempt to reset the password in the connected system by using the Distribution Password from the Identity Manager data store.

Notify the user of password synchronization failure via e-mail: If this option is set to *True*, notify the user by e-mail of any password synchronization failures.

A.2.4 Account Tracking

Account tracking is part of the Identity Reporting Module. For more information, see the [Using Identity Manager 4.0.2 Reports](#).

Enable account tracking: Set this to *True* to enable account tracking policies. Set it to *False* if you do not want to execute account tracking policies.

Realm: Specify the name of the realm, security domain, or namespace in which the account name is unique.

Object Class: Add the object class to track. Class names must be in the application namespace.

Identifiers: Add the account identifier attributes. Attribute names must be in the application namespace.

Status attribute: Name of the attribute in the application namespace to represent the account status.

Status active value: Value of the status attribute that represents an active state.

Status inactive value: Value of the status attribute that represents an inactive state.

Subscription default status: Select the default status the policies assume when an object is subscribed to the application and the status attribute is not set in the Identity Vault.

Publication default status: Select the default status the policies assume when an object is published to the Identity Vault and the status attribute is not set in the application.

A.2.5 Entitlements

There are multiple sections in the *Entitlements* tab. Depending on which packages you installed, different options are enabled or displayed.

- ◆ [“Entitlements” on page 46](#)
- ◆ [“Data Collection” on page 46](#)
- ◆ [“Role Mapping” on page 47](#)
- ◆ [“Resource Mapping” on page 47](#)
- ◆ [“Parameter Format” on page 47](#)
- ◆ [“Entitlement Extensions” on page 47](#)

Entitlements

For more information about entitlements, see [Section 1.2.2, “Entitlements,” on page 12](#).

Use Entitlements to control eDirectory Accounts: Select *True* to enable the driver to manage user accounts based on the driver’s defined entitlements. Select *False* to disable management of user accounts based on the entitlements.

Enable Login Disabled attribute sync: Select *True* if the changes made to the LoginDisabled attribute in the Identity Vault should be synced even if the User Account entitlement (Account) is enabled.

Account action on Entitlement Revoke: Select the action to take when a user account entitlement is revoked. The options are *Disable User*, *Do Nothing*, or *Delete User*. By default, *Disable User* is selected.

Use Group Entitlement: Select *True* to enable the driver to manage user groups based on the driver’s defined entitlements.

Select *False* to disable management of group membership based on the entitlements.

Advanced Settings: Select show to display the entitlement options that allow or deny additional functionality like data collection and others. These settings should rarely be changed.

Data Collection

Data collection enables the Identity Report Module to gather information to generate reports. For more information, see the [Using Identity Manager 4.0.2 Reports](#).

Enable data collection: Select *Yes* to enable data collection for the driver through the Data Collection Service by the Managed System Gateway driver. If you are not going to run reports on data collected by this driver, select *No*.

Allow data collection from user accounts: Select *Yes* to allow data collection by the Data Collection Service through the Managed System Gateway driver for the user accounts.

Allow data collection from groups: Select Yes to allow data collection by the Data Collection Service through the Managed System Gateway driver for groups.

Role Mapping

The Role Mapping Administrator allows you to map business roles with IT roles. For more information, see the [Novell Identity Manager Role Mapping Administrator 4.0.2 User Guide](#).

Enable role mapping: Select Yes to make this driver visible to the Role Mapping Administrator.

Allow mapping of user accounts: Select Yes if you want to allow mapping of user accounts in the Role Mapping Administrator. An account is required before a role, profile, or license can be granted through the Role Mapping Administrator.

Allow mapping of groups: Select Yes if you want to allow mapping of groups in the Role Mapping Administrator.

Resource Mapping

The Roles Based Provisioning Module allows you to map resources to users. For more information, see the [User Application: User Guide](#).

Enables resource mapping: Select Yes to make this driver visible to the Roles Based Provisioning Module.

Allow mapping of user accounts: Select Yes if you want to allow mapping of user accounts in the Roles Based Provisioning Module. An account is required before a role, profile, or license can be granted.

Allow mapping of groups: Select Yes if you want to allow mapping of groups in the Roles Based Provisioning Module.

Parameter Format

Format for Account entitlement: Select the parameter format the entitlement agent must use. The options are *Identity Manager 4* or *Legacy*.

Format for Group entitlement: Select the parameter format the entitlement agent must use. The options are *Identity Manager 4* or *Legacy*.

Entitlement Extensions

User account extensions: The content of this field is added below the entitlement elements in the EntitlementConfiguration resource object.

Group extensions: The content of this field is added below the entitlement element in the EntitlementConfiguration resource object.

Exchange mailbox extensions: The content of this field is added below the entitlement element in the EntitlementConfiguration resource object.

A.2.6 Managed System Information

These settings help the Identity Reporting Module function to generate reports. There are different sections in the *Managed System Information* tab.

- ◆ [“General Information” on page 48](#)
- ◆ [“System Ownership” on page 48](#)
- ◆ [“System Classification” on page 48](#)
- ◆ [“Connection and Miscellaneous Information” on page 49](#)

General Information

Name: Specify a descriptive name for this connected eDirectory system. This name is displayed in the reports.

Description: Specify a brief description of this connected eDirectory system. This description is displayed in the reports.

Location: Specify the physical location of this connected eDirectory system. This location is displayed in the reports.

Vendor: Select Novell as the vendor of the connected eDirectory system. This information is displayed in the reports.

Version: Specify the version of this connected eDirectory system. This version information is displayed in the reports.

System Ownership

Business Owner: Browse to and select the business owner in the Identity Vault for this connected eDirectory system. You must select a user object, not a role, group, or container.

Application Owner: Browse to and select the application owner in the Identity Vault for this connected eDirectory system. You must select a user object, not a role, group, or container.

System Classification

Classification: Select the classification of the connected eDirectory system. This information is displayed in the reports. The options are:

- ◆ Mission-Critical
- ◆ Vital
- ◆ Not-Critical
- ◆ Other

If you select *Other*, you must specify a custom classification for the connected eDirectory system.

Environment: Select the type of environment the connected eDirectory system provides. The options are:

- ◆ Development
- ◆ Test
- ◆ Staging

- ◆ Production
- ◆ Other

If you select *Other*, you must specify a custom classification for the connected eDirectory system.

Connection and Miscellaneous Information

Connection and miscellaneous information: This options is always set to *hide*, so that you don't make changes to these options. These options are system options that are necessary for reporting to work. If you make any changes, reporting stops working.

A.3 Trace Levels

The driver supports the following trace levels:

Table A-1 Supported Trace Levels

Level	Description
0	No Trace Messages
1-2	Basic Trace Messages such as driver start/stop, documents sent/received are displayed
3-12	Previous level plus some additional information message
13	Previous level plus in depth details of messages received in publisher

B Synchronized Attributes

By default, the filter for the basic driver configuration supports the following attributes. You can customize the filter to extend support for additional attributes.

- ♦ [Section B.1, “Default Attributes,” on page 51](#)
- ♦ [Section B.2, “Creating Home Directories,” on page 52](#)

B.1 Default Attributes

assistant	homeState	Postal Code
assistantPhone	homeZipCode	Postal Office Box
businessCategory	Initials	instantMessagingID
C	instantMessagingID	preferredDeliveryMethod
city	Internet EMail Address	preferredName
CN	jackNumber	registeredAddress
co	jobCode	roomNumber
company	L	S
costCenter	Language	SA
costCenterDescription	Login Disabled	Security Equals
children	Mailbox ID	See Also
departmentNumber	Mailbox Location	siteLocation
Description	mailstop	spouse
directReports	manager	Surname
EMail Address	managerWorkforceID	Telephone Number
employeeStatus	Member	teletexTerminalIdentifier
employeeType	mobile	telexNumber
Equivalent To Me	NSCP:employeeNumber	Timezone
Facsimile Telephone Number	nspmDistributionPassword	Title
Full Name	O	tollFreePhoneNumber
Generational Qualifier	otherPhoneNumber	UID
Given Name	OU	uniqueID
Group Membership	pager	userCertificate
homeCity	personalMobile	vehicleInformation

homeEmailAddress	personalTitle	
homeFax	Postal Address	
homePhone	photo	workforceID
homePostalAddress	Physical Delivery Office Name	User

B.2 Creating Home Directories

You can use the user template to create home directories in the destination eDirectory. In the policy, set the value for the *Set Operation Template DN (do-set-op-template-dn)* as the DN of the template that is used to create the home directory.

Example

```

<actions>
  <do-set-op-template-dn>
    <arg-dn>
      <token-text xml:space="preserve">Data\Users\UserCreationTemplate</token-
text>
    </arg-dn>
  </do-set-op-template-dn>
</actions>

```