

Driver for LDAP Implementation Guide

Novell® Identity Manager

3.6

July 23, 2008

www.novell.com



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 © 2007-2008 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. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at [Novell Legal Patents \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
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 Novell trademarks, see [Novell Trademark and Service List \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](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	7
1 Overview	9
1.1 Driver Concepts	9
1.1.1 Synchronizing Data	9
1.1.2 Publication Methods	9
1.1.3 How the LDAP Driver Works	10
1.2 Support for Standard Driver Features	12
1.2.1 Local and Remote Platforms	12
1.2.2 Entitlements	13
1.2.3 Password Synchronization	13
2 Installing the Driver Files	15
2.1 Installing the Driver Files	15
2.2 Installing the Identity Manager Plug-Ins for Password Synchronization with Sun Java System Directory	15
2.2.1 How the Plug-In Works	16
2.2.2 Where to Find the Plug-In	16
2.2.3 Installing the Plug-In	17
3 Preparing the LDAP Server	19
3.1 Creating an LDAP User Object with Authentication Rights	19
3.2 Enabling the Change Log	20
4 Creating a New Driver	21
4.1 Creating the Driver in Designer	21
4.1.1 Importing the Driver Configuration File	21
4.1.2 Configuring the Driver	22
4.1.3 Deploying the Driver	23
4.1.4 Starting the Driver	23
4.2 Creating the Driver in iManager	24
4.2.1 Importing the Driver Configuration File	24
4.2.2 Configuring the Driver	26
4.2.3 Starting the Driver	27
4.3 Activating the Driver	27
5 Upgrading an Existing Driver	29
5.1 Supported Upgrade Paths	29
5.2 What's New in Version 3.6	29
5.3 Upgrade Procedure	29
6 Synchronizing Data	31
6.1 Determining Which Objects Are Synchronized	31
6.2 Defining Schema Mapping	31

6.3	Netscape Directory Server Configuration	33
6.3.1	Defining Object Placement in Netscape Directory Server	33
6.3.2	Working with eDirectory Groups and Netscape	34
6.4	Migrating and Resynchronizing Data	34
7	Configuring SSL Connections	37
7.1	Step 1: Generating a Server Certificate	37
7.2	Step 2: Sending the Certificate Request	38
7.3	Step 3: Installing the Certificate	38
7.4	Step 4: Activating SSL in Netscape Directory Server 4.12.	39
7.5	Step 5: Exporting the Trusted Root from the Directory Tree	39
7.6	Step 6: Importing the Trusted Root Certificate	40
7.6.1	Importing into the LDAP Server's Trust Database	40
7.6.2	Importing into the Client's Certificate Store	40
7.7	Step 7: Adjusting Driver Settings	41
8	Managing the Driver	43
9	Troubleshooting	45
9.1	Troubleshooting Driver Processes	45
9.2	Migrating Users into an Identity Vault	45
9.3	OutOfMemoryError.	45
9.4	LDAP v3 Compatibility	46
9.5	Frequently Asked Questions	46
A	Driver Properties	47
A.1	Driver Configuration	47
A.1.1	Driver Module	47
A.1.2	Driver Object Password (iManager Only)	48
A.1.3	Authentication	48
A.1.4	Startup Option	49
A.1.5	Driver Parameters	50
A.2	Global Configuration Values	54
B	Trace Levels	57

About This Guide

This guide explains how to install, configure, and manage the Identity Manager Driver for LDAP.

- ♦ Chapter 1, “Overview,” on page 9
- ♦ Chapter 2, “Installing the Driver Files,” on page 15
- ♦ Chapter 3, “Preparing the LDAP Server,” on page 19
- ♦ Chapter 4, “Creating a New Driver,” on page 21
- ♦ Chapter 5, “Upgrading an Existing Driver,” on page 29
- ♦ Chapter 6, “Synchronizing Data,” on page 31
- ♦ Chapter 7, “Configuring SSL Connections,” on page 37
- ♦ Chapter 8, “Managing the Driver,” on page 43
- ♦ Chapter 9, “Troubleshooting,” on page 45
- ♦ Appendix A, “Driver Properties,” on page 47
- ♦ Appendix B, “Trace Levels,” on page 57

Audience

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

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Use the User Comment feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of this guide, see *Identity Manager 3.6 Driver for LDAP* on the [Identity Manager 3.6 Drivers Documentation Web site](http://www.novell.com/documentation/idm36drivers/index.html) (<http://www.novell.com/documentation/idm36drivers/index.html>).

Additional Documentation

For information on Identity Manager and other Identity Manager drivers, see the [Identity Manager 3.6 Documentation Web site](http://www.novell.com/documentation/idm36) (<http://www.novell.com/documentation/idm36>).

Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items within a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

The Identity Manager Driver for LDAP (LDAP driver) synchronizes data between the Identity Vault and LDAP-compliant directories. The driver supports the Subscriber and Publisher channels, uses filters to control objects and attributes, and uses policies to control data.

- ♦ [Section 1.1, “Driver Concepts,” on page 9](#)
- ♦ [Section 1.2, “Support for Standard Driver Features,” on page 12](#)

1.1 Driver Concepts

- ♦ [Section 1.1.1, “Synchronizing Data,” on page 9](#)
- ♦ [Section 1.1.2, “Publication Methods,” on page 9](#)
- ♦ [Section 1.1.3, “How the LDAP Driver Works,” on page 10](#)

1.1.1 Synchronizing Data

The Identity Manager Driver for LDAP synchronizes data between an Identity Vault and LDAP-compliant directories. The driver can run anywhere that a Metadirectory server or Identity Manager Remote Loader is running. See [Section 1.2.1, “Local and Remote Platforms,” on page 12](#).

The driver uses the Lightweight Directory Access Protocol to bidirectionally synchronize changes between an Identity Vault and the connected LDAP-compliant directory.

Because of this flexible model for communicating, the driver can synchronize with LDAP-compliant directories running on platforms (for example, HP-UX*, OS/400*, and OS/390*) that are not supported by an Identity Vault.

1.1.2 Publication Methods

The driver can use either of two publication methods to recognize data changes and communicate them to an Identity Vault through Identity Manager:

- ♦ [“Changelog Method” on page 9](#)
- ♦ [“LDAP-Search Method” on page 10](#)

Changelog Method

This method is preferred when a change log is available. Change logs are found on the following:

- ♦ Critical Path* InJoin* Directory
- ♦ IBM* SecureWay* Directory
- ♦ IBM Tivoli* Directory
- ♦ iPlanet* Directory Server
- ♦ Isode* M-Vault
- ♦ Netscape* Directory Server

- ♦ Oracle* Internet Directory
- ♦ Sun* Java* System Directory

LDAP-Search Method

Some servers don't use the changelog mechanism. The LDAP-search method enables the LDAP driver to publish data about the LDAP server to an Identity Vault by searching for changes in predefined contexts in the LDAP directory.

The LDAP-search method synchronizes changes that occur from one poll to the next.

1.1.3 How the LDAP Driver Works

Channels, filters, and policies control data flow.

- ♦ [“Publisher and Subscriber Channels” on page 10](#)
- ♦ [“Filters” on page 10](#)
- ♦ [“Policies” on page 11](#)

Publisher and Subscriber Channels

The LDAP driver supports Publisher and Subscriber channels:

- ♦ The Publisher channel reads information from the LDAP directory change log or an LDAP search and submits that information to an Identity Vault via the Metadirectory engine.

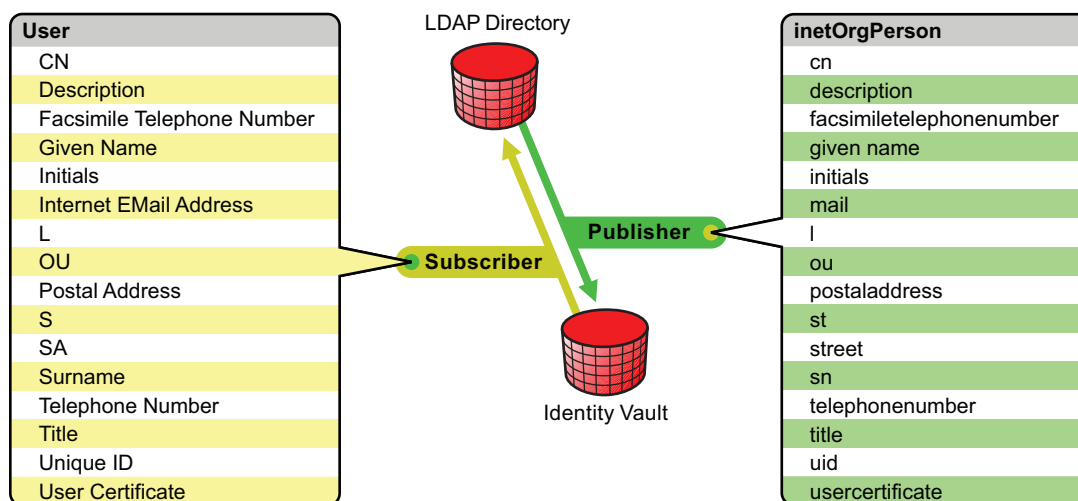
By default, the Publisher channel checks the log every 20 seconds, processing up to 1000 entries at a time, starting with the first unprocessed entry.

- ♦ The Subscriber channel watches for additions and modifications to Identity Vault objects and issues LDAP commands that make changes to the LDAP directory.

Filters

Identity Manager uses filters to control which objects and attributes are shared. The default filter configurations for the LDAP driver allow objects and attributes to be shared, as illustrated in the following figure:

Figure 1-1 LDAP Driver Filters



Policies

Policies are used to control data synchronization between the driver and an Identity Vault.

The following table provides information on default policies. These policies and the individual rules they contain can be customized as explained in [Chapter 6, “Synchronizing Data,” on page 31](#).

Table 1-1 Default Policies

Policy	Description
Mapping	<p>Maps the Identity Vault User object and selected properties to an LDAP inetOrgPerson.</p> <p>Maps the Identity Vault Organizational Unit to an LDAP organizationalUnit.</p> <p>By default, more than a dozen standard properties are mapped.</p>
Publisher Create	Specifies that in order for a User to be created in an Identity Vault, the cn, sn, and mail attributes must be defined. In order for an Organization Unit to be created, the OU attribute must be defined.
Publisher Placement	Specifies that new User objects created in the LDAP directory are placed under a specified Identity Vault container in the same structure that mirrors the object's LDAP container structure. In other words, an Identity Vault container (defined during creation of the driver) becomes the root container in which the LDAP objects are mirrored exactly as they exist in the LDAP directory.
Matching	Specifies that a user object in an Identity Vault is the same object as an inetOrgPerson in the LDAP directory when the e-mail attributes match.

Policy	Description
Subscriber Create	Specifies that in order for a user to be created in the LDAP directory, the CN, Surname, and Internet Email Address attributes must be defined. In order for an Organization Unit to be created, the OU attribute must be defined.
Subscriber Placement	Specifies that new User objects created in the Identity Vault are placed under a specified LDAP container in the same structure that mirrors the object's Identity Vault container structure. In other words, an LDAP container (defined during creation of the driver) becomes the root container in which the Identity Vault objects are mirrored exactly as they exist in the Identity Vault.

1.2 Support for Standard Driver Features

The LDAP driver supports these standard driver features:

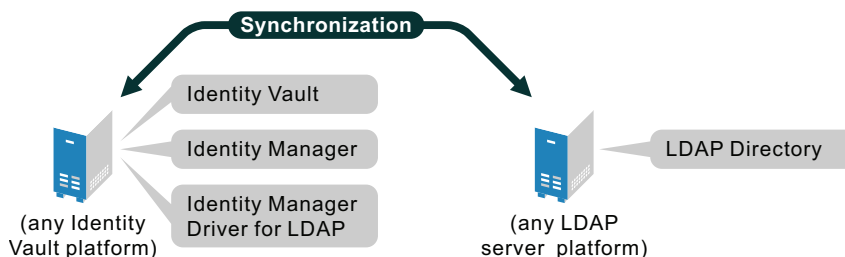
- ♦ [Section 1.2.1, “Local and Remote Platforms,” on page 12](#)
- ♦ [Section 1.2.2, “Entitlements,” on page 13](#)
- ♦ [Section 1.2.3, “Password Synchronization,” on page 13](#)

1.2.1 Local and Remote Platforms

You can install the LDAP driver locally or remotely.

An installation on the same computer where an Identity Vault and the Metadirectory engine are installed is referred to as a local configuration. The following figure illustrates a local configuration:

Figure 1-2 A Local Configuration



If platform or policy constraints make a local configuration difficult, you can install the LDAP driver on the server hosting the target LDAP server. This installation is referred to as a remote configuration and requires the use of the Remote Loader service.

Although a remote configuration is possible, it provides little additional flexibility because of the following:

- ♦ The driver can run on any Identity Vault platform.
- ♦ The driver communicates with the LDAP server on any platform across the wire via the LDAP protocol.

See “[System Requirements](#)” in the *Identity Manager 3.6 Installation Guide* for information about the supported platforms for the Metadirectory server and Remote Loader.

1.2.2 Entitlements

The provided sample configuration for the LDAP driver supports Account and Group Membership entitlements. For more information about entitlements, see the *Identity Manager 3.6 Entitlements Guide*.

1.2.3 Password Synchronization

The LDAP driver supports password synchronization on the Subscriber channel, meaning that you can send passwords from the Identity Vault to any connected LDAP directory.

Password synchronization on the Publisher channel (LDAP directory to Identity Vault) is supported only with Sun Java System Directory version 5.2. See [Section 2.2, “Installing the Identity Manager Plug-Ins for Password Synchronization with Sun Java System Directory,”](#) on page 15.

Installing the Driver Files

By default, the LDAP 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 and the driver configuration file. It does not create the driver in the Identity Vault (see [Chapter 4, "Creating a New Driver," on page 21](#)) or upgrade an existing driver's configuration (see [Chapter 5, "Upgrading an Existing Driver," on page 29](#)).

The following sections explain what to do if the LDAP driver files are not on the server you want and how to install them:

- ♦ [Section 2.1, "Installing the Driver Files," on page 15](#)
- ♦ [Section 2.2, "Installing the Identity Manager Plug-Ins for Password Synchronization with Sun Java System Directory," on page 15](#)

2.1 Installing the Driver Files

If you performed a custom installation and did not install the LDAP driver on the Metadirectory server, you have two options:

- ♦ Install the files on the Metadirectory server, using the instructions in "[Installing the Metadirectory Server](#)" in the *Identity Manager 3.6 Installation Guide*.
- ♦ Install the Remote Loader (required to run the driver on a non-Metadirectory server) and the driver files on a non-Metadirectory server where you want to run the driver. See "[Installing the Remote Loader](#)" in the *Identity Manager 3.6 Installation Guide*.

2.2 Installing the Identity Manager Plug-Ins for Password Synchronization with Sun Java System Directory

The LDAP driver supports password synchronization on the Subscriber channel, meaning that you can send passwords from the Identity Vault to any connected LDAP directory.

Password synchronization on the Publisher channel (LDAP directory to Identity Vault) is supported only with Sun Java System Directory version 5.2 and requires you to install an Identity Manager plug-in to the Sun Java System Directory.

IMPORTANT: You must use Sun Java System Directory 5.2 without any patches. The patches introduced changes to the API used by the plug-in; these changes are not yet supported and cause the plug-in to stop working.

The plug-in, which you install on the Sun Java System Directory Server, is supported on the following platforms and versions:

- ♦ Windows* XP Professional
- ♦ Red Hat* 7.2

- ♦ Solaris* 8 64-bit
- ♦ AIX* 5.1

The following sections provide information to help you use the plug-in:

- ♦ [Section 2.2.1, “How the Plug-In Works,” on page 16](#)
- ♦ [Section 2.2.2, “Where to Find the Plug-In,” on page 16](#)
- ♦ [Section 2.2.3, “Installing the Plug-In,” on page 17](#)

2.2.1 How the Plug-In Works

The plug-in is a post-operation plug-in. Sun Java System Directory notifies the plug-in whenever a password is set or changed. The plug-in then encrypts the password by using the Advanced Encryption Standard (AES) and stores the encrypted password on the novellDistPassword attribute. The LDAP driver can then synchronize the encrypted password to Novell Identity Manager. The LDAP driver decrypts the password and uses it to set the Identity Manager distribution password.

IMPORTANT: Only passwords that are set or modified after the plug-in is installed can be synchronized.

2.2.2 Where to Find the Plug-In

The plug-in is located on the Identity Manager 3.6 DVD and on the Identity Manager 3.6 CD for the Windows, Linux*, Solaris, and AIX platforms.

Table 2-1 *Plug-In Location*

DVD or CD	Location	Filename
Identity Manager 3.6 DVD	<i>root\setup\utilities\sun_password_plugins\platform</i>	Windows: novl-idm-pswd.dll
		Linux: novl-idm-pswd.so
		Solaris: novl-idm-pswd.so
		AIX: novl-idm-pswd.so
Identity Manager 3.6 CD - Windows	<i>root\windows\setup\utilities\sun_password_plugins\platform</i>	Windows: novl-idm-pswd.dll
		Linux: novl-idm-pswd.so
		Solaris: novl-idm-pswd.so
		AIX: novl-idm-pswd.so
Identity Manager 3.6 CD - Linux	<i>root\linux\setup\utilities\sun_password_plugins\platform</i>	Windows: novl-idm-pswd.dll
		Linux: novl-idm-pswd.so
		Solaris: novl-idm-pswd.so
		AIX: novl-idm-pswd.so

DVD or CD	Location	Filename
Identity Manager 3.6 CD - Solaris	<i>root\solaris\setup\utilities\sun_password_plugins\platform</i>	Windows: novl-idm-pswd.dll
		Linux: novl-idm-pswd.so
	<i>root\xaix\setup\utilities\sun_password_plugins\platform</i>	Solaris: novl-idm-pswd.so
		AIX: novl-idm-pswd.so
Identity Manager 3.6 CD - AIX	<i>root\xaix\setup\utilities\sun_password_plugins\platform</i>	Windows: novl-idm-pswd.dll
		Linux: novl-idm-pswd.so
		Solaris: novl-idm-pswd.so
		AIX: novl-idm-pswd.so

2.2.3 Installing the Plug-In

- 1 Locate the correct plug-in file. See [Section 2.2.2, “Where to Find the Plug-In,” on page 16](#) for information.
- 2 Copy the binary plug-in file to the `lib` directory in your Sun Java System Directory installation location.

For example, on Windows the default installation location for Sun Java System Directory is `C:\Program Files\Sun\MPS` and inside that directory is a `lib` directory. Put `novl-idm-pswd.dll` in the `lib` directory.

On other platforms, the default installation location is often `/var/Sun/mps`. You need to locate the Sun Java System Directory installation location on your system, and put the plug-in file inside the `lib` directory.

On Solaris SPARC* computers, the Sun Java System Directory installation includes two versions of most libraries: a 32-bit version and a 64-bit version. By default, the 32-bit version is found at `/var/Sun/mps/lib`. The 64-bit version is found at `/var/Sun/mps/lib/64`.

Both a 32-bit and a 64-bit version of the plug-in are provided. Copy both versions to their respective locations on your Solaris installation. At runtime, the Sun Java System Directory determines which version is the appropriate version to load.

- 3 Locate and edit the `novl-idm-pswd.ldif` or `novl-idm-pswd-win32.ldif` file. The file is located in the `sun_password_plugins` directory on your CD or DVD image.

The `.ldif` file contains plug-in configuration information that you apply to the directory. It also contains two schema definitions:

- ♦ One definition is for the `novelldistPassword` attribute that stores the encrypted password.
- ♦ The other definition is for the `novelldistPasswordUser` auxiliary class that is applied to your users to allow the use of the `novelldistPassword` attribute.

As a convenience, the `.ldif` file also contains an instruction to turn on the Retro Changelog Plugin, which most customers want turned on to enable Publisher channel operations with the Identity Manager LDAP driver. If you know that the changelog is already enabled, or if you don't want to enable the changelog, you can remove the Retro Changelog Plugin section from the `.ldif` file.

Most users need to edit only two items in the `.ldif` file:

- ♦ The `nsslapd-pluginPath` attribute
- ♦ The `nsslapd-pluginarg0` attribute

Ensure that the value of `nsslapd-pluginPath` is the path where you installed the plug-in. For example, if you installed the plug-in in the `/var/Sun/mps/lib` directory, the value should be `/var/Sun/mps/lib/novl-idm-pswd.so`. Set the value of `nsslapd-pluginarg0` to a password that will be used to generate an AES key used to encrypt user passwords. When you create the LDAP driver, you will configure the driver with this same encryption password (see [“Use Sun Password Plugin” on page 53](#)).

Solaris users should set the value of `nsslapd-pluginPath` to the path of the 32-bit version of the plug-in, even if the operating system is 64-bit. (See [Step 2](#).) At runtime, the directory determines whether to load the 32-bit or the 64-bit version of the plug-in.

- 4 Apply the `novl-idm-pswd.ldif` or `novl-idm-pswd-win32.ldif` file to the Sun directory.

To complete this step, you need to know the configuration administrator's DN and password. Typically, the DN will be `"uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot"`. However, the password will vary. You also need to know the LDAP port used by your Sun directory.

The `ldapmodify` command line utility that was installed with your Sun Java System Directories can be used to apply the `.ldif` file. Use a command similar to the following:

```
ldapmodify -h localhost -p 389 -D
"uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRo
ot" -w password -f novl-idm-pswd.ldif
```

- 5 Restart Sun Java System Directory so that your changes take affect and the plug-in starts.

For troubleshooting, note any errors that might appear on the console.

Preparing the LDAP Server

3

You need to do the following to prepare the LDAP server to which you are connecting:

- ♦ Create a user account through which the LDAP driver can authenticate to the LDAP directory.
- ♦ If you plan to use changelog as the publication method (see [Section 1.1.2, “Publication Methods,” on page 9](#)), you need to verify that the change log mechanism of the LDAP server is enabled. This is required only for synchronization of data from the LDAP server to the Identity Vault (Publisher channel). It is not required if you plan only to push data from the Identity Vault to the LDAP directory.

The following sections provide instructions

- ♦ [Section 3.1, “Creating an LDAP User Object with Authentication Rights,” on page 19](#)
- ♦ [Section 3.2, “Enabling the Change Log,” on page 20](#)

3.1 Creating an LDAP User Object with Authentication Rights

When you use the changelog publication method, the driver attempts to prevent loopback situations where an event that occurs on the Subscriber channel is sent back to the Metadirectory engine on the Publisher channel. However, the LDAP-search method relies on the Metadirectory engine to prevent loopback.

With the changelog method, one way that the driver prevents loopback from happening is to look in the change log to see which user made the change. If the user that made the change is the same user that the driver uses to authenticate with, the Publisher assumes that the change was made by the driver’s Subscriber channel.

NOTE: If you use Critical Path InJoin Server, the change log implementation on that server is somewhat limited because it doesn’t provide the DN of the object that initiated the change. Therefore, the creator/modifier DN can’t be used to determine whether the change came from an Identity Vault or not.

In that case, all changes found in the change log are sent by the Publisher to the Metadirectory engine, and the Optimize/Modify discards unnecessary or repetitive changes.

To stop the Publisher channel from discarding legitimate changes, make sure the User object that the driver uses to authenticate with is not used for any other purpose.

For example, suppose you are using the Netscape Directory Server and have configured the driver to use the administrator account CN=Directory Manager. If you want to manually make a change in the Netscape Directory Server and have that change synchronize, you can’t log in and make the change with CN=Directory Manager. You must use another account.

To avoid this problem:

- 1 Create a user account that the driver uses exclusively.
- 2 Assign that user account rights to see the change log and to make any changes that you want the driver to be able to make

For example, at the VMP company, you create a user account for the driver called uid=ldriver,ou=Directory Administrators,o=lansing.vmp.com. You then assign the appropriate rights to the user account by applying the following LDIF to the server by using the LDAPModify tool or the Novell® Import Conversion Export utility.

```
# give the new user rights to read and search the changelog

dn: cn=changelog

changetype: modify

add: aci

aci: (targetattr = "*")(version 3.0; acl "LDAP DirXML Driver"; allow
(compare,read,search) userdn = "ldap:///uid=ldriver,ou=Directory
Administrators,o=lansing.vmp.com"; )

-

# give the new user rights to change anything in the o=lansing.vmp.com
container

dn: o=lansing.vmp.com

changetype: modify

add: aci

aci: (targetattr = "*")(version 3.0; acl "LDAP DirXML Driver"; allow (all)
userdn = "ldap:///uid=ldriver,ou=Directory Administrators,o=lansing.vmp.com";
)

-
```

3.2 Enabling the Change Log

The change log is the part of the LDAP server that enables the driver to recognize changes that require publication from the LDAP directory to an Identity Vault. The LDAP directories supported by this driver support the changelog mechanism.

Critical Path InJoin and Oracle Internet Directory have the change log enabled by default. Unless the change log has been turned off, you don't need to perform any additional steps to enable it.

IBM SecureWay, Netscape Directory Server, and iPlanet Directory Server require you to enable the change log after installation. For information on enabling the change log, refer to the documentation supporting your LDAP directory.

TIP: The iPlanet change log requires you to enable the Retro Changelog Plug-in.

Creating a New Driver

4

After the LDAP driver files are installed on the server where you want to run the driver (see [Chapter 2, “Installing the Driver Files,” on page 15](#)), you can create the driver in the Identity Vault. You do so by importing the basic driver configuration file and then modifying the driver configuration to suit your environment. You can do this in either Designer or iManager.

- ♦ [Section 4.1, “Creating the Driver in Designer,” on page 21](#)
- ♦ [Section 4.2, “Creating the Driver in iManager,” on page 24](#)
- ♦ [Section 4.3, “Activating the Driver,” on page 27](#)

4.1 Creating the Driver in Designer

You create the LDAP driver by importing the driver’s basic configuration file and then modifying the configuration to suit your environment. After you’ve created and configured the driver, you need to deploy it to the Identity Vault and start it.

- ♦ [Section 4.1.1, “Importing the Driver Configuration File,” on page 21](#)
- ♦ [Section 4.1.2, “Configuring the Driver,” on page 22](#)
- ♦ [Section 4.1.3, “Deploying the Driver,” on page 23](#)
- ♦ [Section 4.1.4, “Starting the Driver,” on page 23](#)

4.1.1 Importing the Driver Configuration File

- 1 In Designer, open your project.
- 2 In the Modeler, right-click the driver set where you want to create the driver, then select *New > Driver* to display the Driver Configuration Wizard.
- 3 In the Driver Configuration list, select *LDAP*, then click *Run*.
- 4 On the Import Information Requested page, fill in the following fields:

Driver Name: Specify a name that is unique within the driver set.

Connected System LDAP Base-DN: Specify the base LDAP location for the connected system.

User Container: Select the Identity Vault container where any new users created from LDAP file information will be placed. This value becomes the default for all drivers in the driver set. If you don’t want to change this value for all drivers, leave this field unchanged and change the value on the driver’s Global Configuration Values page after you’ve finished importing the driver.

Group Container: Select the Identity Vault container where any new groups created from LDAP file information will be placed. This value becomes the default for all drivers in the driver set. If you don’t want to change this value for all drivers, leave this field unchanged and change the value on the driver’s Global Configuration Values page after you’ve finished importing the driver.

Driver is Local/Remote: Select *Local* if this driver will run on the Metadirectory server without using the Remote Loader service. Select *Remote* if you want the driver to use the Remote Loader service, either locally on the Metadirectory server or remotely on another server.

LDAP Authentication DN: Specify the DN of the LDAP account the driver will use for authentication.

LDAP Authentication Password: Specify the password for the LDAP authentication account.

LDAP Server: Specify the hostname or IP address and port of the LDAP server. Typical ports are 389 for standard LDAP and 636 for LDAP over SSL.

- 5 (Conditional) If you chose to run the driver remotely, click *Next*, then fill in the fields listed below. Otherwise, skip to **Step 6**.

Remote Host Name and Port: Specify the host name or IP address of the server where the driver's Remote Loader service is running.

Driver Password: Specify the driver object password that is defined in the Remote Loader service. The Remote Loader requires this password to authenticate to the Metadirectory server.

Remote Password: Specify the Remote Loader's password (as defined on the Remote Loader service). The Metadirectory engine (or Remote Loader shim) requires this password to authenticate to the Remote Loader

- 6 Click *Next* to import the driver configuration.

At this point, the driver is created from the basic configuration file. To ensure that the driver works the way you want it to for your environment, you must review and modify (if necessary) the driver's default configuration settings.

- 7 To review or modify the default configuration settings, click *Configure*, then continue with the next section, **Configuring the Driver**.

or

To skip the configuration settings at this time, click *Close*. When you are ready to configure the settings, continue with **Configuring the Driver**.

4.1.2 Configuring the Driver

After importing the driver configuration file, the LDAP driver will run. However, the basic configuration probably won't meet the requirements for your environment. You should complete the following tasks to configure the driver:


- ♦ **Configure the driver parameters:** There are many settings that can help you customize and optimize the driver. The settings are divided into categories such as Driver Configuration, Engine Control Values, and Global Configuration Values (GCVs). Although it is important for you to understand all of the settings, your first priority should be to review the **Driver Parameters** located on the Driver Configuration page. The Driver Parameters let you configure the LDAP directory type, publication method, and other parameters associated with the Publisher channel.
- ♦ **Configure the driver filter:** Modify the driver filter to include the object classes and attributes you want synchronized between the Identity Vault and the LDAP directory. For instructions, see **Chapter 6, "Synchronizing Data," on page 31**.
- ♦ **Configure policies:** Modify the policies as needed. For information about the default configuration policies, see **"Policies" on page 11**.

- ♦ **Secure the driver connection:** Using a secure connection (SSL) between the Identity Vault and the LDAP directory is strongly recommended. To set up this secure connection, see [Chapter 7, “Configuring SSL Connections,” on page 37](#).
- ♦ **Configure password synchronization:** The basic driver configuration is set up to support password synchronization through Universal Password. If you don’t want this setup, see [“Configuring Password Flow ” in the *Identity Manager 3.6 Password Management Guide*](#).

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

4.1.3 Deploying the Driver

After a driver 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.
 - ♦ **Password:** Specify the user’s password.
- 4 Click *OK*.
- 5 Read through the deployment summary, then click *Deploy*.
- 6 Read the successful message, 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. Whatever rights that the driver needs to have on the server, the DriversUser object must have the same security rights.

 - 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.
 - 8b Click *OK*.
 - 8c Repeat [Step 8a](#) and [Step 8b](#) for each object you want to exclude.
 - 8d Click *OK*.
- 9 Click *OK*.

4.1.4 Starting the Driver

When a driver is created, it is stopped by default. To make the driver work, you must start the driver and cause events to occur. Identity Manager is an event-driven system, so after the driver is started, it won’t do anything until an event occurs.

To start the driver:

- 1 In Designer, 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 8, “Managing the Driver,” on page 43](#).

4.2 Creating the Driver in iManager

You create the LDAP driver by importing the driver’s basic configuration file and then modifying the configuration to suit your environment. After you’ve created and configured the driver, you need to start it.

- ♦ [Section 4.2.1, “Importing the Driver Configuration File,” on page 24](#)
- ♦ [Section 4.2.2, “Configuring the Driver,” on page 26](#)
- ♦ [Section 4.2.3, “Starting the Driver,” on page 27](#)

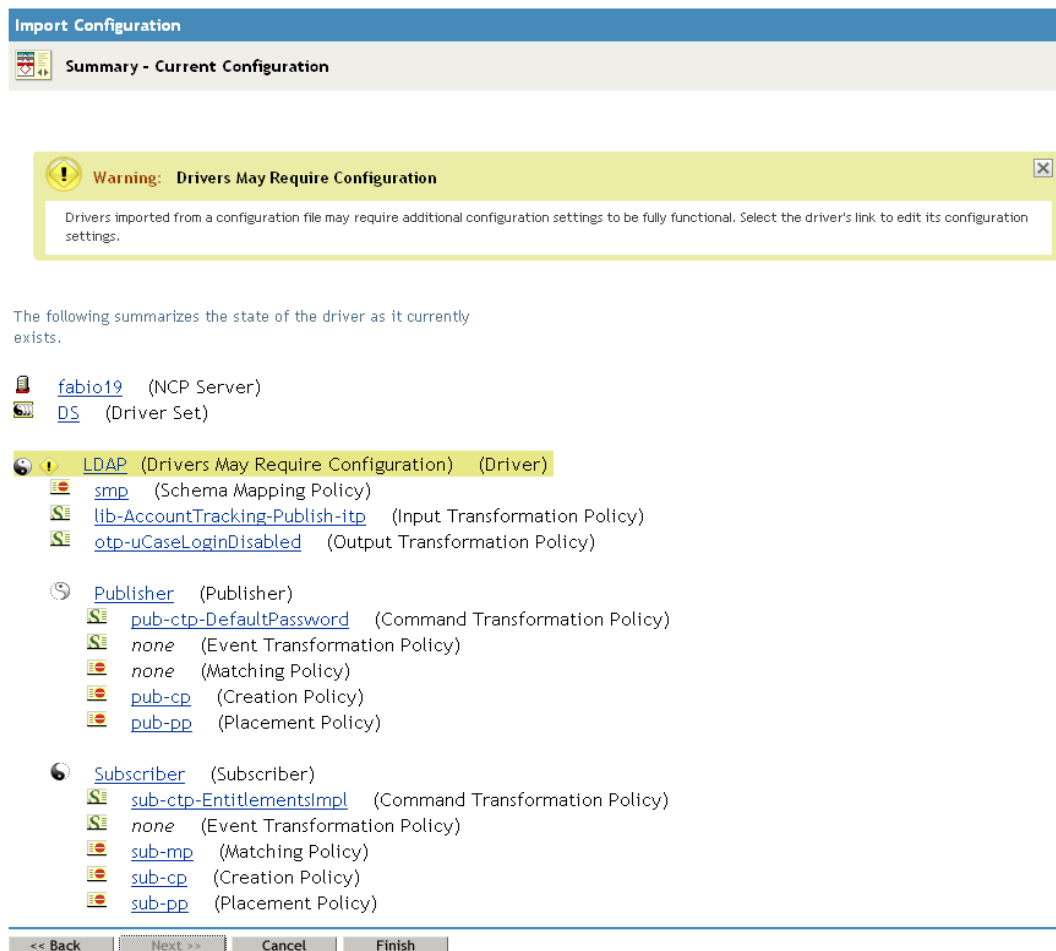
4.2.1 Importing the Driver Configuration File

- 1 In iManager, click  to display the Identity Manager Administration page.
- 2 In the *Administration* list, click *Import Configuration* to launch the Import Configuration Wizard.
- 3 Follow the wizard prompts, filling in the requested information (described below) until you reach the Summary page.

Prompt	Description
Where do you want to place the new driver?	You can add the driver to an existing driver set, or you can create a new driver set and add the driver to the new set. If you choose to create a new driver set, you are prompted to specify the name, context, and server for the driver set.
Import a configuration into this driver set	Use the default option, <i>Import a configuration from the server (.XML file)</i> . In the <i>Show</i> field, select <i>Identity Manager 3.6 configurations</i> . In the <i>Configurations</i> field, select the LDAP file.
Driver name	Type a name for the driver. The name must be unique within the driver set.
Connected System LDAP Base-DN	Specify the base LDAP location for the connected system.
User Container	Select the Identity Vault container where any new users created from LDAP file information will be placed. This value becomes the default for all drivers in the driver set. If you don’t want to change this value for all drivers, leave this field unchanged and change the value on the driver’s Global Configuration Values page after you finish importing the driver.

Prompt	Description
Group Container	Select the Identity Vault container where any new groups created from LDAP file information will be placed. This value becomes the default for all drivers in the driver set. If you don't want to change this value for all drivers, leave this field alone and change the value on the driver's Global Configuration Values page after you finish importing the driver.
Driver is Local/Remote	Select <i>Local</i> if this driver will run on the Metadirectory server without using the Remote Loader service. Select <i>Remote</i> if you want the driver to use the Remote Loader service, either locally on the Metadirectory server or remotely on another server.
Remote Host Name and Port	This applies only if the driver is running remotely. Specify the host name or IP address of the server where the driver's Remote Loader service is running.
Driver Password	This applies only if the driver is running remotely. Specify the driver object password that is defined in the Remote Loader service. The Remote Loader requires this password to authenticate to the Metadirectory server.
Remote Password	This applies only if the driver is running remotely. Specify the Remote Loader's password (as defined on the Remote Loader service). The Metadirectory engine (or Remote Loader shim) requires this password to authenticate to the Remote Loader.
LDAP Authentication DN	Specify the DN of the LDAP account the driver will use for authentication.
LDAP Authentication Password	Specify the password for the LDAP authentication account.
LDAP Server	Specify the hostname or IP address and port of the LDAP server. Typical ports are 389 for standard LDAP and 636 for LDAP over SSL.
Define Security Equivalences	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. Whatever rights that the driver needs to have on the server, the DriversUser object must have the same security rights.
Exclude Administrative Roles	You should exclude any administrative User objects (for example, Admin and DriversUser) from synchronization.

When you finish providing the information required by the wizard, a Summary page similar to the following is displayed.



At this point, the driver is created from the basic configuration file. To ensure that the driver works the way you want it to for your environment, you must review and modify (if necessary) the driver's default configuration settings.

- 4 To modify the default configuration settings, click the linked driver name, then continue with **Configuring the Driver**.

or

To skip the configuration settings at this time, click *Finish*. When you are ready to configure the settings, continue with the next section, **Configuring the Driver**.

4.2.2 Configuring the Driver

After importing the driver configuration file, the LDAP driver will run. However, the basic configuration probably won't meet the requirements for your environment. You should complete the following tasks to configure the driver:

- ♦ **Configure the driver parameters:** There are many settings that can help you customize and optimize the driver. The settings are divided into categories such as Driver Configuration, Engine Control Values, and Global Configuration Values (GCVs). Although it is important for you to understand all of the settings, your first priority should be to review the **Driver**

Parameters located on the Driver Configuration page. The Driver Parameters let you configure the LDAP directory type, publication method, and other parameters associated with the Publisher channel.


- ♦ **Configure the driver filter:** Modify the driver filter to include the object classes and attributes you want synchronized between the Identity Vault and the LDAP directory. For instructions, see [Chapter 6, “Synchronizing Data,” on page 31](#).
- ♦ **Configure policies:** Modify the policies as needed. For information about the default configuration policies, see [“Policies” on page 11](#).
- ♦ **Secure the driver connection:** Using a secure connection (SSL) between the Identity Vault and the LDAP directory is strongly recommended. To set up this secure connection, see [Chapter 7, “Configuring SSL Connections,” on page 37](#).
- ♦ **Configure password synchronization:** The basic driver configuration is set up to support password synchronization through Universal Password. If you don’t want this setup, see [“Configuring Password Flow”](#) in the *Identity Manager 3.6 Password Management Guide*.

After completing the configuration tasks, continue with the next section, [Starting the Driver](#).

4.2.3 Starting the Driver

When a driver is created, it is stopped by default. To make the driver work, you must start the driver and cause events to occur. Identity Manager is an event-driven system, so after the driver is started, it won’t do anything until an event occurs.

To start the driver:

- 1 In iManager, click  to display the Identity Manager Administration page.
- 2 Click *Identity Manager Overview*.
- 3 Browse to and select the driver set object that contains the driver you want to start.
- 4 Click the driver set name to access the Driver Set Overview page.
- 5 Click the upper right corner of the driver, then click *Start driver*.

For information about management tasks with the driver, see [Chapter 8, “Managing the Driver,” on page 43](#).

4.3 Activating the Driver

If you created the driver in a driver set where you’ve already activated the Metadirectory engine and service drivers, the driver inherits the activation. 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.

For information on activation, refer to [“Activating Novell Identity Manager Products”](#) in the *Identity Manager 3.6 Installation Guide*.

Upgrading an Existing Driver

5

The following sections provide information to help you upgrade an existing driver to version 3.6:

- [Section 5.1, “Supported Upgrade Paths,” on page 29](#)
- [Section 5.2, “What’s New in Version 3.6,” on page 29](#)
- [Section 5.3, “Upgrade Procedure,” on page 29](#)

5.1 Supported Upgrade Paths

You can upgrade from any 3.x version of the LDAP driver. Upgrading a pre-3.x version of the driver directly to version 3.6 is not supported.

5.2 What’s New in Version 3.6

Version 3.6 of the driver does not include any new features that are not already in the 3.5.1 version. However, the process for creating a new driver has changed. For detailed information, see [Chapter 4, “Creating a New Driver,” on page 21](#).

5.3 Upgrade Procedure

The process for upgrading the LDAP driver is the same as for other Identity Manager drivers. For detailed instructions, see “[Upgrading](#)” in the *Identity Manager 3.6 Installation Guide*.

Synchronizing Data

6


The following sections provide information to help you control which classes and attributes are synchronized between your Identity Vault and the connected LDAP directory. Not only can you choose which classes and attributes are synchronized, but you can also determine which direction they flow (Identity Vault to LDAP, LDAP to Identity Vault, or both).

- ♦ [Section 6.1, “Determining Which Objects Are Synchronized,” on page 31](#)
- ♦ [Section 6.2, “Defining Schema Mapping,” on page 31](#)
- ♦ [Section 6.3, “Netscape Directory Server Configuration,” on page 33](#)
- ♦ [Section 6.4, “Migrating and Resynchronizing Data,” on page 34](#)

6.1 Determining Which Objects Are Synchronized

Identity Manager uses the driver filter, located on both the Publisher and Subscriber channels, to control which objects are synchronized and to define the authoritative data source for these objects.

The following steps provide instructions for editing the filter in iManager. For information about editing the filter in Designer, see “[Controlling the Flow of Objects with the Filter](#)” in the *Policies in Designer 3.0* guide.

- 1 In iManager, open the LDAP driver Overview page:
 - 1a Click  to display the Identity Manager Administration page.
 - 1b In the *Administration* list, click *Identity Manager Overview*.
 - 1c 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.
 - 1d Click the driver set to open the Driver Set Overview page.
 - 1e Click the LDAP driver icon to display its Overview page.
- 2 Click the Publisher or Subscriber filter icon and make the appropriate changes.

For every object and attribute selected in the filter, the Schema Mapping policy must have a corresponding entry unless the class or attribute names are the same in both directories (see [Section 6.2, “Defining Schema Mapping,” on page 31](#)). Before mapping an attribute, verify that a corresponding attribute actually exists in the target directory.

6.2 Defining Schema Mapping

Different LDAP servers have different schemas. When the driver is first started, it queries the server for the specific schema.

You must be familiar with the characteristics of directory attributes and the LDAP server attributes. The driver handles all LDAP attribute types (cis, ces, tel, dn, int, bin). It also handles the eDirectory™ Facsimile Telephone Number.

When mapping attributes, follow these guidelines:


- ♦ Verify that every class and attribute specified in the Subscriber and Publisher policies is mapped in the Mapping policy unless the class or attribute names are the same in both directories.
- ♦ Before mapping a directory attribute to an LDAP server attribute, verify that an LDAP server attribute actually exists. For example, the Full Name attribute is defined for a User object on an Identity Vault, but fullname doesn't exist in an inetOrgPerson object on Netscape.
- ♦ Always map attributes to attributes of the same type. For example, map strings attributes to strings attributes, octet attributes to binary attributes, or telnumber attributes to telnumber attributes.
- ♦ Map multivalue attributes to multivalue attributes.

The driver doesn't provide data conversion between different attribute types or conversions from multivalue to single-value attributes. The driver also doesn't understand structured attributes except for Facsimile Telephone Number and Postal Address.

Identity Manager is flexible about the syntax that it accepts coming in from the Publisher:

- ♦ **Accepting Non-Structured/Non-Octet Syntax:** Identity Manager accepts any non-structured/non-octet syntax for any other non-structured/non-octet syntax as long as the actual data can be coerced to the appropriate type. That is, if the Identity Vault is looking for a numeric value, the actual data should be a number.
- ♦ **Coercing the Data to Octet:** When Identity Manager is expecting octet data and gets another non-octet/non-structured type, Identity Manager coerces the data to octet by serializing the string value to UTF-8.
- ♦ **Coercing the Data to a String:** When Identity Manager is passed octet data and another non-structured type is expected, Identity Manager coerces the data to a string by decoding the Base64 data. Identity Manager next tries to interpret the result as a UTF-8 encoded string (or the platform's default character encoding if it is not a valid UTF-8 string) and then applies the same rules as **Accepting Non-Structured/Non-Octet Syntax**.
- ♦ **FaxNumber:** For faxNumber, if a non-structured type is passed in, **Accepting Non-Structured/Non-Octet Syntax** and **Coercing the Data to a String** are applied to the data to get the phone number portion of the fax number. The other fields are defaulted.
- ♦ **State:** State. For state, False, No, F, N (in either upper or lowercase), 0 and "" (empty string) are interpreted as False, and any other value is interpreted as True.

The following steps provide instructions for modifying the Schema Mapping Policy in iManager. For information about using Designer, see "**Defining Schema Map Policies**" in the *Policies in Designer 3.0* guide.

- 1 In iManager, open the LDAP driver Overview page:
 - 1a Click  to display the Identity Manager Administration page.
 - 1b In the *Administration* list, click *Identity Manager Overview*.
 - 1c 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.
 - 1d Click the driver set to open the Driver Set Overview page.
 - 1e Click the LDAP driver icon to display its Overview page.
- 2 Click the schema mapping icon on the Publisher or Subscriber channel.

- 3 Click the policy to display the editing page.
- 4 Edit the policy as appropriate for your setup.

6.3 Netscape Directory Server Configuration

The following sections apply only when connecting to Netscape Directory Server:

- ♦ [Section 6.3.1, “Defining Object Placement in Netscape Directory Server,” on page 33](#)
- ♦ [Section 6.3.2, “Working with eDirectory Groups and Netscape,” on page 34](#)

6.3.1 Defining Object Placement in Netscape Directory Server

We recommend following the Netscape naming rules for objects in Netscape Directory Server. A brief explanation of naming rules is included here for your convenience.

The directory contains entries that represent people. These person entries must have names. In other words, you must decide what the relative distinguished name (RDN) is for each person entry. The DN must be a unique, easily recognizable, permanent value. We recommend that you use the uid attribute to specify a unique value associated with the person. An example DN for a person entry is:

```
uid=jsmith,o=novell
```

The directory also contains entries that represent many things other than people (for example, groups, devices, servers, network information, or other data). We recommend that you use the cn attribute in the RDN. Therefore, if you are naming a group entry, name it as follows:

```
cn=administrators,ou=groups,o=novell
```

The directory also contains branch points or containers. You need to decide what attributes to use to identify the branch points. Because attribute names have a meaning, use the attribute name with the type of entry it is representing. The Netscape recommended attributes are defined as follows:

Table 6-1 *Netscape Recommended Attributes*

Attribute Name	Definition
c	Country name
o	Organization name
ou	Organizational Unit
st	State
l	Locality
dc	Domain Component

A Subscriber Placement policy specifies the naming attribute for a classname. The following example is for the User classname. The <placement> statement specifies that uid is used as the naming attribute.

```
<placement-rule>
  <match-class class-name="User"/>
  <match-path prefix="\Novell-Tree\Novell\Users"/>
  <placement>uid=<copy-name/>,ou=People,o=Netscape</
placement>
</placement-rule>
```

The following Subscriber Placement specifies that ou is used as the naming attribute for class-name Organizational Unit.

```
<placement-rule>
  <match-class class-name="Organizational Unit"/>
  <match-path prefix="\Novell-Tree\Novell\Users"/>
  <placement>ou=<copy-name/>,ou=People,o=Netscape</placement>
</placement-rule>
```

To configure a placement policy:

- 1 In iManager, *click Identity Manager > Identity Manager Overview*.
- 2 Locate the driver in its driver set.
- 3 Open the Identity Manager Driver Overview page by clicking the driver.
- 4 Click the Publisher or Subscriber Placement policy icon, then make the appropriate changes.
- 5 Click *Close*.

6.3.2 Working with eDirectory Groups and Netscape

Because group attributes are different in an Identity Vault and Netscape Directory Server, some special processing is required by the driver. On the Publisher channel, special processing takes place when the driver sees the attribute uniquemember in the classname groupofuniquenames.


The driver also sets the Equivalent To Me attribute in the eDirectory Group. The Equivalent To Me attribute must be included in the Publisher filter. The Equivalent To Me attribute need not be in the Schema Mapping policy because the eDirectory attribute name is used. There is no equivalent attribute name in Netscape Directory Server. No special processing is required on the Subscriber channel.

6.4 Migrating and Resynchronizing Data

Identity Manager synchronizes data as the data changes. If you want to synchronize all data immediately, you can choose from the following options:

- ♦ **Migrate Data from the Identity Vault:** Allows you to select containers or objects you want to migrate from an Identity Vault to an LDAP server. When you migrate an object, the Metadirectory engine applies all of the Matching, Placement, and Create policies, as well as the Subscriber filter, to the object.

NOTE: When migrating data from an Identity Vault into the LDAP directory, you might need to change your LDAP server settings to allow migration of large numbers of objects. See [Section 9.2, “Migrating Users into an Identity Vault,” on page 45](#).

- ♦ **Migrate Data into the Identity Vault:** Allows you to define the criteria that Identity Manager uses to migrate objects from an LDAP server into an Identity Vault. When you migrate an object, the Metadirectory engine applies all of the Matching, Placement, and Create policies, as well as the Publisher filter, to the object. Objects are migrated into the Identity Vault by using the order you specify in the Class list.
 - ♦ **Synchronize:** Identity Manager looks in the Subscriber class filter and processes all objects for those classes. Associated objects are merged. Unassociated objects are processed as Add events.
- 1 In iManager, open the LDAP driver Overview page:
 - 1a Click  to display the Identity Manager Administration page.
 - 1b In the *Administration* list, click *Identity Manager Overview*.
 - 1c 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.
 - 1d Click the driver set to open the Driver Set Overview page.
 - 1e Click the LDAP driver icon to display its Overview page.
 - 2 Click *Migrate*, then click the appropriate migration button.

Configuring SSL Connections

7

The driver uses the LDAP protocol to communicate with the LDAP server. Most LDAP servers allow non-encrypted (clear-text) connections. Additionally, when configured correctly, some LDAP servers allow SSL-encrypted connections. SSL connections encrypt all traffic on the TCP/IP socket by using a public/private key pair. The actual LDAP protocol doesn't change, but the communication channel performs the encryption.

The procedure for enabling SSL connections differs slightly from one LDAP server to another. This document covers the process for enabling SSL connections when using Netscape Directory Server 4.12. If you are using another LDAP server, the procedure is similar.

- ♦ [Section 7.1, “Step 1: Generating a Server Certificate,” on page 37](#)
- ♦ [Section 7.2, “Step 2: Sending the Certificate Request,” on page 38](#)
- ♦ [Section 7.3, “Step 3: Installing the Certificate,” on page 38](#)
- ♦ [Section 7.4, “Step 4: Activating SSL in Netscape Directory Server 4.12,” on page 39](#)
- ♦ [Section 7.5, “Step 5: Exporting the Trusted Root from the Directory Tree,” on page 39](#)
- ♦ [Section 7.6, “Step 6: Importing the Trusted Root Certificate,” on page 40](#)
- ♦ [Section 7.7, “Step 7: Adjusting Driver Settings,” on page 41](#)

7.1 Step 1: Generating a Server Certificate

You first need to install a server certificate. The LDAP server itself can generate a certificate, but the certificate must then be signed by a CA that is trusted by the server. One way to get the certificate signed is to use the CA that comes with an Identity Vault.

To generate a certificate request:

- 1** In the navigation tree in Netscape Console, select the server that the driver will communicate with.
- 2** Click *Open Server*.
- 3** Click *Tasks > Certificate Setup Wizard*.
- 4** Provide information to request a certificate.

Depending on the certificates or tokens that might already be installed on the host system, you might see some or all of the following fields:

Select a Token (Cryptographic Device): Select *Internal (Software)*.

Is the Server Certificate Already Requested and Ready to Install? Select *No*.

If a trust database doesn't already exist for this host, one is generated for you.

A trust database is a key pair and certificate database installed on the local host. When you use an internal token, the trust database is the database into which you install the key and certificate.

- 5** Type and confirm the password.

The password must contain at least eight characters, and at least one of them must be numeric. This password helps secure access to the new key database you're creating.

6 Continue providing information as prompted, then click *Next*.

7 After a trust database is created, click *Next*.

8 Type the requested information, then click *Next*.

9 Type the password for the token you selected earlier, then click *Next*.

The Certificate Setup Wizard generates a certificate request for your server. When you see the page, you can send the certificate request to the certification authority.

10 Continue with [Step 2: Sending the Certificate Request](#).

7.2 Step 2: Sending the Certificate Request

1 Copy the server certificate request into Notepad or another text editor.

2 Save the file as `csr.txt`.

Your certificate request e-mail should look like the following:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
```

```
.
```

```
.
```

```
.
```

```
-----END NEW CERTIFICATE REQUEST-----
```

3 In iManager, select *Novell Certificate Server > Issue Certificate*.

4 In the *Filename* field, browse to `csr.txt`, then click *Next*.

5 Select *Organizational Certificate Authority*.

6 Specify SSL as the key type, then click *Next*.

7 Specify the certificate parameters, click *Next*, then click *Finish*.

8 Save the certificate in Base64 format as `cert.b64` to a local disk or diskette.

9 Continue with [Step 3: Installing the Certificate](#).

7.3 Step 3: Installing the Certificate

1 In the navigation tree in Netscape Console, select the server that the driver will be connecting to.

2 Click *Open*.

3 Click *Tasks > Certificate Setup Wizard*.

4 Start the wizard and indicate that you are ready to install the certificate.

5 When prompted, provide the following information:

Select a Token (Cryptographic Device): Select *Internal (Software)*.

Is the Server Certificate Already Requested and Ready to Install? Select *Yes*.

6 Click *Next*.

7 In the *Install Certificate For* field, select *This Server*.

8 In the *Password* field, type the password you used to set up the trust database, then click *Next*.

- 9 In the *Certificate Is Located in This File* field, type the absolute path to the certificate (for example, A:\CERT.B64).
- 10 After the certificate is generated, click *Add*.
- 11 After the certificate is successfully installed, click *Done*.
- 12 Continue with [Step 4: Activating SSL in Netscape Directory Server 4.12](#).

7.4 Step 4: Activating SSL in Netscape Directory Server 4.12

After you install the certificate, complete the following to activate SSL:

- 1 In the navigation tree in Netscape Console, select the server you want to use SSL encryption with.
- 2 Click *Open > Configuration > Encryption*.
- 3 Specify the following information:
 - Enable SSL:** Select this option.
 - Cipher Family:** Select *RSA*.
 - Token to Use:** Select *Internal (Software)*.
 - Certificate to Use:** Select *Server-Cert*.
 - Client Authentication:** Because the driver doesn't support client authentication, deselect *Allow Client Authentication*.
- 4 Click *Save*.
- 5 Click *Tasks*, then restart the server for the changes to take effect.
- 6 Continue with [Step 5: Exporting the Trusted Root from the Directory Tree](#).

7.5 Step 5: Exporting the Trusted Root from the Directory Tree

- 1 In iManager, select *eDirectory Administration > Modify Object*.
- 2 Browse to the Certificate Authority (CA) object, then click *OK*.
- 3 Select *Certificates* from the drop-down list.
- 4 Click *Export*.
- 5 Click *No* at the prompt that displays *Do you want to export the private key with the certificate?*
- 6 Click *Next*.
- 7 In the *Filename* field, specify in a filename (for example, PublicKeyCert), then select *Base64* as the format.
- 8 Click *Export*.
- 9 Continue with [Step 6: Importing the Trusted Root Certificate](#).

7.6 Step 6: Importing the Trusted Root Certificate

You need to import the trusted root certificate into the LDAP server's trust database and the client's certificate store.

- ♦ [Section 7.6.1, “Importing into the LDAP Server’s Trust Database,” on page 40](#)
- ♦ [Section 7.6.2, “Importing into the Client's Certificate Store,” on page 40](#)

7.6.1 Importing into the LDAP Server's Trust Database

You need to import the trusted root certificate into the LDAP server's trust database. Because the server certificate was signed by the Identity Vault's CA, the trust database needs to be configured to trust the Identity Vault CA.

- 1 In the Netscape Console, click *Tasks > Certificate Setup Wizard > Next*.
- 2 In *Select a Token*, accept the default for Internal (*Software*).
- 3 In *Is the Server Certificate Already Requested and Ready to Install*, select *Yes*.
- 4 Click *Next* twice.
- 5 In *Install Certificate For* dialog box, select *Trusted Certificate Authority*.
- 6 Click *Next*.
- 7 Select *The Certificate Is Located in This File*, then type the full path to the `.b64` file containing the trusted root certificate.
- 8 Click *Next*.
- 9 Verify the information on the screen, then click *Add*.
- 10 Click *Done*.
- 11 Continue with [Importing into the Client's Certificate Store](#).

7.6.2 Importing 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 Use the KeyTool class found in `rt.jar`.

For example, if your public key certificate is saved as `PublicKeyCert.b64` on a diskette and you want to import it into a new certificate store file named `.keystore` in the current directory, enter the following at the command line:

```
java sun.security.tools.KeyTool -import -alias TrustedRoot -file  
a:\PublicKeyCert.b64  
  
-keystore .keystore -storepass keystorepass
```

- 2 When you are asked to trust this certificate, select *Yes*, then click *Enter*.
- 3 Copy the `.keystore` file to any directory on the same file system that has the Identity Vault files.
- 4 In iManager, select *Identity Manager > Identity Manager Overview*.

- 5 Search for drivers.
- 6 Click the LDAP Driver object, then click it again in the *Identity Manager Driver Overview* page.
- 7 In the *Keystore Path* parameter, enter the complete path to the `.keystore` file.
- 8 Continue with [Step 7: Adjusting Driver Settings](#).

7.7 Step 7: Adjusting Driver Settings

You need to enable the driver's SSL parameter and adjust the other SSL parameters as needed. For information, see [Table A-5 on page 50](#).

Managing the Driver

8

As you work with the LDAP driver, there are a variety of 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 *Identity Manager 3.6 Common Driver Administration Guide*.

- ♦ [Section 9.1, “Troubleshooting Driver Processes,” on page 45](#)
- ♦ [Section 9.2, “Migrating Users into an Identity Vault,” on page 45](#)
- ♦ [Section 9.3, “OutOfMemoryError,” on page 45](#)
- ♦ [Section 9.4, “LDAP v3 Compatibility,” on page 46](#)
- ♦ [Section 9.5, “Frequently Asked Questions,” on page 46](#)

9.1 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 *Identity Manager 3.6 Common Driver Administration Guide*.

9.2 Migrating Users into an Identity Vault

Some LDAP servers have settings that limit the number of entries that an LDAP query can return. For example, iPlanet Directory Server 5.1 has a default limit of 5000 objects.

When migrating user data from LDAP into an Identity Vault, the driver makes an LDAP query to the server and returns the objects that match the criteria (such as `objectclass=User`).

A limit on the number of entries that can be returned on an LDAP query can cause a migration to stop before it is complete, even though the Identity Manager driver continues to run normally.

To fix this, change the limit. For example, do the following in iPlanet:

- 1 Go to the *Configuration* tab, then select *Database* settings.
- 2 Raise the look-through limit on the LDBM plug-in tab from the default of 5000 to an appropriate number.
This is the number of records the query is allowed to look at while fulfilling the query.
- 3 Go to the *Configuration* tab, select *Directory Server Settings*, select the *Performance* tab, then raise the size limit according to the number of user accounts you need to migrate.
This is the actual number of records that the query is allowed to return.
After these settings have been adjusted, the migration should complete correctly.

9.3 OutOfMemoryError

If you use the LDAP-Search method and the driver shuts down with a `java.lang.OutOfMemoryError`:

- 1 Try setting or increasing the `DHOST_JVM_INITIAL_HEAP` and `DHOST_JVM_MAX_HEAP` environment variables.

- 2 Restart the driver.
- 3 Monitor the driver to make sure that the variables provide enough memory.

For more information, see [TID 10062098 \(http://support.novell.com/cgi-bin/search/searchtid.cgi?/10062098.htm\)](http://support.novell.com/cgi-bin/search/searchtid.cgi?/10062098.htm).

9.4 LDAP v3 Compatibility

The LDAP driver works with most LDAP v3 compatible LDAP servers. The driver is written to the LDAP specification (IETF RFCs 4510-4519). To increase compatibility with some LDAP servers that don't fully meet the RFC 2251 requirements, we have added workarounds to the LDAP driver.

One compatibility issue that cannot be ignored or worked around is the RFC 4511 section 4.1.1 requirement that servers allow Message ID values up to 2,147,483,647 (integer values using four bytes).

Oracle Internet Directory version 2.1.1.0.0 (which is part of Oracle 8i) allows only Message ID values up to 32,767 (integer values using two bytes). Therefore, it can't function properly with the LDAP driver.

If you need compatibility with Oracle Internet Directory, Novell® recommends upgrading to version 9.2.0.1.0 (included with Oracle 9i) or later.

9.5 Frequently Asked Questions

Question: Does the LDAP-search method retrieve everything every time, or just retrieve updates since the last poll?

Answer: The LDAP-search method synchronizes updates from one poll to the next.


Question: If I have a choice between using the LDAP-search method or the changelog method, should I use the LDAP Search method?

Answer: Use the changelog method because it has performance advantages and is the recommended method.

Driver Properties

A


This section provides information about the Driver Configuration and Global Configuration Values properties for the LDAP driver. These are the only unique properties for drivers. 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 *Identity Manager 3.6 Common Driver Administration Guide* for information about the common properties.

The information is organized according to tabs that display in iManager. If a field is different in Designer, it is marked with a Designer  icon.

- ♦ [Section A.1, “Driver Configuration,” on page 47](#)
- ♦ [Section A.2, “Global Configuration Values,” on page 54](#)

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.

By default, the Driver Configuration page is displayed.

In Designer:

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



The Driver Configuration options are divided into the following sections:

- ♦ [Section A.1.1, “Driver Module,” on page 47](#)
- ♦ [Section A.1.2, “Driver Object Password \(iManager Only\),” on page 48](#)
- ♦ [Section A.1.3, “Authentication,” on page 48](#)
- ♦ [Section A.1.4, “Startup Option,” on page 49](#)
- ♦ [Section A.1.5, “Driver Parameters,” on page 50](#)

A.1.1 Driver Module

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

Table A-1 *Driver Module*

Option	Description
<i>Java</i>	<p>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 <code>classes</code> directory as a class file, or in the <code>lib</code> directory as a <code>.jar</code> file. If this option is selected, the driver is running locally.</p> <p>The name of the Java class is:</p> <pre>com.novell.nds.dirxml.driver.ldap.LDAPDriverShim</pre>
<i>Native</i>	<p>This option is not used with the driver.</p>
<i>Connect to Remote Loader</i>	<p>Used when the driver is connecting remotely to the connected system. Designer includes two suboptions:</p> <ul style="list-style-type: none">◆  Driver Object Password: Specifies a password for the Driver object. If you are using the Remote Loader, you must enter a password on this page. Otherwise, the remote driver does not run. The Remote Loader uses this password to authenticate itself to the remote driver shim.◆  Remote Loader Client Configuration for Documentation: Includes information on the Remote Loader client configuration when Designer generates documentation for the driver.

A.1.2 Driver Object Password (iManager Only)











Table A-2 *Driver Object Password*

Option	Description
<i>Driver Object Password</i>	<p>Use this option to set a password for the driver object. If you are using the Remote Loader, you must enter a password on this page. Otherwise, the remote driver does not run. The Remote Loader uses this password to authenticate itself to the remote driver shim.</p>

A.1.3 Authentication

The Authentication section stores the information required to authenticate to the connected system.


Table A-3 *Authentication*

Option	Description
Authentication information for server	Displays or specifies the IP address or server name that the driver is associated with
Authentication ID	Specifies the DN of the LDAP account that the driver will use for authentication.
or	
 <i>User ID</i>	Example: Administrator
Authentication Context	Specify the IP address or name of the LDAP server.
or	
 <i>Connection Information</i>	
Remote Loader Connection Parameters	Used only if the driver is connecting to the application through the Remote Loader. The parameter to enter is hostname=xxx.xxx.xxx.xxx port=xxxx kmo=certificatename, when the host name is the IP address of the application server running the Remote Loader server and the port is the port the Remote Loader is listening on. The default port for the Remote Loader is 8090.
or	
 <i>Host name</i>	
 <i>Port</i>	
 <i>KMO</i>	The <code>kmo</code> entry is optional. It is used only when an SSL connection exists between the Remote Loader and the Metadirectory engine.
 <i>Other parameters</i>	Example: hostname=10.0.0.1 port=8090 kmo=IDMCertificate
Driver Cache Limit (kilobytes)	Specify the maximum event cache file size (in KB). If it is set to zero, the file size is unlimited.
or	
 <i>Cache limit (KB)</i>	 Click <i>Unlimited</i> to set the file size to Unlimited in Designer.
Application Password	Specify the password for the user object listed in the <i>Authentication ID</i> field.
or	
 <i>Set Password</i>	
Remote Loader Password	Used only if the driver is connecting to the application through the Remote Loader. The password is used to control access to the Remote Loader instance. It must be the same password specified during the configuration of the Remote Loader on the connected system.
or	
 <i>Set Password</i>	

A.1.4 Startup Option

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

Table A-4 *Startup Option*

Option	Description
<i>Auto start</i>	The driver starts every time the Identity Manager server is started.
<i>Manual</i>	The driver does not start when the Identity Manager server is started. The driver must be started through Designer or iManager.
<i>Disabled</i>	The driver has a cache file that stores all of the events. When the driver is set to <i>Disabled</i> , this file is deleted and no new events are stored in the file until the driver state is changed to <i>Manual</i> or <i>Auto Start</i> .
 <i>Do not automatically synchronize the driver</i>	This option applies only if the driver is deployed and was previously disabled. If this is not selected, the driver re-synchronizes the next time it is started.

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.

Table A-5 *Driver Parameters*

Option	Description
Driver Settings	
<i>LDAP Directory Type</i>	When Isode M-Vault is the target LDAP directory, set the LDAP Directory Type to <i>M-Vault</i> . Otherwise, use the <i>LDAPv3</i> setting.
<i>Enforce Matching Parenthesis in Schema Elements</i>	Select whether the driver enforces matching parenthesis in the LDAP schema objectclass and attributetype definitions. If you choose <i>No</i> , the driver ignores the parenthesis syntax infractions in the schema definitions.
<i>Additional Allowable Schema Name Characters</i>	Specify extra characters to allow in LDAP objectclass and attributetype names, even when those characters are specifically disallowed by RFC 2252. Some LDAP servers don't always follow the specifications.
<i>Use SSL</i>	Select <i>Yes</i> to use SSL to secure communication between the driver and the LDAP server. If you use SSL, fill in the following parameters: <ul style="list-style-type: none">♦ Keystore Path for SSL Certs: Specify the full path to the keystore file containing the SSL certificates♦ Use Mutual Authentication: Select <i>Yes</i> if you want the driver to use SSL mutual authentication (both client and server), or select <i>No</i> for server authentication only. If you select <i>Yes</i>, you must have the appropriate certificates configured in your keystore.
<i>Key Alias</i>	The alias created when importing the public key certificate into the keystore. Typically, you only need to specify the alias when using mutual authentication.
<i>Keystore Password</i>	Specify the password used to access the keystore file that contains the SSL certificates.
Subscriber Settings	

Option	Description
<i>LDAP Server Supports Binary Attribute Option</i>	Most LDAP servers support the use of the binary attribute option as defined in RFC 2251 section 4.1.5.1. If you don't know whether the LDAP server supports the binary attribute option, select Yes .
Publisher Settings	
<i>Polling Interval in Seconds</i>	Specify the interval at which the driver checks the LDAP server for changes. When new changes are found, they are applied to the Identity Vault.
<i>Temporary File Directory</i>	<p>Specify a directory on the local file system (the one where the driver is running) where temporary state files can be written. If you don't specify a path, the driver uses the default driver path:</p> <ul style="list-style-type: none"> ♦ Metadirectory server: Defaults to the eDirectory™ DIB file directory. ♦ Remote Loader server: Defaults to the root of the Remote Loader directory. <p>These files help maintain driver consistency even when the driver is shut down and help prevent memory shortages during extensive data searches.</p>
<i>Heartbeat interval in minutes</i>	Specify how many minutes of inactivity should elapse before this channel sends a heartbeat document. In practice, more than the number of minutes specified can elapse. That is, this parameter defines a lower bound.
<i>Publication Method</i>	<p>Select whether you want to use LDAP Search or changelog as the publication method. The changelog method is the recommended method for LDAP directories that support it. For more information, see Section 1.1.2, "Publication Methods," on page 9.</p> <p>If you select <i>changelog</i>, fill in the following fields:</p> <ul style="list-style-type: none"> ♦ Changelog Entries to Process on Startup ♦ Maximum Batch Size for Changelog Processing ♦ Preferred LDAP ObjectClass Names ♦ Prevent Loopback <p>If you select LDAP Search, fill in the following fields:</p> <ul style="list-style-type: none"> ♦ Connected system LDAP base-dn ♦ Search Scope ♦ Class Processing Order ♦ Search Results to Synchronize on First Startup ♦ Use Sun Password Plugin

Option	Description
<i>Changelog Entries to Process on Startup</i>	<p>This parameter is displayed only when you select <i>changelog</i> as the <i>Publication Method</i>. It specifies which entries to process on startup.</p> <ul style="list-style-type: none"> ♦ All: The Publisher attempts to process all of the changes found in the change log. The Publisher continues until all changes have been processed. It processes new changes according to the poll rate. ♦ None: When the driver starts running, the Publisher doesn't process any previously existing entries. It processes new changes according to the poll rate. ♦ Previously Unprocessed: This setting is the default. If this is the first time the driver has been run, it behaves like the <i>All</i> option, processing all new changes. <p>If the driver has been run before, this setting causes the Publisher to process only changes that are new since the last time the driver was running. Thereafter, it processes new changes according to the poll rate.</p>
<i>Maximum Batch Size for Changelog Processing</i>	<p>This parameter is displayed only when you select <i>changelog</i> as the <i>Publication Method</i>.</p> <p>When the Publisher channel processes new entries from the LDAP change log, the Publisher asks for the entries in batches of this size (the default is 1000). If there are fewer than this number of change log entries, all of them are processed immediately. If there are more than this number, they are processed in consecutive batches of this size.</p>
<i>Preferred LDAP ObjectClass Names</i>	<p>This parameter is displayed only when you select <i>changelog</i> as the <i>Publication Method</i>.</p> <p>Identity Manager requires that objects be identified by using a single object class. However, many LDAP servers and applications can list multiple object classes for a single object. By default, when the LDAP driver finds an object on the LDAP server or application that has been added, deleted, or modified, it sends the event to the Metadirectory engine and identifies it by using the object class that has the most levels of inheritance in the schema definition.</p> <p>For example, a user object in LDAP is identified with the object classes of inetorgperson, organizationalperson, person, and top. Inetorgperson has the most levels of inheritance in the schema (inheriting from organizationalperson, which inherits from person, which inherits from top). By default, the driver uses inetorgperson as the object class it reports to the Metadirectory engine.</p> <p>If you want to change the default behavior of the driver, you can add the optional driver Publisher parameter named preferredObjectClasses. The value of this parameter can be either one LDAP object class or a list of LDAP object classes separated by spaces.</p> <p>When this parameter is present, the LDAP driver examines each object being presented on the Publisher channel to see if it contains one of the object classes in the list. It looks for them in the order they appear in the preferredObjectClasses parameter. If it finds that one of the listed object classes matches one of the values of the objectclass attribute on the LDAP object, it uses that object class as the one it reports to the Metadirectory engine. If none of the object classes match, it resorts to its default behavior for reporting the primary object class.</p>


Option	Description
<i>Prevent Loopback</i>	<p>This parameter is displayed only when you select <i>changelog</i> as the <i>Publication Method</i>.</p> <p>The Prevent Loopback parameter is used only with the changelog publication method. The LDAP-search method doesn't prevent loopback, other than the loopback prevention built into the Metadirectory engine.</p> <p>The default behavior for the Publisher channel is to avoid sending changes that the Subscriber channel makes. The Publisher channel detects Subscriber channel changes by looking in the LDAP change log 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 LDAP 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.</p>
<i>Connected system LDAP base-dn</i>	<p>This parameter is displayed only when you select <i>LDAP Search</i> as the <i>Publication Method</i>.</p> <p>Specify the LDAP distinguished name (DN) of the container where the polling searches should begin (for example, ou=people,o=company).</p>
<i>Search Scope</i>	<p>This parameter is displayed only when you select <i>LDAP Search</i> as the <i>Publication Method</i>.</p> <p>Indicates the depth of the polling searches. This parameter defaults to search the entire subtree that the LDAP base-dn points to.</p>
<i>Class Processing Order</i>	<p>This parameter is displayed only when you select <i>LDAP Search</i> as the <i>Publication Method</i>.</p> <p>Use this parameter to order certain events when referential attributes are an issue. The value of the parameter is a list of class names from the LDAP server, separated by spaces. For example, to make sure that new users are created before they are added to groups, make sure that interorgperson comes before groupofuniquenames.</p> <p>The driver defines a special class name, <i>others</i>, to mean all classes other than those explicitly listed.</p> <p>The default value for this parameter is <i>others groupofuniquenames</i>.</p>
<i>Search Results to Synchronize on First Startup</i>	<p>This parameter is displayed only when you select <i>LDAP Search</i> as the <i>Publication Method</i>. It defines whether the initial search results (when the driver is first started) are synchronized, or only subsequent changes are synchronized.</p>
<i>Use Sun Password Plugin</i>	<p>The Sun password plug-in is used to synchronize passwords from Sun Java System Directory 5.2 into the Identity Vault. Select Yes to enable the plug-in, then enter the encryption password that was used when installing the plug-in.</p> <p>See Section 2.2, "Installing the Identity Manager Plug-Ins for Password Synchronization with Sun Java System Directory," on page 15 for installation and configuration information.</p>

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 LDAP driver includes many GCVs. You can also add your own 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 organized as follows:

- ♦ [Table A-6, “Driver Parameters,” on page 54](#)
- ♦ [Table A-7, “Entitlements,” on page 55](#)
- ♦ [Table A-8, “Password Management,” on page 55](#)
- ♦ [Table A-9, “Account Tracking,” on page 56](#)


Table A-6 *Driver Parameters*

Option	Description
<i>Connected System or Driver Name</i>	Contains the name of the connected system, application, or Identity Manager driver. This value is used by e-mail notification templates to identify the source of the notification messages.
<i>Connected system LDAP base-dn</i>	Specify the LDAP distinguished name (DN) of the container where the polling searches should begin (for example, ou=people,o=company).

Table A-7 *Entitlements*

Option	Description
<i>Show entitlements configuration</i>	<p>Select <i>show</i> to display the global configuration values for entitlements. Select <i>hide</i> to not have the global configuration values displayed.</p> <p>The driver can use entitlements to manage user accounts and group memberships in the connected LDAP directory. When using entitlements, the driver works in conjunction with entitlement agents such as the Identity Manager User Application or Role-Based Entitlements to control the conditions under provisioning occurs. See “Entitlements” on page 13 for more information.</p>
<i>Use Entitlements to Control LDAP Accounts</i>	<p>Select <i>True</i> to enable the driver to manage LDAP accounts based on the driver’s defined entitlements.</p> <p>Select <i>False</i> to disable management of LDAP accounts based on the entitlements.</p>
<i>Action if user does not have entitlement</i>	Select the action that you want to occur in the LDAP directory if a user in the Identity Vault does not have the LDAP account entitlement. Select <i>Do nothing</i> to not affect the LDAP directory, or select <i>Delete user</i> to remove the user’s LDAP account.

Table A-8 *Password Management*

Option	Description
<i>Show password management policy</i>	<p>Select <i>show</i> to display the global configuration values for password management. Select <i>hide</i> to not have the password management global configuration values displayed.</p> <p>In Designer, you must click the  icon next to an option to edit it. This displays the Password Synchronization Options dialog box that has a better view of the relationship between the different GCVs.</p> <p>In iManager, you should edit the Password Management Options on the <i>Server Variables</i> tab rather than under the GCVs. The Server Variables page has a better view of the relationship between the different GCVs.</p> <p>For more information about how to use the Password Management GCVs, see “Configuring Password Flow” in the <i>Identity Manager 3.6 Password Management Guide</i>.</p>
<i>Application accepts passwords from Identity Manager</i>	If <i>True</i> , allows passwords to flow from the Identity Manager data store to the connected system.
<i>Identity Manager accepts passwords from application</i>	If <i>True</i> , allows passwords to flow from the connected system to Identity Manager.
<i>Publish passwords to NDS password</i>	Use the password from the connected system to set the non-reversible NDS [®] password in eDirectory.
<i>Publish passwords to Distribution Password</i>	Use the password from the connected system to set the NMAST [™] Distribution Password used for Identity Manager password synchronization.

Option	Description
<i>Require password policy validation before publishing passwords</i>	If <i>True</i> , applies NMAS password policies during publish password operations. The password is not written to the data store if it does not comply.
<i>Reset user's external system password to the Identity Manager password on failure</i>	If <i>True</i> , on a publish Distribution Password failure, attempts to reset the password in the connected system by using the Distribution Password from the Identity Manager data store.
<i>Notify the user of password synchronization failure via e-mail</i>	If <i>True</i> , notify the user by e-mail of any password synchronization failures.

Table A-9 *Account Tracking*

Option	Description
<i>Show Account Tracking Configuration</i>	<p>Select <i>show</i> to display the global configuration values for account tracking through Novell Sentinel™. Select <i>hide</i> to not have the global configuration values displayed.</p> <p>The account tracking GCVs enable Sentinel to track Active Directory* accounts based on unique identifiers that you define. You must have both Sentinel 6.1 and the Identity Manager Driver for Sentinel 6.1 installed in order to track account information.</p> <p>For information about Sentinel, see the Sentinel 6.1 Documentation Web site (http://www.novell.com/documentation/sentinel61).</p> <p>The Identity Manager Driver for Sentinel 6.1 is included with the Novell Compliance Management Platform. For information, see the Identity and Security Management product Web site (http://www.novell.com/identityandsecurity/).</p>

Trace Levels

B

The driver supports the following trace levels:

Table B-1 *Supported Trace Levels*

Level	Description
1	Minimal Tracing
2	Previous level and LDAP Server information, LDAP operations in the Subscriber channel, Changelog Information
3	Previous level and LDAPSearch messages in the Publisher channel and all the remaining messages
4	Previous level and LDAPSearch messages in the Publisher channel and all the remaining messages
5	Previous level and password synchronization messages in the Publisher channel

For information about setting driver trace levels, see to “[Viewing Identity Manager Processes](#)” in the *Identity Manager 3.6 Common Driver Administration Guide*.