Novell Identity Manager Driver for LDAP

1.9.2

www.novell.com

IMPLEMENTATION GUIDE

December 7, 2006

Novell®

Legal Notices

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

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

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

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 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 www.novell.com/documentation.

Novell Trademarks

Third-Party Materials

Contents

About This Guide

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

- Chapter 1, “Introducing the Identity Manager Driver for LDAP,” on page 9
- Chapter 2, “Upgrading,” on page 15
- Chapter 3, “Installing the LDAP Driver,” on page 17
- Chapter 4, “Customizing the LDAP Driver,” on page 31
- Chapter 5, “Troubleshooting,” on page 47
- Appendix A, “Documentation Updates,” on page 49

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 document, see *Identity Manager Driver for LDAP* in the Identity Manager Drivers section on the Novell Documentation Web site (http://www.novell.com/documentation).

Additional Documentation

For information on Identity Manager and other Identity Manager drivers, see the Novell Documentation Web site (http://www.novell.com/documentation).

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.

Introducing the Identity Manager Driver for LDAP

1

1.1 What's New?

Table 1-1 *Summary of Released Features*

Feature	LDAP Driver Version	Description
Support for the PasswordModify Extended Operation	1.9	The Identity Manager Driver for LDAP supports the PasswordModify Extended Operation as defined in RFC 3062. If you are using an LDAP directory that supports the PasswordModify extended operation, such as OpenLDAP, the Driver for LDAP uses the extended operation when setting or modifying passwords on the Subscriber channel. If the LDAP directory doesn't support the PasswordModify extended operation, the Driver for LDAP sets a value on the UserPassword attribute, as in previous driver versions. This value is hashed and stored securely This feature doesn't require you to configure anything. The driver is capable of detecting whether the LDAP server supports the operation.
Controlling Whether the ;Binary Option Is Added To Attribute Names	1.9.2	A Subscriber channel parameter controls whether the ;binary option is added to attribute names when values are encoded. See "LDAP Subscriber Settings" on page 32.
Controlling Whether Initial Search Results Are Synchronized	1.9.2	A parameter for the LDAP-Search publication method controls whether the initial search results are synchronized, or only subsequent changes are synchronized. See "LDAP Publisher Settings: Only the LDAP-Search Method" on page 36.

1.2 Changes in Terminology

The following terms have changed from earlier releases:

Table 1-2 *Changes in Terminology*

Earlier Terms	New Terms
DirXML®	Identity Manager
DirXML Server	Metadirectory server
DirXML engine	Metadirectory engine
eDirectory™	Identity Vault (except when referring to eDirectory attributes or classes)

1.3 Driver Overview

The Identity Manager Driver for LDAP synchronizes data between an Identity Vault and LDAP-compliant directories. This driver runs on all platforms where an Identity Vault runs, including Windows*, NetWare®, Linux*, Solaris*, and AIX*. The driver can run anywhere that a Metadirectory server or Identity Manager Remote Loader is running.

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.

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

- The changelog method

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

  - Sun Java System Directory/Sun ONE Directory
  - Netscape* Directory Server
  - iPlanet* Directory Server
  - IBM* SecureWay Directory/IBM Tivoli Directory
  - Critical Path* InJoin* Directory
  - Oracle* Internet Directory

  See Section 4.1.3, “LDAP Publisher Settings: Changelog and LDAP-Search Methods,” on page 33 and Section 4.1.4, “LDAP Publisher Settings: Only the Changelog Method,” on page 34.

- The 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.

  Additional software and changes to the LDAP-compliant directory are not required. LDAP servers that can be synchronized by using the LDAP-search method include the following:

  - OpenLDAP

  See Section 4.1.5, “LDAP Publisher Settings: Only the LDAP-Search Method,” on page 36

For information on what's new in Identity Manager, see "What's New in Identity Manager?" in the *Identity Manager 3.0.1 Installation Guide*.

1.4 Default Driver Configuration

This section discusses implementations, additions, or exceptions specific to this driver. For information on Identity Manager fundamentals, see the *Novell Identity Manager 3.0.1 Administration Guide*.

1.4.1 Data Flow

This section provides information on channels, filters, and policies, all of which control data flow.

Publisher and Subscriber Channels

The driver supports Publisher and Subscriber channels:

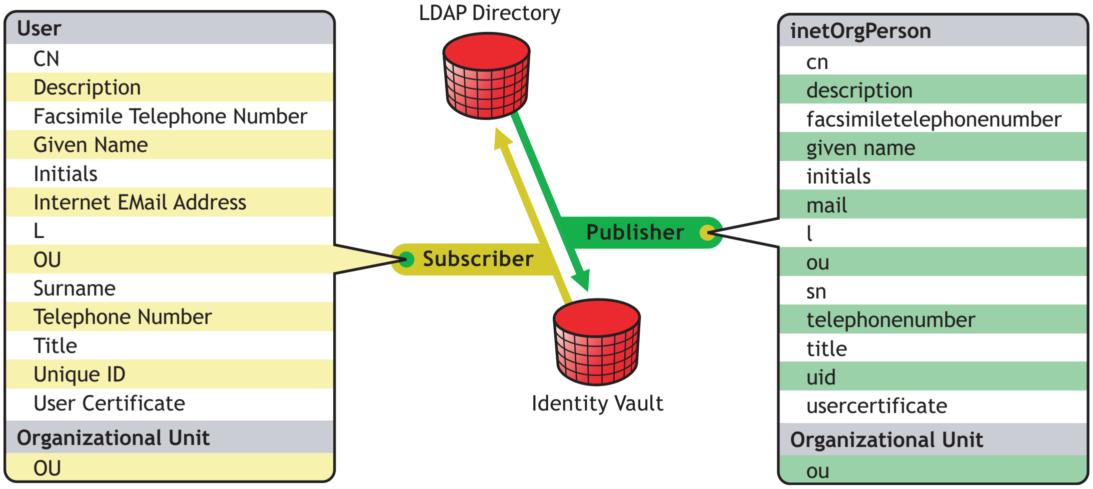
- The Publisher channel reads information from the LDAP directory change log or an LDAP search and submits that information to an Identity Vault via the Metadirectory engine.

  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 LDAP driver comes with two preconfiguration options to set up policies.

- The Flat option implements a flat structure for users in both directories.

  With this configuration, when user objects are created in one directory, they are placed in the root of the container you specified during driver setup for the other directory. (The container name doesn't need to be the same in both the Identity Vault and the LDAP directory). When existing objects are updated, their context is preserved.
- The Mirror option matches the hierarchical structure in the directories.

  With this configuration, when new user objects are created in one directory, they are placed in the matching hierarchical level of the mirror container in the other directory. When existing objects are updated, their context is preserved.

Except for the Placement policy and the fact that the Flat configuration doesn't synchronize Organizational Unit objects, the policies set up for these options are identical.

The following table provides information on default policies. These policies and the individual rules they contain can be customized through Novell iManager as explained in Chapter 4, "Customizing the LDAP Driver," on page 31.

Table 1-3 *Default Policies*

Policy	Description
Mapping	Maps the Identity Vault User object and selected properties to an LDAP inetOrgPerson. Maps the Identity Vault Organizational Unit to an LDAP organizationalUnit. By default, more than a dozen standard properties are mapped.
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	With the Simple placement option, new User objects created in the LDAP directory are placed in the container in an Identity Vault that you specify when importing the driver configuration. The User object is named with the value of cn. With the Mirror placement option, new User objects created in the LDAP directory are placed in the Identity Vault container that mirrors the object's LDAP container.
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.
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.

Policy	Description
Subscriber Placement	If you choose the Flat placement option during the import of the driver configuration, new User objects created in an Identity Vault are based on the value you specified during import. If you choose Mirrored placement during the import of the driver configuration, new User objects created in an Identity Vault are placed in the LDAP directory container that mirrors the object's Identity Vault container.

Upgrading

2

- Section 2.1, "Upgrading the Driver Shim," on page 15
- Section 2.2, "Upgrading the Driver Configuration," on page 16

2.1 Upgrading the Driver Shim

When you upgrade, the new driver shim replaces the previous driver shim but keeps the previous driver's configuration. The new driver shim can run the DirXML® 1.*x* configuration with no changes.

To upgrade the driver shim:

1 Make sure you have updated your driver with all the patches for the version you are currently running.

The new driver shim is intended to work with your existing driver configuration with no changes, assuming that your driver shim and configuration have the latest fixes. Review all TIDs and Product Updates for the version of the driver you are using.

To help minimize upgrade issues, we recommend that you complete this step on all drivers.

2 Install the new driver shim.

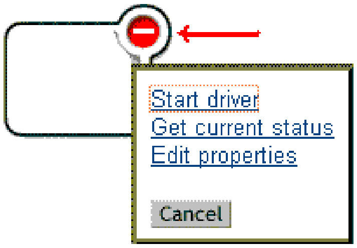
You can do this at the same time that you install the Metadirectory engine, or you can do it after the engine is installed. See Chapter 3, "Installing the LDAP Driver," on page 17.

3 After the shim is installed, restart the driver.

3a In iManager, select *Identity Manager* > *Identity Manager Overview*.

3b Browse to the driver set where the driver exists.

3c Select the driver that you want to restart, click the status icon, then select *Start Driver*.



4 Activate the driver shim with your Identity Manager activation credentials.

For information on activation, see "Activating Novell Identity Manager Products" in the *Identity Manager 3.0.1 Installation Guide*.

After you install the driver shim, upgrade the driver configuration. See Section 2.2, "Upgrading the Driver Configuration," on page 16.

2.2 Upgrading the Driver Configuration

Installing the driver shim does not change your existing configuration. Your existing configuration continues to work with the new driver shim with no changes.

However, if you want to take advantage of the new features, you must upgrade your driver configuration, either by replacing your driver configuration with the new sample configuration, or by converting your existing configuration to Identity Manager format and adding policies to it.

- To replace your existing configuration, import the new sample configuration for your existing driver objects.
- To convert an existing driver configuration so you can edit it with the new Identity Manager plug-ins, see "Upgrading a Driver Configuration from DirXML 1.1a to Identity Manager Format" in the *Novell Identity Manager 3.0.1 Administration Guide*.
- To add Identity Manager Password Synchronization functionality to an existing driver configuration, see "Upgrading Existing Driver Configurations to Support Password Synchronization" in the *Novell Identity Manager 3.0.1 Administration Guide*.

Installing the LDAP Driver

3

- Section 3.1, “Planning Considerations,” on page 17
- Section 3.2, “System Prerequisites,” on page 18
- Section 3.3, “Installation,” on page 19

3.1 Planning Considerations

The LDAP Driver for Identity Manager works with most LDAP v3 compatible LDAP servers. The driver is written to the RFC 2251 specification for LDAP. For information on compatibility issues, see Section 5.3, “LDAP v3 Compatibility,” on page 48.

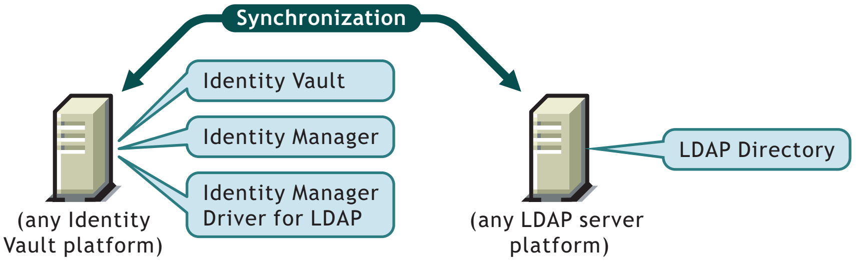
- “Where to Install the LDAP Driver” on page 17
- “Information to Gather” on page 18
- “Assumptions about the LDAP Data Source” on page 18

3.1.1 Where to Install the LDAP Driver

An Identity Manager driver can be installed on the same computer where an Identity Vault and the Metadirectory engine are installed. This installation is referred to as a local configuration.

In a local configuration, you install the LDAP driver on the computer where an Identity Vault and the Metadirectory engine are installed, as shown in the following figure:

Figure 3-1 *A Local Configuration*


Synchronization
Identity Vault
Identity Manager
Identity Manager Driver for LDAP
(any Identity Vault platform)
LDAP Directory
(any LDAP server platform)

If platform or policy constraints make a local configuration difficult, an Identity Manager driver can be installed on the computer hosting the target application. This installation is referred to as a remote configuration.

Although it is possible to install the LDAP driver in a remote configuration, 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.

3.1.2 Upgrading to Identity Manager 3

During an Identity Manager installation, you can install the Driver for LDAP (along with other Identity Manager drivers) at the same time that the Metadirectory engine is installed. See the *Identity Manager 3.0.1 Installation Guide*. You can upgrade from DirXML 1.1a or Identity Manager 2 to Identity Manager 3.

3.1.3 Information to Gather

During installation and setup, you are prompted for information such as the following:

- Whether to use the Flat or Mirror option for synchronizing hierarchical structure. See "Policies" on page 12.
- The Identity Vault and LDAP directory containers that you want to hold synchronized objects.
- The Identity Vault User object to assign as a security equivalent for the driver and the objects to exclude from synchronization.
- The LDAP object and password used to provide driver access to the LDAP directory.

See the table in "Importing the Sample Driver Configuration File" on page 26.

3.1.4 Assumptions about the LDAP Data Source

If you are using the Publisher channel to send data to an Identity Vault about changes in the LDAP directory, you must understand the two methods that the driver uses to publish data:

- The changelog method

  The change log is a mechanism in an LDAP directory. The change log can provide LDAP event information for the driver. This method is preferred when a change log is available.
- The LDAP-search method

  This method enables the LDAP driver to publish to an Identity Vault data about the LDAP servers that don't use change logs.

3.2 System Prerequisites

❑ Novell® Identity Manager

❑ The system requirements of Identity Manager or later

❑ If you are using the changelog method, one of the following LDAP directories:

  - Netscape Directory Server 4.*x* or 6
  - iPlanet Directory Server 5.0 or greater
  - IBM SecureWay Directory 3.2, 4.1.1, or 5.1
  - Critical Path InJoin Directory 3.1
  - Oracle Internet Directory 2.1.1 or greater
  - Sun ONE* 5.2
  - LDAP version 3 compliant directories

3.3 Installation

- "Installing the LDAP Driver" on page 19
- "Setting Up the Driver" on page 25

3.3.1 Installing the LDAP Driver

You can install the driver separately, after the Metadirectory engine is installed.

- "Installing on Windows" on page 19
- "Installing on NetWare" on page 21
- "Installing on Linux, Solaris, or AIX" on page 22

Installing on Windows

Install the Identity Manager Driver for LDAP on a Windows NT* 2003 server, or a Windows NT 2000 with Support Pack 2.

1 Run the installation program from the Identity Manager 2.0 CD or the download image.

   Downloads are available from Novell Downloads (http://download.novell.com/index.jsp).

   If the installation program doesn't autolaunch, you can run `\nt\install.exe.`

2 In the Welcome dialog box, click *Next*, then accept the license agreement.

3 In the first Identity Manager Overview dialog box, review the information, then click *Next*.

   The dialog box provides information on the following:

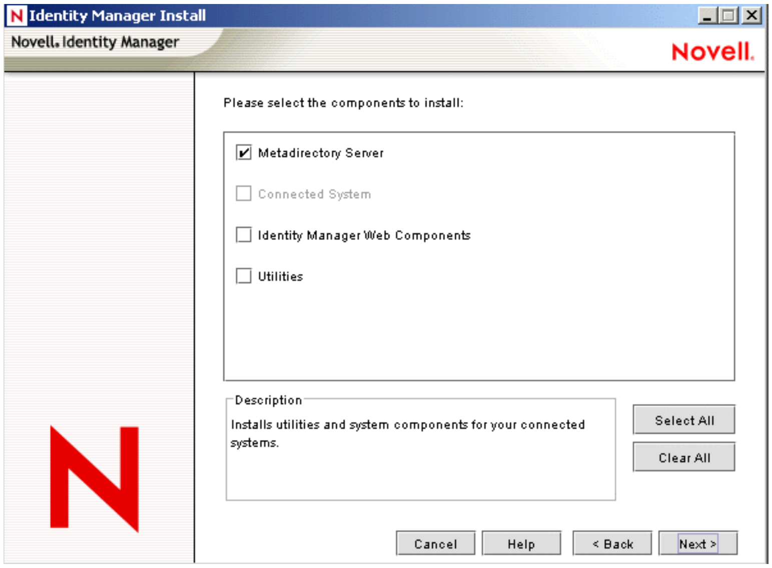
   - A Metadirectory server
   - An Identity Manager connected server system

4 In the second Identity Manager Overview dialog box, review the information, then click *Next*.

   The dialog box provides information on the following:

   - A Web-based administration server
   - Identity Manager utilities

5 In the Please Select the Components to Install dialog box, select only *Metadirectory Server*, then click *Next*.



Please select the components to install:

☑ Metadirectory Server

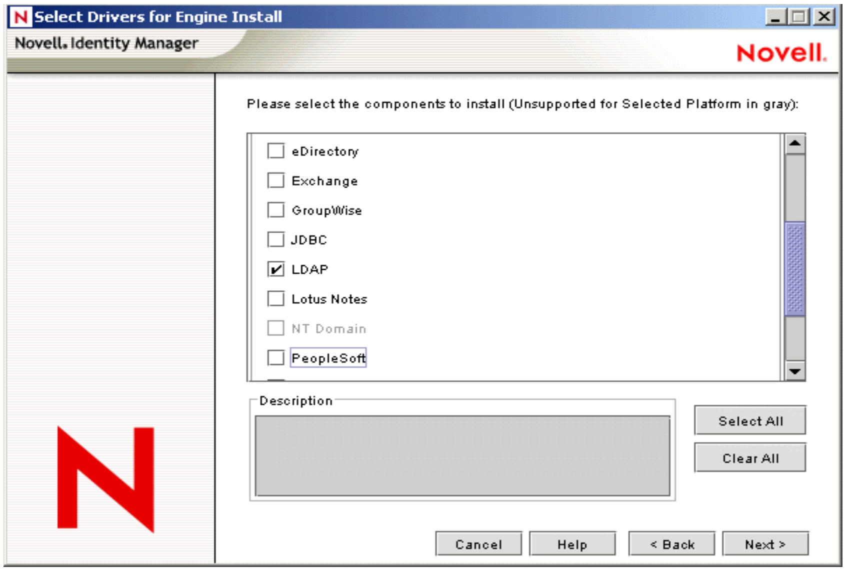
□ Connected System

□ Identity Manager Web Components

□ Utilities

Installs utilities and system components for your connected systems.

6 In the Select Drivers for Engine Install dialog box, select only *LDAP*, then click *Next*.



Please select the components to install (Unsupported for Selected Platform in gray):

□ eDirectory

□ Exchange

□ GroupWise

□ JDBC

☑ LDAP

□ Lotus Notes

□ NT Domain

□ PeopleSoft

7 In the Identity Manager Upgrade Warning dialog box, click *OK*.

8 In the Schema Extension dialog box, type a username and password, then click *Next*.

For the password to be valid, you must have rights to the root.

9 In the Summary dialog box, review the selected options, then click *Finish*.

10 In the Installation Complete dialog box, click *Close*.

After installation you must configure the driver as explained in "Setting Up the Driver" on page 25.

Installing on NetWare

1 At the NetWare® server, insert the Identity Manager 3 CD and mount the CD as a volume.

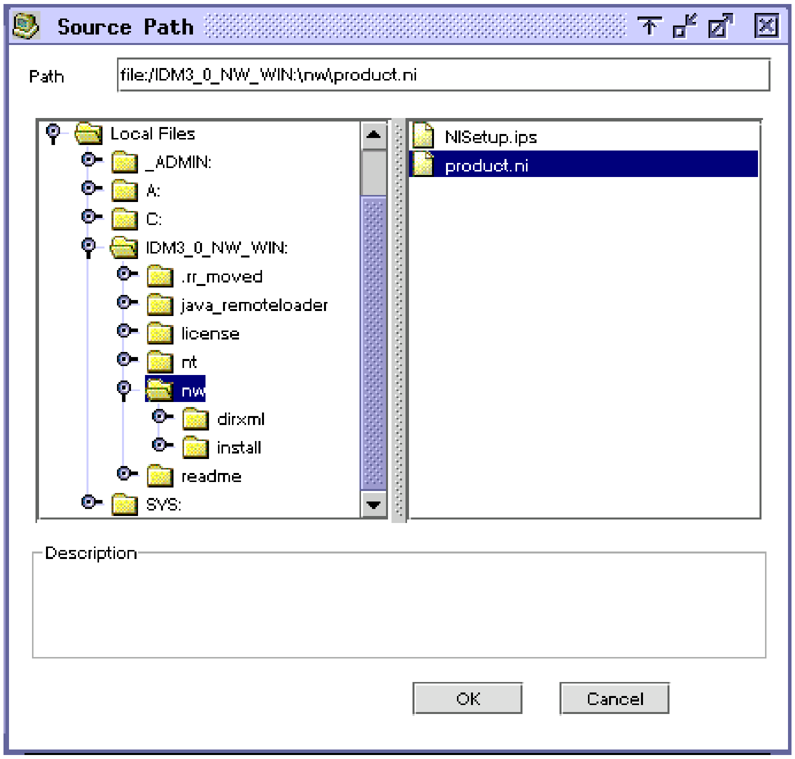
To mount the CD, enter `m cdrom`.

2 (Conditional) If the graphical utility isn't loaded, load it by entering `startx`.

3 In the graphical utility, click the Novell icon, then click *Install*.

4 In the Installed Products dialog box, click *Add*.

5 In the Source Path dialog box, browse to and select the `product.ni` file.



Source Path

Path: file:/IDM3_0_NW_WIN:\nw\product.ni

5a Browse to and expand the CD volume that you mounted earlier.

5b Expand the nw directory, select `product.ni`, then click *OK* twice.

6 In the Welcome dialog box, click *Next*, then accept the license agreement.

7 In the Identity Manager Install dialog box, select only *Metadirectory Server*.

Deselect the following:

- Identity Manager Web Components
- Utilities

8 In the Select Drivers for Engine Install dialog box, select only Delimited Text.

Deselect the following:

- Metadirectory engine
- All drivers except LDAP

9 Click *Next*.

10 In the Identity Manager Upgrade Warning dialog box, click *OK*.

The dialog box advises you to activate a license for the driver within 90 days.

11 In the Schema Extension dialog box, type a username and password, then click *Next*.

12 In the Summary page, review the selected options, then click *Finish*.

13 Click *Close*.

After installation you must configure the driver as explained in "Setting Up the Driver" on page 25.

Installing on Linux, Solaris, or AIX

By default, the Identity Manager Driver for LDAP is installed when you install the Metadirectory engine. If the driver wasn't installed at that time, this section can help you install it.

As you move through the installation program, you can return to a previous section (screen) by entering `previous`.

1 In a terminal session, log in as root.

2 Insert the Identity Manager CD and mount it.

Typically, the CD is automatically mounted. You can manually mount the CD. For example, for SUSE®, type `mount /media/cdrom`.

3 Change to the setup directory.

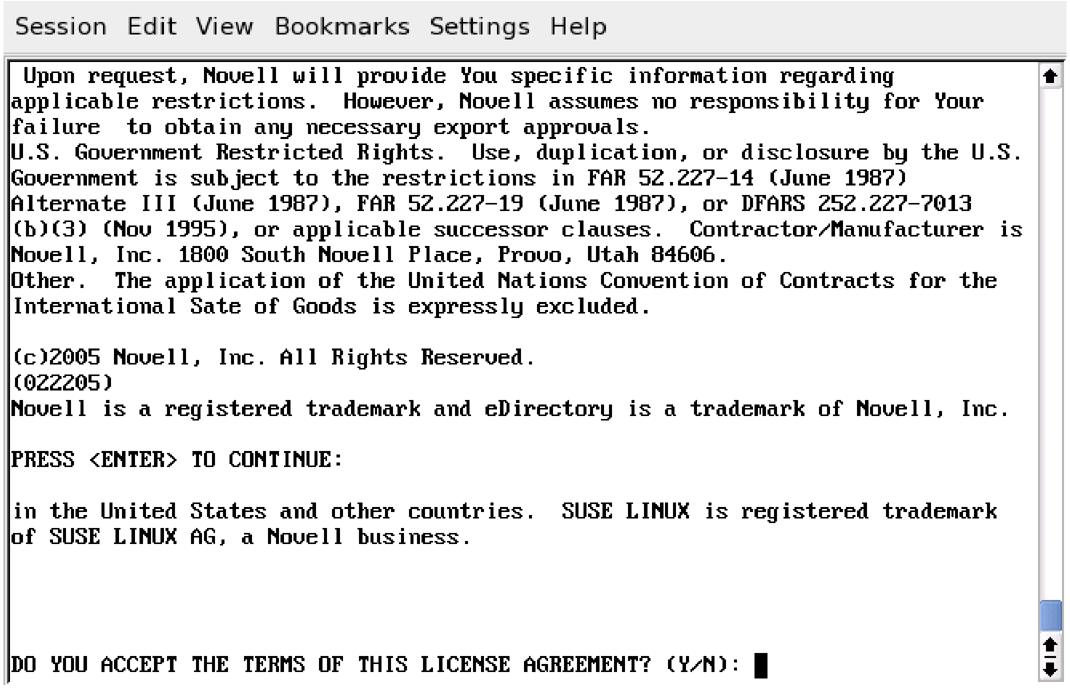
Platform	Path
Red Hat	/mnt/cdrom/linux/setup/
SUSE	/media/cdrom/linux/setup/
Solaris	/cdrom/solaris/_idm_2/setup/
AIX	/media/cdrom/aix/setup/

4 Run the installation program.

For example, for SUSE, run `./dirxml_linux.bin`.

5 In the Introduction section, press Enter.

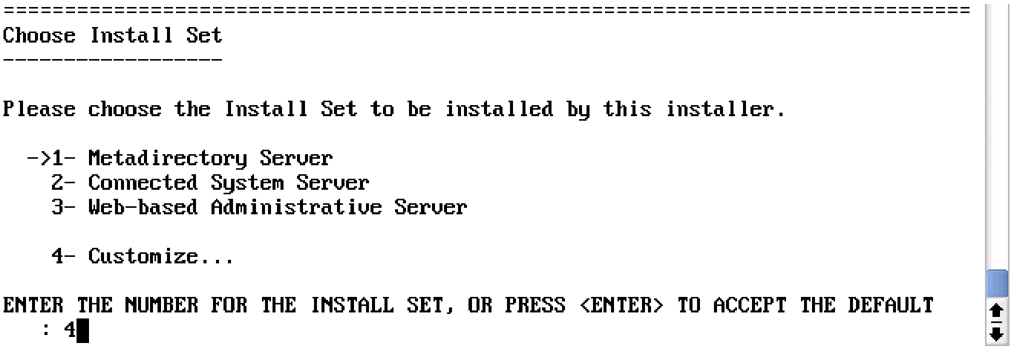
6 Press Enter until you reach the *Do You Accept the Terms of This License Agreement* prompt, type `y to accept the license agreement`, then press Enter.



```
 Upon request, Novell will provide You specific information regarding
applicable restrictions.  However, Novell assumes no responsibility for Your
failure  to obtain any necessary export approvals.
U.S. Government Restricted Rights.  Use, duplication, or disclosure by the U.S.
Government is subject to the restrictions in FAR 52.227-14 (June 1987)
Alternate III (June 1987), FAR 52.227-19 (June 1987), or DFARS 252.227-7013
(b)(3) (Nov 1995), or applicable successor clauses.  Contractor/Manufacturer is
Novell, Inc. 1800 South Novell Place, Provo, Utah 84606.
Other.  The application of the United Nations Convention of Contracts for the
International Sate of Goods is expressly excluded.

(c)2005 Novell, Inc. All Rights Reserved.
(022205)
Novell is a registered trademark and eDirectory is a trademark of Novell, Inc.

PRESS <ENTER> TO CONTINUE:

in the United States and other countries.  SUSE LINUX is registered trademark
of SUSE LINUX AG, a Novell business.



DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N): 
```

7 In the *Choose Install Set* section, select the *Customize* option.

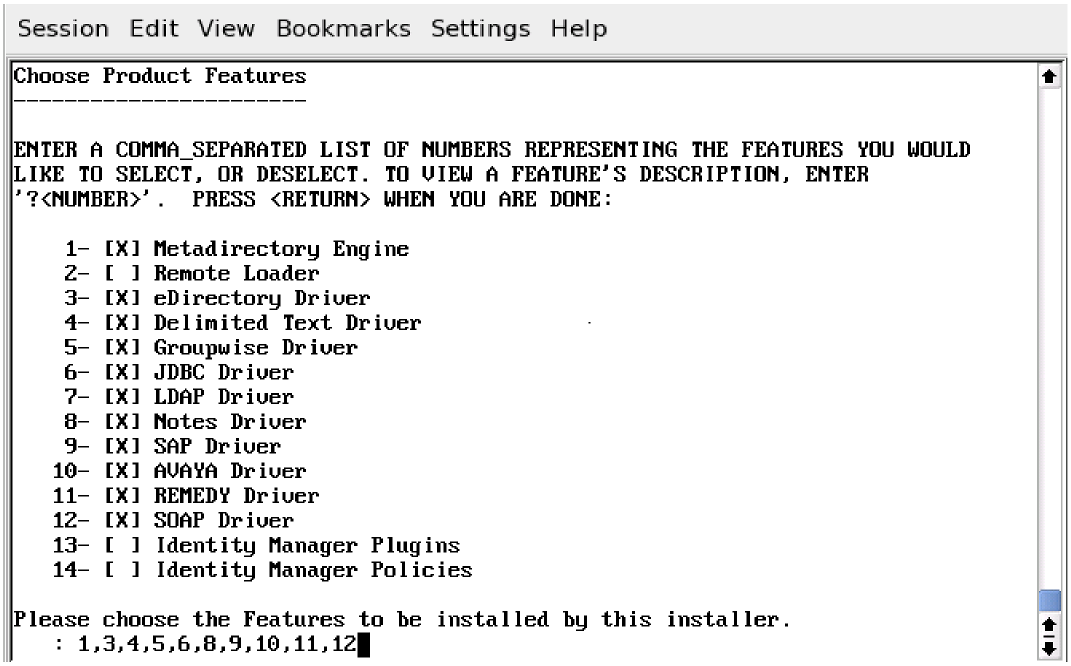
Type `4`, then press Enter.



```
===============================================================================
Choose Install Set
------------------

Please choose the Install Set to be installed by this installer.

  ->1- Metadirectory Server
    2- Connected System Server
    3- Web-based Administrative Server

    4- Customize...

ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
   : 4
```

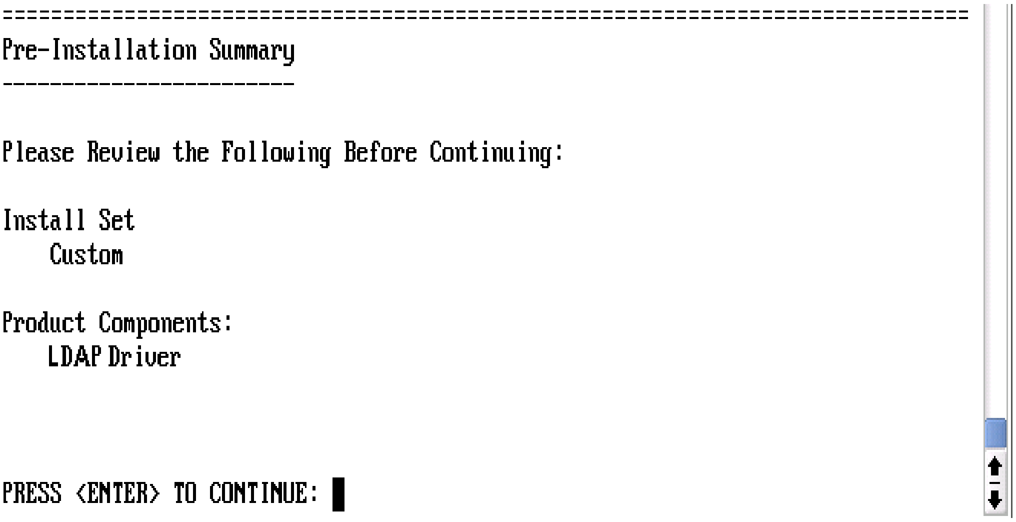
8 In the *Choose Product Features* section, deselect all features except LDAP, then press Enter.

To deselect a feature, type its number. Type a comma between additional features that you deselect.



```
Choose Product Features
-----------------------

ENTER A COMMA_SEPARATED LIST OF NUMBERS REPRESENTING THE FEATURES YOU WOULD
LIKE TO SELECT, OR DESELECT. TO VIEW A FEATURE'S DESCRIPTION, ENTER
'?<NUMBER>'.  PRESS <RETURN> WHEN YOU ARE DONE:

    1- [X] Metadirectory Engine
    2- [ ] Remote Loader
    3- [X] eDirectory Driver
    4- [X] Delimited Text Driver
    5- [X] Groupwise Driver
    6- [X] JDBC Driver
    7- [X] LDAP Driver
    8- [X] Notes Driver
    9- [X] SAP Driver
   10- [X] AVAYA Driver
   11- [X] REMEDY Driver
   12- [X] SOAP Driver
   13- [ ] Identity Manager Plugins
   14- [ ] Identity Manager Policies

Please choose the Features to be installed by this installer.
   : 1,3,4,5,6,8,9,10,11,12
```

9 In the Pre-Installation Summary section, review options.



```
===============================================================================
Pre-Installation Summary
------------------------

Please Review the Following Before Continuing:

Install Set
    Custom

Product Components:
    LDAP Driver



PRESS <ENTER> TO CONTINUE:
```

To return to a previous section, type `previous`, then press Enter.

To continue, press Enter.

10 After the installation is complete, exit the installation by pressing Enter.

After installation you must configure the driver as explained in "Setting Up the Driver" on page 25.

3.3.2 Setting Up the Driver

Setup is not required if you are upgrading an existing driver.

If this is the first time the LDAP driver has been used, complete the setup tasks in the following sections:

- "Preparing the LDAP Server" on page 25
- "Importing the Sample Driver Configuration File" on page 26
- "Starting the Driver" on page 29
- "Migrating and Resynchronizing Data" on page 29
- "Activating the Driver" on page 29

Preparing the LDAP Server

If you use the driver only to synchronize data from an Identity Vault to the LDAP server (on a Subscriber channel), most LDAP servers and applications work without any additional configuration.

You always create a User object that has the necessary rights so the driver can authenticate to the LDAP server.

However, if you require that changes made to entries on the LDAP server synchronize back to an Identity Vault (on a Publisher channel), and if you plan to use the changelog method, you need to perform at least one other configuration task on the LDAP server before running the driver. Verify that the change log mechanism of the LDAP server is enabled.

IMPORTANT: If the LDAP server doesn't have a changelog mechanism, use the LDAP-search method. Otherwise, the driver won't be able to publish events for that server.

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 gets 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 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 Novell's 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"; )
   -
   ```

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.

Importing the Sample Driver Configuration File

- "Importing by Using iManager" on page 27
- "Importing by Using Designer for Identity Manager" on page 28

Importing by Using iManager

Import the LDAP driver configuration by following the instructions to import a driver in “Creating and Configuring a Driver ”in the *Novell Identity Manager 3.0.1 Administration Guide*.

During import, provide the following information for the driver configuration.

Table 3-1 *Settings for the LDAP Driver*

Field	Description
Driver Name	The Identity Vault object name to be assigned to this driver, or the existing driver for which you want to update the configuration.
Placement Type	With the Simple placement option, new User objects created in the LDAP directory are placed in the container in an Identity Vault that you specify when importing the driver configuration. The user object is named with the value of cn. With the Mirror placement option, new User objects created in the LDAP directory are placed in the Identity Vault container that mirrors the object's LDAP container.
eDirectory Container	The container in an Identity Vault where new users should be created. If this container doesn’t exist, you must create it before you start the driver. For the LDAPMirrorSample.xml configuration, this directory is the starting point for the driver’s Placement policy. Subordinate containers should be named the same as the subordinate containers in the LDAP mirror container. For the Flat configuration, this container houses all User objects.
LDAP Container	The container in the LDAP directory where new users should be created. If this container doesn’t exist, you must create it before you start the driver. For the Flat configuration, this directory is the starting point for the driver’s Placement policy. For the LDAPSimplePlacementSample.xml configuration, this container houses all User objects.
LDAP Server	The hostname or IP address and port of the LDAP server.
LDAP Authentication DN	Specify the LDAP DN of the administrator account created for the LDAP driver.
LDAP Authentication Password	The password for the LDAP driver administrator account. You confirm the password by re-entering it in the next field. This is the required password for the authenticated user. If the LDAP driver uses Directory Manager exclusively, the default authenticated user works well. However, if this user is used for any other purpose, you should probably change the default after you get the driver running. See “Creating an LDAP User Object with Authentication Rights” on page 25.
SSL	Encrypts LDAP protocol communications.

Field	Description
Configure Data Flow	◆ Bidirectional means that both LDAP and the Identity Vault are authoritative sources of the data synchronized between them. ◆ LDAP to eDirectory means that LDAP is the authoritative source. ◆ eDirectory to LDAP means that the Identity Vault is the authoritative source.
Install Driver as Remote/Local	Configure the driver for use with the Remote Loader service by selecting Remote, or select Local to configure the driver for local use.
Remote Host Name and Port	Specify the host name or IP address and port number where the Remote Loader Service has been installed and is running for this driver. The default port is 8090.
Driver Password	The Remote Loader uses the driver object password to authenticate itself to the Metadirectory server. The driver object password must be the same password that is specified as the driver object password on the Identity Manager Remote Loader.
Remote Password	This password is used only in the Remote Loader configuration. It allows the Remote Loader to authenticate to the Metadirectory engine. The Remote Loader password is used to control access to the Remote Loader instance. The Remote Loader password must be the same password that is specified as the Remote Loader password on the Identity Manager Remote Loader.
Password Failure Notification User	Sends an e-mail notification to a specified user when a password fails.
Enable Entitlements	Choose Yes or No. Because this is a design decision, you should understand entitlements before choosing to use it. For information about entitlements, see "Creating and Using Entitlements" in the *Novell Identity Manager 3.0.1 Administration Guide*.

Importing by Using Designer for Identity Manager

You can import the basic driver configuration file for the LDAP driver by using Designer for Identity Manager. This basic file creates and configures the objects and policies needed to make the driver work properly.

The following procedure explains one of several ways to import the sample configuration file:

1. Open a project in Designer.
2. In the modeler, right-click the Driver Set object, then select *Add Connected Application*.
3. From the drop-down list, select *LDAP.xml*, then click *Run*.
4. Click *Yes*, in the Perform Prompt Validation window.
5. Configure the driver by filling in the fields.

   Specify information specific to your environment. For information on the settings, see the table in "Importing by Using iManager" on page 27.
6. After specifying parameters, click *OK* to import the driver.
7. Customize and test the driver.
8. Deploy the driver into the Identity Vault.

See “Deploying a Driver to an Identity Vault” in the *Designer for Identity Manager 3: Administration Guide*.

Starting the Driver

If you changed default data locations during configuration, ensure that the new locations exist before you start the driver.

1. In iManager, select *Identity Manager* > I*dentity Manager Overview*.
2. Locate the driver in its driver set.
3. Click the driver status indicator in the upper right corner of the driver icon, then click *Start Driver*.

   If a change log is available, the driver processes all the changes in the change log. To force an initial synchronization, see “Migrating and Resynchronizing Data” on page 29.

Migrating and Resynchronizing Data

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

- **Migrate Data from eDirectory:** 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 5.1, “Migrating Users into an Identity Vault,” on page 47.

- **Migrate Data into eDirectory:** 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.

To use one of the options:

1. In iManager, select *Identity Manager* > *Identity Manager Overview*.
2. Locate the driver set that contains the Identity Manager Driver for LDAP, then double-click the driver icon.
3. Click the appropriate migration button.

Activating the Driver

Activate the driver within 90 days of installation. Otherwise, the driver won’t work.

For information on activation, see “Activating Novell Identity Manager Products” in the *Identity Manager 3.0.1 Installation Guide*.

Customizing the LDAP Driver

4

The LDAP driver includes example configurations that you can use as a starting point for your deployment. However, most Identity Manager deployments require you to modify these examples.

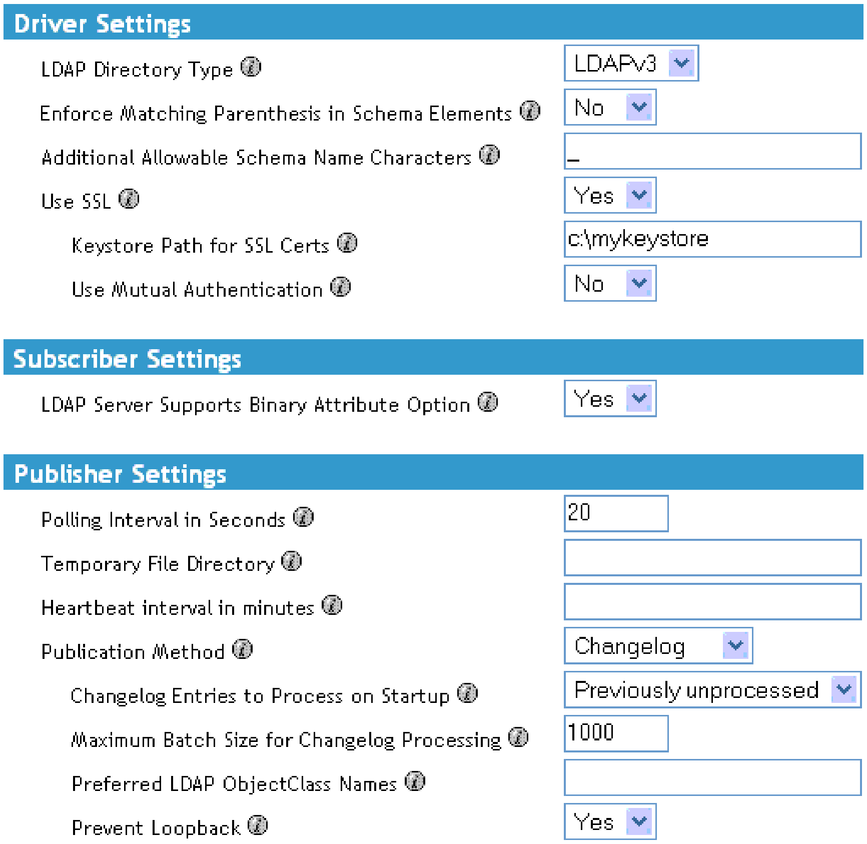
In this section:

- Section 4.1, "Controlling Data Flow from the LDAP Directory to an Identity Vault," on page 31
- Section 4.2, "Configuring Data Synchronization," on page 37
- Section 4.3, "Configuring SSL Connections," on page 41

NOTE: When you customize data synchronization, you must work within the supported standards and conventions for the operating systems and accounts being synchronized. Data containing characters that are valid in one environment, but invalid in another, causes errors.

4.1 Controlling Data Flow from the LDAP Directory to an Identity Vault

Figure 4-1 *Settings in the Sample Configuration File*



Driver Settings

LDAP Directory Type	LDAPv3
Enforce Matching Parenthesis in Schema Elements	No
Additional Allowable Schema Name Characters	_
Use SSL	Yes
Keystore Path for SSL Certs	c:\mykeystore
Use Mutual Authentication	No

Subscriber Settings

LDAP Server Supports Binary Attribute Option	Yes

Publisher Settings

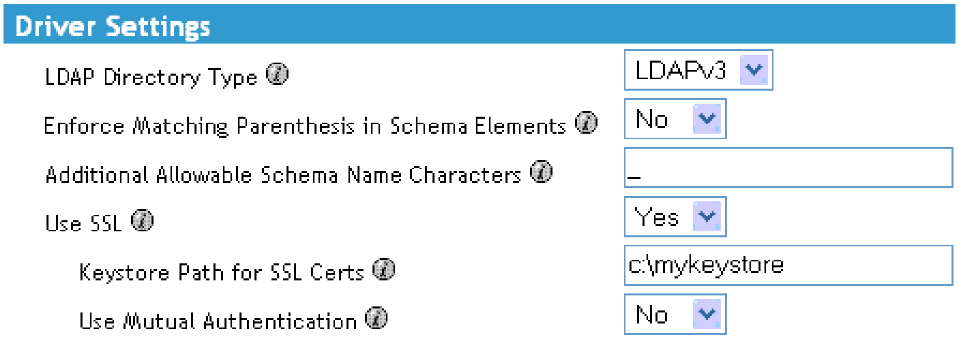
Polling Interval in Seconds	20
Temporary File Directory	
Heartbeat interval in minutes	
Publication Method	Changelog
Changelog Entries to Process on Startup	Previously unprocessed
Maximum Batch Size for Changelog Processing	1000
Preferred LDAP ObjectClass Names	
Prevent Loopback	Yes

Adjusting the driver's operating parameters allows you to tune driver behavior to align with your network environment. For example, you might find the default Publisher channel polling interval to be shorter than your synchronization needs require. Making the interval longer could improve network performance while still maintaining appropriate synchronization.

If the LDAP server has a change log, we recommend that you use the changelog publication method. If a change log is unavailable, you can use the LDAP-search publication method. The changelog method is the preferred method.

4.1.1 LDAP Driver Settings

Figure 4-2 *LDAP Driver Settings*



Driver Settings

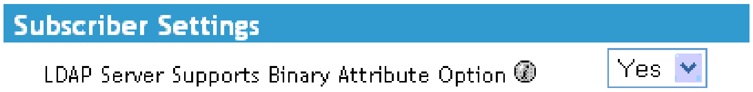
LDAP Directory Type ⓘ	LDAPv3
Enforce Matching Parenthesis in Schema Elements ⓘ	No
Additional Allowable Schema Name Characters ⓘ	_
Use SSL ⓘ	Yes
Keystore Path for SSL Certs ⓘ	c:\mykeystore
Use Mutual Authentication ⓘ	No

1. In iManager, select *Identity Manager > Identity Manager Overview*, then search for the driver set.
2. In the driver set, click the LDAP driver icon.
3. In the driver view, click the LDAP driver icon again.
4. Scroll to *Driver Parameters*.
5. In the *Driver Settings* section, select the desired option.

   For information on a setting, click the Information icon ⓘ.

4.1.2 LDAP Subscriber Settings

Figure 4-3 *The LDAP Subscriber Setting*



Subscriber Settings

LDAP Server Supports Binary Attribute Option ⓘ	Yes

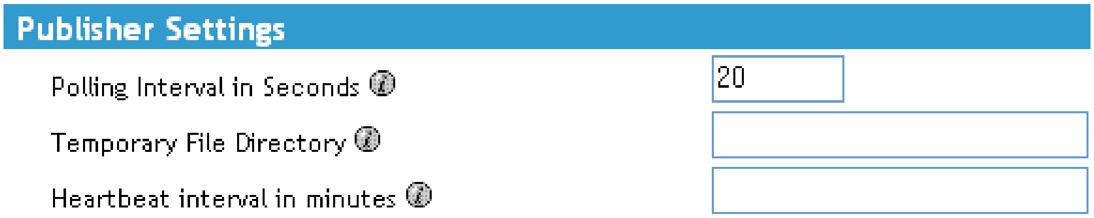
You aren't prompted for this setting when you import the sample configuration file. However, you can change the setting after importing the file. In the *Subscriber Settings* section, select the desired option.

The default setting is *Yes*. 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 that this driver connects to supports the binary attribute option, select *Yes*.

4.1.3 LDAP Publisher Settings: Changelog and LDAP-Search Methods

Figure 4-4 *LDAP Common Publisher Settings*



Publisher Settings

Polling Interval in Seconds: 20

Temporary File Directory:

Heartbeat interval in minutes:

Some settings apply to both the changelog and LDAP-search publication methods. Some settings apply only to the changelog publication method. Other settings apply only to the LDAP-search publication method.

Polling Interval in Seconds

The interval at which the driver checks the LDAP server’s change log or LDAP-search method. When new changes are found, they are applied to the Identity Vault.

The recommended polling interval is 120 seconds.

Temporary File Directory

Set the value to 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.

Table 4-1 *Temporary File Directories*

Platform or Environment	Default Directory
eDirectory	The DIB file directory
Remote Loader	The root Remote Loader directory

These files help do the following:

- Maintain driver consistency even when the driver is shut down
- Prevent memory shortages when the data being searched is extensive

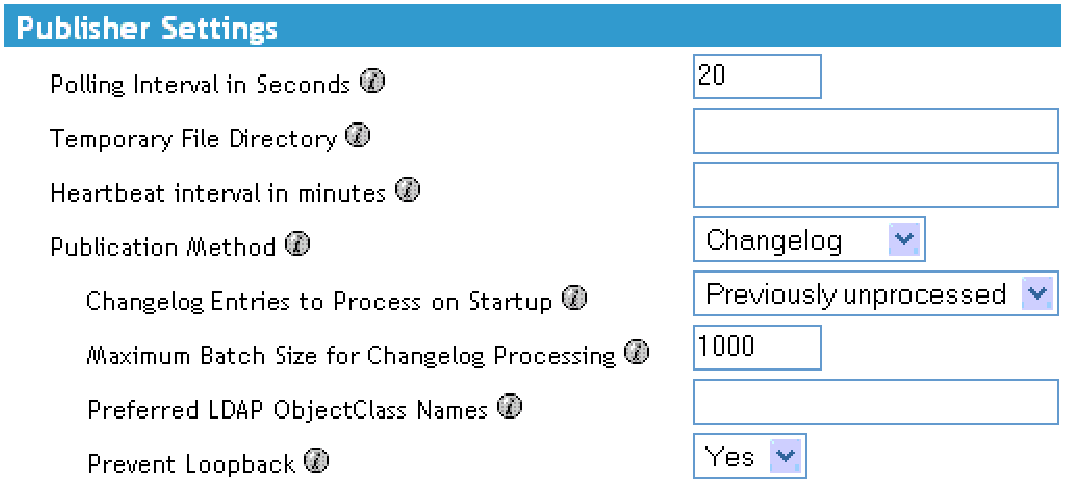
Heartbeat Interval in Minutes

To turn on a heartbeat, type a value. To turn off the heartbeat, leave this field empty.

For information on the driver heartbeat, see “Adding Driver Heartbeat” in the *Novell Identity Manager 3.0.1 Administration Guide*.

4.1.4 LDAP Publisher Settings: Only the Changelog Method

Figure 4-5 *Changelog Settings on the LDAP Publisher Channel*



Publisher Settings

Polling Interval in Seconds	20
Temporary File Directory	
Heartbeat interval in minutes	
Publication Method	Changelog
Changelog Entries to Process on Startup	Previously unprocessed
Maximum Batch Size for Changelog Processing	1000
Preferred LDAP ObjectClass Names	
Prevent Loopback	Yes

Changelog Entries to Process on Startup

This parameter specifies which entries to process on startup.

- 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 1-All, processing all new changes.

  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.

When using the changelog method, the driver looks for a batch size and a Prevent Loopback setting.

Maximum Batch Size for Changelog Processing

When the Publisher channel processes new entries from the LDAP change log, the Publisher asks for the entries in batches of this size. 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.

Preferred LDAP ObjectClass Names

The *Preferred LDAP ObjectClass Name* setting is an optional driver parameter that lets you specify preferred object classes on the Publisher channel.

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 Identity Manager Driver for LDAP 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.

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.

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.

When this parameter is present, the Identity Manager Driver for LDAP 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.

Prevent Loopback

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.

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.

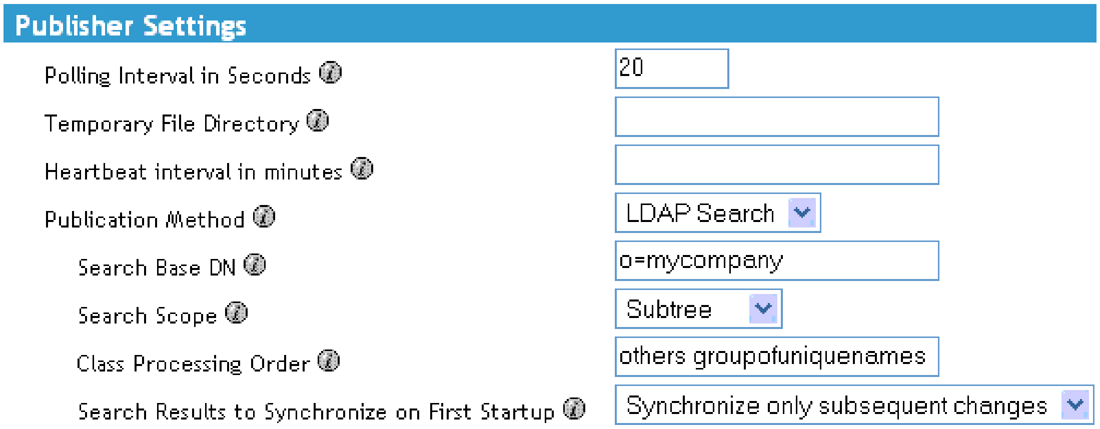
As an example scenario, you might not have a Subscriber channel configured for this driver but you want to be able to use the same DN and password as other processes use to make changes.

If you are certain that you want to allow this type of loopback to occur, edit the driver parameter:

1. In iManager, select *Identity Manager Management* > *Identity Manager Overview*.
2. Find the driver in its driver set.
3. Click the driver to open the Driver Overview page, then click the driver again to open the *Modify Object* page.
4. Scroll to the Publisher Settings section, then set *Prevent Loopback* to *No*.
5. Click *OK*, click *Apply*, then restart the driver for this parameter to function.

4.1.5 LDAP Publisher Settings: Only the LDAP-Search Method

Figure 4-6 *LDAP-Search Settings on the LDAP Publisher Channel*



Publisher Settings

Polling Interval in Seconds	20
Temporary File Directory	
Heartbeat interval in minutes	
Publication Method	LDAP Search
Search Base DN	o=mycompany
Search Scope	Subtree
Class Processing Order	others groupofuniquenames
Search Results to Synchronize on First Startup	Synchronize only subsequent changes

Traditionally, the LDAP driver has been able to detect changes in an LDAP server only by reading its change log. However, some servers don't use the changelog mechanism, which is actually not part of the LDAP standard. Where change logs don't exist, the LDAP driver has previously been unable to publish data about these LDAP servers to an Identity Vault.

However, the LDAP-search publication method doesn't require a change log. This method detects changes by using standard LDAP searches and then comparing the results from one search interval to the next interval.

You can use the LDAP-search publication method as an alternative to the traditional changelog publication method. The Identity Manager Driver for LDAP supports either method. However, the changelog method has performance advantages and is the preferred method when a change log is available.

WARNING: The LDAP-Search method works by comparing the current state of the LDAP server with previous states, and sending updates to the Identity Vault that reflect the changes. When an entry with a specific DN exists in a previous state, but not the current state, the driver has no way to know whether that entry was deleted or whether it was renamed or moved. Therefore, it sends a delete event to the Identity Vault for the previous DN, and if it was renamed or moved, then a new add event is generated. This is usually fine if the LDAP server is the authoritative source for all of the entry attributes. If, however, there are other sources (such as other drivers) that also provide information for the entry in the Identity Vault, then deleting an entry that has only been moved or renamed would be undesirable because it could result in data loss. In this case, you might need to create policy that would veto delete events on the publisher channel, or re-evaluate whether moves or renames should be done at all in the LDAP directory.

To use the LDAP-search publication method, set the following parameters:

- "Search Base DN" on page 37
- "Search Scope (1-Subtree, 2-One Level, 3-Base)" on page 37
- "Class Processing Order" on page 37
- "Search Results to Synchronize on First Startup" on page 37

Search Base DN

A required parameter when you use the Publisher channel if no change log is available. Set the parameter to the LDAP distinguished name (DN) of the container where the polling searches should begin (for example, ou=people,o=company).

To use a change log, leave this parameter blank.

Search Scope (1-Subtree, 2-One Level, 3-Base)

Indicates the depth of the polling searches. This parameter defaults to search the entire subtree that the Search Base DN points to.

Set this parameter when no change log is available.

Class Processing Order

An optional parameter that the Publisher channel uses 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.

The Identity Manager Driver for LDAP defines a special class name, “others,” to mean all classes other than those explicitly listed.

The default value for this parameter is “other groupofuniquenames.”

Use this parameter when no change log is available.

Search Results to Synchronize on First Startup

The first time that the LDAP driver starts, the driver performs the defined LDAP search. The *Search Results to Synchronize on First Startup* setting defines whether the initial search results are synchronized, or only subsequent changes are synchronized.

The *Search Results to Synchronize on First Startup* option appears only if the *Publication Method* parameter is set to *LDAP-Search*. You aren’t prompted for this setting when you import the configuration file. However, you can change the setting after importing the file.

1. In iManager, select *Identity Manager* > *Identity Manager Overview*, then search for the driver set.
2. In the driver set, click the LDAP driver icon.
3. In the driver view, click the LDAP driver icon again.
4. Scroll to *Driver Parameters*.
5. In the *Publisher Settings* section, select the desired option.

   The default setting is *Synchronize only subsequent changes*.

4.2 Configuring Data Synchronization

- Section 4.2.4, “Working with eDirectory Groups and Netscape,” on page 40

4.2.1 Determining Which Objects Are Synchronized

Identity Manager uses filters on the Publisher and Subscriber channels to control which objects are synchronized and to define the authoritative data source for these objects.

The default filters are illustrated in “Filters” on page 11. Use the following procedures to make changes to the default.

Editing the Publisher and Subscriber Filters

1. In iManager, select *Identity Manager* > *Identity Manager Overview*.
2. Locate the driver in its driver set.
3. Click the driver to open the *Identity Manager Driver Overview* page.
4. Click the Publisher or Subscriber Filter icon and make the appropriate changes.

   The Publisher filter must include the Identity Vault mandatory attributes. The Subscriber filter must include the LDAP server required attributes.

   For every object and attribute selected in the filter, the Mapping policy must have a corresponding entry unless the class or attribute names are the same in both directories. Before mapping an attribute, verify that a corresponding attribute actually exists in the target directory.

4.2.2 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 eDirectory 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 an eDirectory™ 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 telenumber attributes to telenumber 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 on 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.

To configure the Schema Mapping policy:

1. In iManager, click *Identity Manager* > *Identity Manager Overview*.
2. Locate the driver in its driver set.
3. Click the driver to open the Identity Manager Driver Overview page.
4. Click the schema mapping icon on the Publisher or Subscriber channel.
5. Edit the policy as appropriate for your setup.

4.2.3 Defining Object Placement in Netscape

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) will be 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 4-2 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>
```

Configuring Placement Policies

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.

4.2.4 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 attribute Equivalent To Me in the eDirectory Group. The attribute Equivalent To Me must be included in the Publisher filter. The attribute Equivalent To Me 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.

4.3 Configuring SSL Connections

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.

- "Step 1: Generating a Server Certificate" on page 41
- "Step 2: Sending the Certificate Request" on page 42
- "Step 3: Installing the Certificate" on page 42
- "Step 4: Activating SSL in Netscape Directory Server 4.12" on page 43
- "Step 5: Exporting the Trusted Root from the eDirectory Tree" on page 43
- "Step 6: Importing the Trusted Root Certificate" on page 43
- "Step 7: Adjusting Driver Settings" on page 44

If you are using another LDAP server, the procedure is similar.

4.3.1 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.

4.3.2 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.

4.3.3 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*.

4.3.4 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. Enter 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, select *Allow Client Authentication*.
4. Click *Save*.
5. Click *Tasks*, then restart the server for the changes to take effect.

4.3.5 Step 5: Exporting the Trusted Root from the eDirectory 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, type in a filename (for example, `PublicKeyCert`), then select *Base64* as the format.
8. Click *Export*.

4.3.6 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.

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* > C*ertificate 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*.

Importing into the Client's Certificate Store

You need to import the trusted root certificate into a certificate store (also called a key store) 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, type 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.

4.3.7 Step 7: Adjusting Driver Settings

The following table lists the driver’s settings and its default values in the sample configurations.

Table 4-3 *Driver Settings and Default Values*

Parameter	Sample Configuration Value	Description
Use SSL for LDAP Connections	no	The value for this parameter should be either Yes or No. It indicates whether or not SSL connections should be used when communicating with the LDAP server. To use SSL, you must also correctly configure the LDAP server. For more information, refer to "Configuring SSL Connections" on page 41,
SSL Port	636	This parameter is ignored unless Use SSL for LDAP Connections is set to Yes. It indicates which port the LDAP server uses for secure connections.
Keystore Path (for SSL Certs)	[blank]	When Use SSL for LDAP Connections is set to Yes, this parameter value should be the complete path to the keystore file that contains the trusted root certificate of the Certificate Authority (CA) that signed the server certificate. For more information about creating the keystore file, refer to "Importing into the Client's Certificate Store" on page 44".

Troubleshooting

5

5.1 Migrating Users into an Identity Vault

Some LDAP servers have settings that limit the number of entries that can be returned by an LDAP query. For example, iPlanet Directory Server 5.1 has a default limit of 2000 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 otherwise.

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

1. Go to the *Configuration* tab, then select *Database* settings.
2. Raise the look-through limit on the LDBM plug-in tab from 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 and raise the Size limit according to the number of user accounts you need to migrate.

   This is the actual number of records the query is allowed to return.

   After these settings have been adjusted, the migration should complete correctly.

5.2 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).

5.3 LDAP v3 Compatibility

The LDAP Driver for Identity Manager works with most LDAP v3 compatible LDAP servers. The driver is written to the RFC 2251 specification for LDAP. 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 nor worked around is the RFC 2251 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 for Identity Manager.

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

5.4 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 had a choice between using the LDAP-search method or the changelog method, should I use the LDAP Search method?

Answer: The changelog method has performance advantages. Use it. The changelog method is the preferred method.

Documentation Updates

A

This section contains new or updated information on the Identity Manager Driver for LDAP.

The documentation is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the documentation changes listed in this section.

If you need to know whether a copy of the PDF documentation you are using is the most recent, check the date that the PDF file was published. The date is in the Legal Notices section, which immediately follows the title page.

New or updated documentation was published on the following dates:

- Section A.1, "May 25, 2006," on page 49
- Section A.2, "August 10, 2006," on page 50
- Section A.3, "September 8, 2006," on page 50
- Section A.4, "October 19, 2006," on page 50
- Section A.5, "December 7, 2006," on page 50

A.1 May 25, 2006

Table A-1 *Changes Made on May 8, 2006*

Location	Change
Section 1.1, "What's New?," on page 9	Added two items to this topic.
Section 3.1, "Planning Considerations," on page 17	Added a paragraph concerning LDAP v3 compatibility issues and the RFC 2251 specification.
Section 4.1, "Controlling Data Flow from the LDAP Directory to an Identity Vault," on page 31	Reorganized this section so the changelog and LDAP-search methods are easier to implement.
"LDAP Subscriber Settings" on page 32	Added information on the new Subscriber parameter.
"Search Results to Synchronize on First Startup" on page 37	Added information on this new Publisher parameter.
Section 5.3, "LDAP v3 Compatibility," on page 48	Added this section.
Section 5.4, "Frequently Asked Questions," on page 48	Added this section.

A.2 August 10, 2006

Updated cross-references to the Identity Manager 3.0.1 documentation set.

A.3 September 8, 2006

Deleted the "Planned Updates" topic.

A.4 October 19, 2006

Table A-2 *Updates as of May 30, 2006*

Location	Change
Section 1.3, "Driver Overview," on page 10	Updated the list of servers that use the changelog method. Added OpenLDAP to the list of servers that use the LDAP-search method.

A.5 December 7, 2006

Added a warning about potential data loss to Section 4.1.5, "LDAP Publisher Settings: Only the LDAP-Search Method," on page 36.