Novell DirXML® Driver for LDAP

1.7

www.novell.com

IMPLEMENTATION GUIDE

August 3, 2004

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.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Copyright © 2002-2004 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.

U.S. Patent Nos. 5,349,642; 5,608,903; 5,671,414; 5,677,851; 5,758,344; 5,784,560; 5,818,936; 5,828,882; 5,832,275; 5,832,483; 5,832,487; 5,870,561; 5,870,739; 5,873,079; 5,878,415; 5,884,304; 5,919,257; 5,933,503; 5,933,826; 5,946,467; 5,956,718; 6,016,499; 6,065,017; 6,105,062; 6,105,132; 6,108,649; 6,167,393; 6,286,010; 6,308,181; 6,345,266; 6,424,976; 6,516,325; 6,519,610; 6,539,381; 6,578,035; 6,615,350; 6,629,132. Patents Pending.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.

www.novell.com

DirXML Driver for LDAP Implementation Guide
August 3, 2004

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

Novell Trademarks

DirXML is a registered trademark of Novell, Inc. in the United States and other countries.
eDirectory is a trademark of Novell, Inc.
NetWare is a registered trademark of Novell, Inc., in the United States and other countries.
Novell is a registered trademark of Novell, Inc., in the United States and other countries.
Nsure is a trademark of Novell, Inc.
SUSE is a registered trademark of SUSE LINUX AG, a Novell company.

Third-Party Trademarks

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

Contents

About This Guide

This guide explains how to install and configure the DirXML® Driver for LDAP.

The guide contains the following sections:

Additional Documentation

For documentation on using Nsure™ Identity Manager, see the Identity Manager Documentation Web site (http://www.novell.com/documentation/lg/dirxml20).

For information on other DirXML drivers, see Driver Implementation Guides (http://www.novell.com/documentation/lg/dirxmldrivers/index.html).

Documentation Updates

For the most recent version of this document, see the DirXML Drivers Documentation Web Site (http://www.novell.com/documentation/lg/dirxmldrivers).

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.

User Comments

We want to hear your comments and suggestions about this manual and the other documentation included with Novell Identity Manager. Send e-mail to proddoc@novell.com.

1 Introducing the DirXML Driver for LDAP

This section covers the following topics:

Driver Overview

The DirXML® Driver for LDAP synchronizes data between Novell® eDirectory™ and LDAP-compliant directories. This driver runs on all platforms supported by eDirectory, including Windows*, NetWare®, Linux*, Solaris*, and AIX*. The driver can run anywhere that a DirXML server or DirXML Remote Loader is running.

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

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

- The change-log method

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

  - Netscape* Directory Server
  - iPlanet* Directory Server
  - IBM* SecureWay Directory
  - Critical Path* InJoin* Directory
  - Oracle* Internet Directory
  - LDAP version 3 compliant directories

- The LDAP-search method

  Some servers don't use the change-log mechanism. The LDAP-search method enables the LDAP driver to publish data about the LDAP server to eDirectory.

  Additional software and changes to the LDAP-compliant directory are not required.

Because of this flexible model for communicating, the driver can synchronize with LDAP-compliant directories running on platforms other than those supported by eDirectory, such as HP-UX*, OS/400, and OS/390.

New Features

Driver Features

This section provides information on new driver features.

- Instead of two sample configurations, a single sample configuration is provided that includes the option to choose between Flat placement and Mirror placement in hierarchal structures.
- An optional driver parameter has been added to let you specify preferred object classes. See "Preferred Object Classes" on page 32.
- Support for Identity Manager Password Synchronization has been added.

  The driver shim works the same way, but new policies have been added to the sample driver configuration to support Identity Manager Password Synchronization.

  You can set or modify the LDAP password using a password from Identity Manager, and you can check the LDAP password to see if it matches the Identity Manager password.

  You could also use a style sheet to manufacture a password to be sent back to Identity Manager, such as a password based on the user's last name. However, LDAP does not support providing the user's actual LDAP password to Identity Manager.

  See the description of the different scenarios for Password Synchronization in "Implementing Password Synchronization" in the *Novell Nsure Identity Manager 2 Administration Guide*.
- An LDAP-search publication method

  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 change-log mechanism, which is actually not part of the LDAP standard. Where change logs haven't existed, the LDAP driver has been unable to publish data about these LDAP servers to eDirectory.

  The new 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 change-log publication method. The DirXML Driver for LDAP supports either method. However, the change-log method has performance advantages and is the preferred method when a change log is available.

Identity Manager Features

For information on new features in Nsure™ Identity Manager, see "What's New in Identity Manager 2?" in the *Novell Nsure Identity Manager 2 Administration Guide*.

Default Driver Configuration

Identity Manager fundamentals are explained in the Novell Nsure Identity Manager 2 Administration Guide. This section discusses implementations, additions, or exceptions specific to this driver.

Data Flow

Publisher and Subscriber Channels

The driver supports Publisher and Subscriber channels:

- The Publisher reads information from the LDAP directory change log or an LDAP search and submits that information to eDirectory via the DirXML engine.

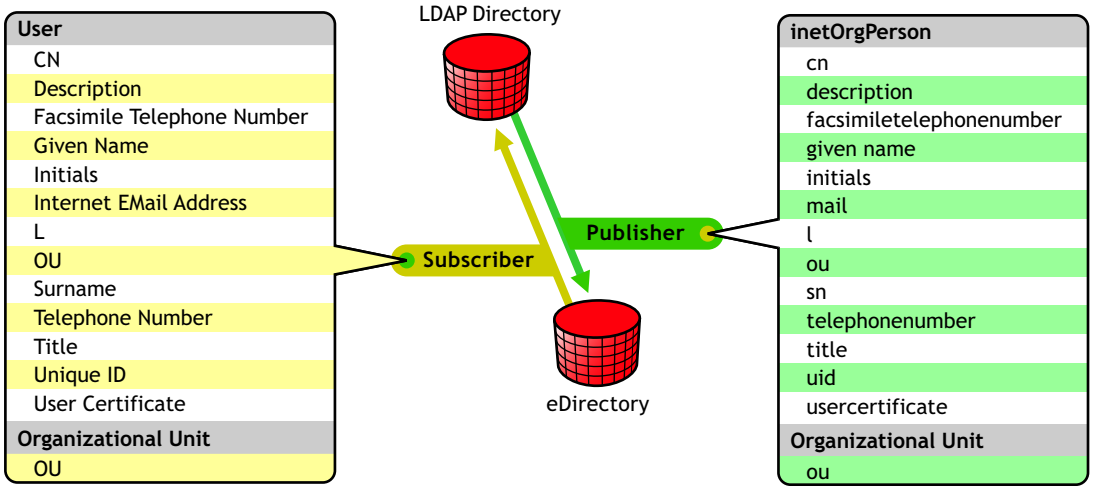
  By default, the Publisher checks the log every 20 seconds, processing up to a 1000 entries at a time, starting with the first unprocessed entry.

- The Subscriber watches for additions and modifications to eDirectory 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 LDAP Driver Filters



Policies

Policies are used to control data synchronization between the driver and eDirectory. 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 eDirectory 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 29.

Policy	Description
Mapping	Maps the eDirectory User object and selected properties to an LDAP inetOrgPerson. Maps the eDirectory 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 eDirectory, 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 eDirectory 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 eDirectory container that mirrors the object's LDAP container.
Matching	Specifies that a user object in eDirectory 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.
Subscriber Placement	If you choose the Flat placement option during the import of the driver configuration, new User objects created in eDirectory 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 eDirectory are placed in the LDAP directory container that mirrors the object's eDirectory container.

2 Installing the LDAP Driver

This section provides information on the following:

- “Planning Considerations” on page 13
- “System Prerequisites” on page 14
- “Installation” on page 14

Planning Considerations

This section provides information on the following:

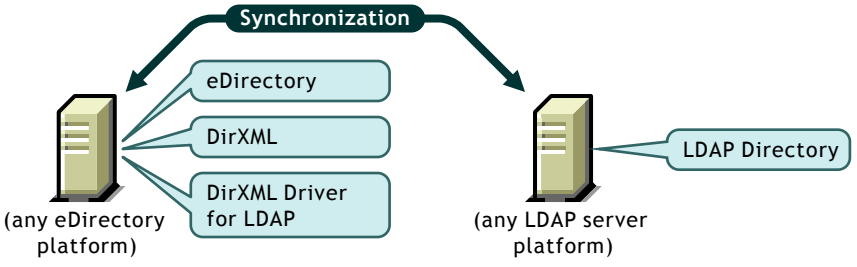
- “Where to Install the LDAP Driver” on page 13
- “Information to Gather” on page 14
- “Assumptions about the LDAP Data Source” on page 14

Where to Install the LDAP Driver

A DirXML® driver can be installed on the same computer where Novell® eDirectory™ and the DirXML 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 eDirectory and the DirXML engine are installed, as shown in the following figure:

Figure 2 A Local Configuration



If platform or policy constraints make a local configuration difficult, a DirXML 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 this driver

- Can run on any eDirectory platform.
- Communicates with the LDAP server on any platform across the wire via the LDAP protocol.

Information to Gather

During installation and setup, you'll be prompted for the information such as the following.

- Whether to use the Flat or Mirror option for synchronizing hierarchical structure. See "Policies" on page 11.
- The eDirectory and LDAP directory containers that you want to hold synchronized objects.
- The eDirectory 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 Driver" on page 22.

Assumptions about the LDAP Data Source

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

- The change-log 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

  Because not all LDAP servers use change logs, this method enables the LDAP driver to publish data about the LDAP server to eDirectory.

System Prerequisites

- ❑ Novell Nsure™ Identity Manager or later
- ❑ The system requirements of Identity Manager or later
- ❑ If you are using the change-log 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
  - SunOne 5.2
  - LDAP version 3 compliant directories

Installation

This section provides information on the following:

- "Installing the LDAP Driver" on page 15
- "Setting Up the Driver" on page 21

Installing the LDAP Driver

You can install the DirXML Driver for LDAP (along with other DirXML drivers) at the same time that the DirXML engine is installed. See "Installation" in the *Novell Nsure Identity Manager 2 Administration Guide*.

As the following sections explain, you can also install the driver separately, after the DirXML engine is installed.

Installing on Windows

Install the DirXML 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.

   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 DirXML Overview dialog box, review information, then click Next.

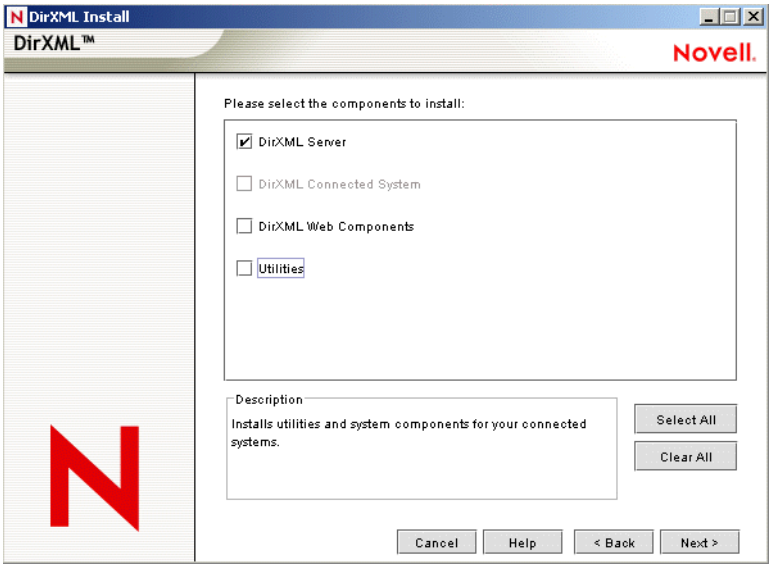
   The dialog box provides information on the following:

   - A DirXML server
   - A DirXML connected server system
4. In the second DirXML Overview dialog box, review information, then click Next.

   The dialog box provides information on the following:

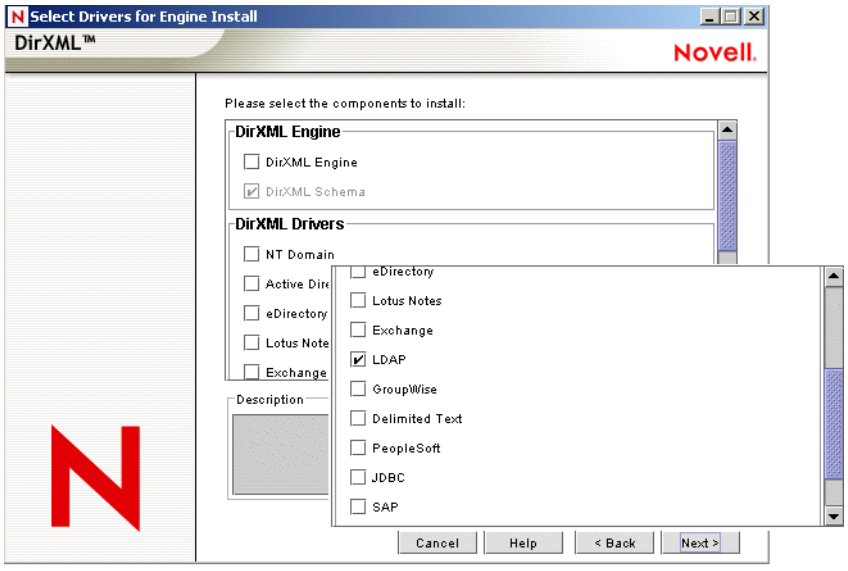
   - A Web-based administration server
   - DirXML utilities
5. In the Please Select the Components to Install dialog box, select only DirXML Server, then click Next.

Figure 3 The DirXML Server check box



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

Figure 4 The LDAP check box



You can't deselect DirXML Schema, which is dimmed. Later, the installation program will extend the schema to enable the newly installed driver to function.

7 In the DirXML 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 21.

Installing on NetWare

1 At the NetWare® server, insert the Identity Manager 2.0 CD and mount the CD as a volume.

To mount the CD, enter `m cdrom`.

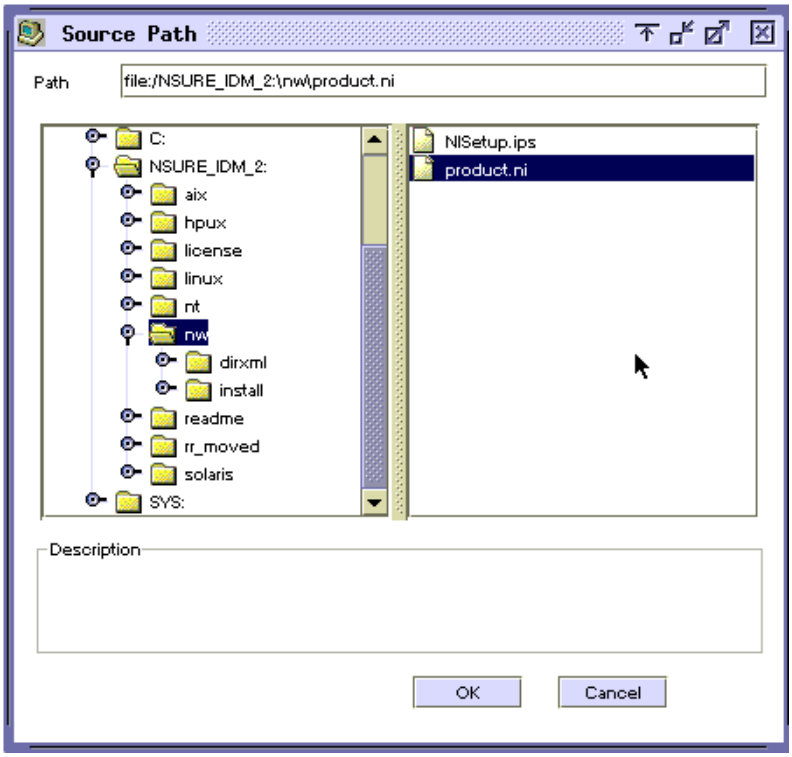
2 (Conditional) If the graphical utility isn't loaded, load it by entering `startx`.

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.

Figure 5 The Source Path dialog box



5a Browse to and expand the CD volume (NSURE_IDM_2) 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 DirXML Install dialog box, select only DirXML Server, then click Next.

Deselect the following:

- DirXML Web Components
- Utilities

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

Deselect the following:

- DirXML Engine
- All drivers except LDAP

9 In the DirXML Upgrade Warning dialog box, click OK.

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

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

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

12 Click Close.

After installation you must configure the driver as explained in "Setting Up the Driver" on page 21.

By default, the DirXML Driver for LDAP is installed when you install the DirXML engine. In case the driver wasn't installed at that time, this section can help you install it.

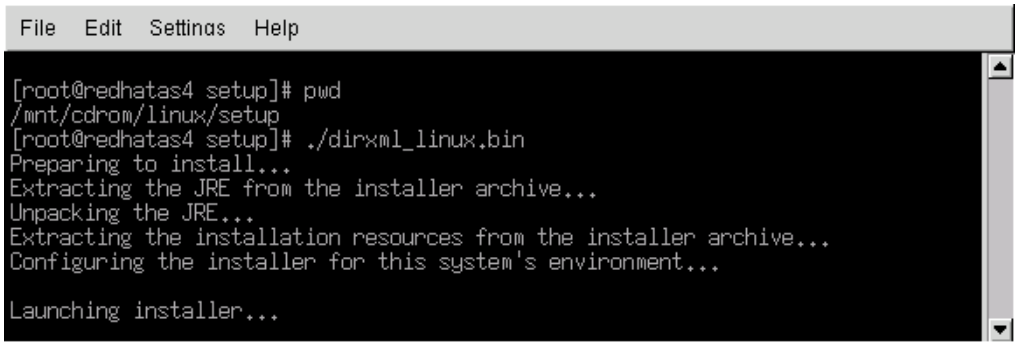
As you move through the installation program, you can return to a previous section (screen) by entering `previous`.

1. In a terminal session, log in as root.
2. Insert the Identity Manager 2.0 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/nsure_idm_2/setup/
AIX	/media/cdrom/aix/setup/

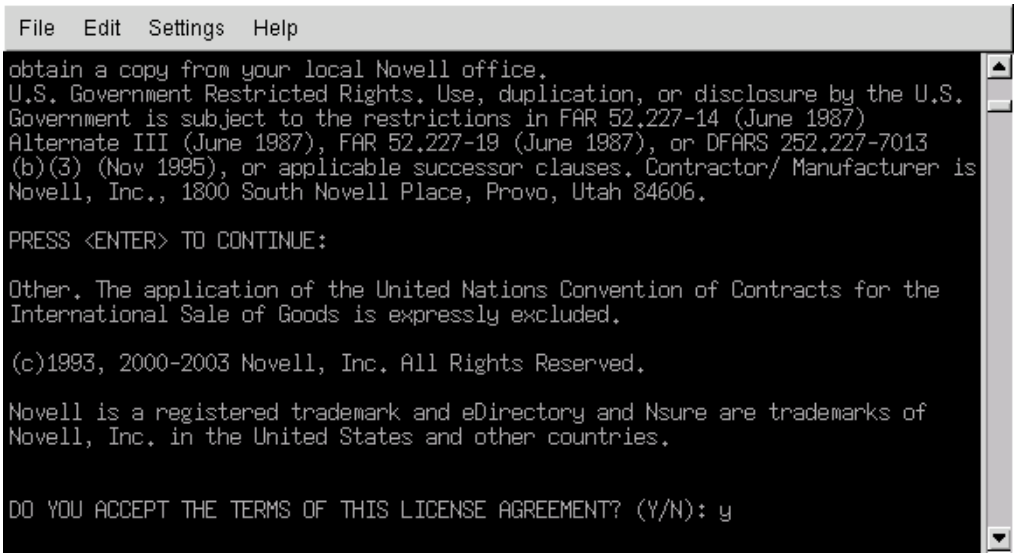
Figure 6 The Linux path to the installation program



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.

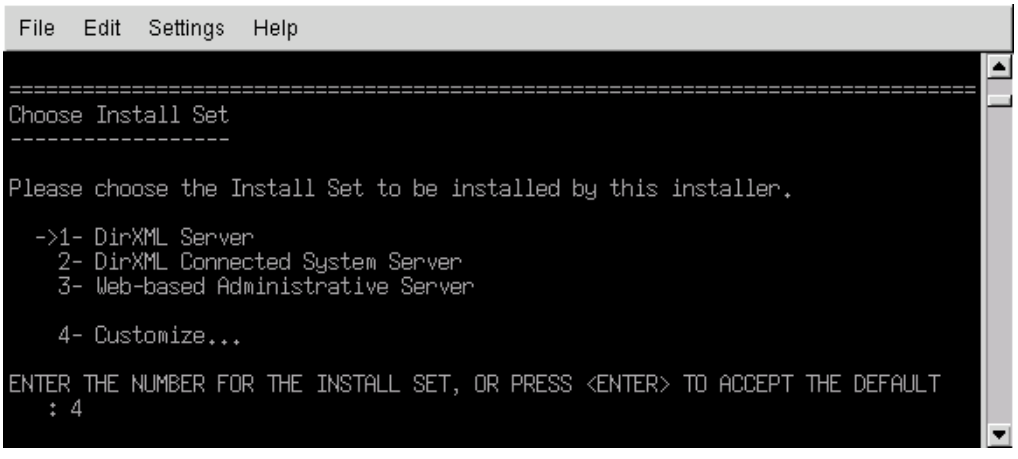
Figure 7 The prompt to accept the license agreement



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

Type 4, then press Enter.

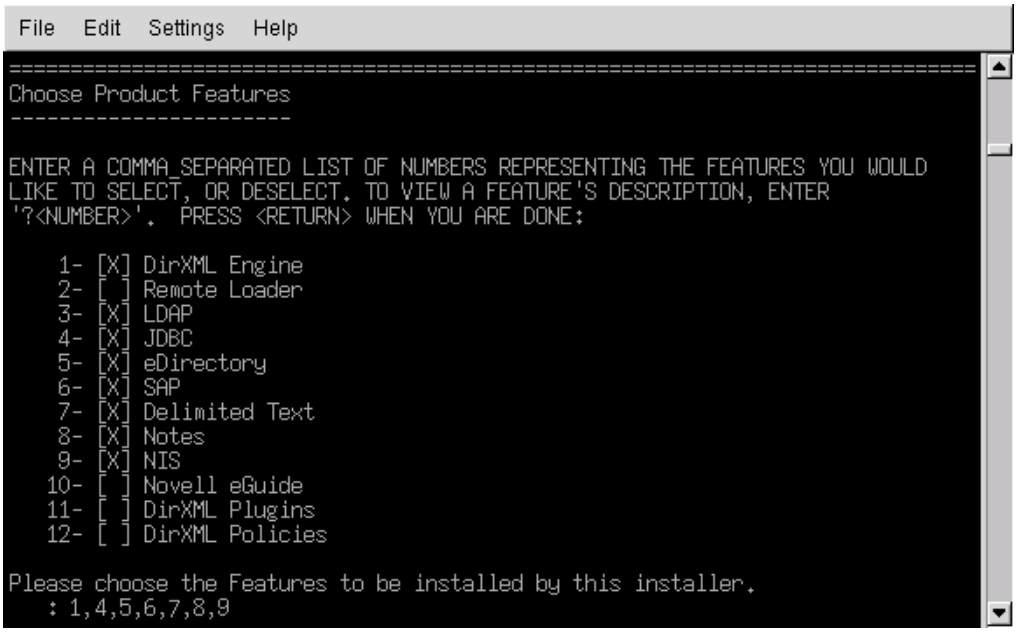
Figure 8 The prompt to select the Customize option



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

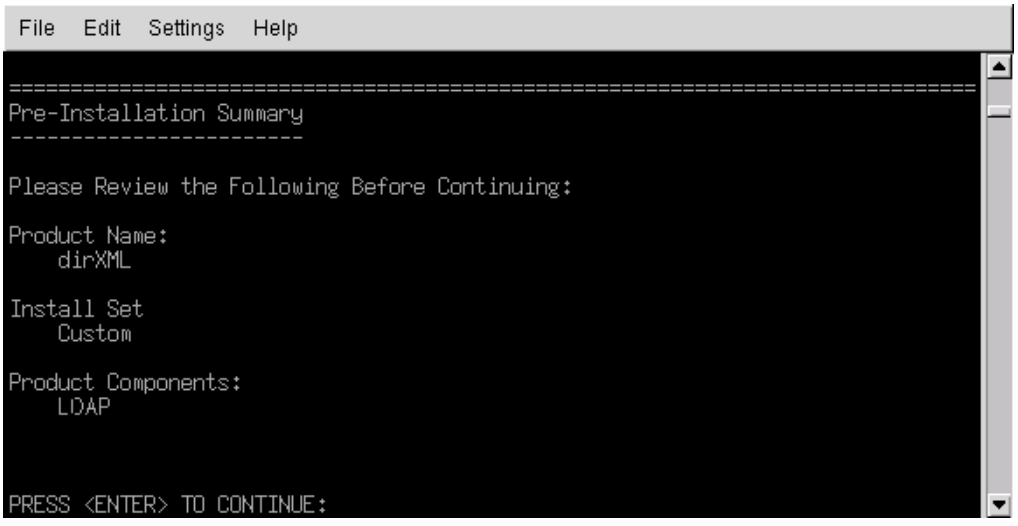
To deselect a feature, type its number. Type a comma between additional features that you deselect.

Figure 9 Options in the Choose Product Features section



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

Figure 10 The Pre-Installation Summary section



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 21.

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, you should complete the setup tasks in the following sections:

- “Preparing the LDAP Server” on page 21
- “Importing the Driver” on page 22
- “Starting the Driver” on page 24
- “Migrating and Resynchronizing Data” on page 24
- “Activating the Driver” on page 25

Preparing the LDAP Server

If you use the driver only to synchronize data from eDirectory 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 eDirectory (on a Publisher channel), and if you plan to use the change-log 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 change-log mechanism, plan to 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 change-log publication method, the driver attempts to prevent loopback situations where an event that occurs on the Subscriber channel gets sent back to the DirXML engine on the Publisher channel. However, the LDAP-search method relies on the DirXML engine to prevent loopback.

With the change-log 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 eDirectory or not.

In that case, all changes found in the change log are sent by the Publisher to the DirXML engine, and the Optimize/Modify discards unneccessary 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 eDirectory. The LDAP directories supported by this driver support the change-log 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 Driver

Import the LDAP driver configuration by following the instructions to import a driver in “Creating and Configuring a Driver ”.

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

Field	Description
Driver Name	The eDirectory 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 eDirectory 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 eDirectory container that mirrors the object's LDAP container.
eDirectory Container	The container in eDirectory 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.
Administrator DN	Enter the LDAP DN of the administrator account created for the LDAP driver.
Administrator 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 21.
Configure Data Flow	◆ Bi-directional means that both LDAP and eDirectory are authoritative sources of the data synchronized between them. ◆ LDAP to eDirectory means that LDAP is the authoritative source. ◆ eDirectory to LDAP means that eDirectory is the authoritative source.
Enable Role-Based Entitlements	Choose Yes or No. Because this is a design decision, you should understand Role-Based Entitlements before choosing to use it. For information about Role-Based Entitlements, see "Using Role-Based Entitlements" in the Novell Nsure Identity Manager 2 Administration Guide.
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	Enter 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.

Field	Description
Driver Password	The Remote Loader uses the driver object password to authenticate itself to the DirXML server. The driver object password must be the same password that is specified as the driver object password on the DirXML Remote Loader.
Remote Password	This password is used only in the Remote Loader configuration. It allows the Remote Loader to authenticate to the DirXML 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 DirXML Remote Loader.

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 DirXML Management > 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 24.

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 eDirectory to an LDAP server. When you migrate an object, the DirXML engine applies all of the Matching, Placement, and Create policies, as well as the Subscriber filter, to the object.

  NOTE: When migrating data from eDirectory into the LDAP directory, you might need to change your LDAP server settings to allow migration of large numbers of objects. See "Migrating Users into eDirectory" on page 43.

- **Migrate Data into eDirectory:** Allows you to define the criteria that Identity Manager uses to migrate objects from an LDAP server into Novell eDirectory. When you migrate an object, the DirXML engine applies all of the Matching, Placement, and Create policies, as well as the Publisher filter, to the object. Objects are migrated into eDirectory 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 DirXML Management > Overview.
2. Locate the driver set that contains the DirXML 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, refer to "Activating Novell Identity Manager Products" in the *Novell Nsure Identity Manager 2 Administration Guide*.

3 Upgrading

This section provides information on the following:

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 DirXML engine, or you can do it after the engine is installed. See Chapter 2, "Installing the LDAP Driver," on page 13.

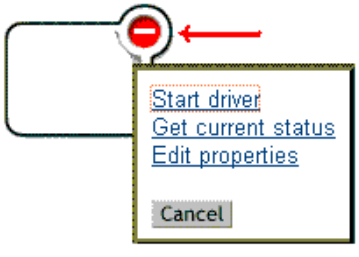
3. After the shim is installed, restart the driver.

   3a. In iManager, select DirXML Management > 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.

Figure 11 The Icon for the Driver's Drop-Down List



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

For information on activation, see "Activating Novell Identity Manager Products" in the *Novell Nsure Identity Manager 2 Administration Guide*.

After you install the driver shim, upgrade the driver configuration. See "Upgrading the Driver Configuration" on page 28.

Upgrading the Driver Configuration

Installing the driver shim does not change your existing configuration. Your existing configuration will continue 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.x to Identity Manager Format" in the *Novell Nsure Identity Manager 2 Administration Guide*.
- To add Identity Manager Password Synchronization functionality to an existing driver configuration, see "Upgrading Existing Driver Configurations to Support Identity Manager Password Synchronization" the *Novell Nsure Identity Manager 2 Administration Guide*.

4 Customizing the LDAP Driver

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

This section provides information on the following:

- “Configuring the Driver Parameters” on page 29
- “Configuring Data Synchronization” on page 34
- “Configuring SSL Connections” on page 37

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.

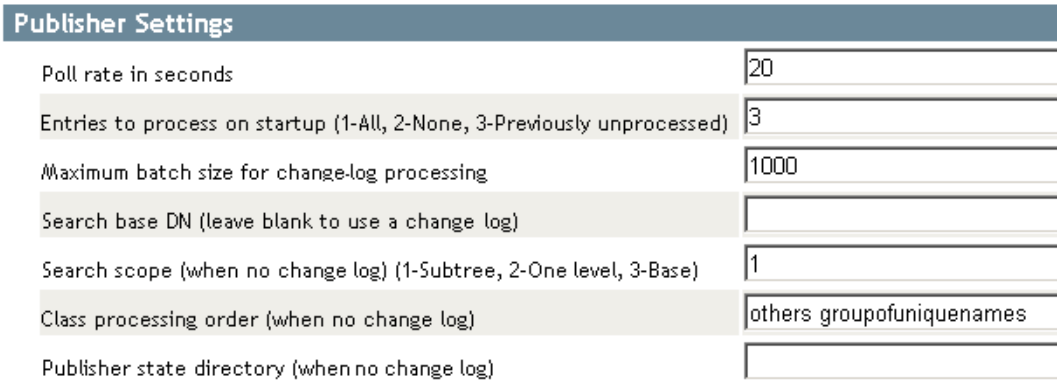
Configuring the Driver Parameters

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 polling interval to be shorter than your synchronization needs require. Making the interval longer could improve network performance while still maintaining appropriate synchronization.

Controlling Data Flow from the LDAP Directory to eDirectory (Publisher Settings)

Use the Publisher channel settings to control the following aspects of data exchange. The following figure illustrates settings in the sample configuration file.

Figure 12 Options for Publisher Settings



You can set two advanced settings by using the Edit DirXML option:

- Prevent Loopback
- Preferred Object Classes

Some settings apply only to the change-log publication method, other settings apply only to the LDAP-search publication method, and some settings apply to both the change-log and LDAP-search publication methods.

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

Publisher Settings for Only the Change-Log Method

Maximum Batch Size for Change-Log Processing

When the Publisher processes new entries from the LDAP change log, it asks for them 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.

Prevent Loopback

The Prevent Loopback parameter is used only with the change-log publication method. The LDAP-search method doesn't prevent loopback, other than the loopback prevention built into the DirXML engine.

Because you seldom need to change the default behavior, this advanced parameter isn't present in the sample configuration. You set the parameter by using Edit DirXML.

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.

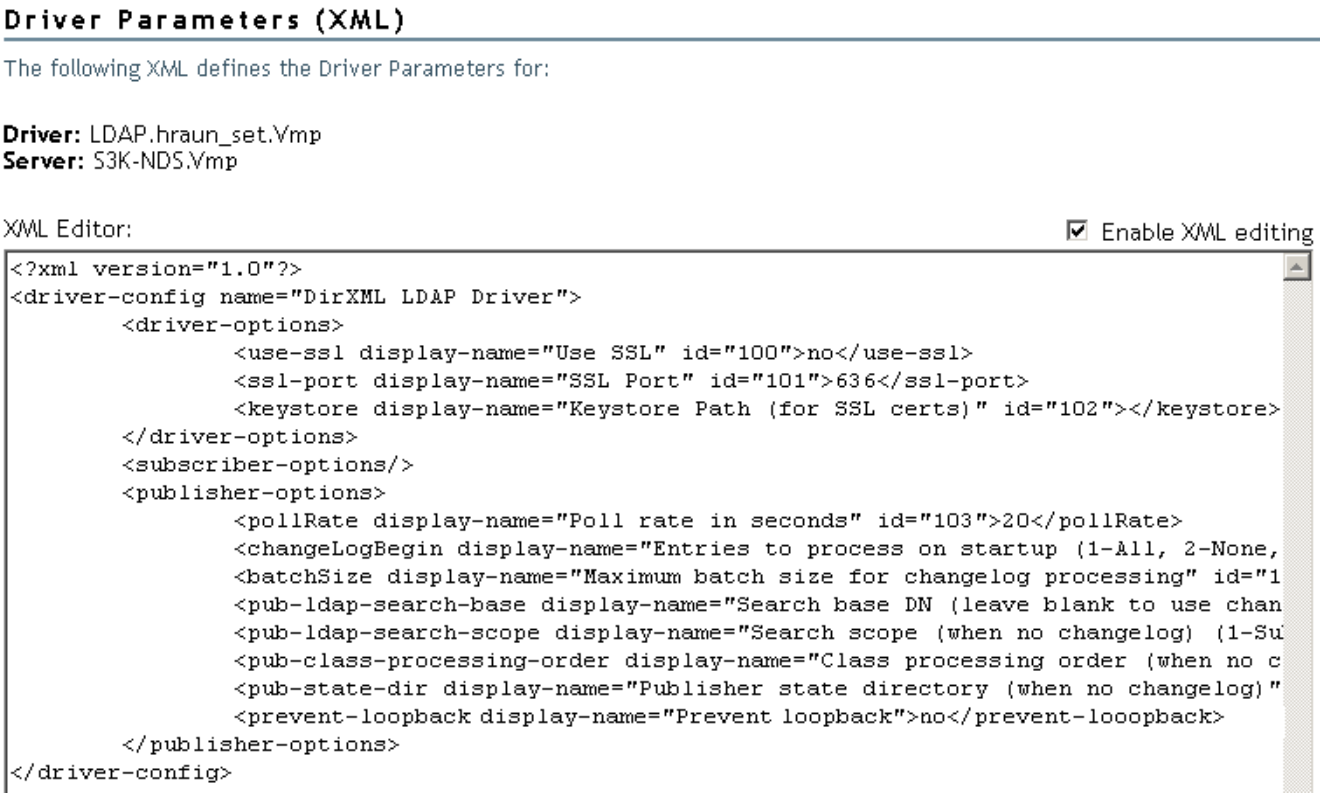
As an example scenario, you might not have a Subscriber channel configured for this driver but you want to be able to use the same DN and password as other processes use to make changes.

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

1. In iManager, click DirXML Management > 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 Driver Configuration parameters section, then click Edit XML.
5. In the Driver Parameters (XML) section, click Enable XML Editing, find the line that contains </publisher-options>, then add the following line immediately above it:

   ```
   <prevent-loopback display-name="Prevent loopback">no</prevent-loopback>
   ```

Figure 13 The Driver Parameters (XML) Section



6 Click OK, click Apply, then restart the driver for this parameter to function.

Publisher Settings for Only the LDAP-Search Method

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 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 DirXML 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.

Publisher State Directory

A required parameter when you use the LDAP-search method. 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. These files help

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

Publisher Settings for Both the Change-Log and LDAP-Search Methods

Poll Rate in Seconds

This is 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 Novell® eDirectory™.

The recommended polling rate is 120 seconds.

Entries to Process on Startup

This parameter specifies which entries to process on startup.

- 1-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.
- 2-None: When the driver starts running, the Publisher doesn’t process any previously existing entries. It processes new changes according to the poll rate.
- 3- 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.

Preferred Object Classes

Preferred Object Classes is an optional driver parameter that lets you specify preferred object classes on the Publisher channel. You set this parameter by using the Edit DirXML option.

Nsure™ Identity Manager requires that objects be identified using a single object class. However, many LDAP servers and applications can list multiple object classes for a single object. By default, when the DirXML 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 DirXML 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 DirXML 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.

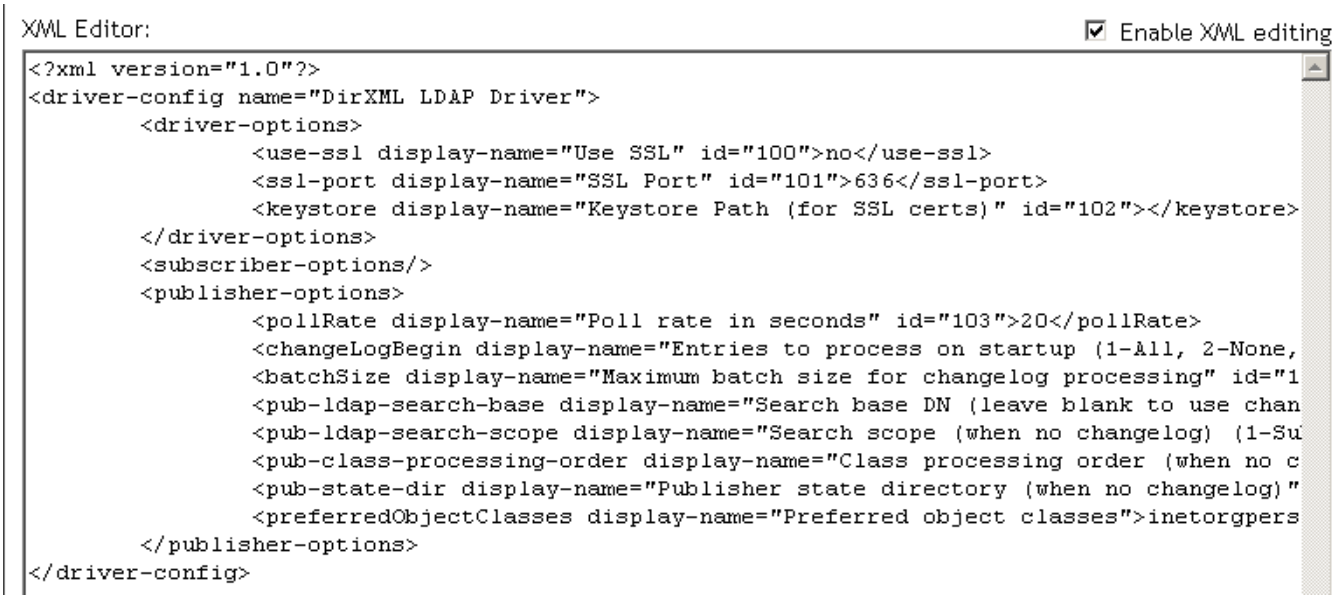
When this parameter is present, the DirXML Driver for LDAP examines each object being presented on the Publisher channel to see if it contains one of the object classes in the list. It looks for them in the order they appear in the preferredObjectClasses parameter. If it finds that one of the listed 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 DirXML engine. If none of the object classes match, it resorts to its default behavior for reporting the primary object class.

To add the optional Preferred Object Classes parameter:

1. In iManager, navigate to the DirXML Driver Overview page for the LDAP driver.
2. Click the LDAP driver icon to access the Modify Object page for that driver.
3. Scroll to the Driver Parameters section, then click Edit XML.
4. On the Driver Parameters (XML) page, select the Enable XML Editing check box.
5. Below the <publisher-options> open tag (but before the closing tag), insert the following XML element. Replace the example of inetorgperson with your list of preferred object classes, separating the names with spaces.

   ```
   <preferredObjectClasses display-name="Preferred object
   classes">inetorgperson</preferredObjectClasses>
   ```

Figure 14 The Publisher-Options XML Tags



6. To save and close the Driver Parameters (XML) page, click OK.
7. To save and close the Modify Object page for the driver, click OK.
8. If the driver was running, restart it.

Configuring Data Synchronization

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, click DirXML Management > Overview.
2. Locate the driver in its driver set.
3. Click the driver to open the Driver Overview Page.
4. Click the Publisher or Subscriber Filter icon and make the appropriate changes.

   The Publisher filter must include the eDirectory 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.

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 eDirectory 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 multi-valued 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 eDirectory 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**. 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 DirXML Management > Overview.
2. Locate the driver in its driver set.
3. Click the driver to open the Driver Overview page.
4. Click the schema mapping icon on the Publisher or Subscriber channel.
5. Edit the policy as appropriate for your setup.

Defining Object Placement

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 will also contain 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:

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 example below 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 Subscriber Placement policy below 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 DirXML Management > Overview.
2. Locate the driver in its driver set.
3. Open the Driver Overview Page by clicking the driver.
4. Click the Publisher or Subscriber Placement policy icon, then make the appropriate changes.

Working with eDirectory Groups

Because group attributes are different in eDirectory 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.

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.

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

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 eDirectory.

To generate a certificate request:

1. In the navigation tree in Netscape Console, select the server 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.

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.

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 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.

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.

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. Click the Certificates tab.
4. Click Export.
5. Click No at the prompt that says "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.

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 eDirectory's CA, the trust database needs to be configured to trust the eDirectory 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.

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 eDirectory files.

4 In iManager, click DirXML Management, click Overview, then search for drivers.

5 Click the LDAP Driver object, then click it again in the next page that appears.

6 In the Keystore Path parameter, enter the complete path to the .keystore file.

Step 7: Adjusting Driver Settings

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

Parameter	Sample Configuration Value
Use SSL for LDAP Connections	no
SSL Port	636
Keystore Path (for SSL Certs)	[blank]

Use SSL for LDAP Connections

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 37.

SSL Port

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)

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 40.

5 Troubleshooting

This section contains troubleshooting tips.

Migrating Users into eDirectory

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 Novell® eDirectory™, 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 DirXML® 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.

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.

See TID 10062098 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10062098.htm).

A Updates

This section contains new or updated information on the DirXML® 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:

April 14, 2004

The following updates were made in this section:

- References to Password Synchronization 2.0 have been changed to Nsure™ Identity Manager Password Synchronization. This change indicates that the new Password Synchronization functionality is not a separate product, but is a feature of Identity Manager.
- References to DirXML 2.0 have been changed to Identity Manager 2. The engine and drivers are still referred to as the DirXML engine and DirXML drivers.

June 22, 2004

The following updates were made in this section:

Location	Change
"Installation" on page 14	Provided steps and graphics for various installs.
Chapter 4, "Customizing the LDAP Driver," on page 29	Added information on the LDAP-search publication method.

August 3, 2004

The following updates were made in this section:

Location	Change
“OutOfMemoryError” on page 43	Added the topic, in case the driver running in LDAP-Search mode runs out of memory and shuts down.