Novell DirXML® Driver for eDirectory™

2.0

www.novell.com

IMPLEMENTATION GUIDE

May 8, 2006

Novell®

Legal Notices

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

www.novell.com

DirXML Driver for eDirectory Implementation Guide

May 4, 2006

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

Novell Trademarks

ConsoleOne is a registered trademark of Novell, Inc. in the United States or other countries.
eDirectory is a trademark of Novell, Inc.
DirXML is a registered trademark of Novell, Inc. in the United States and other countries.
NMAS is a trademark of Novell, Inc.
NDS is a registered trademark of Novell, Inc., in the United States and other countries.
NetWare is a registered trademark of Novell, Inc., in the United States and other countries.
Novell Certificate Server is a trademark of Novell, Inc.
Novell is a registered trademark of Novell, Inc., in the United States and other countries.
Nsure is a trademark of Novell, Inc.

Third-Party Materials

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 eDirectory™.

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 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 Identity Manager. Send e-mail to proddoc@novell.com.

1 Overview

Driver Overview

The DirXML® Driver for eDirectory™ is designed to synchronize objects and attributes between different eDirectory trees (both internal or external trees).

This driver is unique among all other DirXML drivers. Because you are synchronizing data between eDirectory trees, you will always have two drivers installed, each in its own tree. The driver in one tree communicates with the driver in the other tree.

For example, the publisher channel in TreeA communicates with the subscriber in TreeB; and conversely, the publisher in TreeB communicates with the subscriber in TreeA. Therefore, the installation and configuration of the driver must be completed twice—once for the eDirectory driver in TreeA and once for the driver in TreeB.

To use the driver, you must have the Novell® Certificate Server™ running on each server that will host the driver. You must also create a Certificate Authority (CA) for SSL encrypting to work. For instructions on creating CAs and configuring the Certificate Server, refer to "Configuring Secure Identity Manager Data Transfers" on page 29.

New Features

This section provides information on new driver 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*.

- 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 Password Identity Manager Password Synchronization, including synchronizing Universal Password.

  If you are using the driver to connect to eDirectory 8.6.2, you can synchronize only the NDS® Password, as in previous releases.

  If you are using the driver to connect to eDirectory 8.7.3, you have more options to choose from. See the description of the different scenarios in "Implementing Password Synchronization" in the *Novell Nsure Identity Manager 2 Administration Guide*.

  For more instructions specific to eDirectory, see "Password Synchronization" on page 23 in this guide.

- The three options (Mirrored, Flat, and Department) for the structure to use when synchronizing users are now available in one sample configuration instead of a different sample configuration file for each. See Chapter 4, “Using the Sample Driver Configuration,” on page 21.
- You can customize the driver to support Role-Based Entitlements. Although the functionality isn’t provided in the sample configuration, you can create it by following the example of other driver configurations that support Role-Based Entitlements. See “Using Role-Based Entitlements” in the *Novell Nsure Identity Manager 2 Administration Guide*.
- You can customize the driver to provide a driver heartbeat. See “Adding Driver Heartbeat” in the *Novell Nsure Identity Manager 2 Administration Guide*.

2 Installing the Driver

Key Terms

Driver shim. A Java file (NdsToNds.jar) loaded directly by DirXML® or by the remote loader. Communicates event changes to be sent from the DirXML Driver for eDirectory™ to eDirectory, communicates changes from eDirectory to the DirXML Driver for eDirectory, and operates as the link that connects eDirectory and the eDirectory Driver object.

Driver. A set of policies, filters, and objects that act as the connector between eDirectory and the driver shim.

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

To establish a connection between the DirXML engine and eDirectory, you specify the driver's configuration and connection parameters, policies, and filter values.

Driver object. An object in eDirectory.

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

Where to Install the Driver Shim

You install Nsure Identity Manager and the eDirectory driver shim on both of the Novell® eDirectory servers and in the trees that you want to synchronize. This driver does not use the Remote Loader technology because the driver in one tree communicates directly with the driver in the other tree.

The driver uses Novell Certificate Server™ and a Certificate Authority (CA) to ensure data security. All transactions between trees will be secured through SSL technology. For information on data security, see “Configuring Secure Identity Manager Data Transfers” on page 29.

Driver Prerequisites

- ❑ Requirements for Identity Manager.

  See "Installation" in the *Novell Nsure Identity Manager 2 Administration Guide*.
- ❑ The Novell Certificate Server running on each server that hosts the eDirectory driver.
- ❑ A Certificate Authority (CA) so that SSL encrypting can work

Installing the Driver Shim

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

IMPORTANT: Because you are installing the driver on two separate eDirectory servers, you must complete procedures for each server.

You can also install the driver separately, after the DirXML engine is installed.This section assumes that you have already installed the DirXML engine (and, most likely, other drivers) on the server and need to install the eDirectory driver only.

During the installation, NdsToNds.jar is copied to the appropriate directory. The following table shows these locations per platform:

Operating System	Directory
Linux* or Solaris*	/usr/lib/dirxml/classes
NetWare®	sys:system\lib
Windows NT*/2000	novell\nds\lib

After the installation program ends, configure security as explained in "Configuring Secure Identity Manager Data Transfers" on page 29.

Installing to Windows

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:

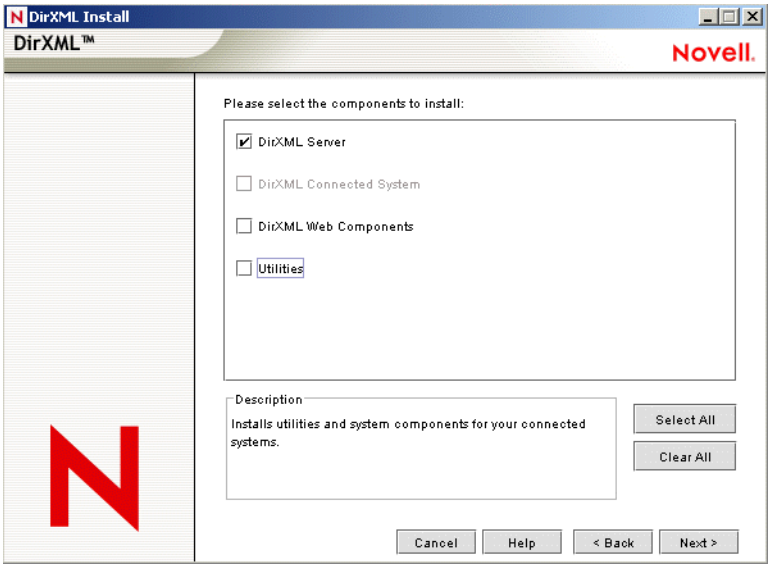
   - A DirXML server
   - A DirXML connected server system
4. In the second DirXML Overview dialog box, review information, then click Next.

   The dialog box provides information on the following:

   - A Web-based administration server
   - DirXML utilities

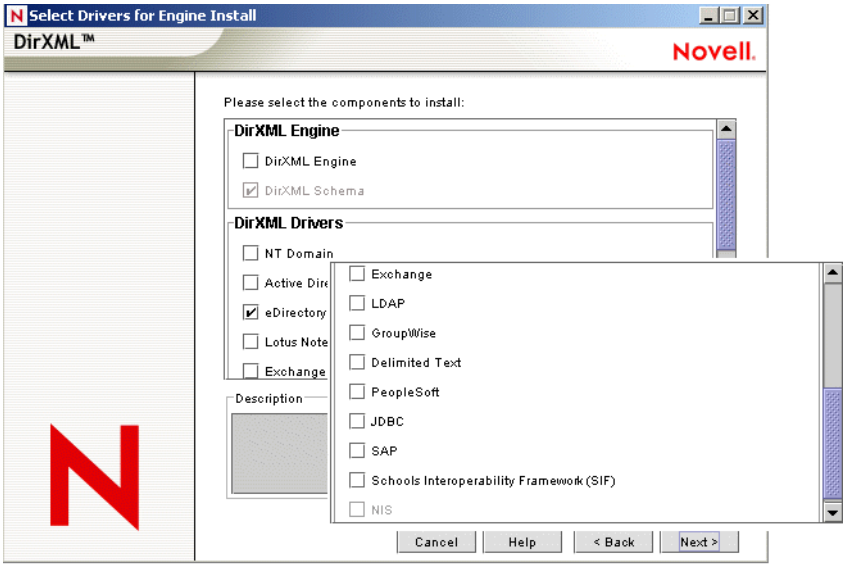
5 In the Please Select the Components to Install dialog box, select only DirXML Server, then click Next.

Figure 1 The DirXML Server check box



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

Figure 2 The Delimited Text check box



This step assumes that you have already installed the DirXML engine, during an earlier install.

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.

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 Chapter 5, “Configuring the Driver,” on page 25.

Installing to 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`**.

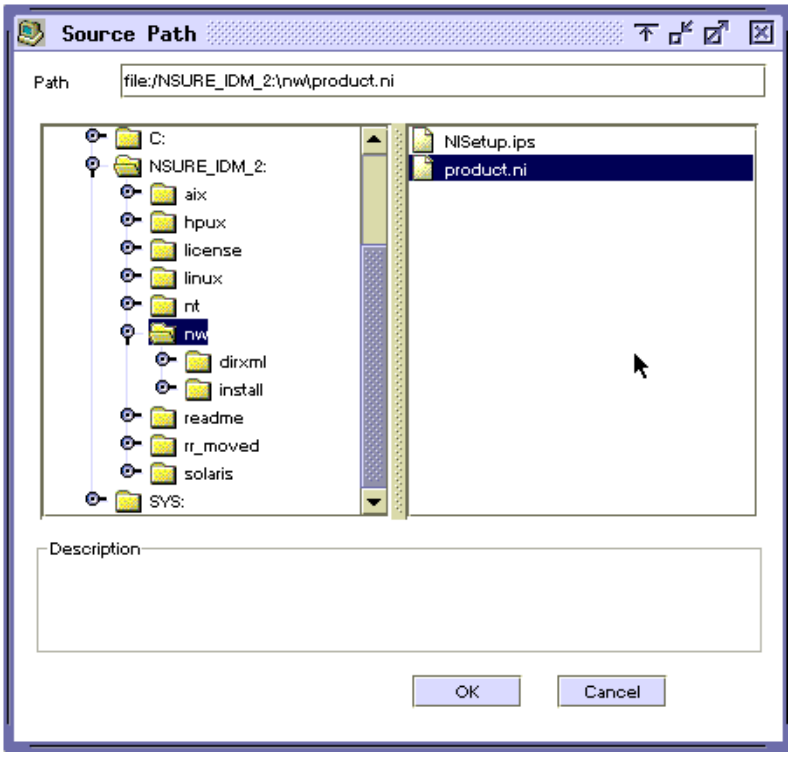
2 (Conditional) If the graphical utility isn't loaded, load it by entering **`startx`**.

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 3 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 eDirectory.

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 Chapter 5, “Configuring the Driver,” on page 25.

Installing to Linux, Solaris, or AIX

By default, the DirXML Driver for eDirectory 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.

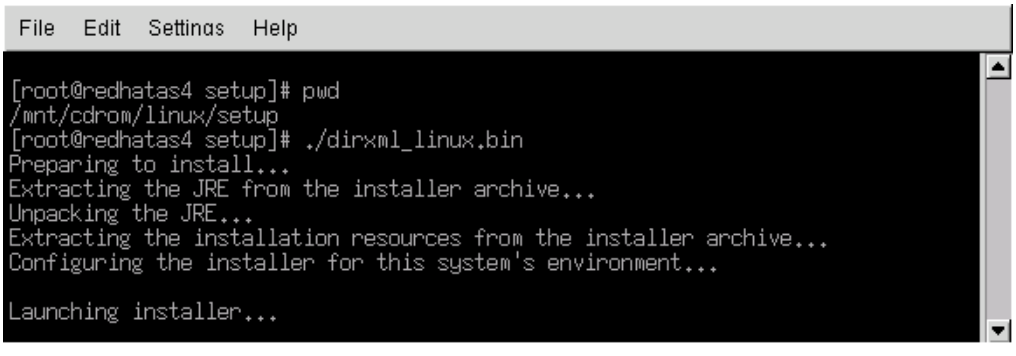
Typically, the CD is automatically mounted. To manually mount the CD:

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/

Figure 4 The Linux path to the installation program



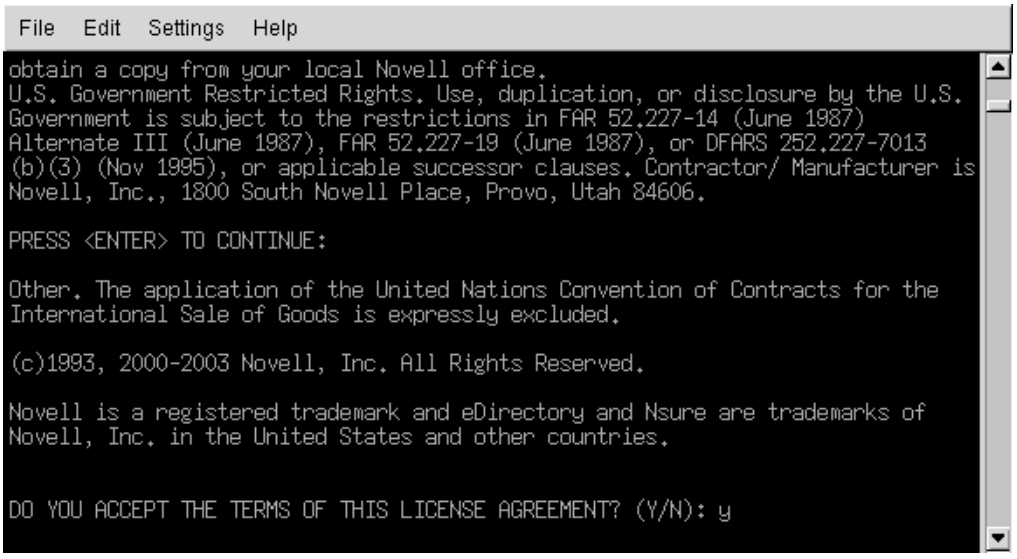
4 Run the installation program by typing **`./dirxml_linux.bin`**.

5 In the Introduction section, press Enter.

6 Accept the license agreement.

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.

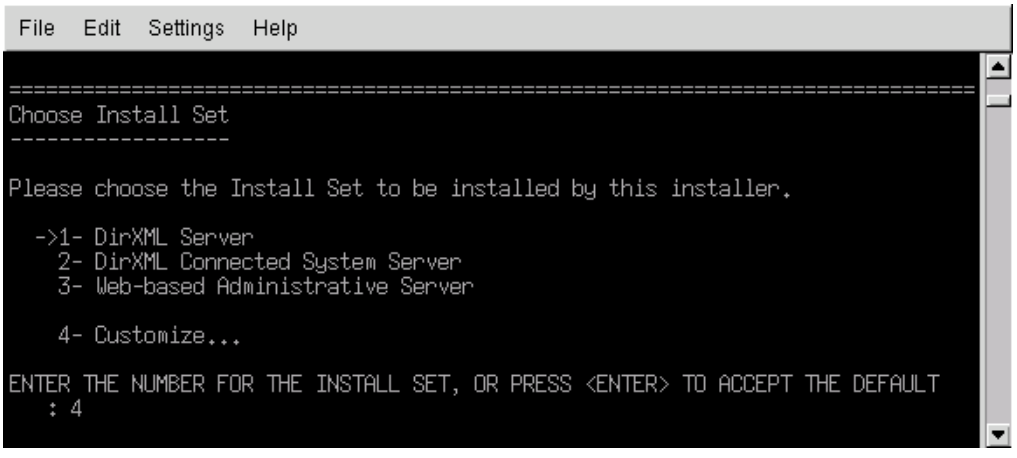
Figure 5 The prompt to accept the license agreement



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

Type 4, then press Enter.

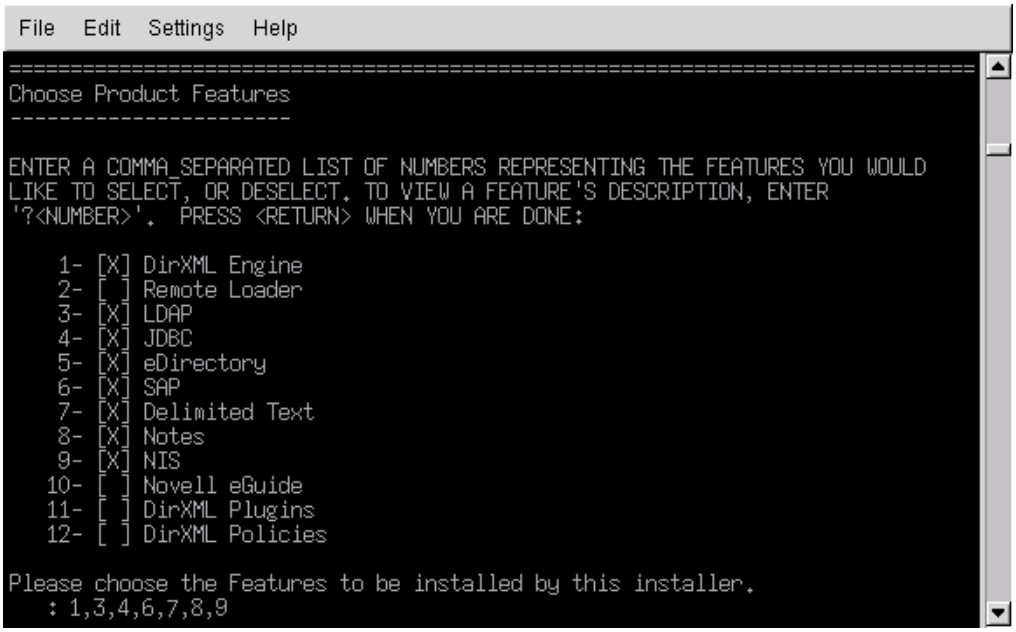
Figure 6 The prompt to select the Customize option



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

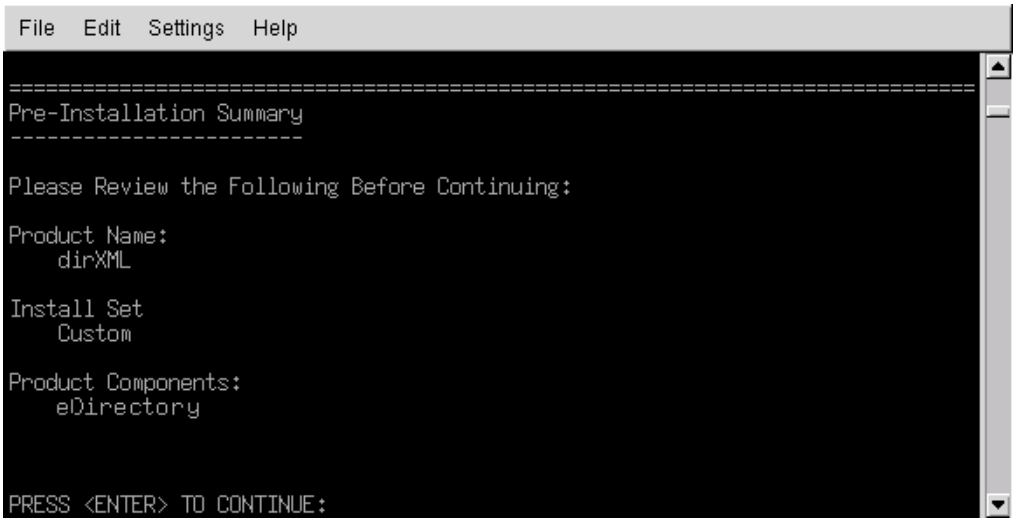
To deselect a feature, type its number. Type a comma between additional features that you deselect.

Figure 7 Options in the Choose Product Features section



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

Figure 8 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 Chapter 5, “Configuring the Driver,” on page 25.

Activating the Driver

Activate the driver within 90 days of installation. Otherwise, the driver will stop running.

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

3 Upgrading the DirXML Driver for eDirectory

Preparing to Upgrade

Make sure you have reviewed all TIDs and Product Updates for the version of the driver you are using.

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.

Upgrading the Driver Shim

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

   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 “Installing the Driver Shim” on page 12.

   When you upgrade, the new driver shim replaces the previous driver shim but keeps the previous driver’s configuration.

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 9 The driver’s status icon

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 20.

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.

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 to configuration to Identity Manager 2 format and adding policies to it.

- To replace your existing configuration, import the new sample configuration for your existing driver objects.

  The sample configuration contains all the new features, such as support for Identity Manager Password Synchronization and Role-Based Entitlements.

- To convert an existing driver configuration so that 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 *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" in *Novell Nsure Identity Manager 2 Administration Guide*.

  The new policies for password synchronization are intended to support Universal Password and Distribution Password. If you are planning to synchronize only the NDS Password, these policies should not be added to the driver configuration. NDS Password is synchronized using Public Key and Private Key attributes instead of these policies.

IMPORTANT: Because you are upgrading the driver on two separate eDirectory servers, you must complete the upgrade procedures for each server.

Upgrade Issues for the eDirectory Driver

If you are upgrading Identity Manager and the eDirectory driver, you might encounter data synchronization errors if your certificates have expired (or if one of the two certificates has expired).

If you create a user on the server that holds a valid certificate, the user won't be synchronized to the server containing the invalid certificate. Also, you might see the following error in DSTrace:

```
SSL handshake failed, X509_V_CERT_HAS_EXPIRED
```

```
SSL handshake failed, SSL_ERROR_ZERO_RETURN,
```

If you create a user on the server that holds an expired certificate, the user will still be synchronized to the server containing a valid certificate. Also, you might see the following error in DSTrace:

```
Error: 14094415: SSL Routines: SSL_READ_BYTES: sslv3 alert certificate
expired.
```

To fix this issue, create new certificates.

4 Using the Sample Driver Configuration

The driver configuration contains the following three options for synchronizing users with the Novell® DirXML® Driver for eDirectory™.

- Mirrored
- Flat
- Department

These options are like the previous version of the driver configuration, except that they are all available in a single configuration file instead of in three separate configuration files.

This section provides information on the following:

- "Importing the Sample Driver Configuration" on page 21
- "Which Attributes Are Synchronized" on page 22
- "Password Synchronization" on page 23

Importing the Sample Driver Configuration

1. Create a new driver or import the configuration onto an existing driver.

   In Novell iManager, select DirXML Utilities, then use one of the tasks as described in "Managing DirXML Drivers" in the *Novell Nsure Identity Manager 2 Administration Guide*.

2. Configure the driver by following the instructions in "Configuring Secure Identity Manager Data Transfers" on page 29.

The wizard prompts you to provide the following information:

Item	Description
Remote Tree Address and Port	Enter the DNS host name or IP address and port of the Nsure™ Identity Manager server in the remote tree. For example: 151.155.144.23:8196 hostname:8196
Configure Data Flow	**Bidirectional:** Both eDirectory trees are authoritative sources of the data synchronized between them. **Authoritative:** The local tree is the authoritative source. **Subordinate:** The local tree is not an authoritative source.

Item	Description
Configuration Option	**Mirrored:** Synchronizes objects hierarchically between the local and remote trees. If you choose this option, use the same option for configuring both eDirectory trees you are synchronizing. This option in the driver configuration synchronizes User, Group, Organization, Country, and Organizational Unit objects. It also mirrors the structure of a subtree in the other tree. **Flat:** Synchronizes all Users and Groups into specific containers. This option synchronizes User and Group objects and places all users in one container and all groups in another container. This option is typically used in conjunction with the Department option (or a similar configuration) in the other tree. This option doesn't create the containers that hold the users and groups. You must create those manually. **Department:** Synchronize Users and Groups by department (OU). This option synchronizes User and Group objects and places all users and groups in a container based on the Department field in your management console. This configuration is typically used in conjunction with the Flat option (or a similar configuration) in the other tree. This option doesn't create the containers for each department. You must create those manually. They must be the same as the container specified during import.
Remote Base Container	Used for Mirrored option only. Enter the base container for synchronization in the remote tree, for example Users.MyOrganization.
Base Container	Used for Mirrored, Flat, and Department options. Enter the base container for synchronization in the local tree, for example Users.MyOrganization. **If using with Mirrored:** The local base container to mirror with the Remote Base Container above. **If using with Flat:** The container to place Users into. **If using with Department:** The parent of the departmental containers.
Group Container	Used for Flat only. Enter the base container for synchronization in the local tree to place Groups into, for example Groups.MyOrganization.

Which Attributes Are Synchronized

The filter for the sample driver configuration synchronizes the following attributes:

accessCardNumber	Initials	preferredDeliveryMethod
ACL	instantMessagingID	preferredName

assistant	internationaliSDNNumber	Private Key
assistantPhone	Internet EMail Address	Public Key
businessCategory	jackNumber	registeredAddress
city	jobCode	roomNumber
CN	L	S
co	Language	SA
company	Mailbox ID	Security Equals
costCenter	Mailbox Location	Security Flags
costCenterDescription	mailstop	See Also
departmentNumber	manager	siteLocation
Description	managerWorkforceID	Surname
destinationIndicator	mobile	Telephone Number
directReports	NSCP:employeeNumber	teletexTerminalIdentifier
EMail Address	otherPhoneNumber	telexNumber
employeeStatus	O	Timezone
employeeType	OU	Title
Equivalent To Me	pager	tollFreePhoneNumber
Facsimile Telephone Number	personalTitle	UID
Full Name	photo	uniqueID
Generational Qualifier	Physical Delivery Office Name	vehicleInformation
Given Name	Postal Address	workforceID
Group Membership	Postal Code	x121Address
Higher Privileges	Postal Office Box	x500UniqueIdentifier

Password Synchronization

This section contains information that is specific to the DirXML Driver for eDirectory, and assumes that you are familiar with the information in "Implementing Password Synchronization" in the *Novell Nsure Identity Manager 2 Administration Guide*.

- The driver shim works the same way, but new policies have been added to the sample driver configuration to support Identity Manager Password Synchronization, including synchronizing Universal Password.
- If you are using the driver to connect to eDirectory 8.6.2, you can synchronize only the NDS Password, as in previous releases.

  If you are using the driver to connect to eDirectory 8.7.3, you have more options to choose from, including synchronizing Universal Password.

  See the description of the different scenarios in "Implementing Password Synchronization" in the *Novell Nsure Identity Manager 2 Administration Guide*.
- If you decide to enforce Password Policy in multiple trees, make sure that the Advanced Password Rules in the Password Policies are compatible in each tree, so that password synchronization can be successful.

If you enforce incompatible Password Policies in multiple eDirectory trees, and choose to set a password back if it does not comply (with the option “If password does not comply, enforce Password Policy on the connected system by resetting user's password to the Distribution Password”), you could encounter a loop in which each eDirectory server tries to change a noncompliant password.

Scenario: Encountering a Loop. To enforce incompatible Password Policies in multiple eDirectory trees, you select the option “If password does not comply, enforce Password Policy on the connected system by resetting user's password to the Distribution Password”. This option sets a password back if it does not comply with the policy. Because each eDirectory server tries to change a noncompliant password, you encounter a loop.

Information about Password Policies is in “Managing Passwords Using Password Policies” in the *Novell Nsure Identity Manager 2 Administration Guide*.

- If the filter for the driver has the setting Synchronize for the Public Key and Private Key attributes, the NDS password is synchronized between trees regardless of any other settings you have created.

  If you want to synchronize passwords using Universal Password, make sure you set the filter on both eDirectory drivers to Ignore for the Public Key and Private Key attributes for all classes that you want to synchronize Universal Password.

- To add Identity Manager Password Synchronization functionality to an existing driver configuration, see “Upgrading Existing Driver Configurations to Support Identity Manager Password Synchronization” in *Novell Nsure Identity Manager 2 Administration Guide*.

  The new policies for password synchronization are intended to support Universal Password and Distribution Password. If you are planning to synchronize only the NDS Password, these policies should not be added to the driver configuration. NDS Password is synchronized using Public Key and Private Key attributes instead of these policies.

- The Check Password Status task in iManager does not work for an eDirectory connected system if the Password Policy has Universal Password enabled and does not have the setting checked for synchronizing Universal Password with NDS Password.

  The Check Password Status task lets you see whether a user’s password in Identity Manager is synchronized with the password on connected systems.

  If you are using the DirXML Driver for eDirectory, and the Password Policy for a user specifies in the Configuration Options tab that the NDS Password should not be updated when the Universal Password is updated, then the Check Password Status task for that user always shows that the password is not synchronized. The password status is shown as not synchronized, even if the Identity Manager Distribution Password and the Universal Password on the eDirectory connected system are in fact the same.

  This is because the eDirectory check password functionality is checking the NDS Password at this time, instead of going through NMAS to refer to the Universal Password.

  The option to update the NDS Password when the Universal Password is updated in the Password Policy is the default setting. If you select this option, Check Password Status should be accurate for the eDirectory connected system.

5 Configuring the Driver

This section gives you specific information for configuring the driver. This driver is unique among DirXML® drivers because there will always be two drivers installed, with each driver in its own tree.

The Subscriber in the first tree communicates with the Publisher in the second tree, and the Subscriber in the second tree communicates with the Publisher in the first tree. Therefore, the setup steps for the driver must be performed for each driver in each tree.

To use the driver, you must have the Novell® Certificate Server™ running on each server that will host the driver. We recommend that you use the Certificate Authority from one of the trees containing the driver to issue the certificates used for SSL. If your tree does not have a Certificate Authority, you will need to create one. You can use an external Certificate Authority.

Use Novell iManager to complete the driver configuration and administration tasks such as configuring driver properties, rules and style sheets, filters, and security.

- "Configuring Driver Object Properties" on page 25
- "Configuring the Publisher Channel Filter" on page 27
- "Configuring the Subscriber Channel Filter" on page 28
- "Configuring Rules on the Publisher Channel" on page 28
- "Configuring Secure Identity Manager Data Transfers" on page 29
- "Using Driver Object Passwords" on page 30

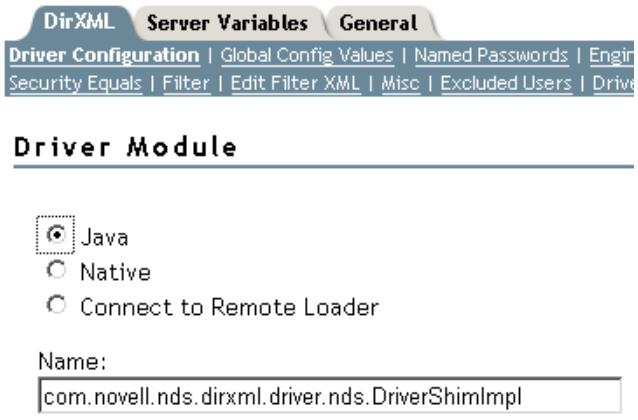
For information about password synchronization, see "Password Synchronization" on page 23.

The following section contains information that will help you configure the driver using Novell iManager.

Configuring Driver Object Properties

1. In iManager, click DirXML Management > Overview.
2. Locate the driver set that contains the eDirectory driver, then click the driver's icon.
3. From the DirXML Driver Overview, click the eDirectory driver object, which will display the driver configurations.
4. Locate the Driver Module section, then select Java.

Figure 10 The Driver Module section

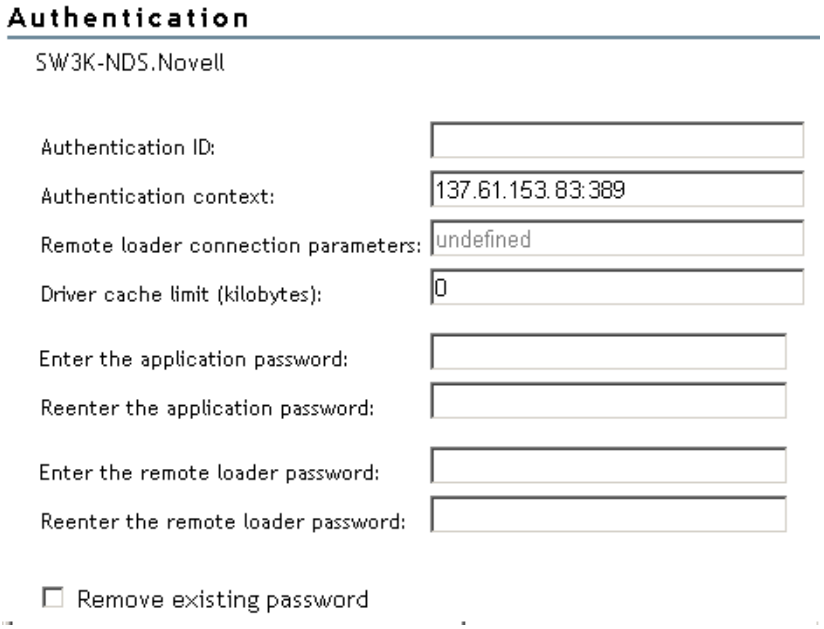


5 In the Name edit box, type the following eDirectory™ Driver Java class name:

`com.novell.nds.dirxml.driver.nds.DriverShimImpl`

6 Scroll to the Authentication section.

Figure 11 The Authentication section



7 Provide information that allows the source server to communicate with the destination server.

Authentication ID

If you want the source server and destination server to exchange secure information (for example, passwords), run the NDS2NDS eDirectory Certificates wizard. This wizard creates Key Material Objects (KMOs) and places the correct KMO name in the Authentication ID exit box.

The KMOs are Secure Socket Layer (SSL) certificates:

Figure 12 Example KMOs

Authentication Context

In the Authentication Context edit box, enter the host name or IP address of the destination server as well as the decimal port number (for example, 182.168.1.1:8196).

NOTE: If you see “java.net.ConnectException: Connection Refused,” no port connection is available on the remote side. This error might be caused by one of the following:

- The driver on the remote side is not running.
- The driver is running but is configured to use a different port.

Remote Loader Connection Parameters

The Remote Loader option isn’t needed (and isn’t used) for the DirXML Driver for eDirectory.

Driver Cache Limit

Don’t modify this edit box unless Novell Technical Services asks you to do so.

8 Click Apply, then click OK.

Configuring the Publisher Channel Filter

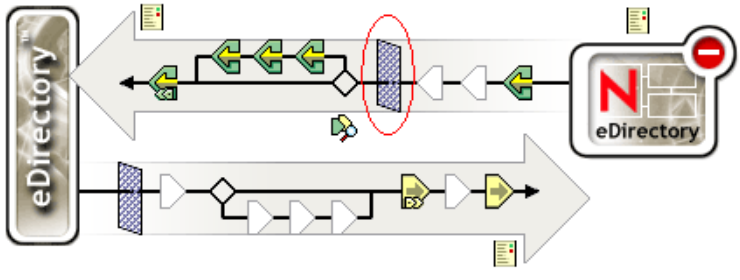
You should modify the filters on the Publisher and Subscriber channels to include object classes and attributes you want available for Nsure™ Identity Manager processing. To modify a filter:

1 In iManager, click DirXML Management > Overview.

2 Locate the driver set containing the eDirectory driver, then click the driver’s icon to display the DirXML Driver Overview page.

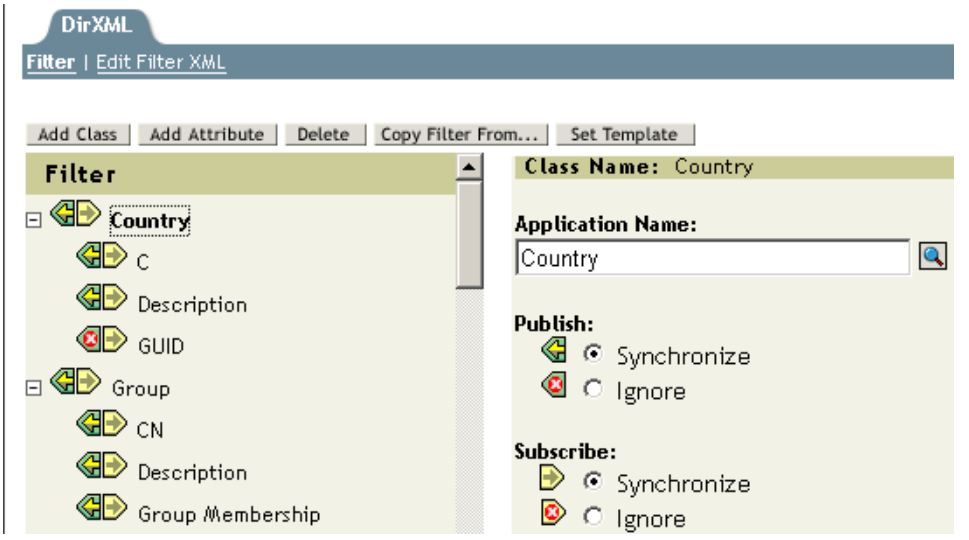
3 Click the filter on the Publisher channel.

Figure 13 The filter on the Publisher channel



4 Customize the driver.

Figure 14 Options in the driver's filter



In this example, Country and Group are classes. To add a class, click Add Class, then select the class. To delete a class, select it, then click Delete.

In this example, CN is an attribute of the Group class. To add an attribute, select the class, click Add Attribute, then select the attribute.

To modify a class or attribute, select it, then select options in the right pane. In this example, the Country attribute is synchronized on the Publisher and Subscriber channels. However, the GUID attribute isn't synchronized on the Publisher channel.

To synchronize the GUID attribute, select it, then click Synchronize under the Publish section.

5 Click Apply, then click OK.

Configuring the Subscriber Channel Filter

1 In iManager, click DirXML Management > Overview.

2 Locate the driver set containing the eDirectory driver, then click the driver's icon to display the DirXML Driver Overview page.

3 Click the Subscriber channel filter object to display the Filter dialog.

4 Customize the driver

5 Click Apply, then click OK.

Configuring Rules on the Publisher Channel

The rules on a driver should generally be placed only on the Publisher object, not on the Subscriber object. The Matching policy cannot operate correctly on the Subscriber channel because an association has not yet been set on the remote side object to match. It is sometimes desirable to place an Event Transform or Create Policy on the Subscriber channel in order to prevent sending unnecessary data across the channel. See "Managing Users on Different Servers Using Scope Filtering" in the *Novell Nsure Identity Manager 2 Administration Guide*.

Configuring Secure Identity Manager Data Transfers

All eDirectory driver communication is secured through SSL. To configure your Novell eDirectory™ system to handle secure Identity Manager data transfers, run the NDS2NDS wizard in Novell iManager.

- "Overview" on page 29
- "Procedure" on page 29

Overview

The following items can help you understand eDirectory driver security:

- The driver uses SSL sockets to provide authentication and a secure connection. SSL uses digital certificates to allow the parties to an SSL connection to authenticate one another. Identity Manager in turn uses Novell Certificate Server certificates for secure management of sensitive data.
- To use the driver, you must have the Novell® Certificate Server™ running in each tree. We recommend that you use the Certificate Authority from one of the trees containing the driver to issue the certificates used for SSL. If your tree does not have a Certificate Authority, you will need to create one. You can use an external Certificate Authority.
- The Novell implementation of SSL that the driver uses is based on Novell Secure Authentication Services (SAS) for eDirectory 8.6.2, and NTLS for eDirectory 8.7.*x*. These must be installed and configured on the server on which the driver is to run, which is usually done automatically by eDirectory.
- To configure driver security, it is necessary to create and reference certificates in the eDirectory trees that will be connected using the driver. Certificate objects in eDirectory are called Key Material Objects (KMOs) because they securely contain both the certificate data (including the public key) and the private key associated with the certificate.

  A minimum of two KMOs (one KMO per tree) must be created for use with the DirXML Driver for eDirectory. This section explains using a single KMO per tree.

  The NDS2NDS Driver Certificate wizard sets up the KMOs.
- For more information:
  - For an overview of Novell Certificate Server, see the Novell Certificate Server online documentation (http://www.novell.com/documentation/crtsrv20/index.html).
  - For more information on CAs, and in particular for information about setting up Certificate Authorities in your trees, see Setting Up Novell PKI Services (http://www.novell.com/documentation/lg/ndsse/ndsseenu/data/h6172k4q.html).

Procedure

This section explains using a single KMO per tree. Before you begin, find out the tree name or IP address of the destination server.

To configure your eDirectory system to handle secure Identity Manager data transfers:

1. Launch iManager and authenticate to your first tree.
2. Click DirXML Utilities > NDS2NDS Driver Certificates.
3. At the Welcome page, enter the requested information for the first tree.

Default values are provided using objects in the tree that you authenticated to when you launched iManager. You must enter or confirm the following information:

- Driver DN: Type the distinguished name of the eDirectory driver, for example, EDir-Workforce.Employee Provisioning.Services.YourOrgName
- The tree name: Enter the IP address for the Workforce Tree.
- A username for an account with Admin privileges, for example, Admin.
- The password for the user.
- The user's context, for example Services.YourOrgName

4 Click Next.

The wizard uses the information you entered to authenticate to the first tree, verify the driver DN, and verify that the driver is associated with a server.

5 Enter the requested information for the second tree.

At the Welcome page, enter the requested information for the first tree.

Enter or confirm the following information:

- Driver DN: Type the distinguished name of the eDirectory driver, for example, EDir-Account.DriverSet.YourOrgName
- The tree name: Type the tree name or IP address for the Account Tree.
- A username for an account with Admin privileges, for example, Admin.
- The password for the user.
- The user's context, for example, London.YourOrgName

6 Click Next.

The wizard uses the information you entered to authenticate to the second tree, verify the driver DN, and verify that the driver is associated with a server.

7 Review the information on the Summary Page, and click Finish.

If KMOs already existed for these trees, the wizard deletes them and then does the following:

- Exports the trusted root of the CA in tree one.
- Creates KMO objects.
- Issues a certificate signing request.
- Places certificate key pair names in the drivers' Authentication ID.

Using Driver Object Passwords

In addition to the mandatory certificates needed to use SSL, for additional security you can configure the driver so that the Subscriber channel on one tree will authenticate to the Publisher channel on the remote tree. You should set matching passwords in both trees.

To set the DirXML driver object password in a tree:

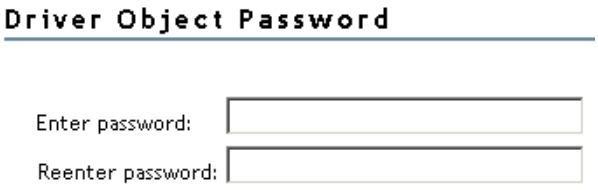
1 In iManager, click DirXML Management > Overview.

2 Locate the driver set containing the eDirectory driver, then click the driver's icon.

3 From the DirXML Driver Overview, click the eDirectory driver object, which will display the driver configurations.

4 Locate the Driver Object Password section.

Figure 15 The Driver Object Password section



5 Enter the password you want, click Apply, then click OK.

Migrating or Copying Objects

Although iManager doesn't have a Copy function, you can use the Migrate from eDirectory option to copy objects from one eDirectory tree to another. The scope of the copying depends on the policies of the driver. For example, depending on policies that apply to the driver, you can copy (sync) all the attributes from one eDirectory tree to another. Such a "copy" requires that you synchronize all the attributes across the trees, put objects in the same location during a migration, and not change any data during the migration.

A time stamp is always associated with a resync operation. A resync operation looks for objects that are already associated (have already been synchronized) but have been changed since the time stamp. It also attempts to look for objects that might have been created since the time stamp. Clicking Resync might cause new users to be synchronized.

Instead of using the Resync option to copy objects, use the Migrate from eDirectory option. This option enables you to specify and synchronize a list of objects. For each object in the list, iManager writes data to the directory. DirXML notes the changes and starts the synchronization process for listed objects.

1 Make sure that Identity Manager 2 is installed on a server in the source eDirectory tree and on a server in the destination eDirectory tree.

2 Configure a DirXML Driver for eDirectory on the server in the source tree.

In the eDirectory driver's Authentication pane, provide the name or IP address and port of the destination server. See "Configuring Driver Object Properties" on page 25.

Select a migration option: Flat, Mirrored, or Department. To preserve the directory structure (including subcontainers and names) when data is migrated from the source tree to the destination tree, select Mirrored.

3 Configure a DirXML Driver for eDirectory on the server in the destination tree.

In the Authentication pane, provide the name or IP address and port of the source server.

4 Set up SSL between the two trees.

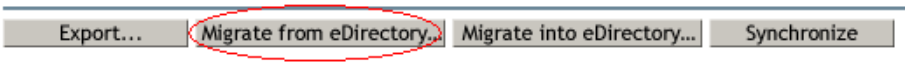
Using the NDS2NDS wizard, create KMO certificates in both trees. See "Procedure" on page 29.

The certificates must be signed, but only one tree has to sign them.

5 In iManager, select DirXML Management, click Overview, then click the driver.

6 Select Migrate from eDirectory.

Figure 16 The Migrate from eDirectory option



With eDirectory-to-eDirectory migrations, migrate from the source tree to the destination tree.

7 Select objects.

For example, select a User object or a Container object. You can search for or browse to the objects. Also, you can add multiple objects.

8 Click OK twice.

The client (for example, iManager) writes a value to each object in the list. This change event causes DirXML to push the data into your destination tree.

A Documentation Updates

This section contains new or updated information on the DirXML® Driver for eDirectory.

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 1, 2004" on page 33
- "April 26, 2004" on page 33
- "August 3, 2004" on page 33

April 1, 2004

- References to Password Synchronization 2.0 have been changed to Nsure™ Identity Manager Password Synchronization, to indicate 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.
- Troubleshooting items have been updated in "Password Synchronization" on page 23.

April 26, 2004

Location	Change
"Installing the Driver Shim" on page 12	Added steps for installing to Windows, NetWare, and Linux.
Throughout the document	Updated information and added graphics.

August 3, 2004

Location	Change
"Migrating or Copying Objects" on page 31	Added this topic.

May 8, 2006

Location	Change
“Configuring Secure Identity Manager Data Transfers” on page 29	Removed two links that are no longer available on Web sites.
“Installing the Driver Shim” on page 12	Clarified that this section assumes that eDirectory has already been installed on the server, and that this section explains how to add an eDirectory driver to the server.