Novell DirXML® Driver for eDirectory™

2.0

www.novell.com

IMPLEMENTATION GUIDE

April 1, 2004

Novell®

Legal Notices

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

www.novell.com

DirXML Driver for eDirectory Implementation Guide
April 1, 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

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.
Nsure 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.

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 eDirectory™.

The guide contains the following sections:

Additional Documentation

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

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. To contact us, send e-mail to proddoc@novell.com.

1 Overview

In this section:

Driver Overview

The DirXML® Driver for eDirectory™, subsequently referred to as the driver, 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.

In order 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 21.

New Features

The following section contains information about the new driver features, as well as new features provided in DirXML 2.0.

In this section:

Driver Features

- Support for Nsure™ 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 17 in this guide.

- The three options for the structure to use when synchronizing users, Mirrored, Flat, and Department, are now available in one sample configuration instead of a different sample configuration file for each. See Chapter 3, "Using the Sample Driver Configuration," on page 15.
- The driver can be customized to support Role-Based Entitlements. The functionality is not provided in the sample configuration, but can be created 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*.
- The driver can be customized to provide a driver heartbeat. See "Adding Driver Heartbeat" in the *Novell Nsure Identity Manager 2 Administration Guide*.

Identity Manager Features

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

2 Installing the Driver

The DirXML® Driver for eDirectory™ can be installed at the same time as the DirXML engine. You can also install the driver separately, as explained in this section, by running the Identity Manager installation and selecting to install the eDirectory driver only.

This section covers the following installation topics:

Where to Install the Driver

You should install Nsure™ Identity Manager and the driver on both of the Novell® eDirectory servers and in the trees you want to synchronize. This driver does not use the Remote Loader technology because it is built to communicate with itself. 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 specific instructions regarding data security, refer to "Configuring Secure Identity Manager Data Transfers" on page 21.

Driver Prerequisites

Meet the prerequisites for Identity Manager in "Installation" in the *Novell Nsure Identity Manager 2 Administration Guide*.

Installing the Driver

You can install the driver shim at the same time you install the DirXML Engine, or after. To install the driver shim, run the Identity Manager installation program and select the DirXML Driver for eDirectory. Instructions are in "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.

During the installation, NdsToNds.jar is copied to the appropriate directory. The following table shows these copy 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, you should configure security as explained in "Configuring Secure Identity Manager Data Transfers" on page 21.

Upgrading the Driver

In this section

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, but this assumes that your driver shim and configuration have the latest fixes.

Upgrading the Driver Shim

- You can install the upgraded driver shim at the same time you install the DirXML Engine, or after. To install the driver shim, run the Identity Manager installation program and select the DirXML Driver for eDirectory. Instructions are in "Installation" in *Novell Nsure Identity Manager 2 Administration Guide*.

  The new driver shim replaces the previous one.
- When you install the driver shim, your driver configuration is preserved, so no post-installation configuration is required until you want to take advantage of the new features included in the Identity Manager sample configuration, such as Identity Manager Password Synchronization features.
- After installing the driver shim, you must restart eDirectory and the driver. To restart the driver in Novell iManager, see "Starting, Stopping, or Restarting a Driver" in *Novell Nsure Identity Manager 2 Administration Guide*.
- After installing the driver shim, you must activate the driver. See "Activating the Driver" on page 13.

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 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 to 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.

  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 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*.

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

Upgrade Issues for eDirectory Driver

- Expired SSL certificates: 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 holding a valid certificate, the user will not be synchronized to the server containing the invalid certificate. You might also see the following error in DSTrace:

  ```
  SSL handshake failed, X509_V_CERT_HAS_EXPIRED
  ```

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

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

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

  To fix this issue, create new certificates.

Activating the Driver

Activation must be completed within 90 days of installation, or the driver will not run.

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

3 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.

In this section:

Importing the Sample Driver Configuration

Create a new driver or import the configuration onto an existing driver using one of the tasks in Novell iManager > DirXML Utilities, as described in "Managing DirXML Drivers" in the *Novell Nsure Identity Manager 2 Administration Guide*.

After importing the configuration, follow the instructions in "Configuring Secure Identity Manager Data Transfers" on page 21.

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:** Synchronize objects hierarchically between the local and remote trees. If you choose this option, you should 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:** Synchronize 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 does not 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 OU attribute (shown as Department in ConsoleOne). This configuration is typically used in conjunction with the Flat option (or a similar configuration) in the other tree. This option does not 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 specified 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 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.

  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.

- 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 will always show that the password is not synchronized. The password status will be 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.

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

4 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 19
- "Configuring the Publisher Channel Filter" on page 20
- "Configuring the Subscriber Channel Filter" on page 20
- "Configuring Rules on the Publisher Channel" on page 21
- "Configuring Secure Identity Manager Data Transfers" on page 21
- "Using Driver Object Passwords" on page 23

For information about password synchronization, see "Password Synchronization" on page 17.

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 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 Module option.
5. Click Java.
6. Enter the following eDirectory™ Driver Java class name:

   `com.novell.nds.dirxml.driver.nds.DriverShimImpl`
7. Click Authentication.

8 Enter the following in the Authentication ID field:

- If you created a single KMO per tree (see "Configuring Secure Identity Manager Data Transfers" on page 21), enter the name of the KMO you created in the tree containing the Driver object your are configuring (for example, Driver Cert).

9 (Conditional) Enter a password for the remote Driver object in the Application Password field.

This step is necessary only if you have chosen to use Driver object passwords for additional security. See "Using Driver Object Passwords" on page 23.

10 In the Authentication Context field, enter the host name or IP address of the server on the remote tree, a colon, and the decimal port number to use for communicating with the remote driver (for example, 255.255.255.255:2000).

A separate port can be specified for Subscriber and Publisher channels by specifying a second port number following a second colon. If a second port number is specified, the Publisher channel uses the second port number rather than using the same port number as the Subscriber channel (for example, 255.255.255.255:2000:2001).

If your server has multiple IP addresses, you can specify the IP address you want the Publisher channel to use. This requires specifying the remote IP address, the Subscriber channel port, the local IP address, and the Publisher channel port. For example. 137.65.134.81:2000:137.65.134.83:2000 specifies that the Subscriber channel will communicate with the remote tree on 137.65.134.81, port 2000, and that the Publisher channel will listen on address 137:65.134.83, port 2000.

NOTE: If you see "java.net.ConnectException: Connection Refused," this means that there is no port connection on the remote side. This error might be caused by either 1) The driver on the remote side is not running, or 2), the driver is running but is configured to use a different port.

11 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 Publisher channel filter object to display the Filter dialog.

4 If the filter is empty, click The Filter is Empty to add classes to the filter.

5 From the Edit Filter dialog, you can mark classes you want added to the filter for Identity Manager processing. When finished, click Apply, then click Ok.

IMPORTANT: You will want to add the Public Key and Private Key attributes to allow for the synchronization of passwords between objects in both eDirectory trees.

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 If the filter is empty, click The Filter is Empty to add classes to the filter.

5 From the Edit Filter dialog, you can mark classes you want added to the filter for Identity Manager processing. When finished, click Apply, then click Ok.

IMPORTANT: You must select the GUID attribute (for Subscriber channel only). This is necessary for the eDirectory DirXML Driver to work properly and for the object's association to be generated.

You might also want to add the Public Key and Private Key attributes to allow for the synchronization of passwords between objects in both eDirectory trees. To help you decide whether to use this method or to synchronize Universal Password, review the scenarios in "Password Synchronization across Connected Systems" in Novell Nsure Identity Manager 2 Administration Guide.

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. You can configure your Novell eDirectory™ system to handle secure Identity Manager data transfers using a wizard in Novell iManager.

- "Overview" on page 21
- "Procedure" on page 22

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 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.
- 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 walks you through the process of setting up the KMOs.

- The driver consists of two separate channels:
  - A Subscriber channel in the first tree that connects as a client to the Publisher channel in the second tree (which acts a server).
  - A Subscriber channel in the second tree that connects as a client to the Publisher channel in the first tree (which acts as a server).

  Both sides of a channel need a certificate signed by the same Certificate Authority (CA). At least one of the two channels (the Publisher or Subscriber) of the driver on one tree needs a certificate signed by the Certificate Authority of the tree on the other side of the channel.

  To use a certificate from one tree in another tree, the Trusted Root certificate from the first tree's Certificate Authority must be exported for use in the second tree.
- For more information:
  - For an overview of Novell Certificate Server, see the Novell Certificate Server online documentation (http://www.novell.com/documentation/lg/crtsrv20/docui/index.html).
  - For an overview of SSL, see the Secure Socket Layer Overview (http://developer.netscape.com/tech/security/ssl/protocol.html).
  - For an overview of certificates, see Certificates and Authentication (http://developer.netscape.com/docs/manuals/security/pkin/contents.htm#1047709).
  - 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.

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

1. Launch iManager and authenticate to your first tree.
2. Click DirXML Management > NDS2NDS Driver Certificate.
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 in 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 in the distinguished name of the eDirectory driver, for example, EDir-Account.DriverSet.YourOrgName
- The tree name: Enter the 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, enter the password you want, click Apply, then click Ok.

A Updates

This section contains information about documentation content changes that have been made in this guide.

The information is grouped according to the date the documentation updates were published.

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, the PDF document contains the date it was published in the Legal Notices section immediately following the title page.

The documentation was updated on the following dates:

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 17.