

Novell DirXML[®] Driver for Active Directory

3.0

www.novell.com

IMPLEMENTATION GUIDE

March 17, 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 © 2000-2004 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.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

DirXML Driver 3.0 for Active Directory Implementation Guide

[March 17, 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.

Third-Party Trademarks

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

Contents

- About This Guide** **7**

- 1 Overview** **9**
 - Driver Overview. 9
 - New Features. 9
 - Driver Features 9
 - Identity Manager Features 10
 - Data Transfers Between Systems 10
 - Publisher and Subscriber Channels 10
 - Default Driver Configuration 10
 - Data Flow 10

- 2 Preparing Active Directory** **13**
 - Active Directory Prerequisites 13
 - Planning Your Installation 13
 - Installation Locations 13
 - Driver Architecture 15
 - Authentication 16
 - Authentication Methods 16
 - Rights and Privileges 16
 - SSL 17
 - SSL Connection Between the Active Directory Driver and the Domain Controller 17
 - SSL Connection Between the Remote Loader and Identity Manager 19
 - Driver Features 19
 - Multi-Valued Attributes 19
 - Managing Account Settings using Custom Boolean Attributes 19
 - Provisioning Exchange Mailboxes using the homeMDB Attribute 20

- 3 Installing the Active Directory Driver** **21**
 - Installing the Driver Shim on the Identity Manager Server 21
 - Installing the Driver Shim to Use the Remote Loader 22
 - Importing a Driver Configuration 23
 - Configuration Parameters. 23

- 4 Upgrading the Active Directory Driver** **27**

- 5 Customizing** **29**
 - Security Parameters 29
 - Recommended Security Configurations 30
 - Activating the Driver 31

- 6 Password Synchronization** **33**
 - Comparison of Password Synchronization 1.0 and Password Synchronization Provided with Identity Manager 33
 - Upgrading Password Synchronization 1.0 to Password Synchronization Provided with Identity Manager. 35
 - Creating Backward Compatibility with Password Synchronization 1.0 by Adding Policies 37
 - New Driver Configuration and Identity Manager Password Synchronization. 39
 - Upgrading Existing Driver Configurations to Support Identity Manager Password Synchronization 40

Setting Up Password Synchronization Filters	42
Troubleshooting Password Synchronization	46
7 Troubleshooting	49
Changes Are Not Synchronizing from Publisher or Subscriber	49
Using Characters Outside the Set of Valid NT Logon Names.	49
Synchronizing c, co, and countryCode Attributes	49
Synchronizing Operational Attributes	50
Windows 2003 Issues	50
Password Complexity is Enforced when Policy Items are Not Defined	50
A Updates	51
March 17, 2004	51

About This Guide

This guide explains how to install and configure the DirXML[®] Driver for Active Directory.

The guide contains the following sections:

- ♦ [Chapter 1, “Overview,” on page 9](#)
- ♦ [Chapter 2, “Preparing Active Directory,” on page 13](#)
- ♦ [Chapter 3, “Installing the Active Directory Driver,” on page 21](#)
- ♦ [Chapter 4, “Upgrading the Active Directory Driver,” on page 27](#)
- ♦ [Chapter 5, “Customizing,” on page 29](#)
- ♦ [Chapter 6, “Password Synchronization,” on page 33](#)
- ♦ [Chapter 7, “Troubleshooting,” on page 49](#)
- ♦ [Appendix A, “Updates,” on page 51](#)

Additional Documentation

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

Documentation Updates

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

This section covers the following topics:

- ◆ “[Driver Overview](#)” on page 9
- ◆ “[New Features](#)” on page 9
- ◆ “[Data Transfers Between Systems](#)” on page 10
- ◆ “[Default Driver Configuration](#)” on page 10

Driver Overview

The DirXML[®] Driver for Active Directory* is designed to synchronize data between Novell[®] eDirectory[™] and the Microsoft* Active Directory* directory service. The synchronization is bi-directional; you determine whether information should flow to and from both directories, or whether information should flow only from one directory to the other.

In addition, this driver can be configured to provision Microsoft Exchange 2000 and Exchange 2003 mailboxes.

New Features

Driver Features

- ◆ Better Support for multi-valued attributes. See “[Multi-Valued Attributes](#)” on page 19.
- ◆ User account control can now be managed using a set of mapped boolean attributes, rather than managing the integer bit settings. See “[Managing Account Settings using Custom Boolean Attributes](#)” on page 19.
- ◆ A new method for provisioning Exchange 2000 and Exchange 2003 mailboxes has been added. See “[Provisioning Exchange Mailboxes using the homeMDB Attribute](#)” on page 20.
- ◆ Support for Windows 2003 Server.
- ◆ Support for Nsure[™] Identity Manager Password Synchronization.

For instructions specific to Active Directory, see [Chapter 6, “Password Synchronization,”](#) on page 33.

See also the description of the different scenarios in “[Implementing Password Synchronization](#)” in *Novell Nsure Identity Manager 2 Administration Guide*.

- ◆ The driver supports Role-Based Entitlements.
See “[Using Role-Based Entitlements](#)” in *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*.

Data Transfers Between Systems

Publisher and Subscriber Channels

The driver supports Publisher and Subscriber channels:

- ◆ The Publisher reads events from Active Directory for the domain hosted on the server that the driver shim is connecting to and submits that information to eDirectory.
- ◆ The Subscriber watches for additions and modifications to eDirectory directory objects and makes changes to Active Directory that reflect those changes.

When the driver is configured so that both Active Directory and eDirectory are allowed to update a specific attribute, the most recent change will determine the attribute value, except in the case of merge operations which are controlled by the filters and merge authority.

Default Driver Configuration

Data Flow

Policies

Policies are used to control data synchronization between the Active Directory and eDirectory.

During the driver configuration, the Active Directory configuration file enables you to select several options that affect the default policies and filters created for you. The following table contains a list of these options and how they affect policy and filter creation:

Option	Description
Configure Data Flow: <input type="button" value="Bi-Directional"/>	Configure Data Flow establishes the Filters on the Publisher and Subscriber channels.
<input type="button" value="Bi-Directional"/>	Bi-directional enables the same filters on both channels. Both channels receive the same set of default objects and attributes.
<input type="button" value="AD to eDirectory"/>	AD to eDirectory places a restrictive filter so changes are not sent from eDirectory to Active Directory.
<input type="button" value="eDirectory to AD"/>	eDirectory to AD places a restrictive filter so changes are not sent from Active Directory to eDirectory.

Option	Description
Publisher Placement: <input type="button" value="Mirrored"/> <input type="button" value="Flat"/>	This controls how objects are placed in eDirectory. Mirrored places objects in the same hierarchy as they exist in Active Directory. Flat places all objects in the base container specified during configuration.
Subscriber Placement: <input type="button" value="Mirrored"/> <input type="button" value="Flat"/>	This controls how objects are placed in Active Directory. Mirrored places objects in the same hierarchy as they exist in eDirectory. Flat places all objects in the base container specified during configuration.

The following table contains a list of the default policies and how they are affected by your selections during configuration:

Policy	Description
Create	In order for an Active Directory user to be created as a user in eDirectory, Full Name must be defined. NOTE: This is enforced in the create policy for a flat hierarchy, and the matching policy for a mirrored hierarchy. In either hierarchy, Full Name must be defined.
Matching	In a flat hierarchy, the matching policy attempts to match the user with an object with the same Full Name in the base container you specify. In a mirrored hierarchy, the matching policy attempts to match the user with an object with the same Fully Distinguished Name.
Placement	In a flat hierarchy, the placement policy places all objects in the base container you specify. In a mirrored hierarchy, the placement policy places all objects in a hierarchy that mirrors that of the data store sending the operation.

Schema Mapping

The following eDirectory User and Group attributes are mapped to Active Directory user and group attributes:

eDirectory	Active Directory
CN	userPrincipalName in user cn in group
Description	description
DirXML-ADAliasName	SAMAccountName
Facsimile Telephone Number	facsimiletelephoneNumber
Full name	displayName

eDirectory	Active Directory
Given Name	givenName
Group Membership	memberOf
Initials	initials
Internet EMail Address	mail
L	physicalDeliveryOfficeName
Locality	locality
Login Allowed Time Map	logonHours
Login Disabled	dirxml-uACAccountDisable
Member	member
OU	ou
Owner	managedBy
Physical Delivery Office Name	l
Postal Code	PostalCode
Postal Office Box	postOfficeBox
S	st
SA	streetAddress
See Also	seeAlso
Surname	sn
Telephone Number	telephoneNumber
Title	title

2

Preparing Active Directory

This section covers the following topics:

- ◆ “Active Directory Prerequisites” on page 13
- ◆ “Planning Your Installation” on page 13
- ◆ “Authentication” on page 16
- ◆ “SSL” on page 17
- ◆ “Driver Features” on page 19

Active Directory Prerequisites

- ◆ Nsure™ Identity Manager 2 or later, including Identity Manager prerequisites.
- ◆ Windows 2003 Server, or Windows 2000 Server with Service Pack 2 or later.
- ◆ Internet Explorer 5.5 or later, on the server running the AD driver, and on the target domain controller.
- ◆ Active Directory domain controller DNS name or IP address depending on the authentication method.

The following is recommended:

- ◆ The server hosting the Active Directory driver be a member of the AD domain. This is required to provision Exchange mailboxes and synchronize passwords. If you do not require these features, then the server can be a member of any domain as long as the simple authentication mode is used.

Planning Your Installation

You will need to determine installation location and security configuration before you start the driver installation. These decisions affect where the driver is installed, and how it is configured.

Installation Locations

The driver itself must run on one of the supported Windows platforms. However, you don't need to install the DirXML engine on this same machine. Using the Remote Loader, you can separate the engine and the driver, allowing you to balance the load on different machines or accommodate corporate directives.

The AD driver can run in any of the following three scenarios:

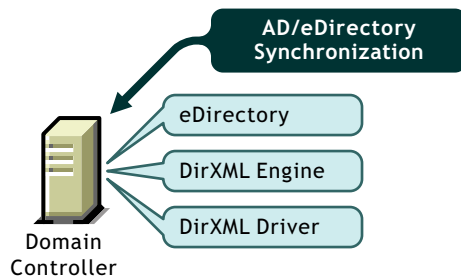
- ◆ **Single Server**

A single Windows domain controller hosts eDirectory, the DirXML engine, and the driver.

This configuration works well for organizations that want to save on hardware costs. It is also the highest-performance configuration because there is no network traffic between Identity Manager and Active Directory.

However, hosting eDirectory and Identity Manager on the domain controller increases the overall load on the controller and increases the risk that the controller may fail. Domain controllers play a critical role in Microsoft networking and many organizations are more concerned about the speed of the domain authentication and the risks associated with a failure on the domain controller than about the cost of additional hardware.

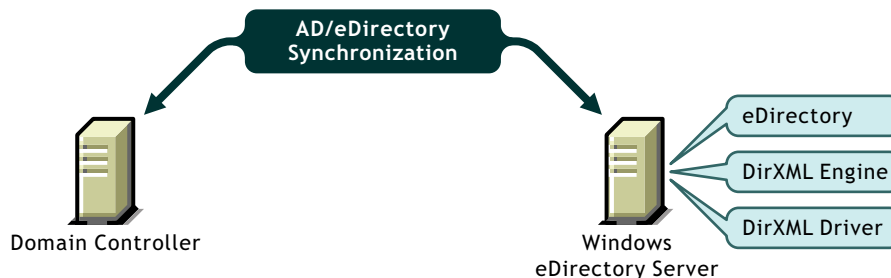
Figure 1 Single Server Installation



◆ **Dual Server**

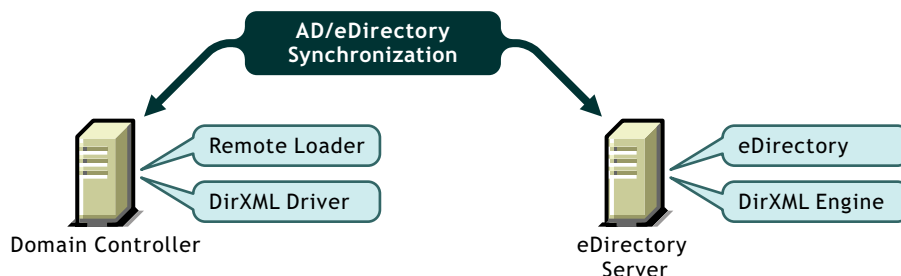
Dual server configurations can be set up in two ways. The first configuration places eDirectory, the DirXML engine, and the driver on a separate computer from the Active Directory domain controller, leaving the domain controller free of any Identity Manager DirXML software.

Figure 2 Dual Server Configuration (1)



The second configuration places eDirectory and the DirXML engine on one computer and the driver and Remote Loader on the Active Directory domain controller.

Figure 3 Dual Server Configuration (2)

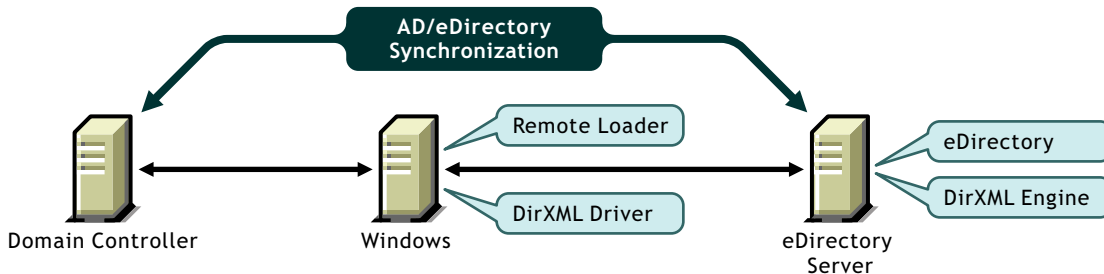


Both configurations eliminate the performance impact of hosting eDirectory and the DirXML engine on the domain controller. The first configuration is attractive if corporate policy disallows running the driver on your domain controller. The second solution is attractive if your eDirectory and Identity Manager installations are on a platform other than one of the supported versions of Windows.

◆ **Triple Server**

A three-server configuration can be used if you have platform requirements and domain controller restrictions in place. It's more complicated to set up this configuration, but it accommodates the constraints of some organizations.

Figure 4 Triple Server Configuration



Driver Architecture

The Active Directory Driver consists of several pieces which operate together to synchronize Active Directory with Identity Manager. The following table contains a description of each of these pieces, and where they fit in the driver architecture:

Component	Description
Driver Shim	<p>The driver shim is a library, loaded directly by DirXML or by the remote loader, which collects the changes to be sent to eDirectory from Active Directory, and communicates changes from eDirectory to Active Directory.</p> <p>The shim operates as the link which connects DirXML and Active Directory. The driver shim is <code>addriver.dll</code>.</p>
Driver	<p>The driver is the set of policies, filters, and objects which acts as the connector between DirXML and the driver shim.</p> <p>Using objects in eDirectory, the driver stores the configuration information required by DirXML to communicate with the driver shim, as well as the policies and filters which customize changes.</p>

The installation scenario you select determines how the driver shim is installed. If you choose to install the driver shim on the same machine as DirXML, the driver shim is called by DirXML directly. If you choose to install the driver shim on another machine, you must use the remote loader. Installing the driver shim in each of these scenarios is discussed in [“Installing the Driver Shim on the Identity Manager Server” on page 21](#) and [“Installing the Driver Shim to Use the Remote Loader” on page 22](#) respectively.

Regardless of the configuration, installing the driver component is the same, and is discussed in [“Importing a Driver Configuration” on page 23](#).

Authentication

This section contains a discussion of the security and authentication issues you must consider before installing the Active Directory driver.

The driver can run in several security modes. The major factors to consider are authentication, encryption, and use of the Remote Loader. If you are using the Remote Loader you must consider security settings on the Remote Loader channel between Identity Manager and the driver, plus the settings between the driver and Active Directory. If you have Windows 2003 or Windows 2000 SP3 or later, you'll want to consider a security option called signing.

A simple prescription for managing security is not possible because the security profile available from Windows varies with service pack, DNS server infrastructure, domain policy, and local policy settings on the server. The following sections explain your security choices and provide suggested configurations. Pay close attention to security when implementing your driver and when upgrading components.

Authentication Methods

Authentication identifies the driver shim to Active Directory, and potentially the local machine.

There are two methods available for Active Directory authentication: negotiate, and simple.

When the driver shim is not running on the domain controller, negotiate is the preferred authentication mechanism. To use negotiate, the server hosting the driver shim must be a member of the domain. Negotiate uses Kerberos, NTLM, or a pluggable authentication scheme if one is installed.

Simple bind is used when the server hosting the driver shim is not a member of the domain. However, not all provisioning services are available using simple bind, such as exchange mailboxes and password synchronization.

Authentication Mechanism	Advantages	Disadvantages
Negotiate	<ul style="list-style-type: none">◆ Driver can be installed on any server in the domain◆ SSL is optional	<ul style="list-style-type: none">◆ Server hosting the driver must be a member of the domain.
Simple	<ul style="list-style-type: none">◆ Driver can be installed on a server that is not a member of the domain	<ul style="list-style-type: none">◆ Some provisioning services are unavailable, such as Exchange mailbox provisioning and password synchronization.◆ SSL is necessary to encrypt clear-text authentication, and required to perform Subscriber password set, check and modify.

Rights and Privileges

We recommend that you create an administrative account to be used exclusively by the Active Directory driver to authenticate to Active Directory. Doing this keeps the Identity Manager

administrative account insulated from changes to other administrative accounts. Advantages to this design are:

- ◆ You can use Active Directory auditing to track the activity of the Active Directory driver.
- ◆ You can implement a password change policy as with other accounts, then make necessary updates to the driver configuration.

This account name and password are stored in the driver configuration, so anytime the account password changes you must change this password. If you change the account password without updating the driver configuration, authentication will fail the next time the driver is restarted.

At a minimum, this account must have *Read* and *Replicating Directory Changes* rights at the root of the domain for the publisher channel to operate. You will also need *Write* rights to any object modified by the subscriber channel. *Write* rights can be restricted to the containers and attributes that are written by the subscriber channel.

In order to instrument Exchange mailboxes, your Identity Manager account must have *Act as part of the Operating System* permission for the logon account.

SSL

Depending on your configuration, SSL can be used in two places. Between the Active Directory driver and your domain controller, and between the remote loader running the Active Directory Driver and Identity Manager. The following table outlines where SSL connections can be used for each of the installation scenarios discussed in [“Planning Your Installation” on page 13](#):

Scenario	SSL Connections Available
Single Server	No SSL connections are necessary.
Dual Servers - Identity Manager and Driver on Same Machine	An SSL connection can be established between the Active Directory driver and the domain controller.
Dual Servers - Identity Manager and Driver on Separate Machines	An SSL connection can be established between Identity Manager and the remote remote loader running the Active Directory Driver.
Triple Servers	An SSL connection can be established between the Active Directory driver and the domain controller. An SSL connection can also be established between Identity Manager and the remote loader running the Active Directory Driver.

SSL Connection Between the Active Directory Driver and the Domain Controller

In order to make SSL connections to an Active Directory domain controller, you must be set up to use SSL. This involves setting up a certificate authority, then creating, exporting, and importing the necessary certificates.

Most organizations already have a certificate authority. In this case, you need to export a valid certificate, then import it to the certificate store on your domain controller. The server hosting the driver shim must trust the root certificate authority to which the issuing certificate authority of this certificate chains.

If you do not have a certificate authority in your organization, one must be established. The tools necessary to do this are provided by Novell, Microsoft, and several other 3rd parties. Establishing a certificate authority is beyond the scope of this guide. More information can be found at:

- ◆ [Novell Certificate Server™ 2.5 Administration Guide \(http://www.novell.com/documentation/lg/crt252/index.html\)](http://www.novell.com/documentation/lg/crt252/index.html)
- ◆ [Microsoft Step-by-Step Guide to Setting up a Certificate Authority \(http://www.microsoft.com/windows2000/techinfo/planning/security/casetupsteps.asp\)](http://www.microsoft.com/windows2000/techinfo/planning/security/casetupsteps.asp)

Once you have a certificate authority, for LDAP SSL to operate successfully, the LDAP server must have the appropriate server authentication certificate installed and the server hosting the driver shim must trust the authority that issued those certificates. Both the server and the client must support 128-bit encryption.

The following steps outline this procedure:

- 1** Generate a certificate which meets the Active Directory LDAP service requirements listed below. This certificate permits the LDAP service on the domain controller to listen for, and automatically accept, SSL connections for both LDAP and global catalog traffic.

NOTE: This information appears in the Microsoft Knowledge Base Article 321051, [How to Enable LDAP over SSL with a Third-Party Certificate Authority \(http://support.microsoft.com/default.aspx?scid=kb;en-us;321051\)](http://support.microsoft.com/default.aspx?scid=kb;en-us;321051). Consult this document for the latest requirements and additional information.

- ◆ The LDAPS certificate is located in the Local Computer's Personal certificate store (programmatically known as the computer's MY certificate store).
 - ◆ A private key matching the certificate is present in the Local Computer's store and is correctly associated with the certificate. The private key must not have strong private key protection enabled.
 - ◆ The Enhanced Key Usage extension includes the Server Authentication (1.3.6.1.5.5.7.3.1) object identifier (also known as OID).
 - ◆ The Active Directory fully qualified domain name (for example, DC01.DOMAIN.COM) of the domain controller must appear in one of the following places:
 - ◆ The Common Name (CN) in the Subject field.
 - ◆ DNS entry in the Subject Alternative Name extension.
 - ◆ Certificate was issued by a CA that the domain controller and the LDAPS clients trust. Trust is established by configuring the clients and the server to trust the root CA to which the issuing CA chains.
- 2** Export this certificate in one of the following standard certificate file formats supported by Windows 2000:
 - ◆ Personal Information Exchange (PFX, also called PKCS #12)
 - ◆ Cryptographic Message Syntax Standard (PKCS #7)
 - ◆ Distinguished Encoding Rules (DER) Encoded Binary X.509
 - ◆ Base64 Encoded X.509
 - 3** Install this certificate on the domain controller. The following links contain instructions for each supported platform:
 - ◆ [HOW TO: Install Imported Certificates on a Web Server in Windows Server 2003 \(http://support.microsoft.com/default.aspx?scid=kb;en-us;816794\)](http://support.microsoft.com/default.aspx?scid=kb;en-us;816794)

- ♦ [HOW TO: Install Imported Certificates on a Web Server in Windows 2000 \(http://support.microsoft.com/default.aspx?scid=kb;EN-US;310178\)](http://support.microsoft.com/default.aspx?scid=kb;EN-US;310178)

Follow the instructions listed under Import the Certificate Into the Local Computer Store.

- 4 Ensure that a trust relationship is established between the server hosting the driver shim and the root certificate authority which issued the certificate. The server hosting the driver shim must trust the root certificate authority to which the issuing certificate authority chains.

For more information about establishing trust for certificates, see the “Policies to establish trust of root certification authorities” topic in Windows 2000 Server Help.

- 5 In iManager, edit the driver properties and change the Use SSL (yes/no) option to yes.
- 6 Restart the driver. When the driver restarts, an SSL connection is negotiated between the domain controller and the server running the Active Directory driver shim.

SSL Connection Between the Remote Loader and Identity Manager

Establishing an SSL connection between the Remote Loader and Identity Manager is discussed in the “[Using the Remote Loader Service](#)” section of the *Novell Nsure Identity Manager 2 Administration Guide*.

Driver Features

This section contains a discussion of driver features you should become familiar with before deploying the Active Directory driver.

Multi-Valued Attributes

The way the Active Directory driver handles multi-valued attributes has changed from version 2.

Version 2 treated multi-valued attributes as single-valued on the Subscriber channel by ignoring all but the first change value in an Add or Modify operation. Version 3 of the Active Directory Driver fully supports multi-valued attributes.

Managing Account Settings using Custom Boolean Attributes

The Active Directory attribute `userAccountControl` is an Integer whose bits control logon account properties, such as whether logon is allowed, passwords are required, or the account is locked. Synchronizing the Boolean properties individually is problematic because each property is embedded in the Integer value.

In version 2, of the Active Directory driver took a shortcut that let you map `userAccountControl` the `eDirectory Login Disabled` attribute, but didn't let you map the other property bits within the attribute.

In version 3, each bit within the `userAccountControl` attribute can be referenced individually as a Boolean value or `userAccountControl` can be managed in-total as an Integer. The driver recognizes a Boolean alias to each bit within `userAccountControl`, as detailed in [Table 1, “Bitfield Aliases to userAccountControl,” on page 20](#). These alias values are included in the schema for any class that includes `userAccountControl`. The alias values are accepted on the Subscriber channel and are presented on the Publisher channel.

The advantage to this feature is that since each bit can be used as a boolean, they can be enabled individually in the Publisher Filter and accessed easily. You can also put userAccountControl into the Publisher Filter to receive change notification and it will be published as an Integer.

The Integer and alias versions of userAccountControl should not be mixed in a single configuration.

The following table contains an alphabetical list of all available aliases:

Table 1 Bitfield Aliases to userAccountControl

Alias	Notes
dirxml-uACDontExpirePassword	
dirxml-uACHomedirRequired	
dirxml-uACInterdomainTrustAccount	Read-only. This property should never be set on the Subscriber channel.
dirxml-uACNormalAccount	Read-only. This property should never be set on the Subscriber channel.
dirxml-uACServerTrustAccount	Read-only. This property should never be set on the Subscriber channel.
dirxml-uACWorkstationTrustAccount	Read-only. This property should never be set on the Subscriber channel.
dirxml-uACAaccountDisable	
dirxml-uACPasswordNotRequired	

Provisioning Exchange Mailboxes using the homeMDB Attribute

Your options for provisioning Exchange 2000 and Exchange 2003 mailboxes has changed from version 2.

In Version 2, Exchange provisioning was accomplished by setting attributes on user objects. A Microsoft program called the Recipient Update Service used this information to provision the Exchange database.

This method still works in version 3 of the Active Directory Driver, but a new method called CDOEXM has been added. With CDOEXM enabled, an Exchange mailbox is provisioned by setting the homeMDB attribute. When the homeMDB attribute is set, all required attributes are set automatically by the driver.

The homeMDB attribute is set during initial configuration, or later by modifying the driver properties. For a discussion of this parameter, see [“Configuration Parameters” on page 23](#).

3

Installing the Active Directory Driver

Installing the Active Directory driver requires two general steps. First, the driver shim must be installed on the DirXML server, or on the Connected System Server, depending on where you would like to host the driver shim. Second, a driver configuration must be created using iManager.

How you install the driver depends on your installation scenario, specifically whether or not you are installing the driver shim on the same server as the DirXML engine. If the driver shim is on a Windows DirXML server, it can run natively. If it is on a different server, it must use the remote loader.

NOTE: The location of your domain controller does not affect the driver installation, it affects the authentication mechanism you select to connect to Active Directory.

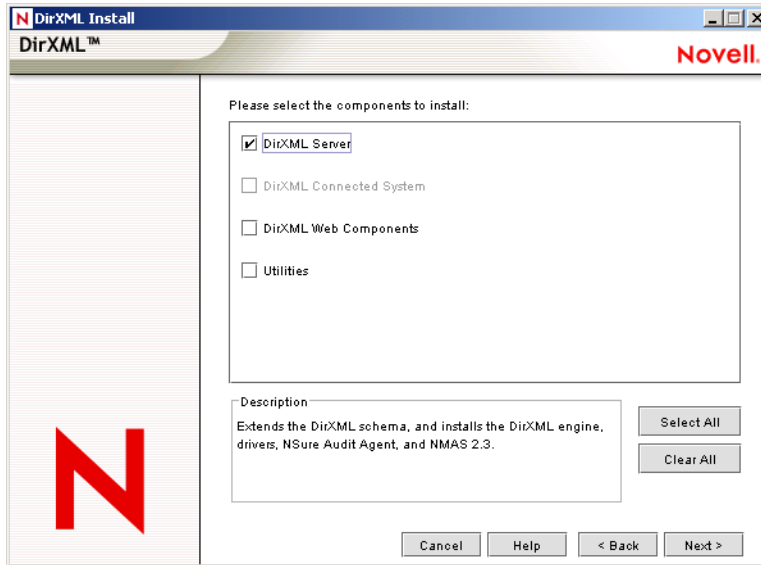
The following tables outline the installation procedure for each installation scenario discussed in [Chapter 2, “Preparing Active Directory,” on page 13](#):

Scenario	Installation Considerations
Single Server	The driver shim and engine are on the same server. To install the driver, follow the instructions in “Installing the Driver Shim on the Identity Manager Server” on page 21 .
Dual Servers - Nsure™ Identity Manager and Driver on Same Machine	

Scenario	Installation Considerations
Dual Servers - Identity Manager and Driver on Separate Machines	The driver shim and engine are on separate servers. To install the driver, follow the instructions in “Installing the Driver Shim to Use the Remote Loader” on page 22 .
Triple Servers	

Installing the Driver Shim on the Identity Manager Server

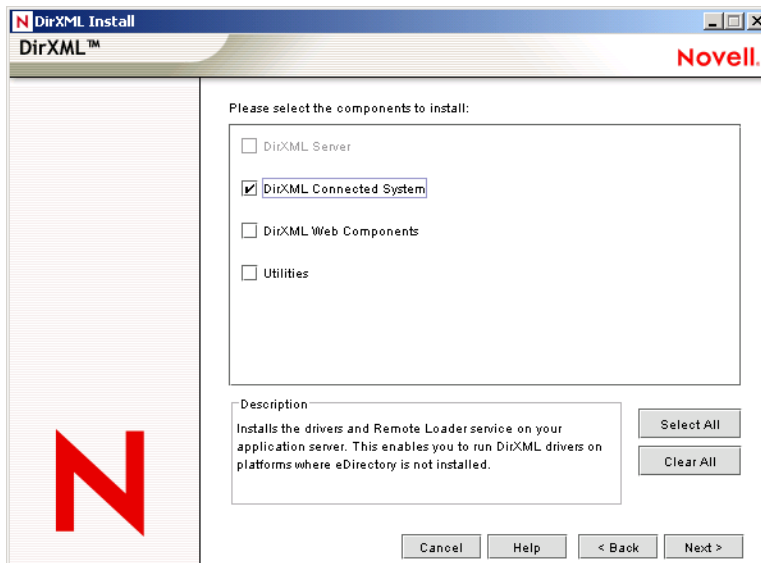
Launch the Identity Manager installation, and select the following option:



This option enables you to install the Active Directory driver shim to run on the same server as Identity Manager. Detailed installation instructions are contained in the “**Installation**” chapter of the *Novell Nsure Identity Manager 2 Administration Guide*.

Installing the Driver Shim to Use the Remote Loader

During the Identity Manager installation, select the following:



This option enables you to install the Active Directory driver shim to run on a separate server. Detailed installation instructions are contained in the “**Installation**” chapter of the *Novell Nsure Identity Manager 2 Administration Guide*.

Importing a Driver Configuration

The Create Driver Wizard helps you import a basic driver configuration for Active Directory. This wizard creates and configures the objects needed to make the driver work properly. For details on using this wizard, see “[Creating and Configuring a Driver](#)” in the *Novell Nsure Identity Manager 2 Administration Guide*.

This section contains instructions and configuration parameters specific to the Active Directory driver. Each of these parameters is explained in “[Configuration Parameters](#)” on page 23.

In addition, you might need to do the following:

- ❑ Create an administrative account for use with Identity Manager, and assign this account the necessary rights. See “[Rights and Privileges](#)” on page 16 for additional information.

Configuration Parameters

The following table contains an explanation of the parameters you must provide during initial driver configuration:

Field	Description
Driver Name	<p>This is the eDirectory object name to be assigned to this driver.</p> <p>Because each Active Directory domain requires a separate driver, you should include the domain name in your driver name.</p>
Authentication Method	<p>The method to authenticate with Active Directory.</p> <p>Select Negotiate to use the Microsoft security package to negotiate authentication type. Typically Kerberos or NTLM is used. In order to use negotiate, the server hosting the driver must be a member of the domain.</p> <p>Select simple to use an LDAP simple bind. If you select simple, SSL is recommended, and required to perform subscriber password set, check, or modify.</p>
Authentication ID	<p>An Active Directory account with administrative privileges to be used by Identity Manager. The name form used depends on the selected authentication mechanism.</p> <p>For simple, provide an LDAP ID, such as:</p> <ul style="list-style-type: none">◆ cn=DirXML,cn=Users,DC=domain,dc=com <p>For negotiate, provide the name form required by your Active Directory authentication mechanism. For example:</p> <ul style="list-style-type: none">◆ Administrator - NT Logon Name◆ Domain/Administrator - Domain qualified NT Logon Name
Password	<p>Enter the password for the user account specified in Authentication ID.</p>

Field	Description
Authentication Server	<p>The name of the Active Directory domain controller to use for synchronization.</p> <p>For example, <code>mycontroller.domain.com</code> for the negotiate authentication method. If you are using simple authentication, this can be the IP address of your server, for example, <code>10.10.128.23</code>.</p> <p>If no value is specified, <code>localhost</code> is used.</p> <p>NOTE: This value is stored in the Authentication Context attribute. To change this value after the initial configuration, modify this attribute as explained in “Security Parameters” on page 29.</p>
Domain Name (in LDAP format)	<p>The Active Directory domain managed by this driver.</p> <p>The driver requires LDAP formatted domain names <code>dc=mydomain,dc=com</code></p>
Domain DNS Name (DNS format)	<p>The DNS name of the Active Directory domain managed by this driver.</p> <p>The driver requires DNS formatted domain names <code>mydomain.com</code></p>
Driver Polling Interval	<p>eDirectory sends changes to Active Directory as they happen. However, changes to Active Directory are sent to eDirectory only as often as the configured polling interval. The default is 1 minute.</p> <p>IMPORTANT: The polling interval affects system performance.</p>
Password Sync Timeout	<p>The number of minutes the driver attempts to sync a password.</p> <p>It is recommended that the pass sync timeout should be set to at least three times the polling interval.</p>
Base container in eDirectory	<p>Specify the base container in eDirectory in dot format. New users are placed in this container by default. For example,</p> <p><code>users.myorg</code></p> <p>If the target container doesn't exist, you must create it before you start the driver.</p>
Base container in AD	<p>Specify the base container in Active Directory, in LDAP format. New users are placed in this container by default. For example,</p> <p><code>CN=Users,DC=MyDomain,DC=com</code></p> <p>If the target container doesn't exist, you must create it before you start the driver.</p>
Configure Data Flow	<p>Bi-directional means that both AD and eDirectory are authoritative sources of the data synchronized between them. AD to eDirectory means that NT is the authoritative source. eDirectory to AD means that eDirectory is the authoritative source.</p> <p>This selection is used to determine how the default policies and filters are created.</p>

Field	Description
Publisher Placement	Choose Flat to place objects strictly within the base container. Choose Mirrored to place objects hierarchically within the base container. This selection is used to build the default Publisher channel placement rules.
Subscriber Placement	Choose Flat to place objects strictly within the base container. Choose Mirrored to place objects hierarchically within the base container. This selection is used to build the default Subscriber channel placement rules.
Support Exchange 2000	Select Exchange support.
Default Exchange MDB (Exchange Only)	The default Exchange Message Database (MDB).
Enable Entitlements	Enable this if you are also using the Entitlements Service driver and want this driver to use Role-Based Entitlements.
Action - Add Account Entitlement (Entitlements Only)	Action taken when a User account is added by Entitlements.
Action - Remove Account Entitlement (Entitlements Only)	Action taken when a User account is removed by Entitlements.
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 (Remote Only)	The Host Name or IP Address and Port Number where the Remote Loader Service has been installed and is running for this driver. The Default Port is 8090.
Driver Password (Remote Only)	The Driver Object Password is used by the Remote Loader to authenticate itself to the Identity Manager server. It must be the same password that is specified as the Driver Object Password on the Remote Loader.
Remote Password (Remote Only)	The Remote Loader password is used to control access to the Remote Loader instance. It must be the same password that is specified as the Remote Loader password on the Remote Loader.

4

Upgrading the Active Directory Driver

Upgrading the Active Directory Driver involves upgrading the components discussed in “[Driver Architecture](#)” on page 15.

To upgrade the driver shim, follow the instructions in [Chapter 3, “Installing the Active Directory Driver,”](#) on page 21.

To upgrade the driver configuration, see “[Upgrading Driver Configurations](#)” in the *Novell Nsure Identity Manager 2 Administration Guide*.

5

Customizing

Before you begin customizing your Active Directory driver, you should become familiar with the default policies and parameters. You should also be familiar with the topics discussed in [Chapter 7, “Troubleshooting,” on page 49](#), to see if any of these issues apply to your environment.

During installation, the driver gathered all of the information needed to run. After the driver is installed, you should become familiar with the default policies and filters that were created for you, and the parameters discussed in this section.

This section contains:

- ♦ [“Security Parameters” on page 29](#)
- ♦ [“Activating the Driver” on page 31](#)

Security Parameters

Each of these security parameters is set during the initial driver configuration.

Understanding how the parameters work together and work with the operating system will help you define your approach to security for Nsure™ Identity Manager data synchronization.

- ♦ **Authentication ID:** This is the account the driver uses to access domain data. Valid username formats are

Username	Format
Domain name	user
Fully Qualified Domain name	domain\user
Simple	cn=DirXML,cn=Users,DC=domain,dc=com

- ♦ **Authentication Context:** This is the DNS name of the Active Directory domain controller if you selected negotiate, or the IP address of your LDAP server if you selected LDAP simple authentication. For example: mycontroller.mydomain.com.

If the driver is running on the Domain Controller and you don't specify an authentication context, the driver will address its connection to the local machine.

- ♦ **Application Password:** This is the password for the Authentication ID account. Set a password whenever you use an Authentication ID.
- ♦ **Use Signing:** This flag enables signing of the Active Directory connection if you are not using the LDAP SSL port. Signing ensures that a malicious computer is not intercepting data.

This setting requires Windows 2003 or Windows 2000 with the most recent support pack, and Internet Explorer 5.5 SP2 or later on both servers. This enables signing and encryption on a Kerberos or NTLM authenticated connection.

Like SSL, this parameter is not available on initial import; it is set through the Driver Parameters page after installation is complete.

- ◆ **Use Sealing:** This flag enables sealing of the Active Directory connection if you are not using the LDAP SSL port. Sealing encrypts the data so that it cannot be viewed by a network monitor.

This setting requires Windows 2003 or Windows 2000 with the most recent support pack, and Internet Explorer 5.5 SP2 or later on both servers. This enables signing and encryption on a Kerberos or NTLM authenticated connection.

Like SSL, this parameter is not available on initial import; it is set through the Driver Parameters page after installation is complete.

- ◆ **Use SSL:** This parameter controls encryption if you connect to Active Directory using the LDAP SSL port. By default the parameter is set to No.

If you set this value to Yes, the SSL pipe is encrypted for the entire conversation. An encrypted pipe is preferred because the driver typically synchronizes sensitive information. However, encryption will slow the general performance of your servers.

This parameter is configurable through the Driver Parameters page after the driver has been imported.

SSL is required for subscriber password check, set, and modify. Publisher password operations are not available using simple bind. SSL is discussed further in [“SSL” on page 17](#).

Recommended Security Configurations

Using Identity Manager Remote Loader

Because authentication is dependent on several parameters such as the server support pack, your DNS infrastructure, and policy and registry settings, the most reliable means of authentication is to install the driver on the computer hosting Active Directory and then use the Remote Loader to connect to the DirXML engine, as illustrated in [Figure 3, “Dual Server Configuration \(2\),” on page 14](#). With this configuration, you will be most successful if you set the driver parameters as follows.

Authentication ID: Domain login name, for example Administrator

Authentication Context: [Blank]

Application Password: Password for the service account

Remote Loader Password: Password for the Remote Loader service

Authentication Method: Negotiate

Signing: No

Sealing: No

Use SSL: No

Insulating the Domain Controller

If you do not want to run the driver on your Active Directory domain controller, as shown in [Figure 1, “Single Server Installation,” on page 14](#) and in [Figure 4, “Triple Server Configuration,” on page 15](#), set the driver parameters as follows:

Authentication ID: NT Logon Name or Domain Qualified Name.

Authentication Context: *hostname*

Password: Password for the specified Authentication ID.

Use Signing: Yes/No, requires Windows 2003 or Windows 2000 with the most recent support pack, and Internet Explorer 5.5 SP2 or later on both servers.

Use Sealing: Yes/No, requires Windows 2003 or Windows 2000 with the most recent support pack, and Internet Explorer 5.5 SP2 or later on both servers.

Use SSL: Yes/No, SSL is required to perform subscriber password check, set, and modify using the simple authentication method.

Using SSL

SSL is recommended if you have selected the simple authentication mechanism, and is required for password synchronization.

Authentication ID: LDAP format Authentication ID

Authentication Context: IP address of domain controller

Password: Password for the specified Authentication ID

Authentication Method: Simple

Use Signing: No

Use Sealing: No

Use SSL: Yes

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*.

6

Password Synchronization

This section assumes that you are familiar with the information in “[Password Synchronization across Connected Systems](#)” in the *Novell Nsure Identity Manager 2 Administration Guide*. The information in this section is specific to this driver.

IMPORTANT: If you have used Password Synchronization 1.0 previously, don’t install the new driver shim until you have read “[Upgrading Password Synchronization 1.0 to Password Synchronization Provided with Identity Manager](#)” on page 35 and understand the implications. If you install the driver shim, you need to add backward compatibility for Password Synchronization 1.0 to your driver policies at the same time, even if you are not planning to use the Password Synchronization provided with Nsure™ Identity Manager right away.

In this section:

- ◆ “[Comparison of Password Synchronization 1.0 and Password Synchronization Provided with Identity Manager](#)” on page 33
- ◆ “[Upgrading Password Synchronization 1.0 to Password Synchronization Provided with Identity Manager](#)” on page 35
- ◆ “[New Driver Configuration and Identity Manager Password Synchronization](#)” on page 39
- ◆ “[Upgrading Existing Driver Configurations to Support Identity Manager Password Synchronization](#)” on page 40
- ◆ “[Setting Up Password Synchronization Filters](#)” on page 42
- ◆ “[Troubleshooting Password Synchronization](#)” on page 46

Comparison of Password Synchronization 1.0 and Password Synchronization Provided with Identity Manager

	Password Synchronization 1.0	Password Synchronization with Identity Manager 2
Product delivery	A product separate from DirXML.	A feature included with Identity Manager, not sold as a separate product.

	Password Synchronization 1.0	Password Synchronization with Identity Manager 2
Platforms	<ul style="list-style-type: none"> ◆ Active Directory ◆ NT Domain 	<p>Full bidirectional password synchronization is supported on these platforms:</p> <ul style="list-style-type: none"> ◆ Active Directory ◆ eDirectory ◆ NIS ◆ NT Domain <p>These connected systems support publishing user passwords to Identity Manager. Because Universal Password (and Distribution Password) is reversible, Identity Manager can distribute passwords to connected systems.</p> <p>Any connected system that supports the Subscriber password element can subscribe to passwords from Identity Manager.</p> <p>See “Connected System Support for Password Synchronization” in the <i>Novell Nsure Identity Manager 2 Administration Guide</i>.</p>
Password used in eDirectory	NDS® Password (non-reversible)	<p>Universal Password (reversible), or Distribution Password (also reversible). The NDS password can also be kept synchronized, if desired. For example scenarios, see “Implementing Password Synchronization” in the <i>Novell Nsure Identity Manager 2 Administration Guide</i>.</p>
Main functionality for Windows connected systems	<p>To send passwords to DirXML so the eDirectory password is synchronized with the Windows password. Because the NDS password is not reversible, passwords were not sent back to NT or AD.</p>	<p>To provide bi-directional password synchronization. Because Universal Password (and Distribution Password) is reversible, passwords can be synchronized in both directions.</p>
LDAP changes	Not supported.	Supported
Novell Client™	Required.	Not required.
nadLoginName attribute	Used for keeping passwords updated.	Not used.

	Password Synchronization 1.0	Password Synchronization with Identity Manager 2
The component that contains the password synchronization functionality	The DirXML driver contained the functionality for updating nadLoginName.	Policies in the driver configuration provide the password synchronization functionality. The driver simply carries out the tasks given by the DirXML engine, which come from logic in the policies. The driver manifest, global configuration values, and driver filter settings must also support password synchronization. These are included in the sample driver configurations, or can be added to an existing driver. See “Upgrading Existing Driver Configurations to Support Identity Manager Password Synchronization” on page 40.
Agents	A separate piece of software.	No agents are installed; instead, the functionality is now part of the driver.

Upgrading Password Synchronization 1.0 to Password Synchronization Provided with Identity Manager

If you are currently using Password Synchronization 1.0, complete the instructions in this section to upgrade.

IMPORTANT: Do not install the identity Manager driver shim until you have reviewed these instructions.

With the exception of one step, these instructions are the same for both NT and AD, so both drivers are mentioned throughout.

To upgrade from Password Synchronization 1.0 to Password Synchronization provided with Identity Manager:

- 1 Make sure your environment is ready to use Universal Password, including upgrading the Novell Client if you are using it in your environment. See [“Preparing to Use Identity Manager Password Synchronization and Universal Password”](#) in the *Novell Nsure Identity Manager 2 Administration Guide*.

Identity Manager Password Synchronization does not require the Novell Client to be installed on Windows machines.

- 2 Install the Identity Manager driver shim to replace the DirXML 1.x driver shim, and immediately complete [Step 3](#).

Use the installation program as described in [“Installation”](#) in the *Novell Nsure Identity Manager 2 Administration Guide*, and select only the DirXML Driver for Active Directory.

- 3 Create backward compatibility with Password Synchronization 1.0, by adding a new policy to the driver configuration as described in [“Creating Backward Compatibility with Password Synchronization 1.0 by Adding Policies” on page 37.](#)

A DirXML 1.x driver shim updates the nadLoginName attribute. The Identity Manager DirXML driver shim does not, so you must add policies to the driver configuration to update nadLoginName. This allows Password Synchronization 1.0 to function as usual when you

install the driver shim, so no password changes are missed while you finish deploying Identity Manager Password Synchronization.

IMPORTANT: If you don't do this, Password Synchronization 1.0 will continue to update existing users, but any new or renamed users will not be synchronized until you deploy Identity Manager Password Synchronization.

When you complete this step, you have the new driver shim and the policies for backward compatibility, so your driver is supporting Password Synchronization 1.0.

If you can't complete the rest of this procedure right away, you can continue to use Password Synchronization 1.0 until you are ready to finish deploying Identity Manager Password Synchronization.

- 4 Add support for Identity Manager Password Synchronization to each driver you want to participate in password synchronization, by either upgrading an existing configuration or replacing an existing configuration:

Upgrade existing configuration: Upgrade your existing DirXML 1.x driver configuration by converting it to Identity Manager format and adding the policies needed for Identity Manager Password Synchronization:

- ◆ Convert the driver to Identity Manager format using a wizard. See [“Upgrading a Driver Configuration from DirXML 1.x to Identity Manager Format”](#) in the *Novell Nsure Identity Manager 2 Administration Guide*.
- ◆ Add policies to support Identity Manager Password Synchronization. You can use an “overlay” configuration file to add the policies, driver manifest, and GCVs, all at once. You must also add an attribute to the Filter. For instructions, see [“Upgrading Existing Driver Configurations to Support Identity Manager Password Synchronization”](#) on page 40.

Replace the existing configuration with Identity Manager configuration, and add

backward compatibility again: The Identity Manager sample driver configuration contains the policies, driver manifest, GCVs, and filter settings to support Identity Manager Password Synchronization. See the instructions in this driver guide for information on importing the new driver configuration.

- ◆ If you choose to replace your existing configuration, make sure you add backward compatibility again, as described in [“Creating Backward Compatibility with Password Synchronization 1.0 by Adding Policies”](#) on page 37. The Identity Manager sample driver configuration does not contain those policies.
 - ◆ Make sure nadLoginName attribute is set to Publish and Subscribe in the filter for NT, and Publish for AD, as it was in your previous driver configuration.
- 5 Install new Password Synchronization filters and configure them if you want the connected system to provide user passwords to Identity Manager. See [“Setting Up Password Synchronization Filters”](#) on page 42.
 - 6 Set up SSL, if necessary. Instructions are contained in [“Authentication”](#) on page 16.

The ability of the driver to set a password in Active Directory (Subscriber channel) requires a secure connection provided by one of the following conditions:

- ◆ The machine running the driver is the same machine as the domain controller.
- ◆ The machine running the driver is in the same domain as the domain controller.
- ◆ The machine running the driver has SSL for LDAP set up between it and the domain controller. Bi-directional password synchronization is available only when using the negotiate authentication mechanism.

Refer to Microsoft documentation for instructions, such as [Configuring Digital Certificates on Domain Controllers](http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/secwin2k/a0701.asp) (<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/secwin2k/a0701.asp>).

NOTE: This is the only step that is required for Active Directory but not for NT Domain.

- 7** Turn on Universal Password for eDirectory user accounts by creating Password Policies with Universal Password enabled.

See “[Managing Passwords Using Password Policies](#)” in the *Novell Nsure Identity Manager 2 Administration Guide*.

We recommend that you assign Password Policies as high up in the tree as possible, to simplify administration.

- 8** Set up the scenario for Password Synchronization that you want to use, using the Password Policies and the Password Synchronization settings for the driver.

See “[Implementing Password Synchronization](#)” in the *Novell Nsure Identity Manager 2 Administration Guide*.

- 9** Test synchronization.

- 10** After Identity Manager Password Synchronization is working, remove Password Synchronization 1.0.

- 10a** Turn off Password Synchronization 1.0 by removing the agent using Add/Remove Programs.

- 10b** In the filter for the driver, change the nadLoginName attribute to Ignore.

- 10c** Remove the backward compatibility policies that are updating nadLoginName from the driver configuration.

- 10d** If desired, you can also remove the nadLoginName attribute from users after Identity Manager Password Synchronization is working, because it is no longer needed.

Creating Backward Compatibility with Password Synchronization 1.0 by Adding Policies

Password Synchronization 1.0 relies on the driver shims updating an attribute named nadLoginName. This is the attribute that indicates whether a user’s password should be synchronized. If a new user was added or the user’s name was changed, the nadLoginName attribute was added or updated to match.

The driver shims in Identity Manager no longer update this attribute because it is not necessary for Identity Manager Password Synchronization. So, after you install the new driver shim, the nadLoginName attribute is not being updated. This means that Password Synchronization 1.0 no longer receives notice of new or renamed users unless you add backward compatibility to your driver configuration.

For a smooth transition from Password Synchronization 1.0 to Identity Manager Password Synchronization, you need backward compatibility with Password Synchronization 1.0.

To create backward compatibility with Password Synchronization 1.0, you must add policies that update the nadLoginName attribute.

These policies must be added for both AD and NT drivers, and they must be added regardless of whether you are updating your existing driver configurations, or replacing them with new

configurations that ship with Identity Manager. The Identity Manager sample driver configurations for AD and NT do not include them by default.

Three policies are necessary, one each for the Subscriber Output Transformation, Publisher Input Transformation, and Publisher Command Transformation. These policies are provided with Identity Manager in a configuration file named Password Synchronization 1.0 Policies for AD and NT. The following procedure explains how to import the new policies and add them to a driver configuration.

- 1** In iManager, click DirXML Utilities > Import Drivers.

The Import Driver Wizard opens.

- 2** Select the driver set where your existing AD or NT driver resides.

- 3** In the list of driver configurations that appears, scroll to the bottom and select Legacy Password Synchronization 1.0 Policies: Backwards Compatibility for AD and NT.

It is listed under the heading Additional Policies.

- 4** Complete the import prompts:

- 4a** Select your existing AD or NT driver.

Selecting the existing driver allows you to add the three policies that are necessary. The import process creates three new policy objects, which you must then insert in the appropriate place in the driver configuration.

- 4b** Specify whether the driver is an AD or NT driver.

The policies imported have minor differences depending on which system is chosen.

- 4c** Browse for and select the nadDomain object associated with the driver you want to update.

It can normally be found under the driver object.

- 4d** (AD only) Enter the name of the NDS attribute mapped to the AD attribute sAMAccountName.

You can find this information in the Schema Mapping policy in the driver configuration.

- 5** Click Next.







Because you chose an existing driver, a page appears asking you to decide how you want the driver to be updated. In this case, you just want to update selected policies.

- 6** Select Update Only Selected Policies in That Driver, and check the check boxes for all three policies listed.



- 7** Click Next, then Finish to complete the wizard.

At this point, the three new policies have been created as policy objects under the driver object, but are not yet part of the driver configuration. To link them in, you must manually insert each of them at the right point in the driver configuration on the Subscriber and Publisher channels.

- 8** Insert each of the three new policies into the correct place on your existing driver configuration. If there are multiple policies for any of these parts of the driver configuration, make sure these new policies are listed last.

Policy Object Name	Where To Insert It
For NT driver use the following:	
PassSync(Pub)-Command Transform Policies	Command Transformation Policies on the Publisher channel 
PassSync(Pub)-Input Transform Policies	Input Transformation Policies on the Publisher channel 
PassSync(Sub)-Command Transform Policies	Command Transformation Policies on the Subscriber channel 
For Active Directory driver use the following:	
PassSync(Pub)-Command Transform Policies	Command Transformation Policies on the Publisher channel 
PassSync(Pub)-Input Transform Policies	Input Transformation Policies on the Publisher channel 
PassSync(Sub)-Output Transform Policies	Output Transformation Policies on the Subscriber channel 

Here's how to do it. Repeat these steps for each policy.

- 8a** Click DirXML Management > Overview. Select the driver set for the driver you are updating.
- 8b** Click the driver you just updated.
A page opens showing a graphical representation of the driver configuration.
- 8c** Click the icon for the place where you need to add one of the three new policies.
- 8d** Click Insert to add the new policy. In the Insert page that appears, click Use an Existing Policy and browse for the new policy object. Click OK.
- 8e** If you have more than one policy in the list for any of the three new policies, use the arrow buttons   to move the new policy down so it is last in the list.
- 9** Repeat this procedure for all your AD and NT Domain drivers.

After you have completed this procedure, the driver configurations for your AD and NT Domain drivers are backward compatible with Password Synchronization 1.0. This means Password Synchronization will continue to function as it did before, allowing you to upgrade to Identity Manager Password Synchronization at your convenience.

New Driver Configuration and Identity Manager Password Synchronization

If you are not using Password Synchronization 1.0, and you are creating a new driver or replacing an existing driver's configuration with the Identity Manager configuration, follow the instructions

in “New Driver Configuration and Identity Manager Password Synchronization” in *Novell Nsure Identity Manager 2 Administration Guide*.

In addition, do the following:

- ◆ Set up SSL, if necessary. Instructions are contained in “Authentication” on page 16.

The ability of the driver to set a password in Active Directory (Subscriber channel) requires a secure connection provided by one of the following conditions:

- ◆ The machine running the driver is the same machine as the domain controller.
- ◆ The machine running the driver is in the same domain as the domain controller.
- ◆ The machine running the driver has SSL for LDAP set up between it and the domain controller. Bi-directional password synchronization is available only when using the negotiate authentication mechanism.

Refer to Microsoft documentation for instructions, such as [Configuring Digital Certificates on Domain Controllers](http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/secwin2k/a0701.asp) (<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/secwin2k/a0701.asp>).

NOTE: This is the only step that is required for Active Directory but not for NT Domain.

- ◆ Install new Password Synchronization filters and configure them if you want the connected system to provide user passwords to Identity Manager. See “Setting Up Password Synchronization Filters” on page 42.
- ◆ Set up the scenario for Password Synchronization that you want to use, using the Password Policies and the Password Synchronization settings for the driver. See “Implementing Password Synchronization” in the *Novell Nsure Identity Manager 2 Administration Guide*.

Upgrading Existing Driver Configurations to Support Identity Manager Password Synchronization

This section explains the process for adding support for Identity Manager Password Synchronization to existing driver configurations.

IMPORTANT: If a driver is being used with Password Synchronization 1.0, you should complete this section only as part of “Upgrading Password Synchronization 1.0 to Password Synchronization Provided with Identity Manager” on page 35, not alone.

The following is an overview of the tasks you must complete, using the procedure in this section:

- ◆ Add driver manifest, global configuration values, and password synchronization policies to the driver configuration. For a list of the policies you add, see “Policies Required in the Driver Configuration” in the *Novell Nsure Identity Manager 2 Administration Guide*.
- ◆ Change the Filter to allow nspmDistributionPassword attribute to be synchronized.

Prerequisites

- Make sure you have converted your existing driver to Identity Manager format, as described in “Upgrading a Driver Configuration from DirXML 1.x to Identity Manager Format” in the *Novell Nsure Identity Manager 2 Administration Guide*.
- Create a backup of your existing driver using the Export Drivers Wizard.
- Make sure you have installed the new driver shim. Some password synchronization features such as Check Password Status won’t work without the Identity Manager driver shim.

Procedure

- 1** In iManager, click DirXML Utilities > Import Drivers.

The Import Driver Wizard opens.

- 2** Select the driver set where your existing driver resides.

- 3** In the list of driver configurations that appears, select Password Synchronization 2.0 Policies. It is listed under Additional Policies. Click Next.

A list of import prompts appears.

- 4** Select your existing driver to update.

- 5** Answer three prompts about the capabilities of the driver and the connected system.

- ◆ Whether the connected system can provide passwords to DirXML.
- ◆ Whether the connected system can accept passwords from DirXML
- ◆ Whether the connected system can check a password to see if it matches the password in DirXML.

If you are uncertain which answers to give, check the settings for your driver type that are provided with the Identity Manager sample configurations. You could create a temporary driver with the Identity Manager driver configurations, and view the settings in the driver manifest for that driver.

- 6** Click Next, then select to update everything about the driver.

This option gives you the driver manifest, global configuration values (GCVs), and password policies necessary for password synchronization.

The driver manifest and GCVs overwrite any values that already exist, but because these kinds of driver parameters are new in Identity Manager, there should be no existing values to overwrite.

The password policies don't overwrite any existing policy objects; they are simply added to the driver object.

NOTE: If you do have driver manifest or GCV values that you want to save, choose the option named Update only Selected Policies for that driver, and check the check boxes for all the policies. This option imports the password policies but does not change the driver manifest or GCVs.

- 7** Click Next, then click Finish to complete the wizard.

At this point, the new policies have been created as policy objects under the driver object, but are not yet part of the driver configuration. To link them in, you must manually insert each of them at the right point in the driver configuration on the Subscriber and Publisher channels.

- 8** Insert each of the new policies into the correct place in your existing driver configuration. If there are multiple policies in a policy set, make sure these password synchronization policies are listed last.



The list of the policies and where to insert them is in “Policies Required in the Driver Configuration” in the *Novell Nsure Identity Manager 2 Administration Guide*.

Here's how to do it. Repeat these steps for each policy.

- 8a** Click DirXML Management > Overview. Select the driver set for the driver you are updating.

- 8b** Click the driver you just updated.

A page opens showing a graphical representation of the driver configuration.

- 8c** Click the icon for the place where you need to add one of the new policies.
- 8d** Click Insert to add the new policy. In the Insert page that appears, click Use an Existing Policy and browse for the new policy object. Click OK.
- 8e** If you have more than one policy in the list for any of the new policies, use the arrow buttons   to move the new policies to the correct location in the list. Make sure the policies are in the order listed in “Policies Required in the Driver Configuration” in the *Novell Nsure Identity Manager 2 Administration Guide*.
- 9** Change the filter for the driver to allow the nspmDistributionPassword attribute to be synchronized.
- 10** Set up SSL, if necessary. Instructions are contained in “Authentication” on page 16.
- The ability of the driver to set a password in Active Directory (Subscriber channel) requires a secure connection provided by one of the following conditions:
- ◆ The machine running the driver is the same machine as the domain controller.
 - ◆ The machine running the driver is in the same domain as the domain controller.
 - ◆ The machine running the driver has SSL for LDAP set up between it and the domain controller. Bi-directional password synchronization is available only when using the negotiate authentication mechanism.
- Refer to Microsoft documentation for instructions, such as [Configuring Digital Certificates on Domain Controllers](http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/secwin2k/a0701.asp) (<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/secwin2k/a0701.asp>).
- NOTE:** This is the only step that is required for Active Directory but not for NT Domain.
- 11** Install new Password Synchronization filters and configure them if you want the connected system to provide user passwords to Identity Manager. See “Setting Up Password Synchronization Filters” on page 42.
- At this point, the driver has the new driver shim, Identity Manager format, and the other pieces that are necessary to support password synchronization: driver manifest, GCVs, password synchronization policies, and filters. Now you can specify how you want passwords to flow to and from connected systems, using the Password Synchronization interface in iManager.
- 12** Set up the scenario for Password Synchronization that you want to use, using the Password Policies and the Password Synchronization settings for the driver. See “Implementing Password Synchronization” in *Novell Nsure Identity Manager 2 Administration Guide*.
- 13** Repeat this procedure for all the drivers that you want to participate in password synchronization.

Setting Up Password Synchronization Filters

After you install the driver, you need to set up the filter to capture passwords.

The driver needs to be installed on only one Windows machine. The other domain controllers don't need the driver installed, but each domain controller does need a filter.dll file installed to capture passwords so they can be sent to Identity Manager. To simplify your setup and administration, a DirXML PassSync utility is provided that lets you do this for all domain controllers from the Windows machine where the driver is installed.

When you install the driver on a Windows machine, this utility is added to the Control Panel. The name of the utility is DirXML PassSync. The same utility is used for both NT domains and Active Directory, and it does the following things:

- ◆ Lets you specify which domain you want to participate in password synchronization.
- ◆ Automatically discovers all the domain controllers for the domain.
- ◆ Automatically installs a filter (pwfilter.dll) on each domain controller to capture password changes. This filter is automatically started when the domain controller is started. The filter captures password changes made by users through Windows clients. The filter sends the password changes to the driver, and the driver updates the Identity Manager data store.

The filter that is installed is registered to the driver. Data is synchronized among the domain controllers in the domain, eventually synchronizing with the domain controller being monitored by the driver. Password data is then synchronized with eDirectory via Identity Manager.

When passwords are changed on a participating domain controller, the filter captures the password, encrypts it, and notifies the driver. The driver then synchronizes this password via Identity Manager to eDirectory. This password can be configured to update the Universal Password in eDirectory, or the Distribution Password. For information on the difference between these two implementations, see the “[Implementing Password Synchronization](#)” in the *Novell Nsure Identity Manager 2 Administration Guide*.

- ◆ Automatically updates the registry on the machine where the driver is running and on each domain controller, to allow password changes to be captured by the filter and sent to the driver.
- ◆ Lets you view the status of the filter on each domain controller.
- ◆ Lets you reboot a domain controller from within the utility. This is necessary when you first add a domain for password synchronization, because the filter that captures password changes is a .dll file that starts when the domain controller is started.

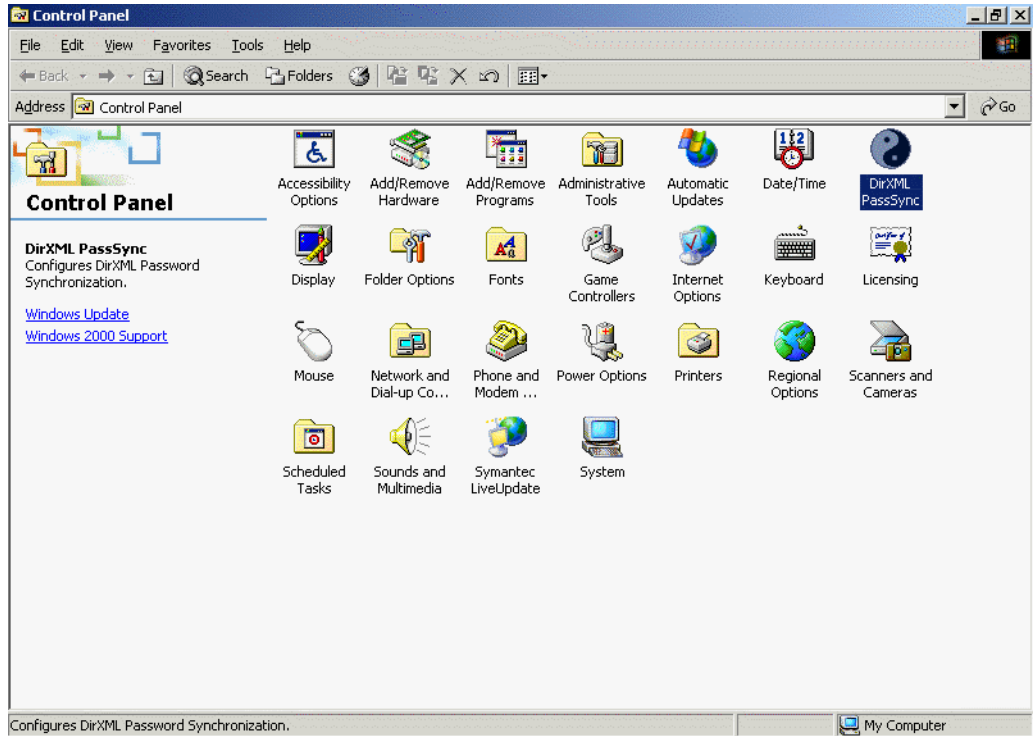
You must complete some simple steps in the DirXML PassSync utility to configure password synchronization before Identity Manager Password Synchronization will work.

(In Password Synchronization 1.0, similar tasks were accomplished using a standalone service called an agent, but in Identity Manager Password Synchronization this functionality is part of the driver.)

Setting up the filter requires a reboot of the domain controller, so you might want to perform this procedure after hours, or reboot only one domain controller at a time.

To set up Password Synchronization filters for your domain:

- 1 At the computer where the driver is installed, click Start > Settings > Control Panel.



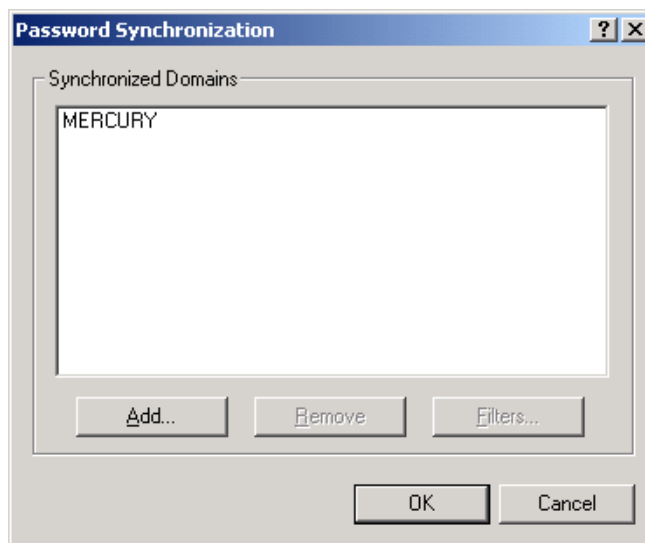
2 Double-click DirXML PassSync.

3 The first time you open the utility, it asks whether this is the machine where the DirXML driver is installed. Click Yes.

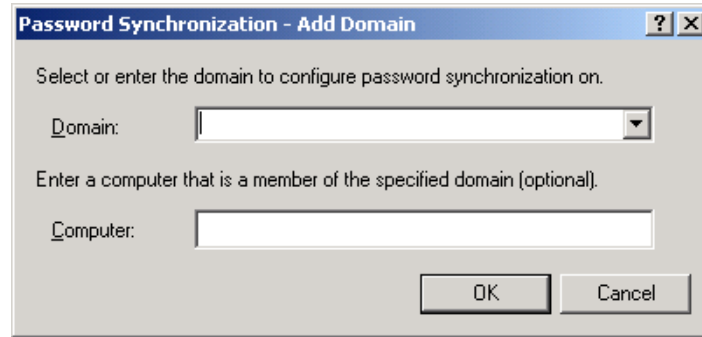
After you complete the configuration, you are not shown this prompt again unless you remove this domain from the list.

NOTE: You must use the DirXML PassSync utility on the machine where the driver is installed. The No option in this dialog box is not supported at this time.

A list appears, labeled Synchronized Domains.



- 4 To add a domain you want to participate in password synchronization, click Add and specify the domain name.



- 5 Log in with administrator rights.

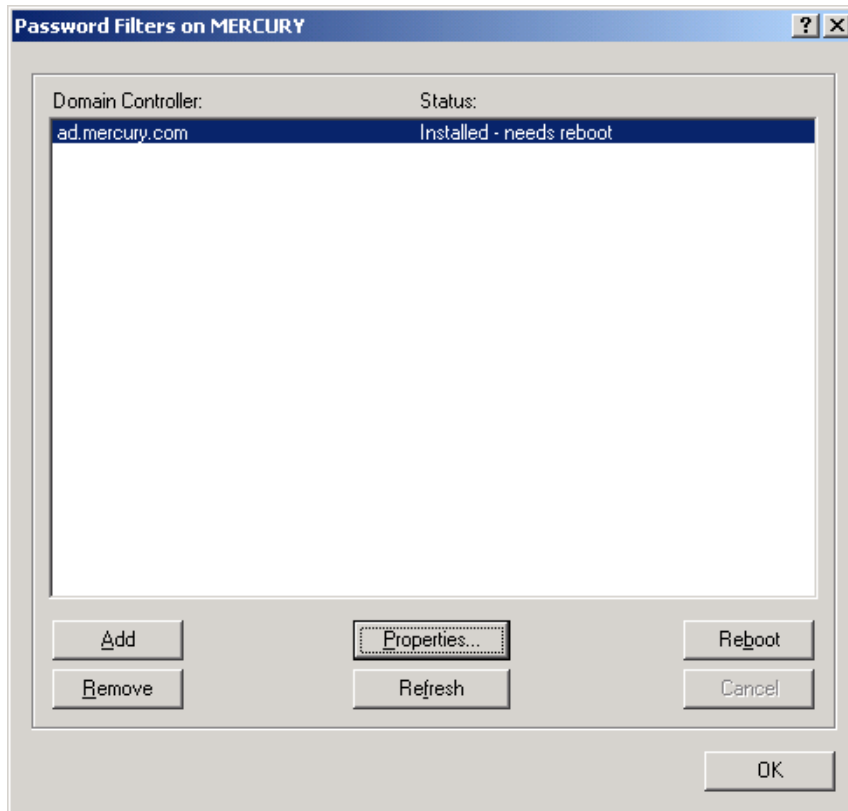
The DirXML PassSync utility discovers all the domain controllers for that domain, and installs pwfilter.dll on each domain controller. It also updates the registry on the computer where you are running the drivers, and on each domain controller. This might take a few minutes.

The pwfilter.dll doesn't capture password changes until the domain controller has been rebooted. The DirXML PassSync utility lets you see a list of all the domain controllers and the status of the filter on them. It also lets you reboot the domain controller from inside the utility.

- 6 Click the name of the domain in the list, then click Filters.

The utility displays the names of all the domain controllers and the status of the filter on each of them.

The status for each domain controller should indicate that it needs rebooting. However, it might take a few minutes for the utility to complete its automated task, and in the meantime the status might say Unknown.



7 Reboot each domain controller.

You can choose to reboot them at a time that makes sense for your environment. Just keep in mind that password synchronization won't be fully functional until every domain controller has been rebooted.

- 8** When the status for the domain controllers says Running, test password synchronization to confirm that it is working.
- 9** To add more domains, click okay to return to the list of domains, and repeat **Step 4** through **Step 8**.

Troubleshooting Password Synchronization

- ◆ The ability of the driver to set a password in Active Directory (Subscriber channel) requires a secure connection provided by one of the following conditions:
 - ◆ The machine running the driver is the same machine as the domain controller.
 - ◆ The machine running the driver is in the same domain as the domain controller.
 - ◆ The machine running the driver has SSL for LDAP set up between it and the domain controller. Bi-directional password synchronization is available only when using the negotiate authentication mechanism.

Refer to Microsoft documentation for instructions, such as [Configuring Digital Certificates on Domain Controllers](http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/secwin2k/a0701.asp) (<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/secwin2k/a0701.asp>).

- ◆ If you see an error about a password not complying when a user is initially created, but the password is set correctly in eDirectory, this might be an issue with the default password in the driver policy not conforming to the Password Policy that applies to that user.

For example, perhaps you want the Active Directory driver to provide the initial password for user when it creates a new user object in eDirectory to match a user in Active Directory. The sample configuration for the Active Directory driver sends the initial password as a separate operation than adding the user, and the sample configuration also includes a policy that provides a default password for a user, based on the user's surname, if no password is provided by Active Directory. Because adding the user and setting the password are done separately, in this case a new user always receives the default password, even if only momentarily, and it is soon updated because the Active Directory driver sends the password right after adding the user. If the default password does not comply with the eDirectory Password Policy for the user, an error is displayed. For example, if a default password created using the user's surname is too short to comply with the Password Policy, you might see a -216 error saying password is too short. However, the situation is soon rectified if the Active Directory driver then sends an initial password that does comply.

Regardless of the driver you are using, if you want a connected system that is creating user objects to provide the initial password, consider doing one of the following. These measures are especially important if the initial password does not come with the add event and instead comes in a subsequent event.

- ◆ Change the policy on the Publisher channel that creates default password, so that the default password conforms to the Password Policies (created using Password Management > Manage Password Policies) that have been defined for your organization in eDirectory. When the initial password comes from the authoritative application, it replaces the default password.

This option is preferable because Novell recommends that a default password policy exists in order to maintain a high level of security within the system.

or

- ◆ Remove the policy on the Publisher channel that creates default password. In the sample configuration, this policy is provided in the Command Transformation policy set. Adding a user without a password is allowed in eDirectory. The assumption for this option is that the password for the newly created user object eventually comes through the Publisher channel, so the user object exists without a password only for a short time.

7

Troubleshooting

This section contains troubleshooting information for the Active Directory driver.

Changes Are Not Synchronizing from Publisher or Subscriber

In order to synchronize changes in Active Directory, the account used by the DirXML driver must have the proper rights set up. See [“Rights and Privileges” on page 16](#) for a detail of the necessary rights.

If using the default policies, you must also meet the requirements for the create, match, and placement policies. See [“Policies” on page 10](#) for a detail of default policy requirements.

Using Characters Outside the Set of Valid NT Logon Names

The default subscriber creation policy generates an NT Logon Name (also known as the sAMAccountName and the Pre-Windows2000 Logon Name) based on the Relative-Distinguished Name of the account in eDirectory. The NT Logon name uses a subset of the ASCII character set. The default policy strips any character outside of the valid range before creating an object in Active Directory. This policy can be changed after import if it does not satisfy the business rules of your company. Businesses that use eDirectory account names outside of the traditional ASCII character set should pay particular attention to this policy.

Synchronizing c, co, and countryCode Attributes

When a country is selected for a user in the management console of Active Directory,* three attributes are set: c, co, and countryCode. The c attribute contains a two-character country code as defined by the ISO. The co attribute contains a longer name for the country, and countryCode contains a numeric value (also defined by the ISO) that represents the country.

By default, the schema in eDirectory includes c and co but not countryCode, because the ISO-defined numeric country codes are intended for use by applications that can't handle alpha characters.

Nsure™ Identity Manager is capable of mapping c and co. It can also map countryCode if you add a similar attribute to the eDirectory schema.

Active Directory's management console tries to keep all three of these attributes synchronized, so that when you set the country in the console, all three attributes have appropriate values. Some administrators might want a similar behavior when the attribute is set through Identity Manager. For example, you might want to configure the driver so that even though only c is in the Filter, co and countryCode are also set when a change for c is sent on the Subscriber channel.

Synchronizing Operational Attributes

Operation attributes are attributes which are maintained by an LDAP server which contains special operational information. Operation attributes are read-only, they can not be synchronized or changed.

The default driver configuration contains a method to synchronize operational attributes.

Windows 2003 Issues

Password Complexity is Enforced when Policy Items are Not Defined

In some circumstances, Windows 2003 enforces password complexity if the policy is Not Defined in either the Domain or Domain Controller.

To avoid this, make sure both group policies have values in the password policy.

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:

- ◆ “[March 17, 2004](#)” on page 51

March 17, 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.
- ◆ Updated attribute list in [Table 1, “Bitfield Aliases to userAccountControl,”](#) on page 20.

