Novell Identity Manager Driver for Active Directory*

3.0.2

www.novell.com

IMPLEMENTATION GUIDE

May 13, 2005

Novell®

Legal Notices

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

www.novell.com

Implementation Guide: Identity Manager Driver for Active Directory
May 13, 2005

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 and other countries.
DirXML is a registered trademark of Novell, Inc. in the United States and other countries.
eDirectory is a trademark of Novell, Inc.
NCP and NetWare Core Protocol are registered trademarks of Novell, Inc.
NDS and Novell eDirectory are registered trademarks 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 is a registered trademark of Novell, Inc. in the United States and other countries.
Novell Certificate Server is a trademark of Novell, Inc.
Novell Client is a registered trademark of Novell, Inc.
Nsure is a trademark of Novell, Inc.

Third-Party Materials

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

Contents

About This Guide

This guide explains how to install, configure, and manage the Identity Manager Driver for Active Directory.

In this guide:

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell® trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

User Comments

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

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

Additional Documentation

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

1 Overview

In this section:

Key Terms

Identity Manager

Novell® Nsure™ Identity Manager is a service that synchronizes data among servers in a set of connected systems by using a robust set of configurable policies. Identity Manager uses the Identify Vault to store shared information, and uses the DirXML® engine for policy-based management of the information as it changes in the vault or connected system. Identity Manager runs on the server where the Identity Vault and the DirXML engine are located.

Connected System

A connected system is any system that can share data with Identity Manager through a driver. Active Directory is a connected system.

Identity Vault

Identity Vault is a persistent database powered by eDirectory™ and used by Identity Manager to hold data for synchronization with a connected system. The vault may be viewed narrowly as a private datastore for Identity Manager or more broadly as a meta-directory that holds enterprise-wide data. Data in the vault is available to any protocol supported by eDirectory, including NCP™ (the traditional protocol used by such utilities as ConsoleOne® and iManager), LDAP, and DSML.

Because the vault is powered by eDirectory, Identity Manager can be easily integrated into your corporate directory infrastructure by using your existing directory tree as the vault.

DirXML Engine

The DirXML engine is the core server that implements the event management and policies of Identity Manager. The engine runs on the Java* Virtual Machine in eDirectory.

Active Directory Driver

A driver implements data sharing policy for a connected system. You control the actions of the driver by using iManager to define the filters and policy. For Active Directory, a driver implements policy for a single domain.

Driver Shim

A driver shim is the component of a driver that converts the XML-based Identity Manager command and event language (XDS) to the protocols and API calls needed to interact with a connected system. The shim is called to execute commands on the connected system after the Output Transform has been run. Commands are usually generated on the Subscriber channel but can be generated by command write-back on the Publisher channel.

The shim also generates events from the connected system for the Input Transform. A driver shim can be implemented either in Java class or as a native Windows* .dll file. The shim for Active Directory is ADDriver.dll.

ADDriver.dll is implemented as a native Windows .dll file. ADDriver uses several different Windows APIs to integrate with Active Directory. These APIs typically require some type of login and authentication to succeed. Also, the APIs might require that the login account have certain rights and privileges within Active Directory and on the machine where ADDriver.dll executes.

If you use the Remote Loader, ADDriver.dll executes on the server where the Remote Loader is running. Otherwise, it executes on the server where the DirXML engine is running.

Remote Loader

A Remote Loader enables a driver shim to execute outside of the DirXML engine (perhaps remotely on a different machine). The Remote Loader is typically used when a requirement of the driver shim is not met by the DirXML server. For example, if the DirXML engine is running on Linux, the Remote Loader is used to execute the Active Directory driver shim on a Windows server.

The Remote Loader is a service that executes the driver shim and passes information between the shim and the DirXML engine. When you use a Remote Loader, you install the driver shim on the server where the Remote Loader is running, not on the server where the DirXML engine is running. You can choose to use SSL to encrypt the connection between the DirXML engine and the Remote Loader.

When you use the Remote Loader with the Active Directory driver shim, two network connections exist:

- Between the domain controller and the Remote Loader
- Between Active Directory and the Active Directory driver shim

New Features

Driver Features

- Flexible prompting.

  The sample driver configuration uses a new feature, flexible prompting, to reduce complexity when importing the configuration. If you choose to install the driver for use with Remote

Loader, or if you choose to use Role-Based Entitlements, an additional page is displayed in the wizard where you provide information for those features.

- Better support for multi-valued attributes.

  See "Multi-Valued Attributes" on page 22.

- Managing the userAccountControl attribute by using a set of mapped Boolean attributes, rather than managing the integer bit settings.

  See "Managing Account Settings using Custom Boolean Attributes" on page 22.

- A new method for provisioning Exchange 2000 and Exchange 2003 mailboxes.

  See "Provisioning Exchange Mailboxes using the homeMDB Attribute" on page 23.

- Using the Identity Manager PassSync Utility to configure password filters on domain controllers individually.

  Now you don't need to allow remote access to the registry. See "Separately Configuring Password Filters on Each Domain Controller" on page 58.

- A new parameter for Password Expiration Time.

- Enhancements to the driver and password filter.

  The driver and password filter now are enhanced to retry passwords only after a successful user add or modify is received. See "Retrying Synchronization after a Failure" on page 61

- Support for Windows 2003 Server.

- Support for Nsure Identity Manager Password Synchronization.

  For instructions specific to Active Directory, see Chapter 7, "Password Synchronization," on page 43.

  See also the description of the different scenarios in "Implementing Password Synchronization" in *Novell Nsure Identity Manager 2.0.1 Administration Guide*.

- Support for Role-Based Entitlements.

  See "Using Role-Based Entitlements" in *Novell Nsure Identity Manager 2.0.1 Administration Guide*.

- Providing a driver heartbeat.

  You can customize the driver to provide a driver heartbeat. See "Adding Driver Heartbeat" in the *Novell Nsure Identity Manager 2.0.1 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 2.0.1 Administration Guide*.

Data Transfers Between Systems

Publisher and Subscriber Channels

The Active Directory driver supports Publisher and Subscriber channels.

The Publisher channel does the following:

- Reads events from Active Directory for the domain hosted on the server that the driver shim is connecting to.
- Submits that information to the Identity Vault.

The Subscriber channel does the following:

- Watches for additions and modifications to Identity Vault objects.
- Makes changes to Active Directory that reflect those changes.

You can configure the driver so that both Active Directory and the Identity Vault are allowed to update a specific attribute. In this configuration, the most recent change determines the attribute value, except in the case of merge operations that are controlled by the filters and merge authority.

Default Driver Configuration

Data Flow

Policies

Policies control data synchronization between Active Directory and an Identity Vault.

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 lists these options and how they affect policies and filters that are created:

Option	Description
Configure Data Flow: Bi-Directional Bi-Directional AD to eDirectory eDirectory to AD	Configure Data Flow establishes the filters on the Publisher and Subscriber channels. Bidirectional enables the same filters on both channels. Both channels receive the same set of default objects and attributes. AD to eDirectory places a restrictive filter so that attribute changes are not sent from the Identity Vault to Active Directory. eDirectory to AD places a restrictive filter so that attribute changes are not sent from Active Directory to the Identity Vault.
Publisher Placement: Mirrored Mirrored Flat	Publisher Placement controls how objects are placed in the Identity Vault. Mirrored places objects in the Identity Vault in the same hierarchy as they exist in Active Directory. Flat places all objects in the base container in the Identity Vault specified during configuration.
Subscriber Placement: Mirrored Mirrored Flat	Subscriber Placement controls how objects are placed in Active Directory. Mirrored places objects in Active Directory in the same hierarchy as they exist in the Identity Vault. Flat places all objects in the base container in Active Directory specified during configuration.

The following table lists default policies and describes how selections during configuration affect the polices:

Policy	Description
Create	In either the mirrored or flat hierarchy, you must define Full Name to create an Active Directory user as a user in the Identity Vault.
Matching	In a mirrored hierarchy, the matching policy attempts to match an object in the same position in the hierarchy. In a flat hierarchy, the matching policy attempts to match the user with an object that has the same Full Name in the base container that you specify.
Placement	In a mirrored hierarchy, the placement policy places all objects in a hierarchy that mirrors the hierarchy of the data store sending the operation. In a flat hierarchy, the placement policy places all objects in the base container that you specify.

Schema Mapping

The following Identity Vault user, group, and Organizational Unit attributes are mapped to Active Directory user and group attributes.

The mappings listed in the tables are default mappings. You can remap same-type attributes.

Attributes Mapped for All Classes

eDirectory	Active Directory
CN	cn
Description	description
Facsimile Telephone Number	facsimiletelephoneNumber
Full name	displayName
Given Name	givenName
Initials	initials
Internet EMail Address	mail
L	physicalDeliveryOfficeName
Locality	locality
Login Disabled	dirxml-uACAccountDisabled
Login Expiration Time	accountExpires
Physical Delivery Office Name	l
Postal Code	PostalCode
Postal Office Box	postOfficeBox
S	st

eDirectory	Active Directory
SA	streetAddress
See Also	seeAlso
Surname	sn
Telephone Number	telephoneNumber
Title	title

eDirectory's L attribute is mapped to Active Directory's physicalDeliveryOfficeName attribute, and eDirectory's Physical Delivery Office Name attribute is mapped to Active Directory's L attribute. Because similarly named fields have the same value, mapping the attributes this way enable the attributes to work well with ConsoleOne and the Microsoft* Management Console.

Attributes Mapped for Users

eDirectory	Active Directory
CN	userPrincipalName cn
DirXML-ADAliasName	sAMAccountName
Login Allowed Time Map	logonHours

Mapped Organizational Unit Attributes

eDirectory	Active Directory
Organizational Unit	organizationalUnit
OU	ou

2 Preparing Active Directory

In this section:

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 Active Directory (AD) driver and on the target domain controller.
- Active Directory domain controller DNS name or IP address, depending on the authentication method.

Also, we recommend that the server hosting the Active Directory driver be a member of the Active Directory domain. This is required to provision Exchange mailboxes and synchronize passwords. If you don't require these features, the server can be a member of any domain as long as the Simple (simple bind) authentication mode is used.

Planning Your Installation

You can install the Active Directory driver on either the domain controller or a member server. Before you start the driver installation, determine

- Where to install the Active Directory driver shim
- How to address security issues

Where To Install the Active Directory Driver and Shim

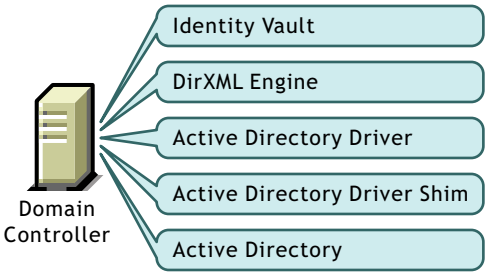
The Active Directory driver shim must run on one of the supported Windows platforms. However, you don't need to install the DirXML engine on this same machine. Using a Remote Loader, you can separate the engine and the driver shim, allowing you to balance the load on different machines or accommodate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

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 Identity Manager (where the DirXML engine and

the Identity Vault are located), Identity Manager calls the driver shim directly. If you choose to install the driver shim on another machine, you must use the Remote Loader.

The driver itself is installed the same way in each of the scenarios. See Chapter 4, “Configuring the Active Directory Driver,” on page 33.

Scenario 1

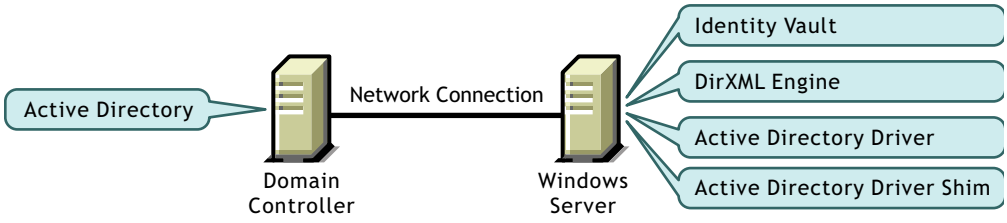


A single Windows domain controller can host Identity Vault, the DirXML engine, and the driver.

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 Identity Vault and the DirXML engine on the domain controller increases the overall load on the controller and increases the risk that the controller might fail. Because domain controllers play a critical role in Microsoft networking, 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.

Scenario 2

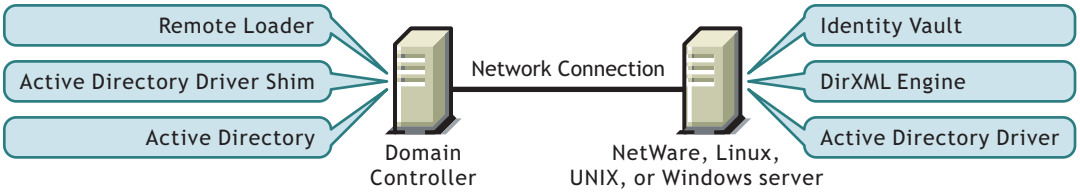


You can install the Identity Vault, the DirXML engine, and the driver on a separate computer from the Active Directory domain controller. This configuration leaves the domain controller free of any Identity Manager software.

This configuration is attractive if corporate policy disallows running the driver on your domain controller.

Scenario 3

You can install the Remote Loader and driver shim on the Active Directory domain controller, but install the Identity Vault and the DirXML engine on a separate server.

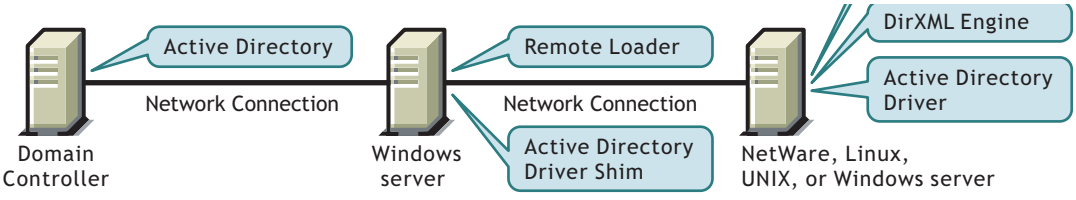


This configuration is attractive if your Identity Vault and DirXML engine (Identity Manager) installations are on a platform other than one of the supported versions of Windows.

Both Scenario 2 and Scenario 3 configurations eliminate the performance impact of hosting the Identity Vault and the DirXML engine on the domain controller.

Scenario 4

If you have platform requirements and domain controller restrictions in place, you can use a three-server configuration.



This configuration is more complicated to set up, but it accommodates the constraints of some organizations. In this figure, the two Windows servers are member servers of the domain.

Addressing Security Issues

This section discusses the security issues you must consider before installing the Active Directory driver.

The major factors to consider are authentication, encryption, and use of the Remote Loader. If you have Windows 2003 or Windows 2000 SP3 or later, consider a security option called signing. See “Use Signing” in “Security Parameters” on page 39.

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. When implementing your driver and when upgrading components, pay close attention to security.

Authentication Methods

Authentication identifies the driver shim to Active Directory and, potentially, the local machine. To authenticate to Active Directory, you can use either the Negotiate method or the Simple (simple bind) method.

Authentication Method	Description	Advantages	Disadvantages
Negotiate	The preferred method. Uses Kerberos*, NTLM, or a pluggable authentication scheme if one is installed.	The driver can be installed on any server in the domain.	The server hosting the driver must be a member of the domain.
Simple	Used when the server hosting the driver shim is not a member of the domain.	The driver can be installed on a server that is not a member of the domain.	Some provisioning services are unavailable, such as Exchange mailbox provisioning and password synchronization.

Encryption

SSL encrypts data. Depending on your configuration, SSL can be used in two places:

- Between the Active Directory driver and the domain controller
- Between the Identity Vault and the Remote Loader running the Active Directory driver

Password synchronization occurs between Active Directory and the Identity Vault (eDirectory). You need to make sure that you use SSL with any communication that goes across the network.

If the DirXML engine, Identity Vault, the Active Directory driver, and Active Directory are on the same machine, you don't need SSL. Communication isn't going across the network.

However, if you are accessing Active Directory remotely by using an Active Directory driver shim on a member server, you need to set up SSL between the Active Directory driver shim and Active Directory. You do this by setting the SSL parameter to Yes on the driver configuration. See Step 5 on page 20, in the "SSL Connection Between the Active Directory Driver and the Domain Controller" topic.

If you are using the Remote Loader on the Domain Controller, you need to set up SSL between the DirXML/Identity Manager engine and the Remote Loader. For additional information on SSL and Remote Loaders, see "Setting Up a Connected System" in the Novell Nsure Identity Manager 2.0.1 Administration Guide.

The following table outlines where SSL connections can be used for each of the scenarios discussed in "Planning Your Installation" on page 15:

Configuration	SSL Connections Available
Single-Server	No SSL connections are necessary.
Two-Server: Identity Manager and the Active Directory driver are on the same server	An SSL connection can be established between the Active Directory driver and the domain controller.
Dual-Server: Identity Manager is on one server but the Active Directory driver is on a separate server	An SSL connection can be established between Identity Manager and the Remote Loader running the Active Directory driver.
Three-Server	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

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.

Setting Up a Certificate Authority

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 that the issuing certificate authority of this certificate chains to.

If you do not have a certificate authority in your organization, you must establish one. Novell, Microsoft, and several other third parties provide the tools necessary to do this. Establishing a certificate authority is beyond the scope of this guide. For more information, see

- Novell Certificate Server™ 2.5 Administration Guide (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)

Creating, Exporting, and Importing Certificates

After you have a certificate authority, for LDAP SSL to operate successfully, the LDAP server must have the appropriate server authentication certificate installed. Also, 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.

1. Generate a certificate that meets the following Active Directory LDAP service requirements:
   - 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 appears in one of the following places:
  - The Common Name (CN) in the Subject field.
  - DNS entry in the Subject Alternative Name extension.
- The 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 that the issuing CA chains to.

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). Consult this document for the latest requirements and additional information.

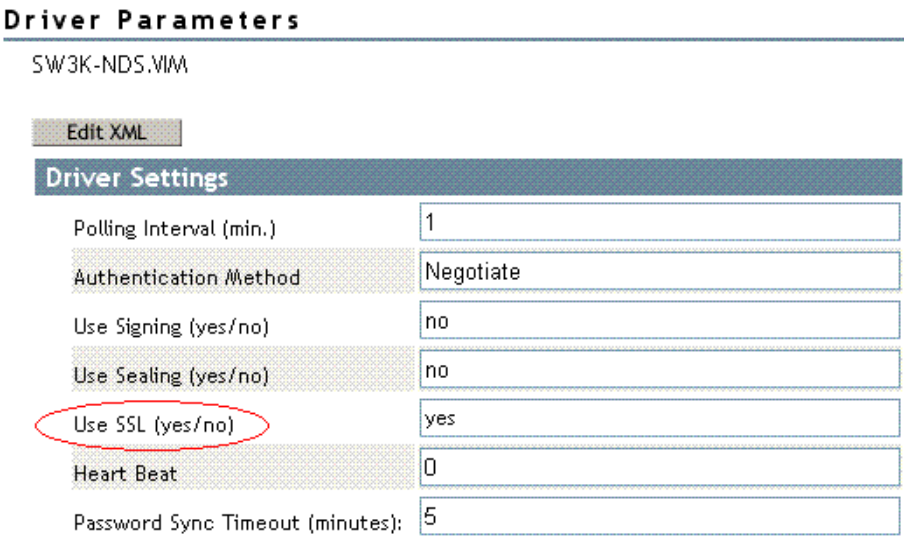
2. Export this certificate in one of the following standard certificate file formats supported by Windows 2000:
   - Personal Information Exchange (PFX, also called PKCS #12)
   - Cryptographic Message Syntax Standard (PKCS #7)
   - Distinguished Encoding Rules (DER) Encoded Binary X.509
   - Base64 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)
   - HOW TO: Install Imported Certificates on a Web Server in Windows 2000 (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 that issued the certificate.

   The server hosting the driver shim must trust the root certificate authority that the issuing certificate authority chains to.

   For more information on 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

If you are using the Remote Loader, you need to set up SSL between the DirXML/Identity Manager engine and the Remote Loader, plus the settings between the driver and Active Directory.

For information on establishing an SSL connection between the Remote Loader and Identity Manager, see "Setting Up Remote Loaders" in the *Novell Nsure Identity Manager 2.0.1 Administration Guide*.

Creating an Administrative Account

In a test environment, use the Administrator account until you get the Active Directory driver working. Then create an administrative account, which has the proper rights (including restricted rights), that the Active Directory driver can use exclusively 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. Therefore, you must change this password whenever the account password changes. If you change the account password without updating the driver configuration, authentication fails 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.

To instrument Exchange mailboxes, your Identity Manager account must have “Act as part of the Operating System” permission for the logon account.

Windows 2003 requires that you have additional rights in order to see deleted objects. See Appendix A, “Changing Permissions on the CN=Deleted Objects Container,” on page 71.

Becoming Familiar with Driver Features

This section discusses 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.

However, when the Active Directory driver synchronizes a a multi-valued attribute with a single-valued attribute, the multi-valued attribute is treated as single-valued. For example, the Telephone Number attribute is single-valued in Active Directory, and multi-valued in Identity Vault. When this attribute is synchronized from Active Directory, only a single value is stored in Identity Vault.

This creates true synchronization and mapping between the two attributes, but can result in a potential loss of data if you have multiple values in an attribute that is mapped to an attribute with a single value. In most cases, a policy can be implemented to preserve the extra values in another location if required in your environment.

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, the Active Directory driver took a shortcut that let you map userAccountControl to 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. 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 because each bit can be used as a Boolean, the bit can be enabled individually in the Publisher filter and accessed easily. You can also put userAccountControl into the Publisher filter to receive change notification as an integer.

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

The following table lists available aliases and hexadecimal values. Read-only attributes cannot be set on the Subscriber channel.

Alias	Hexadecimal	Notes
dirxml-uACDontExpirePassword	0x10000	Read-write
dirxml-uACHomedirRequired	0x0008	Read-write
dirxml-uACInterdomainTrustAccount	0x0800	Read-only
dirxml-uACNormalAccount	0x0200	Read-only
dirxml-uACServerTrustAccount	0x2000	Read-only
dirxml-uACWorkstationTrustAccount	0x1000	Read-only
dirxml-uACAccountDisable	0x0002	Read-write
dirxml-uACPasswordNotRequired	0x0020	Read-write

For troubleshooting tips relating to the userAccountControl attribute, see "Active Directory Account Disabled after a User Add on the Subscriber Channel" on page 68.

Provisioning Exchange Mailboxes using the homeMDB Attribute

Options for provisioning Exchange 2000 and Exchange 2003 mailboxes have changed from version 2.

In Version 2, Exchange provisioning was accomplished by setting attributes on User objects. A Microsoft program (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 (CDOEXM) has been added. With CDOEXM enabled, an Exchange mailbox is provisioned by setting the homeMDB attribute. When the homeMDB attribute is set, the driver automatically sets all required attributes.

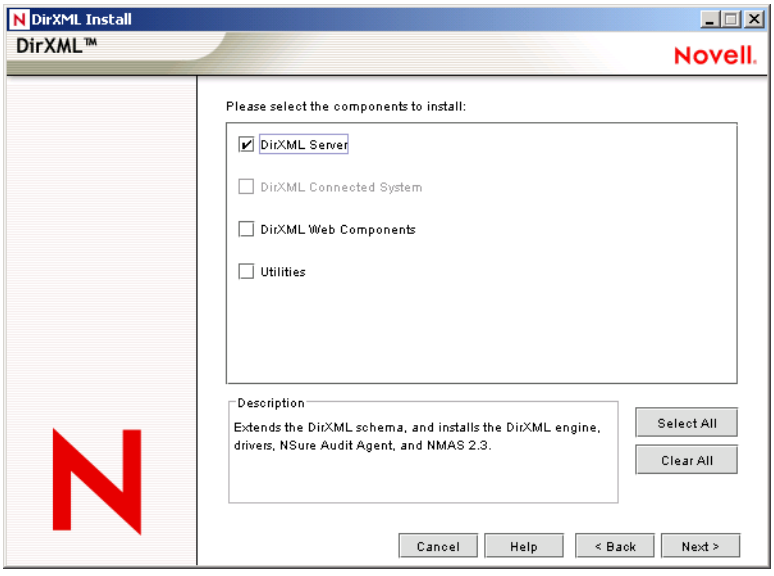
The homeMDB attribute is set during initial configuration, but you can change the setting by modifying the driver policy. For a discussion of this parameter, see "Configuration Parameters" on page 34.

3 Installing the Active Directory Driver

In this section:

Overview: Basic Steps

The following figure illustrates options that you can select when installing Identity Manager.



Option	Description
DirXML Server	Installs the DirXML engine and Identity Manager
DirXML Connected System	Installs the Remote Loader
DirXML Web Components	Installs the preconfigured (example) driver configuration file
Utilities	Installs the Active Directory Discovery Tool

Installing the Active Directory driver shim requires three basic steps:

Step	What to Select during Installation
1. Install the Active Directory driver shim on the DirXML engine server or the Remote Loader server.	Select the DirXML Server or DirXML Connected System option. See "Installing the Active Directory Driver Shim" on page 26.
2. Install the preconfiguration import file for Active Directory on the iManager server.	Select the DirXML Web Components option. See "Installing Preconfiguration Import Files" on page 29.
3. Install the Active Directory Discovery Tool on a workstation used to configure Identity Manager.	Select the Utilities option. See "Installing the Active Directory Discovery Tool" on page 30.

Typically, you install the Active Directory driver components when you install the DirXML server (or Remote Loader) and Web components. However, you can install them later.

Installing the Active Directory Driver Shim

In this section:

Installing the Shim on a DirXML Server

1. On the server where the Identity Vault and the DirXML engine are running, launch the Identity Manager installation.

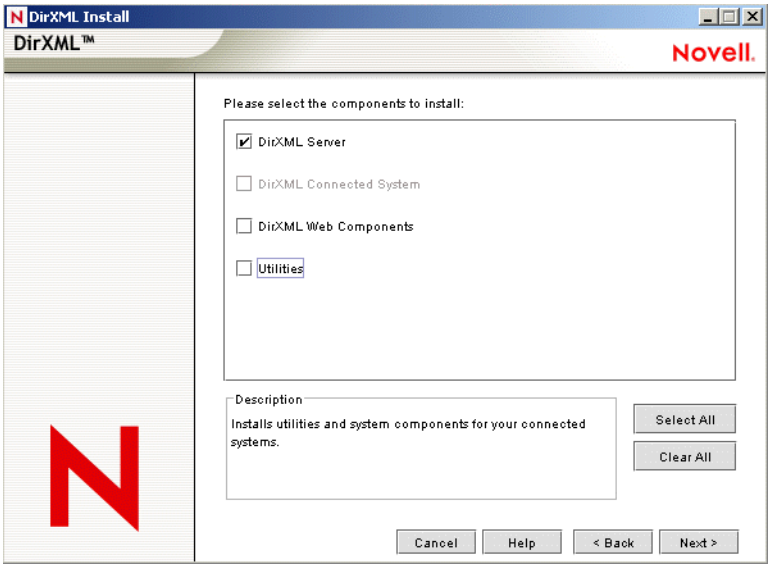
   Run the installation program from the Identity Manager CD or the download image.
2. In the Welcome dialog box, click Next, then accept the license agreement.
3. In the first DirXML Overview dialog box, review information, then click Next.

   The dialog box provides information on the following:

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

   The dialog box provides information on the following:

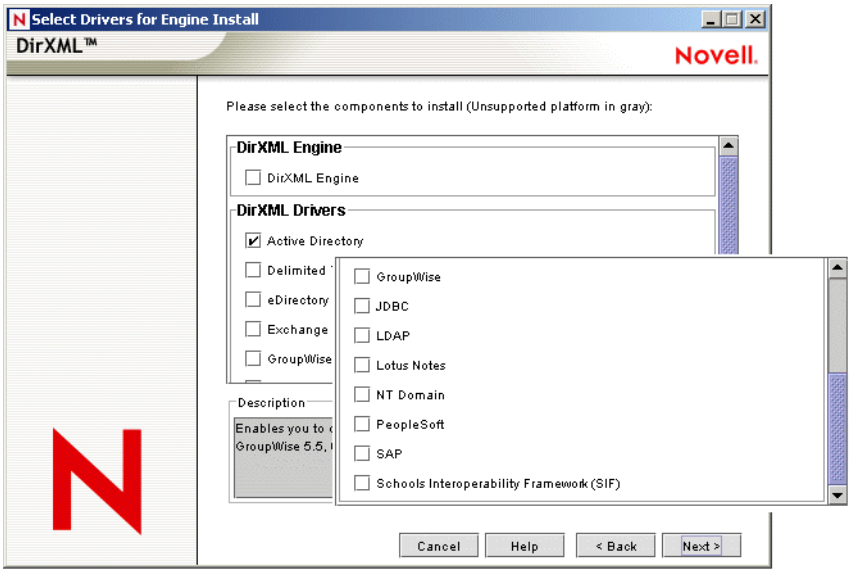
   - A Web-based administration server
   - DirXML utilities
5. In the Please Select the Components to Install dialog box, select DirXML Server, then click Next.



If iManager 2.0.2 is already installed on this machine, and if you prefer to install the iManager plug-ins and configuration files at this time, also select DirXML Web Components.

If you prefer to install the Active Directory Management tool at this time, also select Utilities.

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



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

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

9 Review the selected options, then click Finish.

10 Click Close.

Installing the Shim on a Remote Loader

This option enables you to install the Active Directory driver shim to run on a server that is separate from the server running the DirXML engine.

1. On the server where the Remote Loader is running, launch the Identity Manager installation.

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

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

3. In the first DirXML Overview dialog box, review information, then click Next.

   The dialog box provides information on the following:

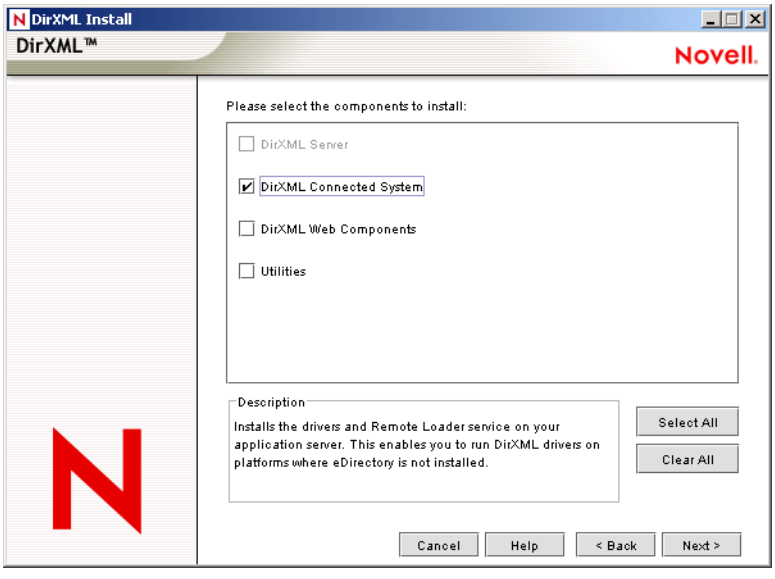
   - A DirXML server
   - A DirXML connected server system

4. In the second DirXML Overview dialog box, review information, then click Next.

   The dialog box provides information on the following:

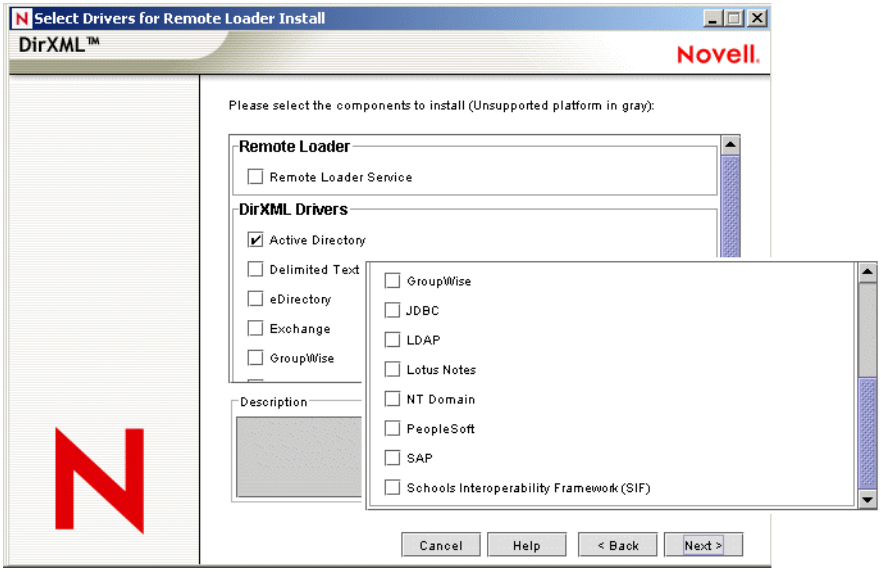
   - A Web-based administration server
   - DirXML utilities

5. In the Please Select the Components to Install dialog box, deselect DirxXML Server and other options, select DirXML Connected System, then click Next.



6. Specify the installation path, then click Next.

7. In the Select Drivers for Engine Install dialog box, select only Active Directory, then click Next.



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

9 In the Password Sync Upgrade Warning dialog box, click OK.

10 Review the selected options, then click Finish.

11 Click Close.

Installing Preconfiguration Import Files

This option installs the plug-ins to Identity Manager and the preconfigured (example) driver configurations. After installing the files, you use iManager to import the Active Directory preconfigured file into a driver set and configure the driver.

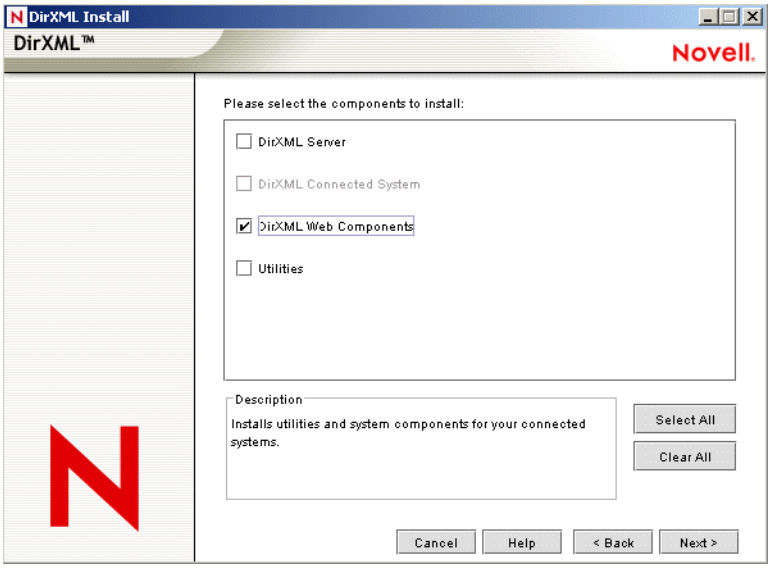
You might have already installed these files, when you installed the DirXML engine or Remote Loader. To install the files separately:

1 On the server where iManager is installed, launch the Identity Manager installation.

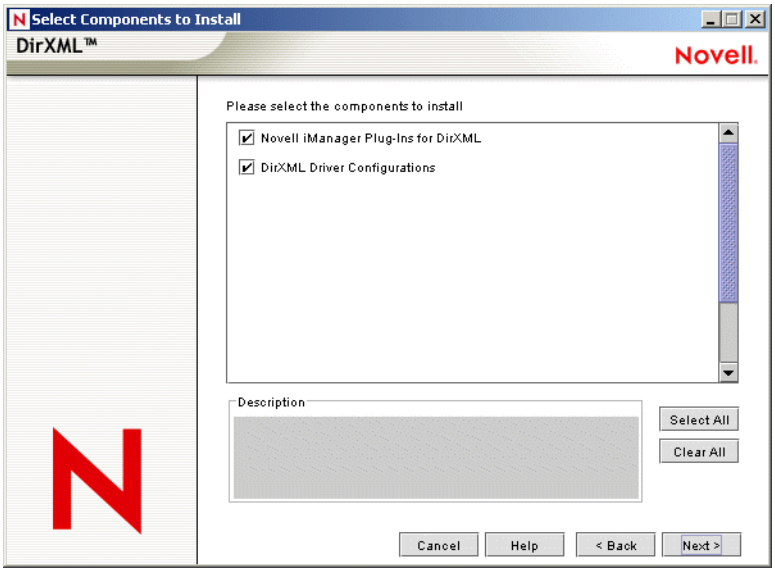
2 In the Welcome dialog box, click Next, then accept the license agreement.

3 In the two DirXML Overview dialog boxes, review information, then click Next.

4 In the Please Select the Components to Install dialog box, deselect all options except DirXML Web Components, then click Next.



5 Select DirXML Driver Configurations, then click Next.



You can install the driver configuration files when you install the Novell iManager plug-ins, or you can install the files separately.

6 Review the selected options, then click Finish.

7 Click Close.

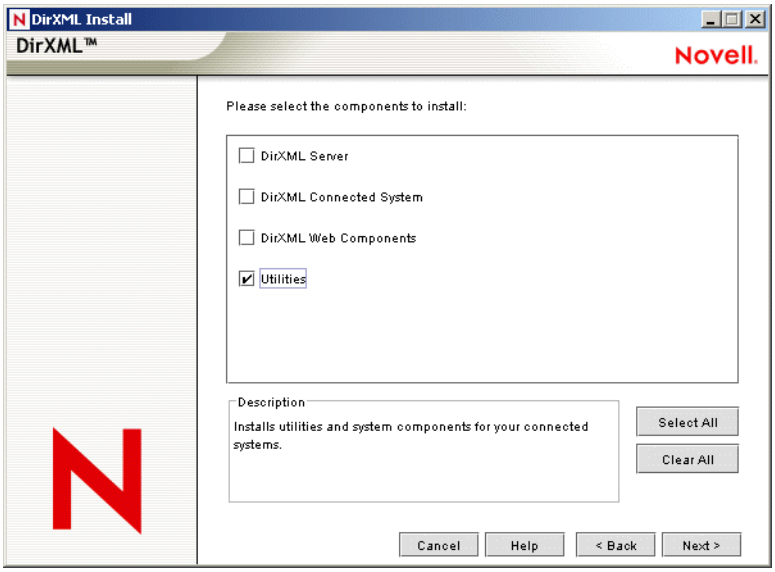
Installing the Active Directory Discovery Tool

1 On the workstation that you use to configure Active Directory, launch the Identity Manager installation.

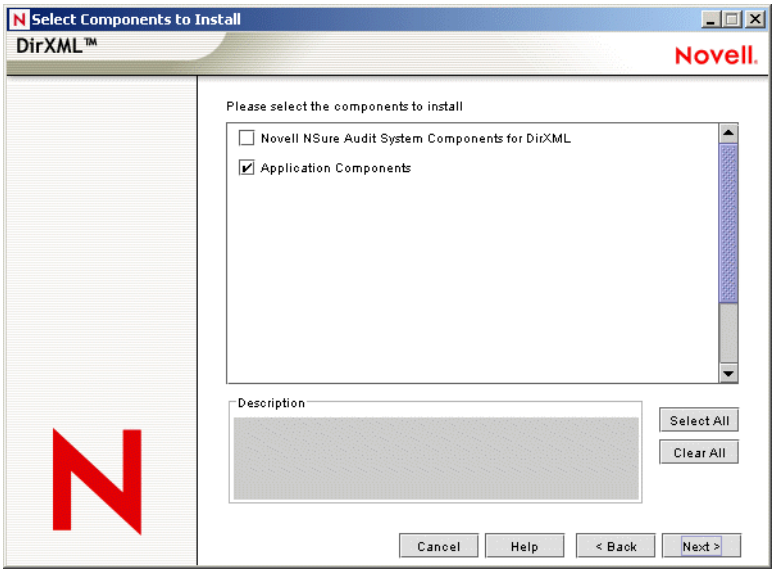
2 In the Welcome dialog box, click Next, then accept the license agreement.

3 In the two DirXML Overview dialog boxes, review information, then click Next.

4 In the Please Select the Components to Install dialog box, deselect all options except Utilities, then click Next.



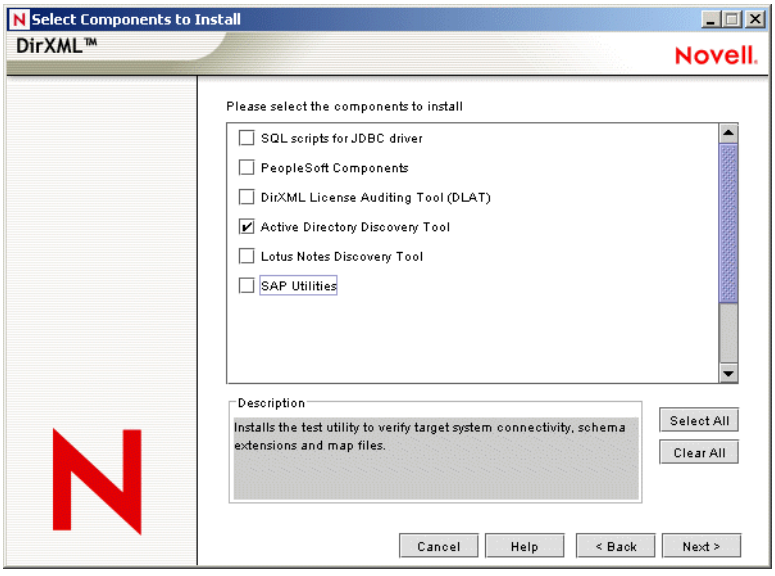
5 Select Application Components, then click Next.



Deselect Novell Nsure Audit System Components for DirXML.

6 Specify the installation path, then click Next.

7 Select only Active Directory Discovery Tool, then click Next.



8 Review the selected options, then click Finish.

9 Click Close.

4 Configuring the Active Directory Driver

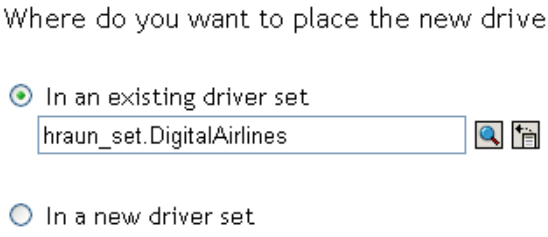
In Novell® iManager, the Create Driver Wizard helps you import a basic driver configuration for Active Directory. This wizard creates and configures the objects needed to make the driver work properly. For details on using this wizard, see "Creating and Configuring a Driver " in the *Novell Nsure Identity Manager 2.0.1 Administration Guide*.

In this section:

Importing the Active Directory Preconfiguration File

The Active Directory preconfiguration file is an example configuration file. You installed this file when you installed the DirXML Web components on an iManager server. Think of the preconfiguration file as a template that you import and customize or configure for your environment.

1. In iManager, select DirXML Utilities > Import Drivers.
2. Select a driver set, then click Next.



   If you place this driver in a new driver set, you must specify a driver set name, context, and associated server.

3. Select the Active Directory driver, then click Next.

4. Configure the driver by using the Active Directory driver wizard.

   For information on the settings, see "Configuration Parameters" on page 34.

Configuration Parameters

The following table explains the parameters you must provide during initial driver configuration:

Field	Description
Driver Name	The eDirectory™ object name to be assigned to this driver. Because each Active Directory domain requires a separate driver, you should include the domain name in your driver name.
Authentication Method	The method to authenticate with Active Directory. Negotiate is the preferred method. Select Negotiate to use the Microsoft security package to negotiate authentication. To use Negotiate, the server hosting the driver must be a member of the domain. If you plan to use password synchronization and are running on a member server, you need SSL. Select Simple to use an LDAP simple bind. If you select Simple, SSL is recommended. Simple bind doesn't support password synchronization or Exchange provisioning.
Authentication ID	An Active Directory account with administrative privileges to be used by Identity Manager. The name form used depends on the selected authentication mechanism. For Negotiate, provide the name form required by your Active Directory authentication mechanism. For example: ◆ Administrator - AD Logon Name ◆ Domain/Administrator - Domain qualified AD Logon Name For Simple, provide an LDAP ID. For example: ◆ cn=DirXML,cn=Users,DC=domain,dc=com
Authentication Password	Enter the password for the user account specified in Authentication ID.
Authentication Server	The name of the Active Directory domain controller to use for synchronization. For example, for the Negotiate authentication method, use the DNS name mycontroller.domain.com. For the Simple authentication method, you can use the IP address of your server (for example, 10.10.128.23 or the DNS name). If no value is specified, localhost is used. **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 39.
Domain Name (in LDAP format)	The Active Directory domain managed by this driver. The driver requires LDAP formatted domain names `dc=mydomain,dc=com`
Domain DNS Name (DNS format)	The DNS name of the Active Directory domain managed by this driver. The driver requires DNS formatted domain names `mydomain.com`

Field	Description
Driver Polling Interval	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. **IMPORTANT:** The polling interval affects system performance. A low polling interval results in frequent searches and fast updates of data. A high polling interval results in periodic bursts of traffic. Although a low polling interval has a greater overall cost, the cost is spread more evenly over time. If you set the interval to 0 (zero), you get a ten-second poll rate.
Password Sync Timeout	The number of minutes the driver attempts to synchronize a password. Set the value large enough to handle whatever temporary backlog of passwords exists. If you are doing bulk changes, set the timeout large enough to handle all the changes. The rule of thumb is to allow one second per password. For example, to synchronize 18,000 passwords, allow 300 minutes (18,000 passwords divided by 60 seconds). A setting of -1 is indefinite. Although this setting can handle bulk changes, it can cause problems. For example, a password might never be able to synchronized because the account wasn't associated. Such a password would therefore remain in the system forever. A number of similar situations could result in a large inventory of unsynchronized passwords held by the system. You must set the password sync timeout to at least three times the polling interval.
Base container in eDirectory	Specify the base container in eDirectory in dot format. New users are placed in this container by default. For example, users.myorg If the container doesn't exist, you must create it before you start the driver.
Base container in Active Directory	Specify the base container in Active Directory, in LDAP format. New users are placed in this container by default. For example, CN=Users,DC=MyDomain,DC=com If the target container doesn't exist, you must create it before you start the driver. If you are creating or using a container other than Users in Active Directory, the container is an OU, not a CN.
Configure Data Flow	Bidirectional means that both Active Directory and eDirectory are authoritative sources of the data synchronized between them. AD to eDirectory means that AD is the authoritative source. eDirectory to AD means that eDirectory is the authoritative source. This selection is used to determine how the default policies and filters are created.

Field	Description
Publisher Placement	Choose Mirrored to place objects hierarchically within the base container. Choose Flat to place objects strictly within the base container. This selection is used to build the default Publisher channel placement rules.
Subscriber Placement	Choose Mirrored to place objects hierarchically within the base container. Choose Flat to place objects strictly within the base container. This selection is used to build the default Subscriber channel placement rules.
Password Failure Notification User	If a password update fails, you can send an e-mail notification to a specified user. Browse to and select the user.
Support Exchange 2000/ 2003	To include additional polices to support Exchange 2000/2003, select Yes.
Default Exchange MDB (Exchange Only)	The default Exchange Message Database (MDB). This setting displays only if you set Support Exchange 2000/2003 to Yes.
Enable Entitlements	Enable this if you are also using the Entitlements Service driver and want this driver to use Role-Based Entitlements. 1. Install an Entitlements driver. 2. Install the Active Directory driver. 3. Enable entitlements.
Action - Add Account Entitlement (Entitlements Only)	Action taken when a User account is added by Entitlements. This setting displays only if you set Enable Entitlements to Yes.
Action - Remove Account Entitlement (Entitlements Only)	Action taken when a User account is removed by Entitlements. This setting displays only if you set Enable Entitlements to Yes.
Driver is Local/Remote	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	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. This setting displays only if you set Driver is Local/Remote to Remote.
Driver Password	The Remote Loader uses the Driver Object Password to authenticate itself to the Identity Manager server. The password must be the same password that is specified as the Driver object password on the Remote Loader. This setting displays only if you set Driver is Local/Remote to Remote.
Remote Password	The Remote Loader password is used to control access to the Remote Loader instance. The password must be the same password that is specified as the Remote Loader password on the Remote Loader. This setting displays only if you set Driver is Local/Remote to Remote.

5 Upgrading the Active Directory Driver

In this section:

Checklist for Upgrading

To upgrade the Active Directory driver, use the following checklist. If you are not an expert with Identity Manager, you might want to engage a capable consultant.

- ❑ To use Password Synchronization 2.0, add the driver manifest and password policies.

  See Upgrading an Existing Driver Configuration to Support Identity Manager Password Synchronization (http://www.novell.com/documentation/dirxml20/index.html?page=/documentation/dirxml20/admin/data/bo16oyy.html).

- ❑ For continued use of Password Synchronization 1.0, add legacy polices to the existing driver configuration.

  See Upgrading Password Synchronization 1.0 to Password Synchronization Provided with Identity Manager (http://www.novell.com/documentation/dirxmldrivers/index.html?page=/documentation/dirxmldrivers/ad/data/bnwjt02.html).

- ❑ Remove the structured formatting of the sAMAccountName in the existing driver's style sheets.

  sAMAccountName was a structured attribute in the DirXML® 1.1a Active Directory 2.0 driver. In the new Active Directory 3.0 driver, it is a string.

  Old format:

```
   <value type="structured">
    <component name="nameSpace">0</component>
    <component association-ref="XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
name="volume"/>
    <component name="path">jsmith</component>
   </value>
```

  New format:

```
  <add-attr attr-name="sAMAccountName">
   <value type="string">jsmith</value>
  </add-attr>
```

- ❑ Upgrade driver configuration parameters.

  We recommend the use of the following settings by default:

```
<?xml version="1.0"?>
<driver-config name="Active Directory Driver">
```

```
    <driver-options>
       <pollingInterval display-name="Polling Interval (min.)"
       id="100">1</pollingInterval>
       <auth-method display-name="Authentication Method"
       id="101">Negotiate</auth-method>
       <signing display-name="Use Signing (yes/no)" id="102">no</signing>
       <signing display-name="Use Signing (yes/no)" id="102">no</signing>
       <use-ssl display-name="Use SSL (yes/no)" id="104">no</use-ssl>
       <pub-heartbeat-interval display-name="Heart Beat" id="105">0</
       pub-heartbeat-interval>
       <pub-password-expire-time display-name="Password Sync Timeout
       (minutes):" id="106">60</pub-password-expire-time>
       <use-CDOEXM display-name="Use CDOEXM for Exchange (yes/no)"
       id="107">no</use-CDOEXM>
    </driver-options>
</driver-config>
```

- Convert the authentication ID to either the Sam Account Name (for example, jsmith) or the domain name/account name format (for example, *domain*/jsmith).
- Change the mapping of the Login Disabled attribute from userAccountControl to dirxml-uACAccountDisable.
- If you are provisioning Exchange accounts, change the driver parameter for CDOEXM to Yes, then remove the following four hard-coded attributes from your existing driver configuration style sheets:
  - msExchHomeServerName
  - legacyExchangeDN
  - homeMTA
  - msExchMailboxSecurityDescriptor

Addressing the Login Disabled Value

eDirectory™ treats a lack of Login Disabled = true as being the same as Login Disabled = false. Therefore, if you install the version 3 Active Directory driver as a new installation (not an upgrade), and if a Login Disabled = false value isn't present, a default policy on the Creation Rule synthesizes that value.

Upgrading from the version 2 driver to the version 3 driver doesn't get this policy default.

6 Managing the Active Directory Driver

In this section:

Security Parameters

During installation, the driver gathers the necessary information and creates default security policies and parameters. Before you begin customizing your Active Directory driver, you should become familiar with the following:

- Default policies and parameters
- The topics discussed in Chapter 8, "Troubleshooting," on page 65, to decide whether any of these issues apply to your environment

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

- **Authentication ID:** The account that the driver uses to access domain data.

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

- **Authentication Context:** The context used to access domain data.

Format	Example	Method
The DNS name of the Active Domain controller	mycontroller.mydomain.com	Negotiate
The DNS name of the Active Domain controller, or the IP address of your LDAP server	mycontroller.mydomain.com 137.65.134.83	Simple

- **Application Password:** The password for the Authentication ID account.
- **Use Signing:** This parameter is for use between the Active Directory driver and Active Directory, but not between the DirXML engine and the Remote Loader. Signing ensures that

a malicious computer is not intercepting data. This flag enables signing of the Active Directory connection if you are not using the LDAP SSL port.

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 on a Kerberos or NTLM v2 authenticated connection.

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

- **Use Sealing:** This parameter is for use between the Active Directory driver and Active Directory, but not between the DirXML engine and the Remote Loader. Sealing encrypts the data so that it cannot be viewed by a network monitor. This flag enables sealing of the Active Directory connection if you are not using the LDAP SSL port.

  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 setting enables encryption on a Kerberos or NTLM v2 authenticated connection.

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

- **Use SSL:** This parameter is for use between the Active Directory driver and Active Directory. This parameter controls encryption if you connect to Active Directory by using the LDAP SSL port. This parameter applies to both the Negotiate and Simple authentication methods.

  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 slows the general performance of your servers.

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

Recommended Security Configurations

Using the Identity Manager Remote Loader

Recommended settings:

Parameter	Description
Authentication ID	The domain logon name, for example Administrator
Authentication Context	The DNS name of the domain controller If you don't want to run the driver on your Active Directory domain controller, use *hostname* for the Negotiate method but use *hostname* or the IP address for the Simple method.
Application Password	The password used for the authentication account
Remote Loader Password	The password for the Remote Loader service
Authentication Method	Negotiate
Use Signing	No. Requires Windows 2003 or Windows 2000 with the most recent support pack, and Internet Explorer 5.5 SP2 or later on both servers.

Parameter	Description
Use Sealing	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. SSL is required to perform Subscriber password check, set, and modify when the driver shim isn't running on the domain controller.

Using SSL

SSL is recommended if you have selected the Simple authentication mechanism because Simple authentication passes passwords in clear text.

Parameter	Description
Authentication ID	LDAP format Authentication ID
Authentication Context	IP address of domain controller
Password	The password for the specified Authentication ID
Use Signing	No
Use Sealing	No.
Use SSL	Yes

Managing Groups

The Active Directory group class defines two types of groups and three scopes for membership in the group. Type and scope are controlled by the groupType attribute which can be set via Identity Manager policy when a group is created in Active Directory and changed by modifying the attribute.

A group holds a collection of object references. The Distribution Group type gives no special rights or privileges to its members and is commonly used as a distribution list for Exchange. The Security Group type is a security principal. Its members receive the rights and privileges of the group. Security Groups have a pre-Windows 2000 logon name (samAccountName) and a Security Identifier (SID) that can be used in Security Descriptor (SD) Access Control Lists (ACL) on other objects to grant or deny rights and privileges to its members.

Group scope controls whether an object from a foreign domain can be a member of the group and also whether the group itself can be a member of another group. The three scopes are Domain Local, Global and Universal. How these scopes behave, or whether the scope is valid at all, depend on whether Active Directory is operating in Windows 2000 Mixed, Windows 2000 Native or Windows 2003 mode.

In general, Domain Local groups can hold references to objects anywhere in the forest but can be assigned permissions only within the domain. Global groups are the opposite. They can only hold references to objects within the domain but can be assigned permissions throughout the forest. Universal groups can hold references and can be assigned permissions throughout the forest. But Universal groups come with their own restrictions and performance issues. Groups should be created and used in conformance with Microsoft recommendations.

The groupType attribute is a 32-bit integer whose bits define type and scope. Groups can have only a single scope at any given time.

GroupType Attribute	Scope	Bits That Define Type and Scope
GROUP_TYPE_GLOBAL_GROUP	Distribution	0x00000002
GROUP_TYPE_DOMAIN_LOCAL_GROUP	Distribution	0x00000004
GROUP_TYPE_UNIVERSAL_GROUP	Distribution	0x00000008
GROUP_TYPE_SECURITY_ENABLED	Security	0x80000000

Activating the Driver

Activate the driver within 90 days of installation. After the 90-day trial period has expired, the driver won't start without the proper activation credential. Events that occur when the driver isn't activated are processed upon activation and subsequent start of the driver.

For activation information, refer to "Activating Novell Identity Manager Products" in the *Novell Nsure Identity Manager 2.0.1 Administration Guide*.

7 Password Synchronization

This section assumes that you are familiar with the information in "Password Synchronization across Connected Systems" in the *Novell Nsure Identity Manager 2.0.1 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 45 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:

For information on troubleshooting password synchronization, see "Tips on Password Synchronization" on page 67.

Comparing Password Synchronization 1.0 and Password Synchronization Provided with Identity Manager

Functionality	In Password Synchronization 1.0	In 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.

Functionality	In Password Synchronization 1.0	In Password Synchronization with Identity Manager 2
Platforms	• Active Directory • NT Domain	Full bidirectional password synchronization is supported on these platforms: • Active Directory • eDirectory™ • NIS • NT Domain These connected systems support publishing user passwords to Identity Manager. Because Universal Password and Distribution Password are reversible, Identity Manager can distribute passwords to connected systems. Any connected system that supports the Subscriber password element can subscribe to passwords from Identity Manager. See "Connected System Support for Password Synchronization" in the *Novell Nsure Identity Manager 2.0.1 Administration Guide*.
Password used in eDirectory	NDS® Password (non-reversible)	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 *Novell Nsure Identity Manager 2.0.1 Administration Guide*.
Main functionality for Windows connected systems	To provide bidirectional password synchronization so that the eDirectory password is synchronized with the Windows password. However, each workstation requires the Novell Client.	To provide bidirectional password synchronization. Because Universal Password and Distribution Password are reversible, passwords can be synchronized in both directions. Accomplished within the Identity Manager Publisher and Subscriber channels.
LDAP password changes	Not supported.	Supported.
Novell Client™	Required.	Not required.
nadLoginName attribute	Used for keeping passwords updated.	Not used.

Functionality	In Password Synchronization 1.0	In 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 an Existing Driver Configuration to Support Identity Manager Password Synchronization" on page 50.
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.

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.

   See "Preparing to Use Identity Manager Password Synchronization and Universal Password" in the *Novell Nsure Identity Manager 2.0.1 Administration Guide*.

   Enabling Universal Password doesn't automatically cause password changes in both systems. Universal Password synchronization starts working only after users change their passwords.

   Scenario: Universal Password. At DigitalAirlines, network administrator Sandy enables Universal Passwords. User Markus logs in and changes his password. The Universal Password for Markus is set on both systems. However, user Marie logs in but doesn't change her password. She continues to log in by using her unchanged password. Universal Password functionality for Marie isn't set until she changes her password.

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 2.0.1 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 47.

A DirXML 1.*x* driver shim updates the nadLoginName attribute, but the Identity Manager DirXML driver shim doesn't. Therefore, 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 create backward compatibility, Password Synchronization 1.0 continues to update existing users, but any new or renamed users can't be synchronized until you deploy Identity Manager Password Synchronization.

After you complete this step, you have the new driver shim and the policies for backward compatibility. Therefore, 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.

Either upgrade an existing configuration or replace 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 2.0.1 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 an Existing Driver Configuration to Support Identity Manager Password Synchronization" on page 50.

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 47. The Identity Manager sample driver configuration does not contain those policies.
- Make sure the nadLoginName attribute is set to Publish, 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 53.

6 Set up SSL, if necessary.

For instructions, see "Addressing Security Issues" on page 17.

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 not in the domain requires the Simple method and SSL set up between it and the domain controller. Bidirectional 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).

7. Turn on Universal Password for Identity Vault user accounts by creating Password Policies with Universal Password enabled.

   See "Managing Passwords by Using Password Policies" in the *Novell Nsure Identity Manager 2.0.1 Administration Guide*.

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

8. Using the Password Policies and the Password Synchronization settings for the driver, set up the scenario that you want to use for Password Synchronization.

   See "Implementing Password Synchronization" in the *Novell Nsure Identity Manager 2.0.1 Administration Guide*.

9. Test password synchronization.

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

    10a Using Add/Remove Programs, turn off Password Synchronization 1.0 by removing the agent.

    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 attribute 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. Therefore, 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 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 Active Directory do not include the policies 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 Active Directory. 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 Drivers Wizard opens.

2. Select the driver set where your existing Active Directory driver resides.

3. In the list of driver configurations that appears, scroll to the Additional Policies section and select Legacy Password Synchronization 1.0 Policies: Backwards Compatibility for Active Directory.

4. Complete the import prompts:

   4a. Select your existing Active Directory 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 Active Directory 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. (Active Directory only) Specify the name of the NDS attribute mapped to the Active Directory 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 select the check boxes for all three policies listed.

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

   At this point, the three new policies have been created as Policy objects under the Driver object, but they aren't 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 any of these parts of the driver configuration has multiple policies, make sure these new policies are listed last.

Policy Object Name	Where To Insert It
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 

Repeat these steps for each policy.

8a Click DirXML Management > Overview.

8b Select the driver set for the driver you are updating.

8c Click the driver you just updated.

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

8d Click the icon for the place where you need to add one of the three new policies.

8e Click Insert to add the new policy.

In the Insert page that appears, click Use an Existing Policy, browse for the new policy object, then click OK.

8f 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 Active Directory drivers.

After you have completed this procedure, the driver configurations for your Active Directory drivers are backward compatible with Password Synchronization 1.0. This means Password Synchronization continues 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 2.0.1 Administration Guide*.

In addition, do the following:

- Set up SSL, if necessary. See "Addressing Security Issues" on page 17.

  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 not in the domain requires the Simple method and SSL set up between it and the domain controller. Bidirectional 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).

- 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 53.
- 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 2.0.1 Administration Guide*.

Upgrading an Existing Driver Configuration to Support Identity Manager Password Synchronization

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 45, 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 2.0.1 Administration Guide*.
- Change the filter to allow Subscriber notify and Publisher ignore on the nspmDistributionPassword attribute.

Prerequisites

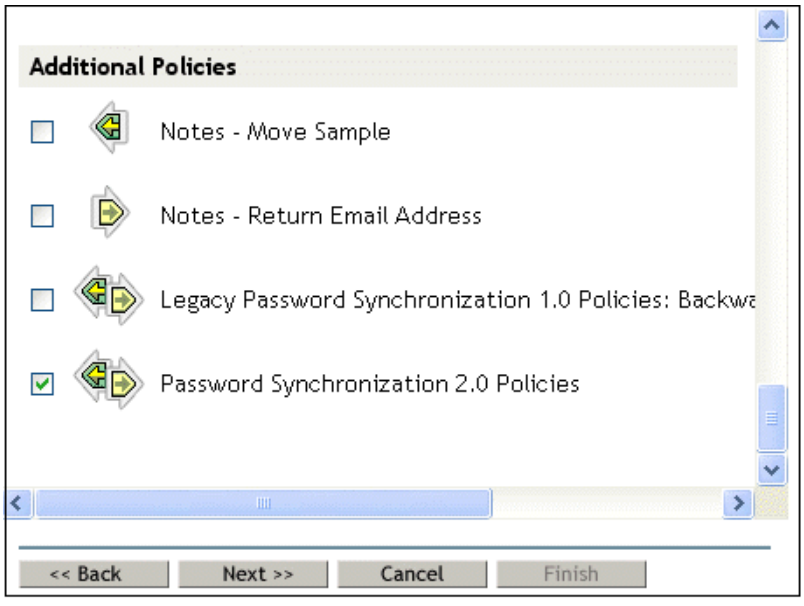
- ❑ Make sure you have converted your existing driver to Identity Manager format, as described in "Upgrading a Driver Configuration from DirXML 1.x to Identity Manager Format"in the *Novell Nsure Identity Manager 2.0.1 Administration Guide*.
- ❑ Create a backup of your existing driver using the Export 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

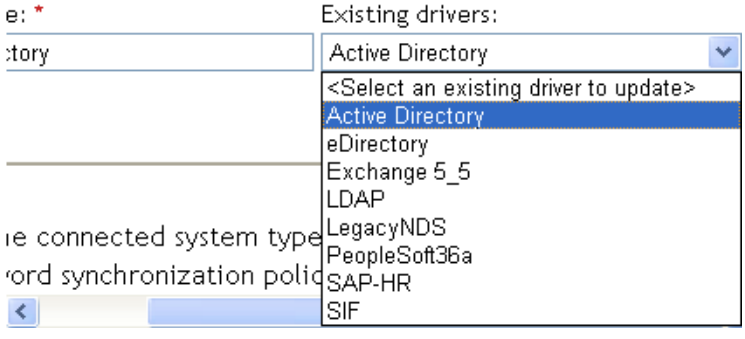
1. In iManager, click DirXML Utilities > Import Drivers.

   The Import Drivers Wizard opens.

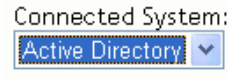
2. Select the driver set where your existing driver resides, then click Next.
3. In the list of driver configurations that appears, select Password Synchronization 2.0 Policies, then click Next.



4 Select Active Directory from the drop-down list.



5 Select Active Directory as the connected system, then click Next.



6 Answer yes to 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.

7 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.

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 select the check boxes for all the policies. This option imports the password policies but doesn't change the driver manifest or GCVs.

8 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. However, the new policies aren't 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.

9 Insert each of the new policies into the correct place in your existing driver configuration.

If a policy set has multiple policies, 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 2.0.1 Administration Guide*.

Repeat these steps for each policy.

9a Click DirXML Management > Overview, then select the driver set for the driver you are updating.

9b Click the driver you just updated.

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

9c Click the icon for the place where you need to add one of the new policies.

9d Click Insert to add the new policy.

In the Insert page that appears, click Use an Existing Policy, browse for the new policy object, then click OK.

9e 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 2.0.1 Administration Guide*.

10 Change the filter for the driver to allow the nspmDistributionPassword attribute to be synchronized.

Enable Notify on the Subscriber channel only. Set the Publisher channel to Ignore.

11 Set up SSL, if necessary.

Instructions are contained in "Addressing Security Issues" on page 17.

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 not in the domain requires the Simple method and SSL set up between it and the domain controller. Bidirectional 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).

12 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 53.

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.

13 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 2.0.1 Administration Guide*.

14 Repeat this procedure for all the drivers that you want to participate in password synchronization.

Setting Up Password Synchronization Filters

The driver needs to be configured to run on only one Windows machine.

However, after you install and configure the driver, do the following on each of the other domain controllers:

1 Install a password filter (pwfilter.dll file).

2 Configure the registry to capture passwords so that passwords can be sent to Identity Manager.

The password filter is automatically started when the domain controller is started. The filter captures password changes that users make by using Windows clients, encrypts the changes, and sends them to the driver to update the Identity Manager data store.

NOTE: For information about configuring Password Synchronization, see "Implementing Password Synchronization" in the *Novell Nsure Identity Manager 2.0.1 Administration Guide*.

To simplify your setup and administration of password filters, a DirXML PassSync utility is added to the Control Panel when the driver is installed. This utility gives you two choices for setting up the password filters, depending on whether you are willing to allow remote access to the registry on your domain controllers:

- **If you allow remote access to the registry:** From the single machine where you plan to run the driver, configure the password filter for all the domain controllers, using the DirXML PassSync utility.

  This method lets you configure all the domain controllers from one place.

  If you configure all the domain controllers from one machine, the DirXML PassSync utility provides the following features to help you during setup:

  - Lets you specify which domain you want to participate in password synchronization.
  - Automatically discovers all the domain controllers for the domain.
  - Lets you remotely install the pwfilter.dll on each domain controller.

- Automatically updates the registry on the machine where the driver is running and on each domain controller.
- Lets you view the status of the filter on each domain controller.
- Lets you reboot a domain controller remotely.

  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.

See "Configuring Password Filters for All Domain Controllers from One Machine" on page 54.

- **If you don't allow remote access to the registry:** Set up the password filters on each domain controller separately. To do this, go to each domain controller, install the driver files so you have the DirXML PassSync utility, and use the utility on each machine to install the password filter and update the registry.

  See "Separately Configuring Password Filters on Each Domain Controller" on page 58.

Configuring Password Filters for All Domain Controllers from One Machine

This procedure explains how to install and configure the password filter on each domain controller, all from the same machine where you are running the driver.

Use this method if you allow remote access to the registry.

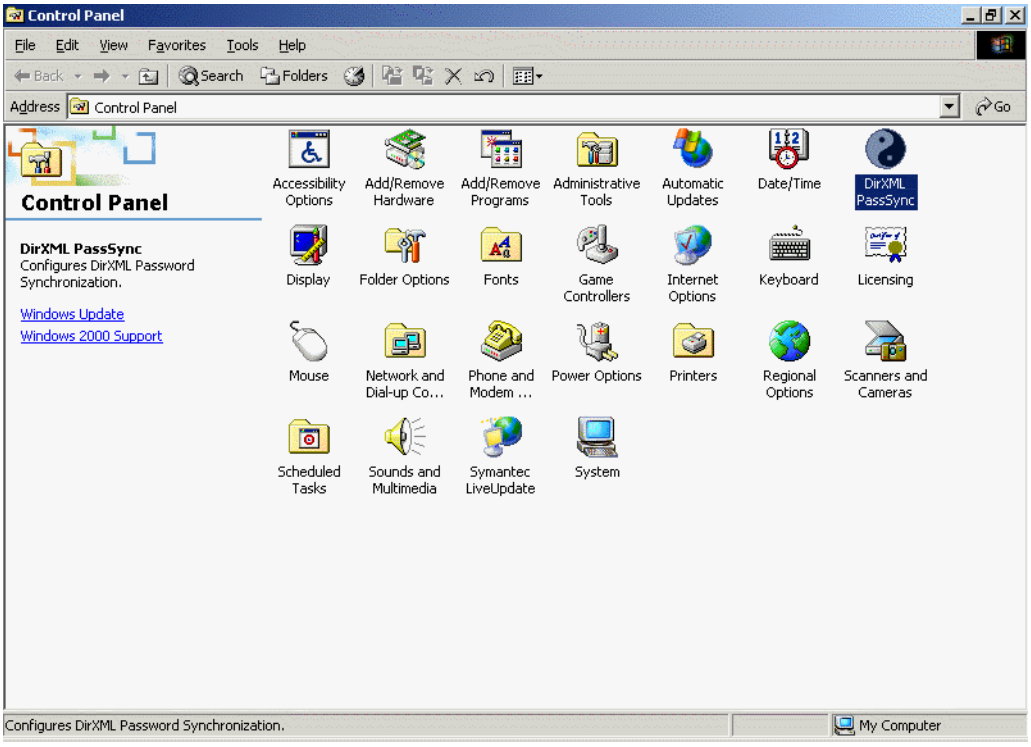
Because setting up the filter requires rebooting the domain controller, you might want to perform this procedure after hours, or reboot only one domain controller at a time. If the domain has more than one domain controller, keep in mind that each domain controller where you want Password Synchronization to function must have the filter installed and must be rebooted.

1. Confirm that port 135 (the RPC endpoint mapper) is accessible on the domain controllers and on the machine where the DirXML Driver for Active Directory is configured to run.

   If you are using NetBIOS over TCP, you also need these ports:

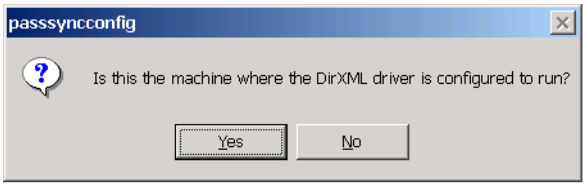
   - 137: NetBIOS name service
   - 138: NetBIOS datagram service
   - 139: NetBIOS session service

   A firewall could prevent the ports from being accessible remotely.
2. At the computer where the driver is installed, click Start > Settings > Control Panel.



3 Double-click DirXML PassSync.

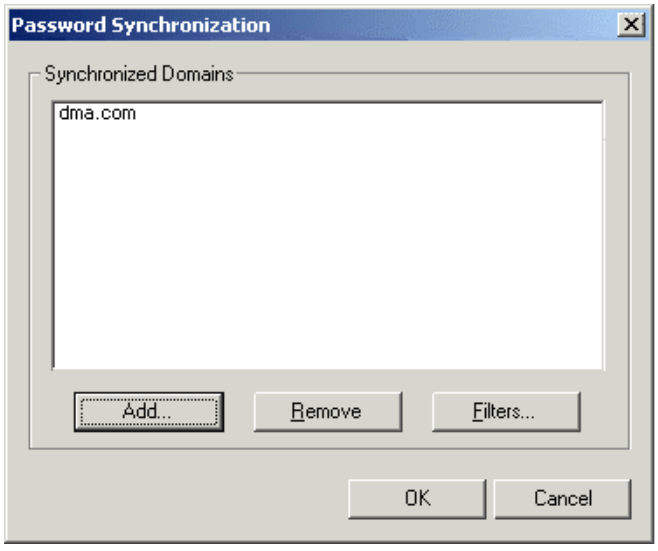
The first time you open the utility, it asks whether this is the machine where the DirXML driver is installed.



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

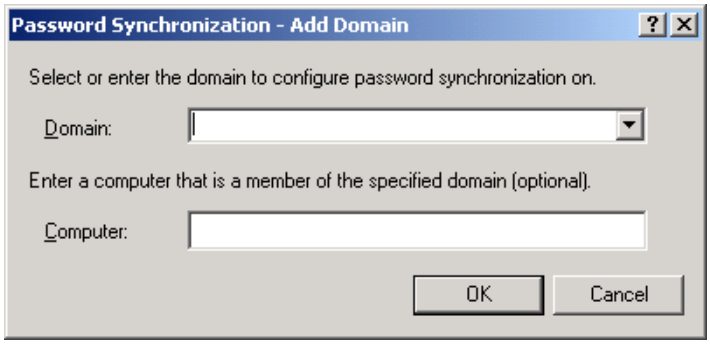
4 Click Yes.

A list appears, labeled Synchronized Domains.

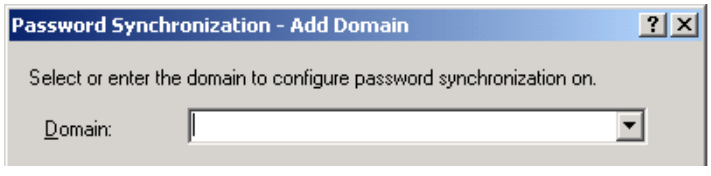


5 To add a domain that you want to participate in password synchronization, click Add.

The Add Domain dialog box appears.

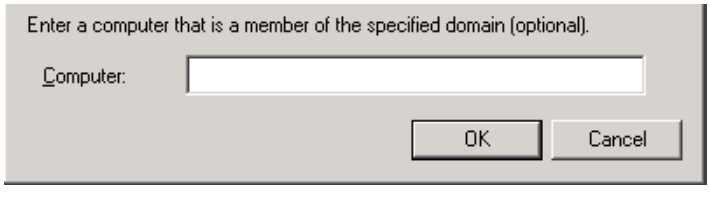


6 Specify or select the domain name that you want to add.



The drop-down list displays known domains.

7 (Optional) Specify a computer in the domain.



If you leave the Computer edit box blank, PassSync queries the local machine. Therefore, if you are running PassSync on a domain controller, you don't need to enter a name. PassSync queries the local machine (in this case, a domain controller) and gets (from the database) the list of all domain controllers in the domain.

If you aren't installing on a domain controller, enter the name of a computer that is in the domain and that can get to a domain controller.

If you receive an error message indicating that PassSync can't locate a domain, enter a different name.

8. Decide whether to use the domain's DNS name.

   The DNS name provides more advanced authentication and the ability to more reliably discover domains in bigger installations. However, the choice depends on your environment.

9. Log in with administrator rights.

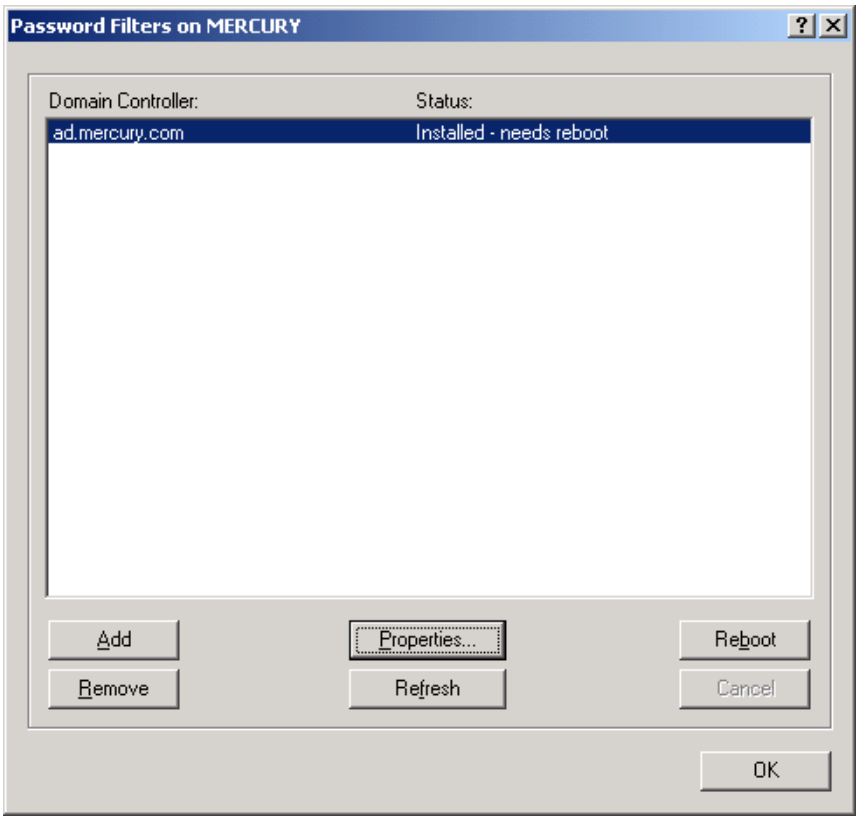
   The DirXML PassSync utility discovers all the domain controllers for that domain, and installs pwfilter.dll on each domain controller. It also updates the registry on the computer where you are running the drivers, and on each domain controller. This might take a few minutes.

   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.

10. 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.



11 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.

12 When the status for all domain controllers says Running, test password synchronization to confirm that it is working.

13 To add more domains, click OK to return to the list of domains, and repeat Step 6 through Step 12.

Separately Configuring Password Filters on Each Domain Controller

This procedure explains how to install and configure the password filter on each domain controller, one at a time.

Use this method if you don't want to allow remote access to the registry.

In this procedure, you install the driver so that you have the DirXML PassSync utility. Then you use the utility to install the pwfilter.dll file, specify the port to use, and specify which host machine is running the DirXML Driver for Active Directory.

Because setting up the filter requires rebooting the domain controller, you might want to perform this procedure after hours, or reboot only one domain controller at a time. If a domain has more than one domain controller, keep in mind that each domain controller where you want Password Synchronization to function must have the filter installed and must be rebooted.

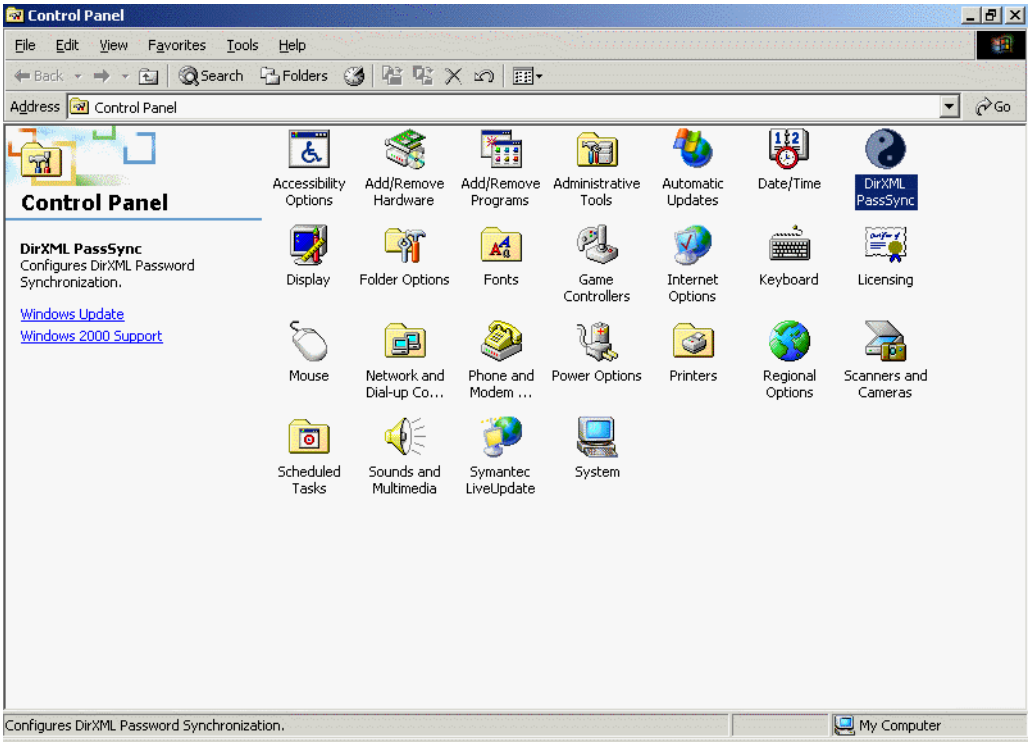
1 Confirm that these ports are available on both the domain controller and the machine where the DirXML Driver for Active Directory is configured to run:

- 135: The RPC endpoint mapper
- 137: NetBIOS name service
- 138: NetBIOS datagram service
- 139: NetBIOS session service

2. On the domain controller, use the Identity Manager Installation to install only the DirXML Driver for Active Directory.

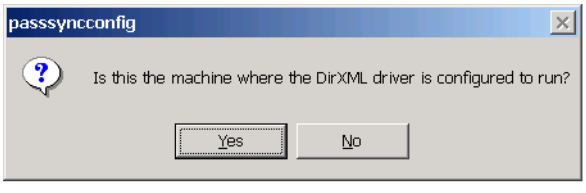
   Installing the driver installs the DirXML PassSync utility.

3. Click Start > Settings > Control Panel, then locate the DirXML PassSync utility.



4. Double-click DirXML PassSync.

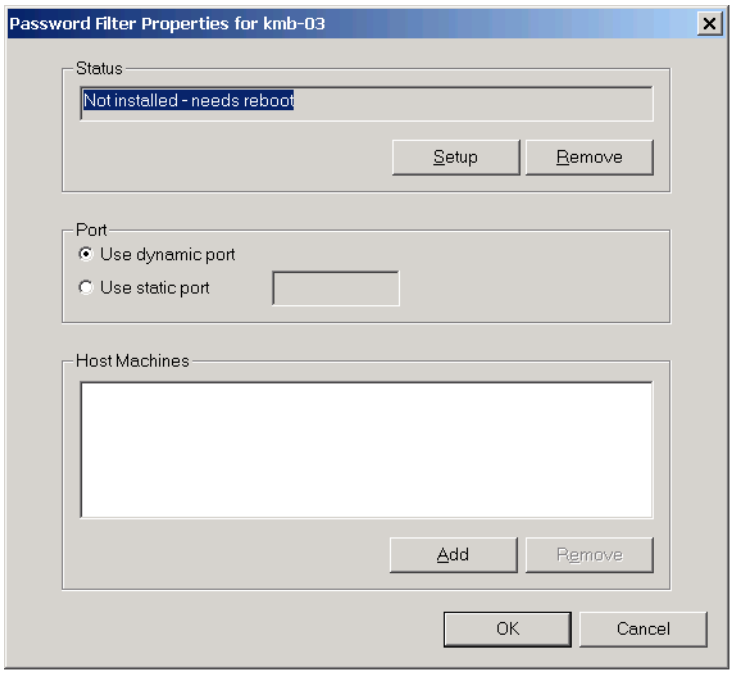
   The first time you open the utility, it asks whether this is the machine where the DirXML driver is installed.



5. Click No.

   After you complete the configuration, you are not shown this prompt again unless you remove the password filter by using the Remove button in the Password Filter Properties dialog box.

   After you click No, the Password Filter Properties dialog box appears, with a status message indicating that the password filter is not yet set up on this domain controller.

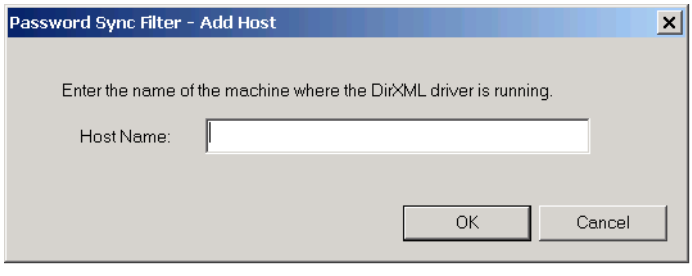


6 Click the Setup button to install the password filter, pwfilter.dll.

7 For the Port setting, specify whether to use dynamic port or static port.

Use the static port option only if you have decided to configure your remote procedure call (RPC) for the domain controller differently than the default.

8 Specify the location of the DirXML driver, click the Add button, specify the Host Name of the machine that is running the DirXML driver in the Password Sync Filter - Add Host dialog box, then click OK.



This step is necessary so that the password filter knows where to send the password changes. The password filter captures password changes, and must send them to the DirXML driver to update the Identity Manager data store.

9 In the Password Filter Properties dialog box, click OK.

10 Reboot the domain controller to complete the installation of the password filter.

You can choose to reboot 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 the password filter installed and has been rebooted.

After the installation is complete and the domain controller is rebooted, the password filter is loaded automatically whenever the domain controller starts up.

11 Check the status for the password filter again by clicking Start > Settings > Control Panel, and double-clicking the DirXML PassSync utility.

Confirm that the status says Running.

12 Repeat Step 2 through Step 11 for each domain controller that you want to participate in Password Synchronization.

13 When the status says Running for all the domain controllers, test Password Synchronization to confirm that it is working.

Retrying Synchronization after a Failure

The driver and the password filter have been enhanced to improve how password synchronization is retried after a failure.

Retrying after an Add or Modify Event

If a password change sent from Active Directory is not completed successfully in eDirectory, the driver caches the password. It is not retried again until an add or modify event occurs for the user that the password belongs to. (Previously, these saved passwords were retried at every polling interval.)

When the driver polls for changes in Active Directory, the driver receives add or modify events for users. For each user add or modify event, the driver checks to see if it has a password saved for this new user. If it does, the driver sends the password to eDirectory as a modify user event.

If you have set up Password Synchronization to send e-mail messages to users when password synchronization fails, this enhancement minimizes the number of e-mails that a user might receive.

Password Expiration Time

A parameter named Password Expiration Time has been added. This parameter lets you determine how long to save a particular user's password if synchronization is not successful on the first try. The driver saves a password until it is successfully changed in the Identity Vault, or until the Password Expiration Time elapses.

You are prompted to specify an expiration time when you import the sample driver configuration. If you don't specify a time, or if the time (interval field) contains invalid characters, the default setting is 60 minutes. If the time specified is less than three times the polling interval specified, the driver changes the time to be three times the polling interval.

Set the value large enough to handle whatever temporary backlog of passwords exists. If you are doing bulk changes, set the timeout large enough to handle all the changes. The rule of thumb is to allow one second per password. For example, to synchronize 18,000 passwords, allow 300 minutes (18,000 passwords divided by 60 seconds).

A setting of -1 is indefinite. Although this setting can handle bulk changes, it can cause problems. For example, a password might never be able to synchronized because the account wasn't associated. Such a password would therefore remain in the system forever. A number of similar situations could result in a large inventory of unsynchronized passwords held by the system.

On the Publisher channel, password synchronization might occur before the Add event. The driver retries immediately following the Add event.

Scenario: No Effect

A new user with a password is created in Active Directory. The filter immediately sends the new password to the driver. However, the driver hasn't yet received that user add event because the event occurred between polling intervals. Because the driver has not yet created the user in the Identity Vault, the password synchronization is not successful on this first attempt. The driver caches the password.

At the next polling interval, the driver receives the add user event for the new user. The driver also checks to see if it has a password cached for this new user. The driver sends the add user event to the Identity Vault, and also sends a modify user event to synchronize the password.

In this case, the password synchronization is delayed by only one polling interval.

The Password Expiration Time parameter doesn't have an effect in this situation.

Scenario: Increasing the Expiration Time

A new user with a password is created in Active Directory. However, the user information doesn't meet the requirements of the Create policy for the Active Directory driver.

For example, perhaps the Create rule requires a full name, and the required information is missing. Like the No Effect example, the filter sends the password change to the driver immediately. However, on the first try the password change is not successful in the Identity Vault because the user doesn't exist yet. The driver caches the password.

In this case, however, even when the driver polls for changes in Active Directory and discovers the new user, the driver can't create the new user because the user information doesn't meet the Create policy's requirements.

Creating the new user and synchronizing the password are delayed until all the user information is added in Active Directory to satisfy the Create policy. Then the driver adds the new user in the Identity Vault, checks to see if it has a password cached for this new user, and sends a modify user event to synchronize the password.

The Password Expiration Time parameter affects this scenario only if the time interval elapses before the user information in Active Directory meets the requirements of the Create policy. If the Add event comes in after the password has expired and the driver doesn't have the password cached for that user, synchronization can't occur. Because the driver doesn't have a cached password, the driver uses the default password in the password policy.

After the user changed the password in either Active Directory or the Identity Vault, that password is synchronized.

If Password Synchronization is set up for bidirectional flow of passwords, a password can also be synchronized from the Identity Vault to Active Directory when a password change is made in the Identity Vault.

If your Create policy is restrictive, and it generally takes longer than a day for a new user's information to be completed in Active Directory, you might want to increase the Password Expiration Time parameter interval accordingly. The driver can then cache the passwords until the user is finally created in the Identity Vault.

Scenario: Never Meeting Requirements

A user with a password is created in Active Directory. However, this user never meets the criteria of the Create policy for the Active Directory driver.

For example, perhaps the new user in Active Directory has a Description that indicates the user is a contractor, and the Create policy blocks creation of User objects for contractors because the business policy is that contract employees are not intended to have a corresponding user account in the Identity Vault. Like the previous example, the filter immediately sends the password change, but the password synchronization isn't successful on the first attempt. The driver caches the password.

In this case, a corresponding user account is never created in the Identity Vault. Therefore, the driver never synchronizes the cached password. After the Password Expiration Time has passed, the driver removes the user password from its cache.

Scenario: E-Mail Notifications

Markus has an Active Directory account and a corresponding eDirectory account. He changes his Active Directory password, which contains six characters. However, the password doesn't meet the eight-character minimum required by the Password Policy that the administrator created in eDirectory. Password Synchronization is configured to reject passwords that do not meet the policy and to send a notification e-mail to Markus saying that password synchronization failed. The driver caches the password and retries it only if a change is made to the User object in Active Directory.

In this case, shortly after changing a password, Markus receives an e-mail stating that the password synchronization wasn't successful. Markus receives the same e-mail message each time the driver retries the password.

If Markus changes the password in Active Directory to one that complies with the Password Policy, the driver synchronizes the new password to the Identity Vault successfully.

If Markus doesn't change to a compliant password, the password synchronization is never successful. When the Password Expiration Time elapses, the driver deletes the cached password and no longer retries it.

8 Troubleshooting

In this section:

Changes Are Not Synchronizing from the Publisher or Subscriber

To synchronize changes in Active Directory, the account used by the DirXML® driver must have the proper rights set up. For information on the necessary rights, see "Creating an Administrative Account" on page 21.

If you use the default policies, you must also meet the requirements for the create, match, and placement policies. For information on default policy requirements, see "Policies" on page 12.

Using Characters Outside the 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 the Identity Vault. 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.

If the policy doesn't satisfy the business rules of your company, you can change the policy after import. Businesses that use Identity Vault account names outside of the traditional ASCII character set should pay particular attention to this policy.

Synchronizing c, co, and countryCode Attributes

When you use the Active Directory management console to select a country for a user, three attributes are set:

Attribute	Description
c	Contains a two-character country code as defined by the ISO.
co	Contains a longer name for the country.
countryCode	Contains a numeric value (also defined by the ISO) that represents the country.

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

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 that are maintained by an LDAP server that contains special operational information. Operation attributes are read-only. They can't be synchronized or changed.

Password Complexity on Windows 2003

Passwords must meet criteria that the password policies specify.

Complexities and requirements in Windows 2000/2003 password policies are different from complexities and requirements in eDirectory.

If you plan to use Password Synchronization, create and use passwords that match the rules of complexity in both Active Directory and eDirectory. Otherwise, the passwords will fail.

TIP: Get the password policies for both systems as similar to each other as you can. In a lab environment, disable strong-password functionality on Windows 2003 servers before installing the Active Directory driver. After the Active Directory driver is working properly, make sure that passwords used in eDirectory and Active Directory satisfy the rules of complexity for both systems. Then re-enable strong-password functionality on the Windows 2003 server.

For troubleshooting tips, see TID 10083320 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10083320.htm).

Error Message LDAP_SERVER_DOWN

The error code LDAP_SERVER_DOWN usually means that the driver can't open the LDAP port on the Active Directory domain controller configured for synchronization. This can happen for several reasons.

- The server named in the driver authentication context is incorrect. The authentication context should hold the DNS name or the IP address of the domain controller you use for synchronization. If you leave the parameter empty, the driver attempts to connect to the machine that is running the driver shim (either the same server that is running IDM, or the server hosting the Remote Loader).
- You are using an IP address for authentication context, and you have disabled non-Kerberos authentication to Active Directory. Kerberos requires a DNS name for authentication context.

  The driver shim can authenticate only using the pre-Windows 2000 Logon method or simple bind. If you have disabled NTLM, NTLM2, and simple bind on your network, you might receive the LDAP_SERVER_DOWN message.
- You have configured the driver to use an SSL connection to Active Directory. This message means that something is wrong with the certificate that you imported to the driver shim server (or no certificate was imported at all).

Tips on Password Synchronization

We recommend that you use a secure connection when you are synchronizing passwords. Vulnerable connections are between the following:

- The DirXML engine and the Remote Loader
- The Remote Loader and Active Directory

  This is true only when you run the Remote Loader remotely from the domain controller that you're connecting to.
- The DirXML engine and Active Directory when you aren't using the Remote Loader

  This is true only if the domain controller isn't local to this machine.

You can create a secure connection by doing one or more of the following:

- Configure SSL between the DirXML engine and the Remote Loader
- Run the Remote Loader on the domain controller
- Configure SSL between the driver shim and Active Directory

  This doesn't apply if you are running the driver on the domain controller that you're connecting to.

For password synchronization to work when the driver shim isn't running on the domain controller, you must have SSL configured.

Providing Initial Passwords

If you see an error about a password not complying when a user is initially created, you need to check your password policies.

For example, perhaps you want the Active Directory driver to provide the initial password for a user when the Active Directory driver creates a User object in the Identity Vault. When a user is created, the driver shim creates the user and then sets the password.

Because adding the user and setting the password are done separately, the new user in this example receives the default password, even if only momentarily. The password is soon updated because the Active Directory driver sends it immediately after adding the user.

If the default password doesn't comply with the eDirectory Password Policy for the user, an error is displayed. For example, if a default password that was created by using the user's surname is too short to comply with the Password Policy, you might see a -216 error saying that the 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:

- Change the policy on the Publisher channel that creates default passwords, so that default passwords conform to the Password Policies (created by using the Manage Password Policies option in Password Management) that have been defined for your organization in the Identity Vault. When the initial password comes from the authoritative application, it replaces the default password.

  This option is preferable. We recommend that a default password policy exist in order to maintain a high level of security within the system.

- 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.

These measures are especially important if the initial password doesn't come with the add event but instead comes in a subsequent event.

Where to Set the SSL Parameter

The SSL parameter in the driver configuration is for SSL between the Active Directory driver and Active Directory. It isn't for SSL between the DirXML engine and the Remote Loader. See "Encryption" on page 18.

Active Directory Account Disabled after a User Add on the Subscriber Channel

The default configuration maps the Identity Vault Logon Disabled attribute to the dirxml-uACAccountDisable bit of the userAccountControl attribute in Active Directory. A Subscriber add operation might set Logon Disabled to false (account enabled), but the Publisher loopback of the add operation reports that Logon Disabled is true (account disabled).

Additionally, inspecting the object in Active Directory might show that the account is disabled. This happens in part because of the way that the driver creates objects in Active Directory and in part because of a mismatch of policies between the driver and Active Directory itself.

Account Disabled in Active Directory Users and Computers

If the account remains disabled in Active Directory after the provisioning cycle completes, you might have a mismatch between policies configured for the driver and policies enforced by Active Directory.

Take for example a Password Required policy. If a user add operation contains an invalid password (or no password at all), the account created in Active Directory should be disabled. But Active Directory might set the dirxml-uACPasswordNotRequired bit in userAccountControl without the driver's knowledge.

Interestingly, this causes the logon enable action of the add operation to fail if the add operation does not include a policy for dirxml-uACPasswordNotRequired. Therefore, the account stays disabled.

Later (perhaps almost immediately because of a merge operation), the driver might attempt to enable the account again by setting Logon Disabled to false. If you want to override Active Directory policy and ensure that accounts always require a password, you should set dirxml-uACPasswordNotRequired to false whenever Logon Disabled changes on the Subscriber channel.

Moving a Parent Mailbox to a Child Domain

If you move a parent mailbox to a mailbox store in a child domain by changing a user's homeMDB attribute, the driver fails the move. The error code returned is 0x80072030.

This error occurs on inter-domain moves. Moving an Exchange parent mailbox to a child domain isn’t supported.

Restoring Active Directory

When you need to restore some or all of Active Directory, the driver might pick up interim events and perform unwanted actions on the Identity Vault. To restore safely, temporarily disable the driver during the restore operation and then bring the Identity Vault back into synchronization with Active Directory.

1. Disable the driver.
2. Delete the Dirxml-DriverStorage attribute on the driver object in the Identity Vault.
3. Restore Active Directory.
4. Set the Active Directory driver to Manual or Automatic startup.
5. Start the driver.
6. Re-migrate to find unassociated objects.

Moving the Driver to a Different Domain Controller

You can configure the driver to synchronize against a different domain controller by changing the driver Authentication Context parameter. When you restart the driver, the state information that the driver uses to track changes in Active Directory is invalid, and Active Directory might replay a large number of old events to bring the state back to the current time.

You can avoid this replay by removing the driver state information while updating the Authentication Context:

1. Stop the driver.
2. Delete the Dirxml-DriverStorage attribute on the Driver object in the Identity Vault.
3. Update the Authentication Context parameter.
4. Start the driver.

   This causes a resync of associated objects in the Identity Vault.
5. Re-migrate to find unassociated objects in Active Directory.

A Changing Permissions on the CN=Deleted Objects Container

When an Active Directory object is deleted, a small portion of the object remains for a specified time so that other domain controllers that are replicating changes become aware of the deletion. By default, only the System account and members of the Administrators group can view the contents of this container. This section describes how to modify the permissions on the CN=Deleted Objects container.

Changing permissions on the Deleted Objects container mignt be necessary if you have enterprise applications or services that bind to Active Directory with a non-System or non-Admin account and poll for directory changes.

This process requires dscals.exe from the Active Directory Application Mode (ADAM) package. This version is an upgrade from the one in the Windows Server 2003 Support Tools and now supports the required capabilities. The ADAM Administration Tools are supported on Windows XP Professional, Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition, and Windows Server 2003 DatacenterEdition.

To get and install the ADAM Administration Tools:

1. From the ADAM Web page (http://www.microsoft.com/downloads/details.aspx?FamilyId=9688F8B9-1034-4EF6-A3E5-2A2A57B5C8E4&displaylang=en), download the ADAM retail package.
2. Double-click the downloaded file and provide a directory that the archive will be extracted into.
3. Launch the Active Directory Application Mode Setup Wizard by double-clicking adamsetup.exe, then click Next.
4. Review and accept the license terms, then click Next.
5. Select ADAM administration tools only, then click Next.
6. Review the selections, then click Next.
7. When Setup has concluded, click Finish.

After ADAM Administration Tools is installed, modify the permissions on the CN=Deleted Objects container:

1. Log in with a user account that is a member of the Domain Adminis group.
2. Click Start > All Programs > ADAM > ADAM Tools Command Prompt.
3. In the Command Prompt, type the following command:

   ```
   dsacls "CN=Deleted Objects,DC=Contoso,DC=com" /takeownership
   ```

   Substitute the distinguished name of the Deleted Objects container for your own domain.

   Each domain in the forest will have its own Deleted Objects container.

The following output should be displayed:

```
Owner: Contoso\Domain Admins
Group: NT AUTHORITY\SYSTEM
Access list:
{This object is protected from inheriting permissions from the parent}
Allow BUILTIN\Administrators  SPECIAL ACCESS
                              LIST CONTENTS
                              READ PROPERTY
Allow NT AUTHORITY\SYSTEM     SPECIAL ACCESS
                              DELETE
                              READ PERMISSONS
                              WRITE PERMISSIONS
                              CHANGE OWNERSHIP
                              CREATE CHILD
                              DELETE CHILD
                              LIST CONTENTS
                              WRITE SELF
                              WRITE PROPERTY
                              READ PROPERTY
The command completed successfully
```

4 To grant a security principal permission to view the objects in the CN=Deleted Objects container, enter the following command:

```
dsacls "CN=Deleted Objects,DC=Contoso,DC=com" /g CONTOSO\JaneDoe:LCRP
```

In this example, the user CONTOSO\JaneDoe has been granted List Contents and Read Property permissions on the container. These permissions are sufficient to allow the user to view the contents of the Deleted Objects container. However, these permissions don't allow the user to make any changes to objects in that container. These permissions are equivalent to the default permissions granted to the Administrators group. By default, only the System account has permission to modify objects in the Deleted Objects container.

The following output should be displayed:

```
Owner: CONTOSO\Domain Admins
Group: NT AUTHORITY\SYSTEM
Access list:
{This object is protected from inheriting permissions from the parent}
Allow BUILTIN\Administrators  SPECIAL ACCESS
                              LIST CONTENTS
                              READ PROPERTY
Allow NT AUTHORITY\SYSTEM     SPECIAL ACCESS
                              DELETE
                              READ PERMISSONS
                              WRITE PERMISSIONS
                              CHANGE OWNERSHIP
                              CREATE CHILD
                              DELETE CHILD
                              LIST CONTENTS
                              WRITE SELF
                              WRITE PROPERTY
                              READ PROPERTY
Allow CONTOSO\JaneDoe         SPECIAL ACCESS
                              LIST CONTENTS
                              READ PROPERTY
The command completed successfully.
```

The user CONTOSO\JaneDoe now has permissions to view deleted objects in the CONTOSO domain.

B 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:

July 21, 2004

Added additional information on the way multi-valued attributes are synchronized by the Active Directory driver. See "Multi-Valued Attributes" on page 22.

March 17, 2004

- Changed references to Password Synchronization 2.0 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.
- Changed references to DirXML 2.0 to Identity Manager 2. The engine and drivers are still referred to as the DirXML engine and DirXML drivers.
- Updated the attribute list in "Managing Account Settings using Custom Boolean Attributes" on page 22.

August 3, 2004

Added "Retrying Synchronization after a Failure" on page 61.

September 28, 2004

Revised "Retrying Synchronization after a Failure" on page 61 to clarify that the driver (not the filter) caches failed passwords and retries them.

April 25, 2005

Made the following changes:

Location	Change
Throughout the document	Updated information, including figures, and revised for clarity.
"Key Terms" on page 9	Added this section
Chapter 5, "Upgrading the Active Directory Driver," on page 37	Revised this section
"Managing Groups" on page 41	Added this topic
"Error Message LDAP_SERVER_DOWN" on page 67	Added this topic
"Tips on Password Synchronization" on page 67	Added this topic
"Where to Set the SSL Parameter" on page 68	Added this topic
"Active Directory Account Disabled after a User Add on the Subscriber Channel" on page 68	Added this topic
Appendix A, "Changing Permissions on the CN=Deleted Objects Container," on page 71	Added this appendix

April 29, 2005

Revised Step 1 in "Configuring Password Filters for All Domain Controllers from One Machine" on page 54, concerning ports that must be available on the domain controller. Although you can use NetBIOS over TCP, you can also use WINS or DNS.

May 13, 2005

Revised information on where to place SSL when using password synchronization. See “Tips on Password Synchronization” on page 67.