Novell
DirXML® Driver for NT Domain

1.4

IMPLEMENTATION GUIDE

Novell®

Legal Notices

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.

NDS is a registered trademark of Novell, Inc., in the United States and other countries.

NetWare is a registered trademark of Novell, Inc., in the United States and other countries.

Novell Client is a trademark of Novell, Inc.

Novell is a registered trademark of Novell, Inc., in the United States and other countries.

Novell Directory Services is a registered trademark of Novell, Inc., in the United States and other countries.

Nsure is a trademark of Novell, Inc.

ZENworks is a registered trademark of Novell, Inc., in the United States and other countries.

Third-Party Trademarks

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

Contents

About This Guide

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

The guide contains the following sections:

Additional Documentation

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

Documentation Updates

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

Documentation Conventions

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

A trademark symbol ($^\circledR$, ^{TM}, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

User Comments

We want to hear your comments and suggestions about this manual and the other documentation included with Novell Nsure Identity Manager. To contact us, send e-mail to proddoc@novell.com.

1 Introducing the DirXML Driver for NT Domain

The DirXML® Driver for NT Domain is designed to manage and synchronize Novell® eDirectory™ with Windows* NT* 4 Domains. The DirXML Driver for NT Domain runs on the Windows NT 4 server.

The driver does the following:

- Synchronizes User objects between eDirectory and NT 4 Domains.
- Does a simple mapping between similar attributes.
- Can be used to migrate User objects between eDirectory and NT 4.

The driver does not serve as a general-purpose NT 4 Domain administration tool.

In this section:

- "New Features" on page 9
- "Default Driver Configuration" on page 10

New Features

In this section

- "Driver Features" on page 9
- "Identity Manager Features" on page 10

Driver Features

- You can use the DirXML PassSync Utility to individually configure password filters on domain controllers. This means you don't have to allow remote access to the registry. See "Separately Configuring Password Filters on Each Domain Controller" on page 44.

- A new parameter is provided for Password Expiration Time, and the driver and password filter are now enhanced to retry passwords only after a successful user add or modify is received. See "Password Expiration Time" on page 24.

- 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 the 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.

- You can now query for two additional classes: GlobalGroup and LocalGroup. Although you can't synchronize them on the Subscriber or Publisher channel, you can use the querying feature to synchronize them in an indirect way, so that the driver would use the MemberOf attribute on a user to put the user in a corresponding group in eDirectory. See "Querying GlobalGroup or LocalGroup" on page 32.

- Nsure™ Identity Manager Password Synchronization is supported in the new sample driver configuration. The new password synchronization features include the following:

  - A Novell Client™ no longer needs to be installed on a Windows machine.

  - You can implement bidirectional password synchronization between NT Domain and other connected systems.

  For more information, see Chapter 5, "Password Synchronization," on page 35.

- Role-Based Entitlements is supported as an option in the new sample driver configuration.

  Using Role-Based Entitlements is a design decision. Don't choose this option unless you have reviewed "Using Role-Based Entitlements" in the *Novell Nsure Identity Manager 2 Administration Guide*.

- The driver can be configured to send a driver heartbeat. See "Adding Driver Heartbeat" in the *Novell Nsure Identity Manager 2 Administration Guide*.

Identity Manager Features

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

Default Driver Configuration

Identity Manager fundamentals are explained in the *Nsure Identity Manager 2 Administration Guide* (http://www.novell.com/documentation/lg/dirxml20/admin/data/alxnk27.html). This section discusses implementations, additions, or exceptions specific to the NT Domain driver.

Data Flow

Publisher and Subscriber Channels

The driver supports Publisher and Subscriber channels:

- The Publisher reads events from an NT Domain PDC's registry and submits that information to eDirectory via the DirXML engine.

- The Subscriber watches for additions and modifications to eDirectory objects and makes changes to NT Domain that reflect those changes.

Policies

Policies are used to control data synchronization between NT Domain and eDirectory. The NT Domain sample driver configuration provides a set of policies, some of which are described in the table below. These policies can be customized through Novell iManager as explained in Chapter 4, "Customizing the NT Domain Driver," on page 23.

Policy	Description
Schema Map	Configured on the driver object.
	Maps the following eDirectory User class and properties to NT Domain Username class and attributes:
	CN, name
	Description, Comment
	Full Name, FullName
	Login Disabled, Disable
	Password Allow Change, PasswordChange
	Password Required, PasswordRequired
	Login Allowed Time Map, LogonHours
	Login Expiration Time, AcctExpires
Create	Configured on the Publisher channel.
	Requires that the Surname attribute must be specified in order for a User object to be created.
	NT does not use this attribute, but eDirectory requires it. To satisfy the eDirectory requirement, the Create policy sets a default Surname for all users, *Unknown*, or you can specify your own when importing the driver configuration.
Matching	Configured on the Publisher and Subscriber channels.
	Specifies that a user in eDirectory is the same user as a user in NT when the value of CN is the same in both places.
	NOTE: Because the NT Domain APIs allow queries of only the user name attribute, this policy should not be changed.
Placement	Configured on the Publisher and Subscriber channels.
	Specifies that new users are named by the value of the leafmost part of the source distinguished name and be placed in the containers you defined during driver setup. You should create these containers before you start the driver.

2 Installing the NT Domain Driver

The DirXML® Driver for NT Domain can be installed along with other DirXML drivers at the same time that the DirXML engine is installed. This method of installation is documented in the *Novell Nsure Identity Manager 2 Administration Guide*.

The driver can also be installed separately after the DirXML engine is installed, by running the Nsure™ Identity Manager installation and selecting only the NT Domain driver.

This section covers the following installation topics:

Where to Install the NT Domain Driver

The NT Domain driver provides synchronization for a single domain. Multiple domains require multiple DirXML driver installations. Consider setting up synchronization for a single domain initially and then using Identity Manager's driver export and import functionality to expedite synchronization setup for additional domains. See the *Novell Nsure Identity Manager 2 Administration Guide* for information about driver export and import.

The NT Domain driver can be installed in any of the following configurations:

- As shown in Figure 1, "Installation Configuration: Remote Loader," on page 13, install Novell® eDirectory™ and the DirXML engine on a Backup Domain Controller (BDC) or Member server. Then, install the NT Domain driver and the Remote Loader service on the Primary Domain Controller (PDC).

  This configuration allows you to insulate the PDC, with the exception of the installation of two components that don't require much disk space or many processing cycles.

  It also allows the DirXML driver direct access to the PDC. From this position, the driver can manage any recovery scenarios independent of connection and API constraints.

Figure 1   Installation Configuration: Remote Loader
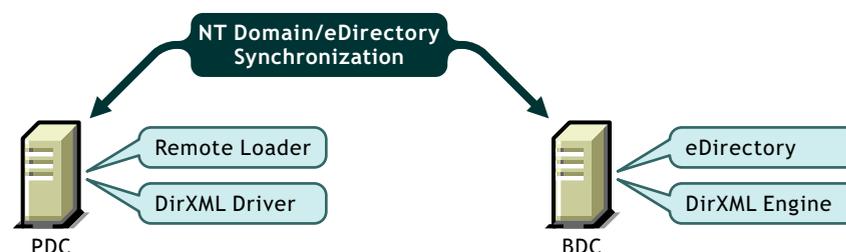
◆ As shown in Figure 2, "Installation Configuration: All Components on the PDC," on page 14, install Novell eDirectory, the DirXML engine, and the NT Domain driver on the PDC.

This configuration is optimal for processing speed because all components are installed on the same computer. Additionally, it allows the DirXML driver direct access to the PDC. From this position, the driver can manage any recovery scenarios independent of connection and API constraints.

However, the PDC is often restricted territory. Placing eDirectory on the PDC might be prohibited by your corporate policy.

To set up all components on the PDC, see "Installing the NT Domain Driver (Local Install)" on page 15.

Figure 2   Installation Configuration: All Components on the PDC
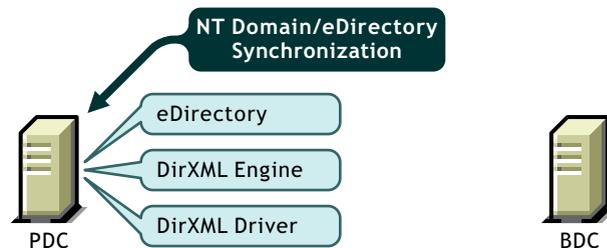
◆ As shown in Figure 3, "Installation Configuration: All Components on the BDC," on page 14, install Novell eDirectory, the DirXML engine, and the NT Domain driver on the BDC.

This configuration insulates the PDC completely.

However, because the driver must communicate with the PDC, this configuration can be problematic if the driver encounters any connection or other communication problems. For this reason, the previous configurations are recommended before this configuration.

To set up all components on the BDC, see "Installing the NT Domain Driver (Local Install)" on page 15.

Figure 3   Installation Configuration: All Components on the BDC
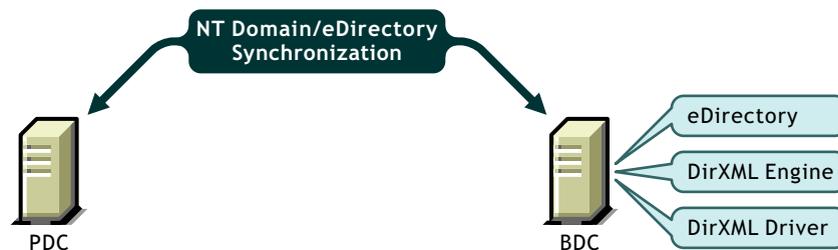
Prerequisites

❑ Novell Nsure Identity Manager and its prerequisites, as listed in "Installation" in the *Novell Nsure Identity Manager 2 Administration Guide*

❑ Windows NT 4 with Service Pack 6

❑ Collect required information, as explained in "Information Needed For Installation" on page 15

❑ Before importing the driver configuration, create the containers that you need to specify during import. The import prompts are described in "Importing the Driver Configuration" on page 17.

Information Needed For Installation

Collect the following information before installing the driver shim and importing the driver configuration:

- The name of the NT 4 PDC that the driver will be synchronizing with.

- The name of the domain you want to synchronize with.

- The eDirectory context where you want to synchronize the User objects.

- The name and password for an NT domain user with the rights to manipulate User objects in the domain.

When you create or import the sample driver configuration, wizard prompts you for the information listed in "Importing the Driver Configuration" on page 17.

Installation

In this section:

- "Installing the NT Domain Driver (Local Install)" on page 15
- "Installing the NT Domain Driver (Remote Loader Installation)" on page 15
- "Post-Installation Tasks" on page 16

Installing the NT Domain Driver (Local Install)

In a local configuration, the driver is installed on the same computer that is hosting the DirXML engine.

Install the components on the appropriate machine, as described in "Where to Install the NT Domain Driver" on page 13.

For instructions, see "Installation" in the *Novell Nsure Identity Manager 2 Administration Guide*.

After installation, you must set up the driver as explained in "Post-Installation Tasks" on page 16.

Installing the NT Domain Driver (Remote Loader Installation)

In a remote configuration, the driver and the Remote Loader service are installed on a computer other than the one hosting the DirXML engine.

Install the components on the appropriate machines as described in "Where to Install the NT Domain Driver" on page 13.

For instructions on installing the driver and Remote Loader, see "Installation" in the *Novell Nsure Identity Manager 2 Administration Guide*.

After installation, you must set up the driver as explained in "Post-Installation Tasks" on page 16.

Post-Installation Tasks

Post-installation setup is not required if you are upgrading an existing driver.

If this is the first time the NT Domain driver has been used, you should complete the post-installation tasks in the following sections:

- "Creating an Admin User" on page 16
- "Granting Rights to the Driver" on page 16
- "Importing the Driver Configuration" on page 17
- "Starting the Driver" on page 18
- "Migrating and Resynchronizing Data" on page 18
- "Activating the Driver" on page 19

Creating an Admin User

The driver needs Read/Write rights to the domain. When you set up the driver, you will be prompted to provide an NT account that the driver can use to access the domain. You can configure the driver to use any existing account with the appropriate rights, or to ease future management, you can create a new account to be used exclusively by the driver.

Granting Rights to the Driver

After you complete the Identity Manager installation, you need to grant rights to the driver so that it can access the SAM keys in the registry of the server that has the domain you want to use.

Creating an Administrator equivalent gives the driver rights to read and write to the domain, but, by default, even the Administrator cannot access the registry until you explicitly assign that access.

To grant the rights:

1 Log in to NT as Administrator.

2 Run regedt32.

3 Select the HKEY_LOCAL_MACHINE window.

4 Select the SAM key, then on the Security menu, select Permissions.

5 Select the Replace Permission on Existing Subkeys check box.

6 Give Full Control permission to Admin user you created for the driver, then click OK.

7 Click Yes to replace the permission on all existing subkeys within SAM.

8 Close the registry.

Importing the Driver Configuration

The sample NT Domain driver configuration creates and configures the objects needed to make the driver work properly. Follow the instructions in "Creating and Configuring a Driver " in the *Novell Nsure Identity Manager 2 Administration Guide*, and provide the following information.

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 additional information for those features.

Import Prompt	Description
Driver name	The name of the driver contained in the driver configuration file is NT Domains. Specify the actual name you want to use for the driver.
Domain Server	Enter the name of the server that contains the NT Domain that you want the driver to use, for example, DOMAIN_SERVER. This should be entered in uppercase characters.
Domain Name	Enter the name of the NT Domain that you want the driver to use, for example DOMAIN_NAME. This should be entered in uppercase characters.
Authoritative User	Enter the NT Domain User the driver will use for domain authentication, for example, Administrator.
Authoritative Password	Enter the password for the User previously specified. If you change the password in NT, you must also update the password in the driver configuration.
Container	Enter the eDirectory container where the driver will match on objects to synchronize with NT, for example, Users.MyOrganization.
Default Surname	NT Domain Users do not have a Surname attribute. Enter a default Surname which will be used in the default Publisher Create policy. This may also be used as the default password (see the Publisher Command Transform, where the sample driver configuration enters the default surname).
Polling Interval (milliseconds)	Specify the number of milliseconds to delay before querying NT for changes.
Password Sync Timeout (minutes)	Specify the number of minutes for the driver to attempt to sync a given password. The driver will not try to sync the password once this interval has been exceeded. This interval should be at least twice as long as the polling interval. See "Password Expiration Time" on page 24.
Configure Data Flow	Data flow can be configured at this time for the driver. Select the data flow that you desire. Bi-directional means that both NT and eDirectory are authoritative sources of the data synchronized between them. NT to eDirectory means that NT is the authoritative source. eDirectory to NT means that eDirectory is the authoritative source.
Password Sync/Set Failure Notification User	Password synchronization policies may send an e-mail concerning the failure of a password synchronization or password set for the associated user. This will fail if that user does not have an e-mail address specified. To avoid such a failure, you may specify a default user (by DN) to which all notifications will be sent.

Import Prompt	Description
Enable Entitlements	Choose Yes if you are also using the Entitlements Service driver and want this driver to use Role-Based Entitlements. Otherwise, choose No.
	Using Role-Based Entitlements is a design decision. Don't choose this option unless you have reviewed "Using Role-Based Entitlements" in the *Novell Nsure Identity Manager 2 Administration Guide*.
	Two other prompts are related to the use of Role-Based Entitlements and are answered only if you choose Yes.
Action - Add Account Entitlement	Used only with Role-Based Entitlements.
	Choose what action is taken when a User account is added by Entitlements.
Action - Remove Account Entitlement	Used only with Role-Based Entitlements.
	Choose what action is taken when a User account is removed by Entitlements.
Install Driver as Remote/Local	Configure the driver for use with the Remote Loader service by selecting Remote, or select Local to configure the driver for local use. If Local is selected, skip the remaining prompts.
Remote Host Name and Port	For remote driver configuration only.
	Enter the Host Name or IP Address and Port Number where the Remote Loader Service has been installed and is running for this driver. The Default Port is 8090.
Driver Password	For remote driver configuration only.
	The Driver Object Password is used by the Remote Loader to authenticate itself to the DirXML server. It must be the same password that is specified as the Driver Object Password on the DirXML Remote Loader.
Remote Password	For remote driver configuration only.
	The Remote Loader password is used to control access to the Remote Loader instance. It must be the same password that is specified as the Remote Loader password on the DirXML Remote Loader.

Starting the Driver

Follow the steps in "Starting, Stopping, or Restarting a Driver" in the *Novell Nsure Identity Manager 2 Administration Guide*.

When the driver starts, you can open DSTrace to see the driver work its way through the registry and list every user in the domain. However, because activation is used in this release of Identity Manager, you might notice a short delay of 30 seconds or more at startup while the driver completes an activation query.

Synchronization takes place on an object-by-object basis as changes are made to individual objects. If you want to have an immediate synchronization, you must initiate that process as explained in the next section, "Migrating and Resynchronizing Data" on page 18.

Migrating and Resynchronizing Data

Identity Manager synchronizes data as it changes. If you want to synchronize all data immediately, you can choose from the following options:

- **Migrate data from eDirectory:** Allows you to select containers or objects you want to migrate from eDirectory to an application. When you migrate an object, the DirXML engine

applies all of the Matching, Placement, and Create policies, as well as the Subscriber filter, to the object.

- ◆ **Migrate data into eDirectory:** Allows you to define the criteria Identity Manager uses to migrate objects from an application into Novell eDirectory. When you migrate an object, the DirXML engine applies all of the Matching, Placement, and Create policies, as well as the Publisher filter, to the object. Objects are migrated into eDirectory using the order you specify in the Class list.

- ◆ **Synchronize:** The DirXML engine looks in the Subscriber class filter and processes all objects for those classes. Associated objects are merged. Unassociated objects are processed as Add events.

To use one of the options explained above, follow the steps in "Starting, Stopping, or Restarting a Driver" in the *Novell Nsure Identity Manager 2 Administration Guide*.

Keep the following points in mind when forcing data synchronization:

- ◆ When migrating into eDirectory, you can migrate either all Users or a specific User, but not a subset of Users. This constraint is imposed by the limited search capabilities of NT domains. Wildcards do not work for queries on the Publisher channel.

- ◆ When migrating a single user into eDirectory, specify the eDirectory user attribute mapped to the NT user name attribute (by default this is CN). Queries on other attributes are not supported by NT.

- ◆ If you have User accounts in both eDirectory and the domain and you want both systems to update data, synchronize data both ways.

- ◆ If the driver shuts down with an error, the driver performs a synchronization the next time it is started. In the synchronization, the driver issues a Modify command at startup for each User object found in the domain.

  The DirXML engine accepts the Modify command if the User has an association. If the User does not have an association, the engine queries the driver for all of the attributes in the Publisher filter. The engine then creates the User.

Activating the Driver

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

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

3 Upgrading

In this section:

Upgrading the Driver Shim

The new driver shim replaces the previous driver shim but keeps the previous driver's configuration. The new driver shim can run the DirXML® 1.*x* configuration with no changes (unless you are using Password Synchronization 1.0).

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

We recommend this step for all drivers, to help minimize upgrade issues.

2 Install the new driver shim. You can do this at the same time that you install the engine, or you can do it after the engine is installed.

Follow the instructions in "Installation" in the *Novell Nsure Identity Manager 2 Administration Guide*.

WARNING: If you have been using Password Synchronization 1.0, don't install the upgraded DirXML Driver for NT Domain driver shim until you have read "Upgrading from Password Synchronization 1.0 to Identity Manager Password Synchronization" on page 22 and are ready to add policies to your driver configuration to provide backward compatibility with Password Synchronzation 1.0.

Running an Nsure™ Identity Manager DirXML driver shim or configuration with the DirXML 1.*x* engine is not supported.

3 After the shim is installed, Novell® eDirectory™ and the driver need to be restarted. Follow the instructions in "Starting, Stopping, or Restarting a Driver" in the *Novell Nsure Identity Manager 2 Administration Guide*.

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

See "Activating the Driver" on page 19.

After you install the driver shim, you can continue with "Upgrading the Driver Configuration" on page 22.

Upgrading the Driver Configuration

A DirXML 1.*x* driver configuration can be run with an Identity Manager DirXML driver shim and the Identity Manager DirXML engine, with no changes to the driver configuration (unless you are using Password Synchronization 1.0; see "Upgrading from Password Synchronization 1.0 to Identity Manager Password Synchronization" on page 22).

However, to edit a DirXML 1.*x* driver configuration, you must either use the DirXML 1.*x* iManager plug-ins or ConsoleOne®, or run the wizard that converts DirXML 1.*x* configurations to Identity Manager format so you can edit the configuration using the Identity Manager iManager plug-ins. See "Managing DirXML 1.x Drivers in an Identity Manager Environment" and "Upgrading a Driver Configuration from DirXML 1.x to Identity Manager Format" in the *Novell Nsure Identity Manager 2 Administration Guide*.

NOTE: Running an Identity Manager driver configuration with a DirXML 1.*x* driver shim is not supported.

To take advantage of the features of Identity Manager, review the sample configuration provided for NT, and see "Upgrading from Password Synchronization 1.0 to Identity Manager Password Synchronization" on page 22 or "Upgrading to Support Identity Manager Password Synchronization" on page 22. See also the *Novell Nsure Identity Manager 2 Administration Guide* for information about the new features.

Upgrading from Password Synchronization 1.0 to Identity Manager Password Synchronization

If you have been using Password Synchronization 1.0 with the DirXML Driver for NT, keep in mind the following items:

- Don't install the Identity Manager version of the driver shim until you are ready to add backward compatibility to your driver.
- Identity Manager Password Synchronization does not require the Novell Client™ to be installed on the Windows machine.

For instructions on adding backward compatibility to your driver, see "Upgrading Password Synchronization 1.0 to Password Synchronization Provided with Identity Manager" on page 37 in this guide.

Upgrading to Support Identity Manager Password Synchronization

This task is for driver objects that have not been used with Password Synchronization 1.0. It is for drivers that have existing configurations that you want to save, but you want to add support for Identity Manager Password Synchronization. See the instructions in "Upgrading Existing Driver Configurations to Support Identity Manager Password Synchronization" on page 41.

4 Customizing the NT Domain Driver

This section covers some general categories of customization:

-

  When you change driver parameters, you are tuning driver behavior to align with your network environment. For example, you might find the default publisher polling interval to be shorter than your synchronization needs require. Making the interval longer could improve network performance while still maintaining appropriate synchronization.

-

  The real power of Novell® Nsure™ Identity Manager is in managing the shared data itself. This section covers some common customizations for the NT Domain driver, such as Exchange integration and local/global group resolution.

  NOTE: When you customize data synchronization, you must work within the supported standards and conventions for the operating systems and accounts being synchronized. Data containing characters that are valid in one environment, but invalid in another, will cause errors.

  Also, keep in mind that attribute names are case sensitive.

For information about synchronizing passwords, see .

Configuring Driver Parameters

Use Novell iManager to make the appropriate adjustments to any of the following properties: log level, polling rate, password expiration time, security options, and startup options.

In this section:

-
-
-
-
-

Log Level

The log level determines the kinds of errors that are sent to the DirXML status logs, DSTrace, and Nsure Audit. For complete information about Nsure Audit and Identity Manager, see the *Novell Nsure Identity Manager 2 Administration Guide*.

You can set one of the following options:

- Log errors

- Log errors and warnings
- Log all messages
- Only update the last log time
- Logging off

To set the log level:

1 In iManager, select DirXML Management > Overview.

2 Select the driver set containing the driver, click the driver icon to see the driver overview, then click the driver icon again to edit driver parameters.

3 Click the Log Level link at the top of the page, select a level, then click OK.

Polling Rate

The driver re-reads the SAM registry once each polling interval, looking for new or modified users. Setting the polling rate too fast will use up all available processing cycles. The minimum polling rate is three seconds, 3000 milliseconds. The recommended rate is one minute, 60000 milliseconds.

1 In iManager, select DirXML Management > Overview.

2 Select the driver set containing the driver, click the driver icon to see the driver overview, then click the driver icon again to edit driver parameters.

3 Select a polling rate from the list, then click OK.

Password Expiration Time

The driver and the password filter have been enhanced in the following ways to improve how password synchronization is retried after a failure:

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

  When the driver polls for changes in NT, it 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 a user might receive.

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

  You are prompted to specify this interval when you import the sample driver configuration.

  If no interval is specified, or if the interval field contains invalid characters, the default setting is 60 minutes. If the interval specified is less than twice the polling interval specified, the driver changes the interval to be at least twice the polling interval.

For more understanding of why these enhancements are important, review the following information.

The driver checks for changes to users in NT based on a polling interval. In contrast, the password filter is event-driven, meaning that it sends password changes from NT to the driver as soon as they occur. After a user is created in eDirectory to correspond to an NT user, this immediate response for password synchronization is helpful. But because of the differences between polling and event-driven activity, password synchronization for new users might not be immediate.

Issues such as the difference between polling and event-driven activity, and business practices such as Create policies and Password Policies, can lead to scenarios like the following. This list explains how the Password Expiration Time parameter is applicable in each case.

- A new user is created in NT with a password. The filter sends the new password to the driver immediately, but the driver has not yet received that user add event because the event occurred between polling intervals. Because the driver has not yet created the user in eDirectory, 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, and also checks to see if it has a password cached for this new user. The driver sends the add user event to eDirectory, 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 does not have an effect in this situation.

- A new user is created in NT with a password, but the user information does not meet the requirements of the Create policy for the NT driver. For example, perhaps the Create rule requires a full name, and the required information is missing. Like the previous example, the filter sends the password change to the driver immediately, but on the first try the password change is not successful in eDirectory because the user does not exist yet. The driver caches the password.

  In this case however, even when the driver polls for changes in NT and discovers the new user, the driver cannot create the new user because the user information does not meet the requirements of the Create policy.

  The new user creation and password synchronization is delayed until all the user information is added in NT to satisfy the Create policy. Then the driver adds the new user in eDirectory, 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 NT meets the requirements of the Create policy. After the Password Expiration Time parameter elapses, the driver removes the the password change from the cache. If later the user meets the requirements and is created in eDirectory after the Password Expiration Time has passed, this means that the driver does not have a password cached for that user and cannot synchronize a password in eDirectory at that time. Instead, the password is synchronized the next time it is changed in NT.

  If Password Synchronization is set up for bidirectional flow of passwords, a password can also be synchronized from eDirectory to NT when a password change is made in eDirectory.

  If your Create policy is restrictive, and it generally takes a couple days for a new user's information to be completed in NT, you might want to increase the Password Expiration Time parameter interval accordingly, so that passwords are cached by the driver until the user is finally created in eDirectory.

- A user is created in NT with a password, but this user never meets the criteria of the Create policy for the NT driver. For example, perhaps the new user in NT 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 eDirectory. Like the previous example, the filter sends the password change immediately, but the password synchronization is not successful on the first attempt. The driver caches the password.

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

◆ A user with an NT account and a corresponding eDirectory account changes his NT password. The NT password chosen by the user contains 6 characters, so it does not meet the 8-character minimum required by the Password Policy 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 the user saying that password synchronization failed. The driver caches the password, and retries it only if a change is made to the user object in NT.

In this case, shortly after the user changes his password, he receives an e-mail stating that the password synchronization was not successful. He receives the same e-mail message each time the driver retries the password.

If the user changes his password in NT to one that complies with the Password Policy, the driver synchronizes the new password to eDirectory successfully.

If the user does not 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.

Security Options

Creating a new user that has Read/Write rights to the domain and to the SAM registry will make Identity Manager easier to manage. This user account will be used exclusively by the NT Domain Driver. This user is also a user you'll want to exclude from synchronization because its sole purpose is to provide rights for the NT Domain Driver. After you've created this user, you can assign the driver to use that user account.

To set up these security options:

1 In iManager, select DirXML Management > Overview.

2 Select the driver set containing the driver, click the driver icon to see the driver overview, then click the driver icon again to edit driver parameters.

3 Click Driver Configuration at the top of the page, then enter the appropriate data in the Authentication fields.

Startup Options

You can set driver startup to any of the following three options:

◆ **Auto Start:** Any time the DirXML engine is started the driver is started automatically. After you have the driver configured, it is good to use this option.

◆ **Manual:** The driver will not start until it is started through the status indicator on the driver icon. If an error brings the driver down, it will not restart until manually started. This option is often used during driver modification and testing cycles. The engine will buffer changes to be processed when driver is started.

◆ **Disabled:** If the driver is disabled, the DirXML engine will not cache events. However, upon driver startup, data changes resulting from Add or Modify (of objects with an association) events will be synchronized. Data changes resulting from Delete, Rename, or Move events will not be synchronized.

To set startup options:

1 In iManager, select DirXML Management > Overview.

2 Select the driver set containing the driver, click the driver icon to see the driver overview, then click the driver icon again to edit driver parameters.

3 Click Driver Configuration at the top of the page, then select one of the three options listed under Startup Options.

Configuring Data Synchronization

This section covers the following configuration topics:

Integrating the DirXML Driver for NT Domain and the DirXML Driver for Exchange

IMPORTANT: If you are using both the NT driver and the Exchange driver, you should complete the following procedure.

The DirXML Driver for NT Domain and the DirXML Driver for Exchange can both create users in the domain. To avoid a conflict, a mechanism can be set up using Identity Manager policies to solve this problem.

The DirXML Driver for NT Domain has a User attribute called DirXML-NTAccountName. This attribute contains the DomainName/UserName attribute. This value is what the Exchange MailBox and Remote objects need to associate to a domain account. For that association to occur correctly, the value in DirXML-NTAccountName needs to be put in the MailBox attribute Assoc-NT-Account. Keep in mind that attribute names are case sensitive.

1 Using DirXML Script, edit the existing Subscriber Create policy for the Exchange driver (or create a new policy) so that a new MailBox object is not created unless the DirXML-NTAccountName attribute is populated.

2 Verify the DirXML-NTAccountName attribute is in both the Publisher filter on the DirXML Driver for NT Domain and the Subscriber filter on the DirXML Driver for Exchange.

3 Restart both drivers.

Data Flow in the NT Domain and Exchange 5.5 Drivers

The changes outlined in "Integrating the DirXML Driver for NT Domain and the DirXML Driver for Exchange" on page 27 will ensure the following control flow:

1. A user is created in eDirectory.

2. The DirXML Driver for NT Domain is handed a create request. The DirXML Driver for Exchange Create event is vetoed because of the absence of the DirXML-NTAccountName attribute.

3. The DirXML Driver for NT Domain creates the NT account and feeds back the name of the NT account just created to the DirXML-NTAccountName attribute.

4. The DirXML Driver for Exchange is now notified. It creates the mailbox and associates the mailbox with the NT account information stored in NDS.

NOTE: Although the examples used DirXML-NTAccountName as the eDirectory attribute to hold the NT account information, you are free to choose any attribute that works for you.

Filtering Out Non-User User Objects

The NT registry tracks some non-user data along with user data. For example, information about workstation objects appears as User objects in the NT User Manager. This information is synchronized to eDirectory unless you filter it out using a style sheet. The following style sheet can be used in the Event Transformation to ensure that only real user objects are synchronized.

```
<xsl:template match="node()|@*">
 <xsl:copy>
   <xsl:apply-templates select="node()|@*"/>
 </xsl:copy>
</xsl:template>

<!-- Test for Non-User user objects like workstations that have a $ in the
name -->

 <xsl:template match="add[@class-name='User']|modify[@class-
   name='User']|sync[@class-name='User']">
     <xsl:choose>
        <xsl:when test="contains(@src-dn,'$')"/>
        <xsl:otherwise>
           <xsl:copy>
               <xsl:apply-templates select="node() | @*"/>
           </xsl:copy>
         </xsl:otherwise>
      </xsl:choose>
  </xsl:template>
</xsl:stylesheet>
```

Synchronizing Group Information

The driver allows you to synchronize group information in both the user attributes holding group membership information and the group objects themselves.

This functionality allows you to see which groups a user is a part of, whether you're looking at the user in eDirectory or in NT.

To synchronize group information:

1 Ensure the groups to be synchronized exist as identically named objects in both eDirectory and in NT.

For example, if you want to synchronize group informaton for the NT global group, Domain User, you should create a group object named Domain User in eDirectory.

2 Create a DirXML association between the NT group and the eDirectory group.

2a In iManager, select eDirectory Administration > Modify Object.

2b Browse to the eDirectory group that will be synchronized, then click Ok.

2c Click the DirXML tab, then click Add.

The Add Association dialog box appears.

2d Specify the DirXML driver for NT in the Integration Driver Object field.

2e Enter the NT group name in the Associated Object ID field using upper case as shown in the following syntax:

`\`*DOMAINNAME*`\`*GROUPNAME*

2f Click OK.

The new association is displayed in the Associations page.

3 Edit the Schema Mapping policy to map the NT UserLocalGroups and UserGlobalGroups attributes to eDirectory attributes.

3a Click DirXML Management > Overview, then select the driver set containing the DirXML driver for NT.

3b Click the driver to display the Driver Overview page.

3c Double-click the Schema Map policy and map the new attributes.

You can map the NT attributes to any multivalue string attribute. UserGlobalGroups is commonly mapped to the GroupMembership attribute.

4 If you are publishing data from NT to eDirectory, double-click the Publisher filter icon and add the new attributes.

5 If you are subscribing to data held in eDirectory, double-click the Subscriber filter icon and add the new attributes.

6 Click Ok.

Group information will begin to synchronize when the driver is restarted and a change to user information occurs.

NOTE: If you use User Manager to change the group membership attribute values without making changes to any other data, this update does not synchronize immediately. Changes will be synchronized the next time the NT user logs in or the next time user object data changes.

Changing the Location of User Objects Using Placement Policies

Modify the Subscriber and Publisher Placement policies to match the eDirectory container with the NT domain name you have set up. Placement policies are created when you import the sample driver configuration file.

To modify Placement policies:

1 In iManager, select DirXML Management > Overview.

2 Select the driver set containing the driver, then click the driver icon.

The Driver Overview is displayed. Policies can be edited here.

3 Double-click the Placement policy you want to edit, then make the appropriate changes.

Changing Which Attributes Are Synchronized Using Publisher and Subscriber Filters

1 In iManager, select DirXML Management > Overview.

2 Select the driver set containing the driver, then click the driver icon.

The Driver Overview is displayed. Policies can be edited here.

3 Double-click the filter icon and add or remove the appropriate attributes.

Select the eDirectory user attributes that you want to synchronize with.

The driver supports the Domain User object. The attributes that the driver supports within the User object are the attributes that are accessible by using the USER_INFO_3 data structure using the NetUser APIs.

The following table lists the supported attributes.

IMPORTANT: Keep in mind that attribute names are case sensitive.

Driver Attribute	USER_INFO_3 Name	Data Type	Description
Name	usri3_name	LPWSTR	Specifies the name of the user account. The name cannot exceed UNLEN.
(May be set through a Create policy.)	usri3_password	LPWSTR	The password of the user. The length cannot exceed PWLEN.
PasswordAge	usri3_password_age	DWORD	Read-only. Specifies the number of seconds elapsed since the password was last changed.
PrivilegeLevel	usri3_priv	DWORD	Specifies the privilege level of the user: Guest, User, or Administrator.
HomeDirectory	usri3_home_dir	LPWSTR	Points to a Unicode* string that contains the path of the home directory of the user. The string can be null. The string cannot exceed PATHLEN. The Subscriber, on an Add event, will create the folder specified by the path as a Shared to Everyone folder, if it does not already exist.
Comment	usri3_comment	LPWSTR	Points to a Unicode string that contains a comment. The string can be null. The comment cannot exceed 1024.
Flags	usri3_flags	DWORD	Contains values that determine several features. See USER_INFO_3 documentation.
LogonDisable	usri3_flags	LPWSTR TRUE or FALSE	Represents a bit in the usri_flags that is the UF_ACCOUNTDISABLE. The user's account is disabled.
PasswordChange	usri3_flags	LPWSTR TRUE or FALSE	Represents a bit in the usri_flags that is the UF_PASSWD_CANT_CHANGE. The user cannot change the password if this value is TRUE.

Driver Attribute	USER_INFO_3 Name	Data Type	Description
PasswordRequired	usri3_flags	LPWSTR TRUE or FALSE	Represents a bit in the usri_flags that is the PASSWD_NOTREQ. No password is required.
ScriptPath	usri3_script_path	LPWSTR	Points to a Unicode string specifying the path of the user's logon script. The string can be null. The string cannot exceed PATHLEN.
AuthorizationFlags	usri3_auth_flags	DWORD	Read-only. Specifies an unsigned long integer that contains values that specify the user's privileges.
FullName	usri3_full_name	LPWSTR	Points to a Unicode string that contains the full name of the user. This string can be null or up to 1024 characters in length.
UserComment	usri3_usr_comment	LPWSTR	Points to a Unicode string that contains a user comment. This string can be null or up to 1024 characters in length.
AppParams	usri3_parms	LPWSTR	Read-only. A Unicode string used by Microsoft* products.
Workstations	usri3_workstations	LPWSTR	Points to a Unicode string that contains the names of the workstations from which the user can log on. This string can be null or up to 1024 characters in length.
LastLogon	usri3_last_logon	DWORD	Read-only. Specifies when the last logon occurred. The value is stored as the number of seconds elapsed since 00:00:00, January 1, 1970.
LastLogoff	usri3_last_logoff	DWORD	Specifies when the last logoff occurred. The value is stored as the number of seconds elapsed since 00:00:00, January 1, 1970.
AccExpires	usri3_acct_expires	DWORD	Specifies when the account will expire. The value is stored as the number of seconds elapsed since 00:00:00, January 1, 1970. A value of TIMEQ_FOREVER indicates that the account never expires. The driver will map this to what eDirectory is looking for.
MaxStorage	usri3_max_storage	DWORD	Specifies the maximum amount of disk space the user can use. Use USER_MAXSTORAGE_UNLIMITED to use all available disk space.
UnitsPerWeek	usri3_units_per_week	DWORD	Read-only. Specifies the number of equal-length time units into which the week is divided.
LogonHours	usri3_logon_hours	PWORD	The driver maps this to an octet string that specifies an account's allowed login time periods for each day of the week to a precision of one-half hour.
BadPasswordCnt	usri3_bad_pw_count	DWORD	Read-only. Specifies the number of times the user tried to log in to the account using the incorrect password.
NumLogons	usri3_num_logons	DWORD	Read-only. Counts the number of successful times the user logged in to this account.
LogonServer	usri3_logon_server	LPWSTR	Read-only. Points to a Unicode string that contains the name of the server to which login requests are sent.

Driver Attribute	USER_INFO_3 Name	Data Type	Description
CountryCode	usri3_country_code	DWORD	Specifies the country code for the user's language of choice.
CodePage	usri3_code_page	DWORD	Specifies the code page for the user's language of choice.
UserID	usri3_user_id	DWORD	Read-only. Specifies the relative ID (RID) of the user.
PrimaryGroupID	usri3_primary_group_id	DWORD	Specifies the relative ID (RID) of the primary Global Group of the user.
Profile	usri3_profile	LPWSTR	Specifies a path to the user's profile. This value can be a null string, a local absolute path, or a UNC path. The length of the string cannot exceed PATHLEN.
HomeDirDrive	usri3_home_dir_drive	LPWSTR	Specifies the drive letter assigned to the user's home directory for login purposes.
PasswordExpired	usri3_password_expired	DWORD	Determines whether the password of the user has expired. Use zero if the password has not expired and non-zero if it has expired. Although this attribute is supported, keep in mind that the eDirectory attribute named Password Expiration Time is used to expire a password by setting a date and time that is previous to the current date, instead of by setting a zero or non-zero value. This means that these attributes are not easily mapped to each other.

The driver also supports the UserGlobalGroups and UserLocalGroups that are accessible through the NetUserGroup API.

The following table lists the supported attributes:

Driver Attribute	Data Type	Description
UserGlobalGroups	LPWSTR	A multi-valued attribute that contains the global groups the user is a member of.
UserLocalGroups	LPWSTR	A multi-valued attribute that contains the global groups the user is a member of.

Querying GlobalGroup or LocalGroup

You can query for GlobalGroup or LocalGroup objects, although you can't synchronize them on the Subscriber or Publisher channel.

The query supports the following attributes.

- **GlobalGroup:** Name, Comment, MemberOf
- **LocalGroup:** Name, Comment

A query is successful if the SearchClass is GlobalGroup or LocalGroup and any of the following are true:

- The query includes all of the attributes.

- ◆ The query includes some of the attributes.

- ◆ The query includes none of the attributes.

This feature could be used to synchronize GlobalGroups or LocalGroups in an indirect way. For example, using a style sheet you could configure the driver to query for them when you are migrating users, and create corresponding Group objects in eDirectory. Doing this would allow the MemberOf attribute for an NT user to work for making a user a member of matching groups in eDirectory (this aspect would work without an additional style sheet). To keep the GlobalGroups and LocalGroups mirrored in eDirectory using this method, you would need to migrate again periodically as new groups are added or removed from NT.

In the sample driver configuration, this feature is used if you choose the Role-Based Entitlements option, to allow you to assign a user to a GlobalGroup or LocalGroup in NT as an entitlement. (Using Role-Based Entitlements is a design decision. Don't choose this option unless you have reviewed "Using Role-Based Entitlements" in the *Novell Nsure Identity Manager 2 Administration Guide*.)

5 Password Synchronization

This section assumes that you are familiar with the information in "Password Synchronization across Connected Systems" in the *Novell Nsure Identity Manager 2 Administration Guide*. The information in this section is specific to this driver.

IMPORTANT: If you have used Password Synchronization 1.0 previously, don't install the new driver shim until you have read "Upgrading Password Synchronization 1.0 to Password Synchronization Provided with Identity Manager" on page 37 and understand the implications. If you install the driver shim, you need to add backward compatibility for Password Synchronization 1.0 to your driver policies at the same time, even if you are not planning to use the Password Synchronization provided with Nsure™ Identity Manager right away.

In this section:

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

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

	Password Synchronization 1.0	Password Synchronization with Identity Manager 2
Platforms	◆ 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) is 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 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 Administration Guide*.
Main functionality for Windows connected systems	To send passwords to DirXML so the eDirectory password is synchronized with the Windows password. Because the NDS password is not reversible, passwords were not sent back to NT or AD.	To provide bi-directional password synchronization. Because Universal Password (and Distribution Password) is reversible, passwords can be synchronized in both directions.
LDAP changes	Not supported.	Supported
Novell Client™	Required.	Not required.
nadLoginName attribute	Used for keeping passwords updated.	Not used.
The component that contains the password synchronization functionality	The DirXML driver contained the functionality for updating nadLoginName.	Policies in the driver configuration provide the password synchronization functionality. The driver simply carries out the tasks given by the DirXML engine, which come from logic in the policies. The driver manifest, global configuration values, and driver filter settings must also support password synchronization. These are included in the sample driver configurations, or can be added to an existing driver. See "Upgrading Existing Driver Configurations to Support Identity Manager Password Synchronization" on page 41.
Agents	A separate piece of software.	No agents are installed; instead, the functionality is now part of the driver.

Upgrading Password Synchronization 1.0 to Password Synchronization Provided with Identity Manager

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

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

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

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

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

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

2 Install the Identity Manager driver shim to replace the DirXML 1.*x* driver shim, and immediately complete Step 3.

Use the installation program as described in "Installation" in the *Novell Nsure Identity Manager 2 Administration Guide*, and select only the DirXML Driver for NT Domain.

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 39.

A DirXML 1.*x* driver shim updates the nadLoginName attribute. The Identity Manager DirXML driver shim does not, so you must add policies to the driver configuration to update nadLoginName. This allows Password Synchronization 1.0 to function as usual when you install the driver shim, so no password changes are missed while you finish deploying Identity Manager Password Synchronization.

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

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

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

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

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

◆ Convert the driver to Identity Manager format using a wizard. See "Upgrading a Driver Configuration from DirXML 1.x to Identity Manager Format" in the *Novell Nsure Identity Manager 2 Administration Guide*.

- Add policies to support Identity Manager Password Synchronization. You can use an "overlay" configuration file to add the policies, driver manifest, and GCVs, all at once. You must also add an attribute to the Filter. For instructions, see "Upgrading Existing Driver Configurations to Support Identity Manager Password Synchronization" on page 41.

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 39. The Identity Manager sample driver configuration does not contain those policies.

- Make sure nadLoginName attribute is set to Publish and Subscribe in the filter for NT, and Publish for AD, as it was in your previous driver configuration.

5 Install new Password Synchronization filters and configure them if you want the connected system to provide user passwords to Identity Manager. See "Setting Up Password Synchronization Filters" on page 43.

6 Turn on Universal Password for eDirectory user accounts by creating Password Policies with Universal Password enabled.

See "Managing Passwords by Using Password Policies" in the *Novell Nsure Identity Manager 2 Administration Guide*.

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

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

See "Implementing Password Synchronization" in the *Novell Nsure Identity Manager 2 Administration Guide*.

8 Test synchronization.

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

9a Turn off Password Synchronization 1.0 by removing the agent using Add/Remove Programs.

9b In the filter for the driver, change the nadLoginName attribute to Ignore.

9c Remove the backward compatibility policies that are updating nadLoginName from the driver configuration.

9d If desired, you can also remove the nadLoginName attribute from users after Identity Manager Password Synchronization is working, because it is no longer needed.

Creating Backward Compatibility with Password Synchronization 1.0 by Adding Policies

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

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

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

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

These policies must be added for both AD and NT drivers, and they must be added regardless of whether you are updating your existing driver configurations, or replacing them with new configurations that ship with Identity Manager. The Identity Manager sample driver configurations for AD and NT do not include them by default.

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

1 In iManager, click DirXML Utitities > Import Drivers.

The Import Driver Wizard opens.

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

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

It is listed under the heading Additional Policies.

4 Complete the import prompts:

4a Select your existing AD or NT driver.

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

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

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

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

It can normally be found under the driver object.

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

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

5 Click Next.

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

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

7 Click Next, then Finish to complete the wizard.

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

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

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

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

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

8b Click the driver you just updated.

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

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

8d Click Insert to add the new policy. In the Insert page that appears, click Use an Existing Policy and browse for the new policy object. Click OK.

8e If you have more than one policy in the list for any of the three new policies, use the arrow buttons ▲▼ to move the new policy down so it is last in the list.

9 Repeat this procedure for all your AD and NT Domain drivers.

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

New Driver Configuration and Identity Manager Password Synchronization

If you are not using Password Synchronization 1.0, and you are creating a new driver or replacing an existing driver's configuration with the Identity Manager configuration, follow the instructions in "New Driver Configuration and Identity Manager Password Synchronization" in *Novell Nsure Identity Manager 2 Administration Guide*.

In addition, do the following:

* 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 43.

* Set up the scenario for Password Synchronization that you want to use, using the Password Policies and the Password Synchronization settings for the driver. See "Implementing Password Synchronization" in the *Novell Nsure Identity Manager 2 Administration Guide*.

Upgrading Existing Driver Configurations to Support Identity Manager Password Synchronization

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

IMPORTANT: If a driver is being used with Password Synchronization 1.0, you should complete this section only as part of "Upgrading Password Synchronization 1.0 to Password Synchronization Provided with Identity Manager" on page 37, not alone.

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

* Add driver manifest, global configuration values, and password synchronization policies to the driver configuration. For a list of the policies you add, see "Policies Required in the Driver Configuration" in the *Novell Nsure Identity Manager 2 Administration Guide*.

* Change the Filter to allow nspmDistributionPassword attribute to be synchronized.

Prerequisites

❑ Make sure you have converted your existing driver to Identity Manager format, as described in "Upgrading a Driver Configuration from DirXML 1.x to Identity Manager Format" in the *Novell Nsure Identity Manager 2 Administration Guide*.

❑ Create a backup of your existing driver using the Export Drivers Wizard.

❑ Make sure you have installed the new driver shim. Some password synchronization features such as Check Password Status won't work without the Identity Manager driver shim.

Procedure

1 In iManager, click DirXML Utitities > Import Drivers.

The Import Driver Wizard opens.

2 Select the driver set where your existing driver resides.

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

A list of import prompts appears.

4 Select your existing driver to update.

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

◆ Whether the connected system can provide passwords to DirXML.

◆ Whether the connected system can accept passwords from DirXML

◆ Whether the connected system can check a password to see if it matches the password in DirXML.

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

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

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

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

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

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

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

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

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

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

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

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

8b Click the driver you just updated.

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

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

8d Click Insert to add the new policy. In the Insert page that appears, click Use an Existing Policy and browse for the new policy object. Click OK.

8e If you have more than one policy in the list for any of the new policies, use the arrow buttons ▲ ▼ to move the new policies to the correct location in the list. Make sure the policies are in the order listed in "Policies Required in the Driver Configuration" in the *Novell Nsure Identity Manager 2 Administration Guide*.

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

10 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 43.

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.

11 Set up the scenario for Password Synchronization that you want to use, using the Password Policies and the Password Synchronization settings for the driver. See "Implementing Password Synchronization" in *Novell Nsure Identity Manager 2 Administration Guide*.

12 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 the driver, each of the other domain controllers needs a password filter (pwfilter.dll file) installed and the registry configured 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 made by users through Windows clients, encrypts them, 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 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 don't allow remote access to the registry:** You set up the password filters on each domain controller separately. To do this, you 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 44.

- **If you allow remote access to the registry:** From the single machine where you plan to run the driver, you 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 .

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 NT.

Setting up the filter requires rebooting the domain controller, so you might want to perform this procedure after hours, or reboot only one domain controller at a time. If there is more than one domain controller in the domain, 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 NT 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 NT.
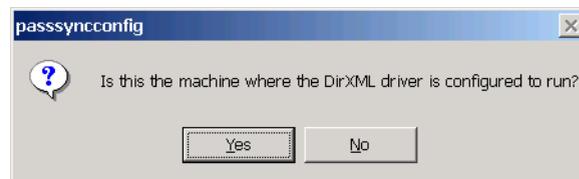
Installing the driver installs the DirXML PassSync utility.

3 Click Start > Settings > Control Panel, and locate the DirXML PassSync utility.
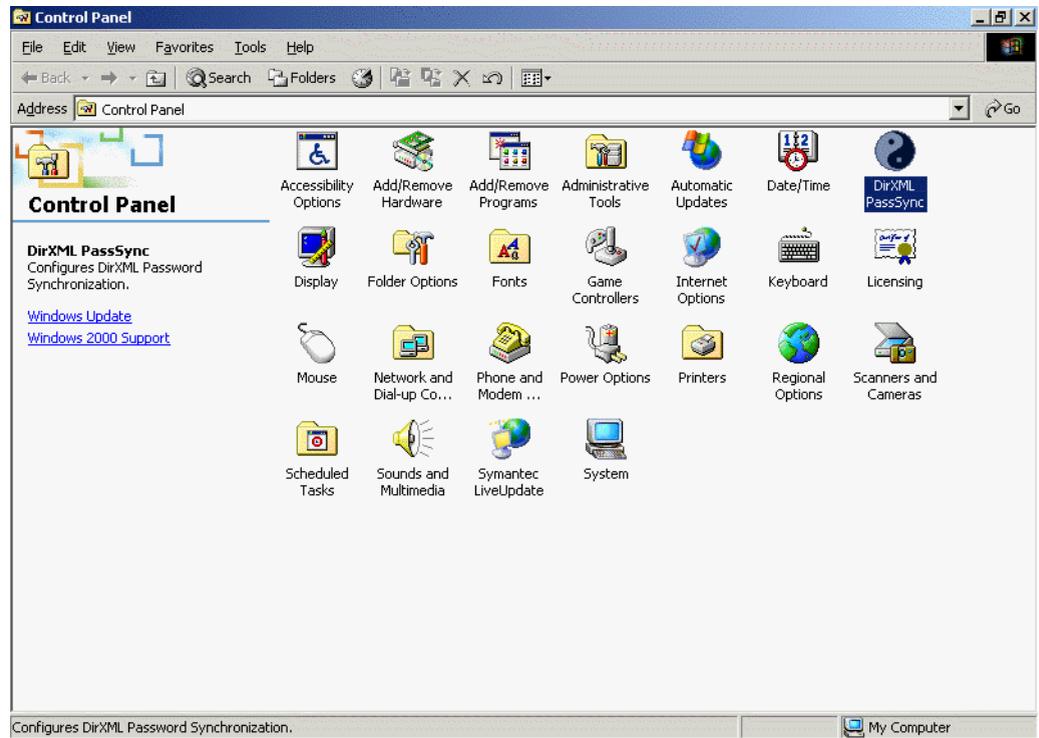
4 Double-click DirXML PassSync.

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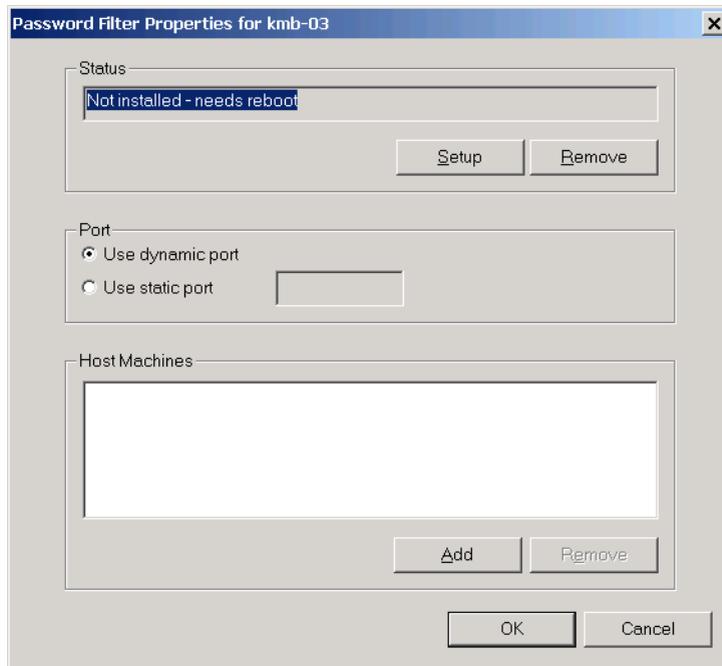
6 Click the Setup button to install the password filter, pwfilter.dll.

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, then specify the Host Name of the machine that is running the DirXML driver in the Password Sync Filter - Add Host dialog box. 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.

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.

Setting up the filter requires rebooting the domain controller, so you might want to perform this procedure after hours, or reboot only one domain controller at a time. If there is more than one domain controller in the domain, 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 the domain controllers and on the machine where the DirXML Driver for NT is configured to run:

◆ 135: The RPC endpoint mapper

◆ 137: NetBIOS name service

◆ 138: NetBIOS datagram service

◆ 139: NetBIOS session service

2 At the computer where the driver is installed, click Start > Settings > Control Panel.
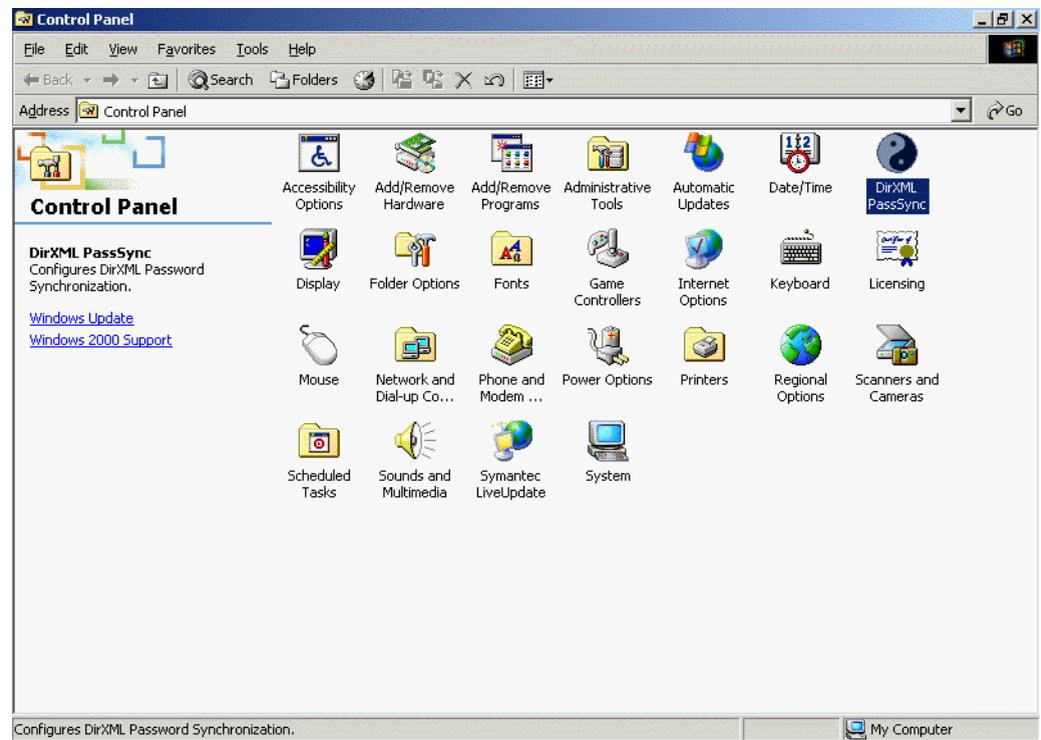
3 Double-click DirXML PassSync.

The first time you open the utility, it asks whether this is the machine where the DirXML driver is installed.
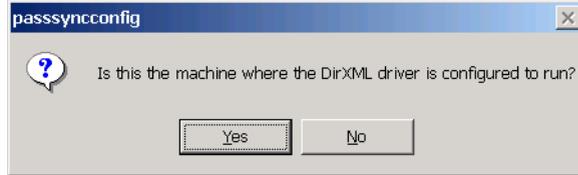
After you complete the configuration, you are not shown this prompt again unless you remove this domain from the list.

4 Click Yes.

A list appears labeled Synchronized Domains.
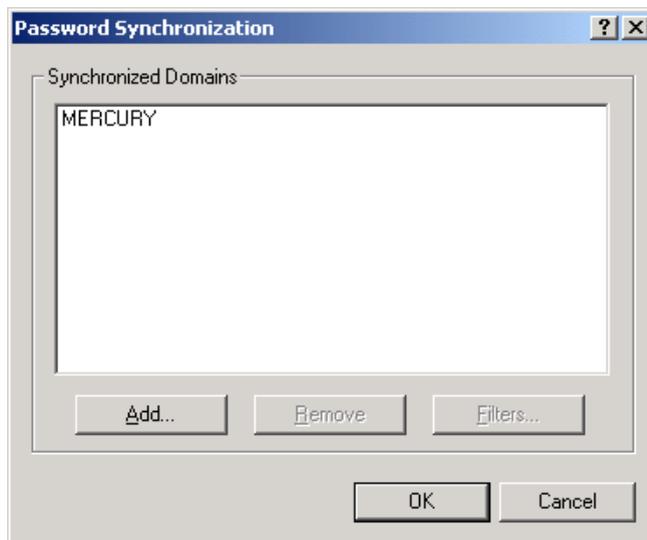
5 To add a domain you want to participate in password synchronization, click Add and specify the domain name.

**6** 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.

7 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.
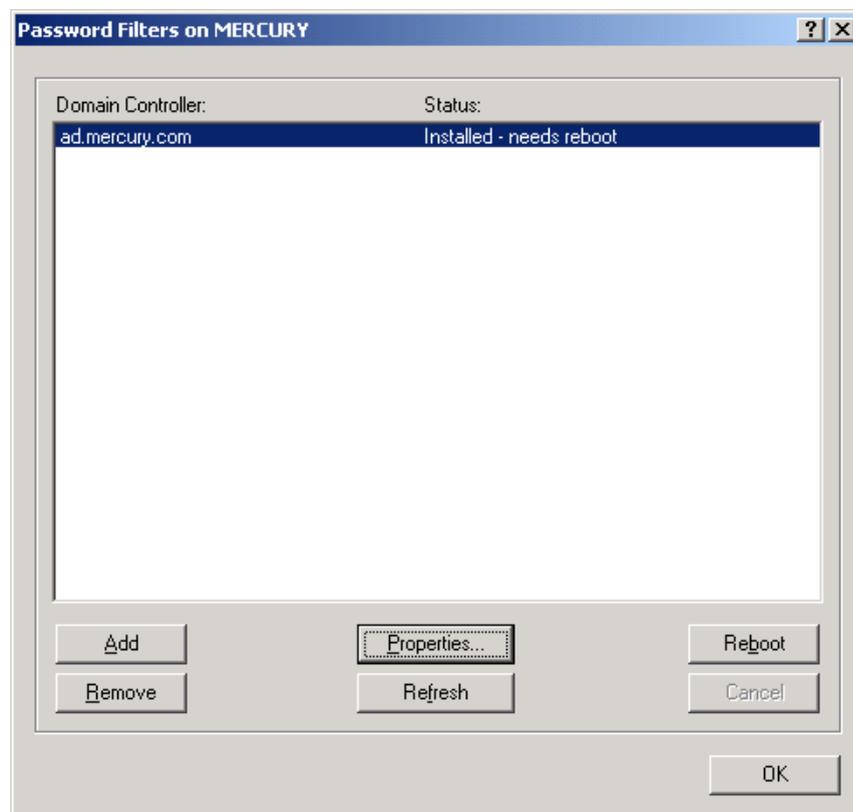
8 Reboot each domain controller.

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.

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

10 To add more domains, click OK to return to the list of domains, and repeat Step 5 through Step 9.

Troubleshooting Password Synchronization

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

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

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

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

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

    or

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

6 Troubleshooting

You can log Nsure™ Identity Manager events using Nsure Audit. Using this service in combination with the driver log level setting provides you with tracking control at a very granular level. For more information, see "Logging and Reporting Using Nsure Audit" in the Novell Nsure Identity Manager 2 Administration Guide.

Troubleshooting

The following section identifies common error messages and the possible causes.

♦ `Error Wrong Destination DN:` The destination DN sent to the driver was wrong or not present. This can occur when a User object was changed in a container not covered in the Subscriber Placement policy.

♦ `Error Password Length is to long. Password not set.:` The password sent to the driver was too long and the driver was unable to set the password.

♦ `***Error*** Failed to attach to the registry = error#:` The driver was unable to attach to the system registry. The error was fatal, so the driver will shut down. Check the error code to see why.

♦ `***Error*** Failed to attach to the registry retrying = error#:` The driver was unable to attach to the system registry but the error suggested to try again later. Check the error code to see why.

♦ `***Error Unable to logon as User %S to Domain %S error code = error#:` The driver was unable to log in as the user in the domain specified. Check the error code to see why.

♦ `Error: Missing Poll Rate parameter:` The poll rate in the driver parameters has not been set.

♦ `Error: Missing Publisher State parameter:` This is the first time the driver has been run.

♦ `Returning an error to DS:` An error has occurred and the driver is returning the error.

♦ `LogonUser = error #:` The driver has tried to log in as the user specified in the driver parameters. Check the error number to see possible reasons why logon failed.

♦ `ImpersonateLoggedOnUser = error #:` The driver has tried to impersonate the user. Check the error number to see possible reason why the impersonation failed.

♦ `***Failed MKDIR directory path = error #:` The driver attempted to create a directory. MKDIR failed to create a directory path and returned the error #. Check the error number for the reason for the failure.

♦ `***Failed SharDir directory path:` The driver attempted to share the directory path with Everyone but failed.

- ◆ `***ERROR ADD failed, NERR_PasswordTooShort`

  `***ERROR ADD failed, NERR_InvalidComputer`

  `***ERROR ADD failed, ERROR_ACCESS_DENIED`

  `***ERROR ADD failed, NERR_NotPrimary`

  `***ERROR ADD failed, NERR_GroupExists`

  `***ERROR ADD failed, NERR_UserExists`

  `***ERROR ADD failed, NERR_ServiceCtlBusy`

  `***ERROR ADD failed, ERROR_INVALID_PARAMETER`

  The Subscriber has attempted to add a user to the domain. It failed because of the reason stated.

- ◆ `***ERROR ADD failed. = error #, username:` The Subscriber has attempted to add a username to the domain. It failed because of the error # stated.

- ◆ `***ERROR MODIFY failed, NERR_PasswordTooShort ***ERROR MODIFY failed, NERR_InvalidComputer ***ERROR MODIFY failed, ERROR_ACCESS_DENIED ***ERROR MODIFY failed, NERR_NotPrimary ***ERROR MODIFY failed, NERR_GroupExists ***ERROR MODIFY failed, NERR_UserExists ***ERROR MODIFY failed, NERR_ServiceCtlBusy ***ERROR MODIFY failed, ERROR_INVALID_PARAMETER`

  The Subscriber has attempted to modify a user in the domain. It failed because of the reason stated.

- ◆ `***ERROR MODIFY failed. = error #, username:` The Subscriber has attempted to modify a username in the domain. It failed because of the error # stated.

- ◆ `***ERROR RENAME failed, NERR_PasswordTooShort ***ERROR RENAME failed, NERR_InvalidComputer ***ERROR RENAME failed, ERROR_ACCESS_DENIED ***ERROR RENAME failed, NERR_NotPrimary ***ERROR RENAME failed, NERR_GroupExists ***ERROR RENAME failed, NERR_UserExists ***ERROR RENAME failed, NERR_ServiceCtlBusy ***ERROR RENAME failed, ERROR_INVALID_PARAMETER`

  The Subscriber has attempted to rename a user in the domain. It failed because of the reason stated.

- ◆ `***ERROR RENAME failed. = error #, username:` The Subscriber has attempted to rename a username in the domain. It failed because of the error # stated.

- ◆ `***ERROR GETINFO failed, NERR_UserNotFound ***ERROR GETINFO failed, ERROR_ACCESS_DENIED ***ERROR GETINFO failed, NERR_InvalidComputer ***ERROR GETINFO failed`

  A query was requested and failed for the reason stated.

- ◆ `***ERROR DELETE failed, NERR_PasswordTooShort ***ERROR DELETE failed, NERR_InvalidComputer ***ERROR DELETE failed, ERROR_ACCESS_DENIED ***ERROR DELETE failed, NERR_NotPrimary ***ERROR DELETE failed, NERR_GroupExists ***ERROR DELETE failed, NERR_UserExists ***ERROR DELETE failed, NERR_ServiceCtlBusy ***ERROR DELETE failed, ERROR_INVALID_PARAMETER ***ERROR DELETE failed`

The Subscriber has attempted to delete a user from the domain. It failed because of the reason stated.

- `HeapReAlloc error!:` Not enough memory.

- `LookupAccountName error! error#:` LookupAccountName was not successful because of error#.

- `SetSecurityDescriptorDacl error! error#:` SetSecurityDescriptorDacl was not successful because of error#.

- `NetShareAdd error! error#:` NetShareAdd was not successful because of error#.

- `Publisher Error NO MEMORY:` The Publisher ran out of memory.

- `Error out of memory:` The Publisher ran out of memory.

- `Unable to process Nt4 User data:` This error occurs when the Subscriber channel was unable to complete a request to the NT domain.

A **Updates**

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

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

The documentation is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the documentation changes listed in this section.

If you need to know whether a copy of the PDF documentation you are using is the most recent, the PDF document contains the date it was published in the Legal Notices section immediately following the title page.

The documentation was updated on the following dates:

March 18, 2004

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

August 3, 2004

- Some items for the driver have been added to "New Features" on page 9 for the new version of the driver.
- A section has been added describing a new feature for Password Synchronization. See "Password Expiration Time" on page 24.
- A section has been added describing how to configure password filters without allowing remote access to the registry. See "Separately Configuring Password Filters on Each Domain Controller" on page 44.
- In Chapter 2, "Installing the NT Domain Driver," on page 13, the requirement for Windows NT 4 with Service Pack 5 was changed to Service Pack 6.

August 16, 2004

Minor editorial changes were made.

September 28, 2004

The section on "Password Expiration Time" on page 24 was revised to make it clear that the driver caches failed passwords and retries them, not the filter.