

# Novell DirXML<sup>®</sup> Driver for NT Domain

1.1a

[www.novell.com](http://www.novell.com)

IMPLEMENTATION GUIDE

103-000260-001

# N

Novell<sup>®</sup>

## Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Copyright © 2002 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Patents Pending.

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

[www.novell.com](http://www.novell.com)

Implementation Guide

[December 13, 2002](#)

**Online Documentation:** To access the online documentation for this and other Novell products, and to get updates, see [www.novell.com/documentation](http://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 Directory Services is a registered trademark of Novell, Inc., in the United States and other countries.

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** **7**
  
- 1 Introducing the DirXML Driver for NT Domain** **9**
  - Driver Overview. . . . . 9
  - New Features. . . . . 10
  - Default Driver Configuration . . . . . 10
    - Data Flow . . . . . 10
  
- 2 Installing the NT Domain Driver** **13**
  - Planning Considerations . . . . . 13
    - Where to Install the NT Domain Driver . . . . . 13
  - Prerequisites . . . . . 16
    - Information Needed For Installation. . . . . 16
  - Installation and Upgrade . . . . . 16
    - Installing the NT Domain Driver (Local Install) . . . . . 16
    - Installing the NT Domain Driver (Remote Loader Installation) . . . . . 17
    - Upgrading the NT Domain Driver . . . . . 18
    - Post-Installation Tasks . . . . . 18
  
- 3 Customizing the NT Domain Driver** **25**
  - Configuring Driver Parameters . . . . . 25
    - Log Level . . . . . 26
    - Polling Rate . . . . . 26
    - Security Options . . . . . 27
    - Startup Options . . . . . 27
  - Configuring Data Synchronization . . . . . 28
    - Integrating the DirXML Driver for NT Domain and the DirXML Driver for Exchange . . . . . 28
    - Filtering Out Non-User User Objects . . . . . 30
    - Synchronizing Group Information . . . . . 30
    - Changing the Location of User Objects Using Placement Rules . . . . . 32
    - Changing Which Attributes Are Synchronized Using Publisher and Subscriber Filters . . . . . 32
  
- 4 Troubleshooting** **37**
  - Troubleshooting . . . . . 37
  
- 5 Documentation Content Updates** **41**
  - November 15, 2002. . . . . 41
    - Installing the NT Domain Driver. . . . . 42
    - Customizing the NT Domain Driver . . . . . 42



# About This Guide

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

The guide contains the following sections:

- ◆ **Chapter 1, “Introducing the DirXML Driver for NT Domain,” on page 9**  
This section introduces new features and explains the default driver configuration.
- ◆ **Chapter 2, “Installing the NT Domain Driver,” on page 13**  
This section covers both the installation and upgrade processes as well as post-installation setup tasks.
- ◆ **Chapter 3, “Customizing the NT Domain Driver,” on page 25**  
This section explains how to customize driver parameters and data synchronization. It provides examples for common customizations.
- ◆ **Chapter 4, “Troubleshooting,” on page 37**  
This section lists common error messages and possible causes.

## Additional Documentation

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

## Documentation Updates

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

## Documentation Conventions

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

A trademark symbol (®, 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 DirXML. To contact us, send e-mail to [proddoc@novell.com](mailto:proddoc@novell.com).



# 1

## Introducing the DirXML Driver for NT Domain

This section covers the following topics:

- ◆ “Driver Overview” on page 9
- ◆ “New Features” on page 9
- ◆ “Default Driver Configuration” on page 10

### Driver Overview

The DirXML<sup>®</sup> Driver for NT Domain is designed to manage and synchronize Novell<sup>®</sup> eDirectory<sup>™</sup> 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. It also does not synchronize user passwords between eDirectory and the NT 4 Domain. However Password Synchronization for Windows can be installed separately to accomplish this task. See [Password Synchronization for Windows \(http://www.novell.com/documentation/lg/pwdsync10/index.html\)](http://www.novell.com/documentation/lg/pwdsync10/index.html) for more information.

### New Features

The following are new features with this release of the driver:

- ◆ The DirXML Driver for Windows NT has been renamed the DirXML Driver for NT Domain.
- ◆ The driver now supports two new attributes that are part of the User object.
  - ◆ UserLocalGroups
  - ◆ UserGlobalGroups

These attributes are multi-valued strings that list the local and global groups that the user is a part of.

- ◆ The driver initiates the creation of an Exchange mailbox if the DirXML Driver for Exchange is also installed.

When a User object is created in eDirectory and synchronized to the Domain, the Nt4AccountName attribute is populated with *Domain name/user name*. This attribute is the key to the Exchange driver for creating an Exchange mailbox. If the Nt4AccountName

attribute is in the Publisher filter, the Publisher generates a modify event to the DirXML engine, which writes the changes to eDirectory. With this attribute in eDirectory, the Create rule for Exchange, which requires the Nt4AccountName to be populated, is satisfied and the mailbox is created.

## Default Driver Configuration

DirXML fundamentals are explained in the [DirXML Administration Guide \(http://www.novell.com/documentation/lg/dirxml11a/index.html\)](http://www.novell.com/documentation/lg/dirxml11a/index.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.

## Rules

Rules are used to control data synchronization between NT Domain and eDirectory. The NT Domain driver comes with the set of preconfigured rules detailed in [Table 1, "Rules for NT Domain Driver," on page 10](#). These rules can be customized through Novell iManager as explained in [Chapter 3, "Customizing the NT Domain Driver," on page 25](#).

**Table 1** Rules for NT Domain Driver

Rule	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 rule sets a default Surname for all users: <i>Unknown</i> .

---

Rule	Description
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.  <b>NOTE:</b> Because the NT Domain APIs allow queries of only the user name attribute, this rule should not be changed.
Placement	Configured on the Publisher and Subscriber channels.  Specifies that new users will be 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<sup>®</sup> 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 *DirXML 1.1a Administration Guide* (<http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/a2iii88.html>).

The driver can also be installed separately, as explained in this section, by running the DirXML installation and selecting only the NT Domain driver.

This section covers the following installation topics:

- ♦ “Planning Considerations” on page 13
- ♦ “Prerequisites” on page 15
- ♦ “Installation and Upgrade” on page 15

### Planning Considerations

#### 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 DirXML’s driver export and import functionality to expedite synchronization setup for additional domains. See the *DirXML 1.1a Administration Guide* (<http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/a2iii88.html>) for information about driver export and import.

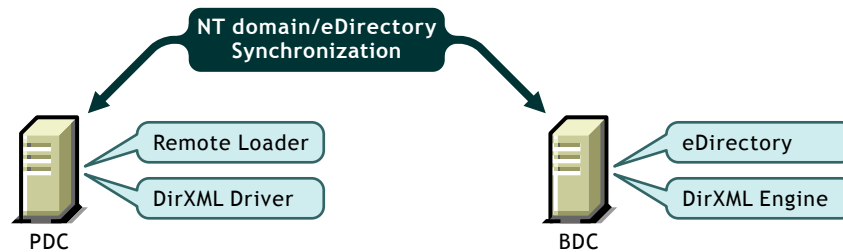
The NT Domain driver can be installed in any of the following configurations:

- ♦ As shown in **Figure 1, “Installation Configuration: Remote Loader,”** on page 14, install Novell<sup>®</sup> eDirectory<sup>™</sup> 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**



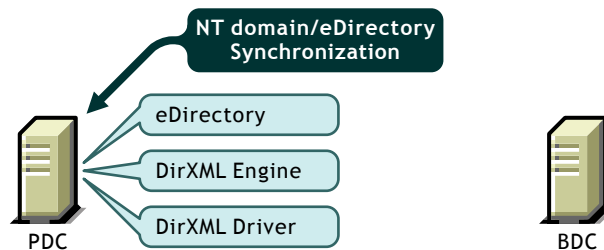
- ◆ As shown in [Figure 2, “Installation Configuration: All Components on the PDC,”](#) on page 14, install Novell eDirectory, the DirXML engine, and the NT Domain driver on the PDC.

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**



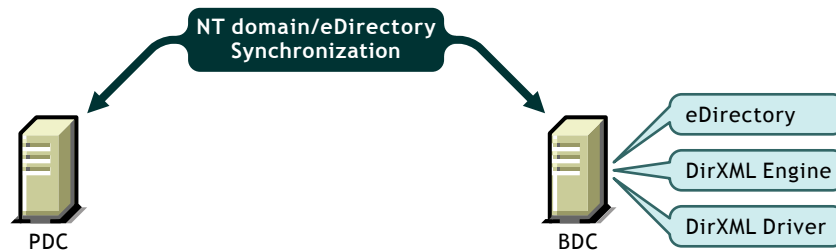
- ◆ As shown in [Figure 3, “Installation Configuration: All Components on the BDC,”](#) on page 15, install Novell eDirectory, the DirXML engine, and the NT Domain driver on the BDC.

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 DirXML 1.1 or later
- ◆ Windows NT 4 with Service Pack 5
- ◆ Novell iManager or ConsoleOne®

For information about setting up iManager, see the *DirXML 1.1a Administration Guide* (<http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/a2iii88.html>).

**NOTE:** You can still use ConsoleOne to manage DirXML. DirXML management using ConsoleOne is explained in the *DirXML 1.1 documentation* (<http://www.novell.com/documentation/lg/dirxml11/index.html>).

## Information Needed For Installation

Collect the following information before installation:

- ◆ 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.

## Installation and Upgrade

### 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. To install the driver locally, run the DirXML 1.1a installation program and select DirXML Engine and Drivers > DirXML Driver for NT4 Domain.

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. To set up a remote configuration:

- 1 Insert the DirXML CD and click Next at the Welcome screen.

- 2** At the License page, click I Accept.
- 3** At the Components dialog box, select DirXML Remote Loader Service and click Next.
- 4** Accept the default installation path for the Remote Loader, then click Next.
- 5** Mark the following items, then click Next.
  - ◆ DirXML Driver for NT Domain
  - ◆ DirXML Remote Loader Service
- 6** Review the Product Summary, and then click Finish to install Remote Loader files.
- 7** When prompted, create a shortcut.
- 8** Run the DirXML Remote Loader Configuration Wizard from your desktop.
- 9** At the Welcome page, click Next.
- 10** Keep the default Command Port number, then click Next.
- 11** Keep the default Configuration File Name, then click Next.
- 12** In the DirXML Driver dialog, mark Native, then click Next.
- 13** In the Connection to DirXML dialog, leave the default Port settings.
- 14** Set Trace Level to 3, so that you'll get minimal tracking data for troubleshooting, specify a location and filename for trace file, then click Next.
- 15** Mark Install the Remote Loader Instance as a Service, then click Next.
- 16** Set Remote Loader and Driver Object passwords.
- 17** Review the summary, then click Finish.
- 18** When prompted, start the service.

Continue with driver setup as explained in [“Post-Installation Tasks” on page 16](#).

## Upgrading the NT Domain Driver

To upgrade your DirXML Driver for NT Domain, run the DirXML installation program and select DirXML Engine and Drivers > DirXML Driver for NT4 Domain. You can do this at the same time that you install the engine or you can do it after the engine is installed.

The new driver replaces the previous driver but keeps the previous driver's configuration. Simply confirm the settings read by the driver import file.

No post-installation configuration is required. However, you must restart the driver. To do this in Novell iManager, select DirXML Management > Overview. Then click the driver status indicator in the upper right corner of the driver icon and click Start Driver.

If you are upgrading from 1.1, no re-activation is required. If you are upgrading from an earlier release of DirXML, you must re-activate the driver. See [“Activating the Driver” on page 19](#).

You should also ensure that the name and path specified in the Driver Module section of the Driver Configuration is correct. The name should be NTDomainShim.dll.

## Post-Installation Tasks

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 17
- ◆ “Granting Rights to the Driver” on page 17
- ◆ “Setting Up the Driver” on page 17
- ◆ “Starting the Driver” on page 18
- ◆ “Migrating and Resynchronizing Data” on page 19
- ◆ “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 DirXML 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** Check 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.

## Setting Up the Driver

The preconfigured NT Domain driver file will create and configure the objects needed to make the driver work properly. To import the preconfigured driver:

- 1** In iManager, select DirXML Management > Create Driver.
- 2** Select a driver set.  
If you place this driver in a new driver set, you must specify a driver set name, context, and associated server.
- 3** Mark Import a Preconfigured Driver from the Server and select the NTDomainImport.xml file.

The preconfigured driver file is installed on the Web server when you set up iManager.

- 4** At the prompts, provide the information you collected earlier. You will be prompted to enter the following:
  - ◆ Driver name: The eDirectory object name to be assigned to this driver.
  - ◆ Domain server: The PDC for the domain you will synchronize with. Enclose the name in quotation marks. This value will be used in the publisher placement rule.
  - ◆ Domain name: The domain you want to synchronize with eDirectory.
  - ◆ Polling rate: The interval at which the driver will check the domain for changes. Setting the polling rate to less than 3000 milliseconds will impact performance.
  - ◆ Authoritative user: An account with Read/Write rights to the domain that the driver can use for domain access. We recommend creating an account to be used exclusively by the driver rather than assigning the driver to an existing account.
  - ◆ User password: The password for the Authoritative user.
  - ◆ eDirectory container for placement: The container where new objects being synchronized from NT to eDirectory should be placed. By default, this is also the only container from which User objects will be synchronized to NT. If you want eDirectory objects in other containers to be synchronized you will have to create additional placement rules.
  - ◆ Create rule: The default value for the required eDirectory Surname attribute. eDirectory requires a Surname attribute for a User object. The domain does not use this attribute, so one needs to be manufactured. The wizard builds a Publisher Create rule that will set a default user surname. You can accept the default user surname of Unknown or set your own default.
- 5** When the import is finished, click Yes to define security equivalence on the imported driver.
  - 5a** Click Add, then select an object with Admin rights (or any other rights that you want the driver to have).
  - 5b** Click Apply, then click Close.
- 6** Click Yes to specify excluded users:
  - 6a** Click Add, then select any users you want to exclude (such as the admin user).
  - 6b** Click Apply, then click Close.
- 7** Click Finish.

The DirXML objects necessary for synchronization with NT have now been created.

## Starting the Driver

- 1** In iManager, select DirXML Management > Overview.
- 2** Locate the driver in its driver set.
- 3** Click the driver status indicator in the upper right corner of the driver icon, then click Start Driver.

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 was added to this release of DirXML, you'll 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 19](#).

## Migrating and Resynchronizing Data

DirXML will synchronize 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 rules, as well as the Subscriber filter, to the object.
- ♦ **Migrate data into eDirectory:** Allows you to define the criteria DirXML 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 rules, as well as the Publisher filter, to the object. Objects are migrated into eDirectory using the order you specify in the Class list.
- ♦ **Synchronize:** DirXML looks in the Subscriber class filter and processes all objects for those classes. Associated objects will be merged. Unassociated objects will be processed as Add events.

To use one of the options explained above:

- 1** In iManager, select DirXML Management > Overview.
- 2** Locate the driver set containing the NT Domain driver, then double-click the driver icon.
- 3** Click the appropriate migration button.

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 will perform a synchronization the next time it is started. In the synchronization, the driver will issue a Modify command at startup for each User object found in the domain.

The DirXML engine will accept the Modify command if the User has an association. If the User does not have an association, the engine will query the driver for all of the attributes in the Publisher filter. The engine will then create the User.

## Activating the Driver

DirXML and DirXML drivers must be activated within 90 days of installation, or they will not run. At any time during the 90 days, or afterward, you can choose to active DirXML products to a fully licensed state.

To activate your driver, you should:

- ♦ Purchase DirXML licenses
- ♦ Generate a Product Activation Request

- ◆ Submit the Product Activation Request
- ◆ Install the Product Activation Credential received from Novell

For more information about completing these tasks, refer to [Activating Your DirXML Product \(http://www.novell.com/documentation/lg/dirxml11a/index.html\)](http://www.novell.com/documentation/lg/dirxml11a/index.html).

# 3

## Customizing the NT Domain Driver

This section covers two general categories of customization:

- ◆ “Configuring Driver Parameters” on page 25

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.

- ◆ “Configuring Data Synchronization” on page 27

The real power of DirXML<sup>®</sup> 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.

### Configuring Driver Parameters

Use Novell<sup>®</sup> iManager to make the appropriate adjustments to any of the following properties: log level, polling rate, security options, and startup options.

#### Log Level

The log level determines the kinds of errors that are sent to the DirXML status logs, DSTrace, and the eDirectory Report and Notification service. Report and Notification is a new and highly customizable means of tracking DirXML activity. For complete information about Report and Notification, see [Tracking DirXML Status \(http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/afae8bz.html\)](http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/afae8bz.html) in the *DirXML 1.1a Administration Guide (http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/a2iii88.html)*.

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.

## Security Options

Creating a new user that has Read/Write rights to the domain and to the SAM registry will make DirXML management easier. 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, DirXML 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” on page 27](#)
- ♦ [“Filtering Out Non-User User Objects” on page 28](#)
- ♦ [“Synchronizing Group Information” on page 28](#)
- ♦ [“Changing the Location of User Objects Using Placement Rules” on page 29](#)
- ♦ [“Changing Which Attributes Are Synchronized Using Publisher and Subscriber Filters” on page 30](#)

## 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 DirXML rules to solve this problem.

The DirXML Driver for NT Domain has a User attribute called Nt4AccountName. 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 Nt4AccountName needs to be put in the MailBox attribute Assoc-NT-Account. Keep in mind that attribute names are case sensitive.

- 1** Pick an existing NDS<sup>®</sup> attribute (for example, preferredName) to hold the value of NT User objects attribute Nt4AccountName.
- 2** Change the DirXML Driver for NT Domain Schema Mapping rule to map preferredName to Nt4AccountName.

For example:

```
<attr-name>
  <nds-name>preferredName</nds-name>
  <app-name>Nt4AccountName</app-name>
</attr-name>
```

- 3** Change the DirXML Driver for Exchange Schema Mapping rule to map preferredName to Assoc-NT-Account.

For example:

```
<attr-name>
  <nds-name>preferredName</nds-name>
  <app-name>Assoc-NT-Account</app-name>
</attr-name>
```

- 4 Make a Create rule for the DirXML Driver for Exchange that will not allow a new MailBox object to be created unless the preferredName attribute is populated.

For example:

```
<rule name="SubscriberCreateRule">
  <create-rules>
    <create-rule class-name="User">
      <required-attr attr-name="preferredName" />
      <required-attr attr-name="Given Name" />
    </create-rule>
  </create-rules>
</rule>
```

- 5 Add the preferredName attribute to the Publisher filter on the DirXML Driver for NT Domain and the Subscriber filter on the DirXML Driver for Exchange.
- 6 Restart both drivers.

### Data Flow in the NT Domain and Exchange 5.5 Drivers

These 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 preferredName 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 preferredName 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 preferredName 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="add[@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>
```

## 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 information 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 rule 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 rule and map the new attributes.  
  
You can map the NT attributes to any multivalued 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 Rules

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

To modify Placement rules:

- 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. Rules, style sheets, and filters can be edited here.
- 3 Double-click the Placement Rule you want to edit, then make the appropriate changes.

**IMPORTANT:** All Placement rules must use the slash syntax.

## 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. Rules, style sheets, and filters 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 rule.)	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.

<b>Driver Attribute</b>	<b>USER_INFO_3 Name</b>	<b>Data Type</b>	<b>Description</b>
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.
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.

Driver Attribute	USER_INFO_3 Name	Data Type	Description
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.
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.

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.

# 4 Troubleshooting

You can use the Novell® eDirectory™ Report and Notification Service to control how and where DirXML® messages are delivered. Using this service in combination with the driver log level setting provides you with tracking control at a very granular level and with the option for immediate notice when problems occur. For more information, see [Tracking DirXML Status \(http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/afae8bz.html\)](http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/afae8bz.html) in the *DirXML 1.1a Administration Guide* (<http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/a2iii88.html>).

## 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 rule.
- ◆ `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.



# 5

## Documentation Content Updates

This section contains information on documentation content changes that have been made in the *Implementation Guide* for the DirXML Driver for NT Domain. The information will help you to keep current on updates to the documentation.

The information is grouped according to the date the documentation updates were published. Within a dated section, the changes are alphabetically listed by the names of the main table of contents sections for Policy and Distribution Services.

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:

- ♦ “November 15, 2002” on page 41
- ♦ “April 21, 2003” on page 42

### November 15, 2002

Updates were made to the following sections. The changes are explained below.

- ♦ [Installing the NT Domain Driver](#)
- ♦ [Customizing the NT Domain Driver](#)

### Installing the NT Domain Driver

The following updates were made in this section:

Location	Change
<a href="#">“Upgrading the NT Domain Driver” on page 16</a>	Added information about updating the driver name and path in the Driver Configuration.
<a href="#">“Migrating and Resynchronizing Data” on page 19</a>	Corrected explanation of Synchronize. Synchronize will update objects regardless of association.

### Customizing the NT Domain Driver

The following updates were made in this section:

Location	Change
<a href="#">"Security Options" on page 26</a>	Corrected explanation of the driver password. It is not used to restrict access to driver configuration.
<a href="#">"Startup Options" on page 26</a>	Corrected explanation of the Disabled option. Under some conditions, data changes occurring when the driver is Disabled can be synchronized.
<a href="#">"Integrating the DirXML Driver for NT Domain and the DirXML Driver for Exchange" on page 27</a>	Corrected the <app-name> statement in step 3. It changed from <pre>&lt;app-name&gt; Assoc-NT-Account &lt;/app-name&gt;</pre> to <pre>&lt;app-name&gt;Assoc-NT-Account&lt;/app-name&gt;</pre>
<a href="#">"Integrating the DirXML Driver for NT Domain and the DirXML Driver for Exchange" on page 27</a>	Corrected attribute assignments in step 5.
<a href="#">"Synchronizing Group Information" on page 28</a>	This section was called Resolving Local and Global Groups. The name was changed and the procedure updated to cover modifications required on group objects.

## April 21, 2003

- ◆ The case of the attribute name "Nt4AccountName" is now correct. (The incorrect instances had shown the case as "NT4AccountName.") To avoid problems, keep in mind that attribute names are case sensitive.
- ◆ The attribute names "UserGlobalGroups" and "UserLocalGroups" are now correct. (The incorrect instances had shown the names as singular instead of plural: "UserGlobalGroup" and "UserLocalGroup." The incorrect instances appeared only in [Chapter 3, "Customizing the NT Domain Driver," on page 25.](#))