# Novell DirXML® Starter Pack

1.0

www.novell.com

LAB GUIDE

December 15, 2003

Novell®

## Legal Notices

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

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

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

U.S. Patent No. 5,157,663; 5,349,642; 5,455,932; 5,553,139; 5,553,143; 5,572,528; 5,594,863; 5,608,903; 5,633,931; 5,652,854; 5,671,414; 5,677,851; 5,692,129; 5,701,459; 5,717,912; 5,758,069; 5,758,344; 5,781,724; 5,781,733; 5,784,560; 5,787,439; 5,818,936; 5,828,882; 5,832,274; 5,832,275; 5,832,483; 5,832,487; 5,859,978; 5,870,561; 5,870,739; 5,873,079; 5,878,415; 5,884,304; 5,893,118; 5,903,650; 5,903,720; 5,905,860; 5,910,803; 5,913,025; 5,913,209; 5,915,253; 5,925,108; 5,933,503; 5,933,826; 5,946,002; 5,946,467; 5,956,718; 5,956,745; 5,964,872; 5,974,474; 5,983,223; 5,983,234; 5,987,471; 5,991,810; 6,002,398; 6,014,667; 6,016,499; 6,023,586; 6,029,247; 6,052,724; 6,061,726; 6,061,740; 6,061,743; 6,065,017; 6,081,774; 6,081,814; 6,094,672; 6,098,090; 6,105,062; 6,105,069; 6,105,132; 6,115,039; 6,119,122; 6,144,959; 6,151,688; 6,157,925; 6,167,393; 6,173,289; 6,216,123; 6,219,652; 6,233,859; 6,247,149; 6,269,391; 6,286,010; 6,308,181; 6,314,520; 6,324,670; 6,338,112; 6,345,266; 6,353,898; 6,424,976; 6,466,944; 6,477,583; 6,477,648; 6,484,186; 6,496,865; 6,510,450; 6,516,325; 6,519,610; 6,532,451; 6,532,491; 6,539,381; RE37,178. Patents Pending.

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

www.novell.com

DirXML Starter Pack Lab Guide for Novell Nterprise Linux Services
December 15, 2003

**Online Documentation:** To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

## Novell Trademarks

## Third-Party Trademarks

# Contents

# About This Guide

DirXML® is a data-sharing solution that leverages Novell® eDirectory™ to synchronize, transform, and distribute information across applications, databases, and directories.

The solution included with Novell Nterprise™ Linux* Services provides licensed synchronization of information held in NT Domains, Active Directory* Domains, and eDirectory trees. When data from one system changes, DirXML detects and propagates these changes to other connected systems based on the business policies you define.

This document contains information that will help you get DirXML installed in a default configuration. The guide contains the following sections:

- Chapter 1, "Introducing the Novell DirXML Starter Pack," on page 9

  Understanding the design and purpose of the DirXML Starter Pack is key to a successful deployment. This section explains the product architecture and default data flow.

- Chapter 2, "Planning Your Installation," on page 21

  DirXML provides great flexibility for where you install components and how data can be synchronized. This section introduces issues you'll want to consider before starting your installation.

- Chapter 3, "Installing the Novell DirXML Starter Pack," on page 27

  For installation instructions, please refer to the Novell Nterprise Linux Services Installation Guide (http://www.novell.com/documentation/lg/nnls/install/data/front.html#bktitle).

- Chapter 4, "Setting Up Participating Systems," on page 31

  Each system that will participate in data synchronization requires installation of a DirXML driver. After driver installation, you must provide the drivers with system-specific information. This section walks you through driver installation, configuration, and validation.

- Chapter 5, "Setting Up Password Synchronization," on page 63

  After drivers have been successfully installed, you can install the password synchronization components. This section explains how to install these components and make password synchronization work in your environment.

- Appendix A, "Activating Novell DirXML Products," on page 79

  DirXML and DirXML drivers must be activated within 90 days of installation, otherwise they will shut down. This section explains how to request and install an activation credential.

### Additional Documentation

For documentation on using DirXML and the DirXML drivers, see the DirXML Documentation Web site (http://www.novell.com/documentation/lg/dirxml11a).

## Documentation Updates

For the most recent version of the *DirXML Starter Pack for NNLS Installation Guide*, see the Novell Nterprise Linux Services Documentation Web Site (http://www.novell.com/documentation/lg/index.html).

## Documentation Conventions

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

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

## User Comments

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

# 1 Introducing the Novell DirXML Starter Pack

Today's businesses are faced with the challenge of managing user accounts in many independent systems. The creation and management of separate user accounts is expensive and prone to data synchronization errors.

DirXML® is a data-sharing solution that leverages Novell® eDirectory™ to automatically synchronize, transform, and distribute information across applications, databases, and directories.

The solution included with Novell Nterprise Linux Services provides licensed synchronization of information held in NT Domains, Active Directory, and eDirectory. Additionally, evaluation drivers for several other systems including PeopleSoft*, GroupWise®, and Lotus Notes*, are included to allow you to explore data synchronization for your other systems.

When data from one system changes, DirXML detects and propagates these changes to other connected systems based on the business policies you define. Using DirXML rules and style sheets, you can make any of these systems the authoritative source for all or some of the data, or you can make each of the systems equally responsible for updating any data changes.

This solution also offers you the ability to synchronize user passwords. With PasswordSync, a user is required to remember only a single password to log in to any of these systems. Administrators can manage passwords in the system of their choice. Any time a password is changed in one of these environments, it will be updated in all of them.

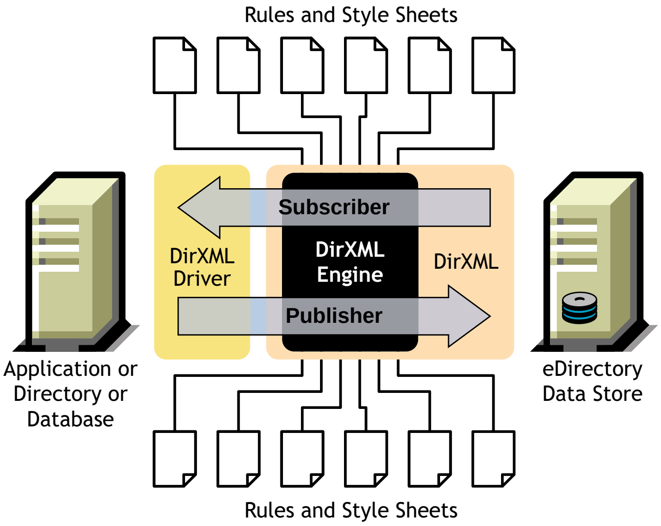
This section contains information on the DirXML data sharing model, and the data flow and object placement between eDirectory and other applications:

- "The DirXML Data Sharing Model" on page 9
- "Default Data Flow" on page 14

## The DirXML Data Sharing Model

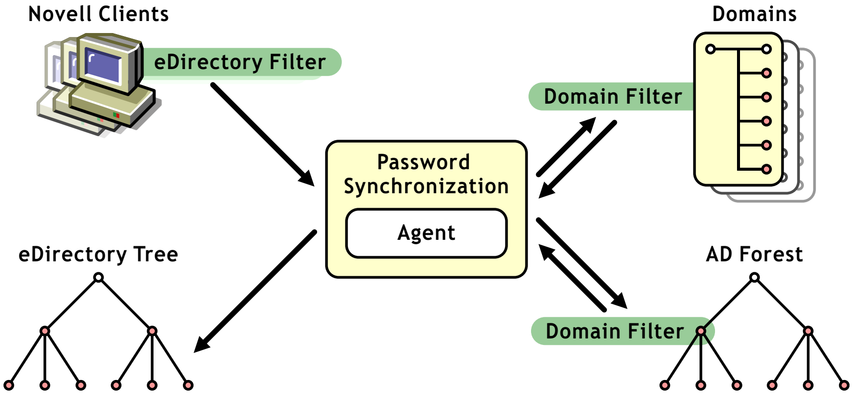
In simplest terms, DirXML delivers application-specific drivers and a data transformation engine to communicate data changes between applications. DirXML drivers take their direction for what data to manage and how to manage it from DirXML rules and style sheets. You customize these rules and style sheets to meet requirements unique to your environment.

**Figure 1 DirXML Architecture**



DirXML employs PasswordSync Filters to capture password changes and PasswordSync Agents to communicate those changes to eDirectory.

**Figure 2 Password Synchronization Model**



These DirXML components and their functions are described briefly in the following sections.

- DirXML Engine
- DirXML Driver for Active Directory
- DirXML Driver for NT Domain
- DirXML Driver for eDirectory
- Evaluation Drivers
- Filters, Rules, and Style Sheets
- Password Synchronization Filters and Agents
- DirXML Objects in eDirectory
- Management Utilities

For a more complete discussion of DirXML and PasswordSync architecture, see the following documents:

- Understanding the DirXML Architecture (http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/a3a6f54.html)
- Understanding Password Synchronization (http://www.novell.com/documentation/lg/pwdsync10/passsync/data/adtyhxw.html)

## DirXML Engine

The DirXML engine is the communication foundation for any number of drivers communicating with various databases, directories, and applications. The DirXML engine translates data events into XML documents and uses rules to determine how the data modifications are sent to participating applications. The engine ensures consistent processing methods for disparate data.

## DirXML Driver for Active Directory

This driver is installed on your Linux server, but runs remotely on a Windows* workstation or server and is designed to synchronize data between Active Directory and participating applications. Using the Active Directory driver, you can also enable an Active Directory object as a Microsoft Exchange 2000 mailbox. The driver comes with a configuration file to help you set up initial data processing policies and driver behavior.

## DirXML Driver for NT Domain

This driver is installed on your Linux server, but runs remotely on a Windows workstation or server and is designed to synchronize data between an NT 4 domain and participating applications. It comes with a configuration file to help you set up initial data processing policies and driver behavior.

## DirXML Driver for eDirectory

This driver runs on an eDirectory server (a Linux, NetWare, or Windows server for this Starter Pack) and is designed to synchronize objects and attributes between different eDirectory trees. Because you are synchronizing data between eDirectory trees, you will always have two drivers installed, each in its own tree. The driver in one tree communicates with the driver in the other tree. The driver comes with a configuration file to help you set up initial data processing rules and driver behavior.

## Evaluation Drivers

In addition to the licensed drivers that are included when you purchase the DirXML Starter Pack, additional drivers are included in the media for your evaluation. They may include the following:

- DirXML Driver for LDAP
- DirXML Driver for JDBC*
- DirXML Driver for Delimited Text
- DirXML Driver for PeopleSoft
- DirXML Driver for SAP* HR
- DirXML Driver for GroupWise

- DirXML Driver for Exchange
- DirXML Driver for Lotus Notes
- DirXML Driver for SIF

Evaluation drivers are fully functional, separately licensed drivers. They provide you with the opportunity to explore data synchronization for additional systems.

**NOTE:** Evaluation drivers are not provided as product updates. To download patches and fixes for DirXML drivers, visit Product Updates (http://support.novell.com/filefinder/5069/index.html).

You are invited to install these drivers and test them with your own data; however, unless activated, an evaluation driver will stop working 90 days after installation. To continue using the driver, you must purchase and activate it. This purchase and activation is separate from the purchase and activation of the Starter Pack.

If you decide not to purchase an evaluation driver that you have tested, you should uninstall it and reverse any data changes resulting from your use of the driver.

## Filters, Rules, and Style Sheets

Filters, rules, and style sheets are the driver-specific controls that manage data exchange and transformation. They are applied to data coming from the target system into eDirectory (*Publisher* data) and to data going from eDirectory into the target system (*Subscriber* data).

**Filters** specify which objects and attributes can be shared between the target system and eDirectory. A driver generally has two filters: the *Subscriber* filter, which determines the objects and attributes that are owned by eDirectory and are pushed to the application, and the *Publisher* filter, which determines the objects and attributes that are owned by the application and pushed to eDirectory.

**Rules** are used to define requirements for object creation, matching, and placement. For example, a Creation rule might require that a User object include values for the Given Name and Surname attributes before the creation can take place.

**Style Sheets** are XSLT documents used to transform events and data. For example, you might have an event transformation style sheet that generates an initial password based on user-specific data when a new account is created. Complex customizations are managed with style sheets and require XSLT expertise.

## Password Synchronization Filters and Agents

PasswordSync Filters intercept password changes and then route the change notifications to PasswordSync Agents for distribution. Filters also receive relayed notice of password changes from agents and then set new passwords in the domain. A filter must be installed on every domain controller in each domain that participates in password synchronization.

The PasswordSync Agent is a service that runs on a Windows computer. When an agent receives password change notifications, it finds an available domain controller for each of the domains that it services and then sends the notification to the filters installed on these domain controllers. You can install agents on several workstations to improve performance when network topology issues arise and to provide redundancy for fault tolerance.

Agents and filters are indirectly dependent on DirXML drivers; they rely on the drivers to ensure that the necessary password synchronization objects and attributes are established initially.

## DirXML Objects in eDirectory

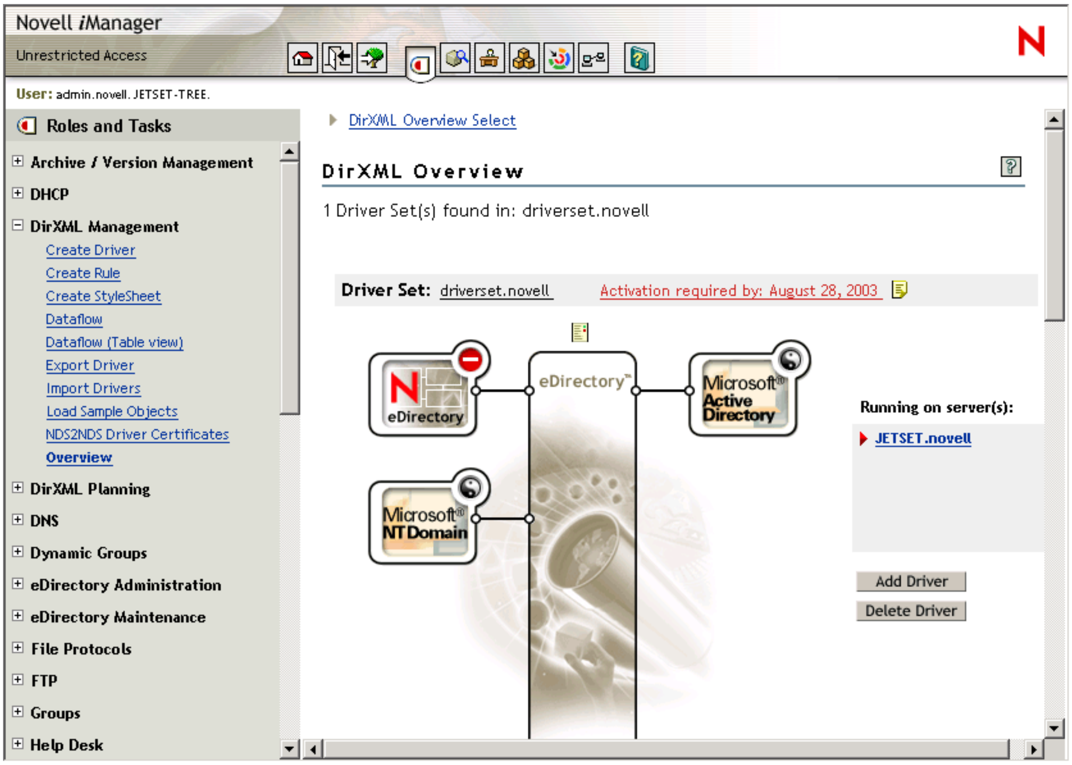
DirXML components are represented as objects in the eDirectory tree. These objects include the following:

| Object | Description |
|---|---|
| Driver Set | A driver set is a container that holds DirXML drivers. Only one driver set can be active on a server at a time. As a result, all active drivers must be grouped into the same driver set. |
| Driver | A DirXML driver object represents a driver that connects to an application that integrates with eDirectory. |
| Rule | DirXML rule objects define the criteria for data exchanges. DirXML includes the following kinds of rules:<br>◆ Matching Rule: Specifies what constitutes a match when objects already exist in both eDirectory and the target application<br>◆ Creation Rule: Determines the requirements for object creation<br>◆ Placement Rule: determines object placement<br>◆ Schema Mapping Rule: Establishes the mapping between objects and attributes in the target application and those in eDirectory<br>Each driver comes with a default set of rule definitions that you can modify to meet the data sharing requirements of your environment. |
| nadPwdSync | This object represents a PasswordSync Agent. The agent uses this object to authenticate to eDirectory and gain access to other objects participating in password synchronization, including users, nadDomains, and servers. |
| nadPwdProvider | This object provides the connection between a PasswordSync Agent (represented as the parent nadPwdSync Object) and a domain. It holds domain-specific information required by the agent. |
| nadDomain | The nadDomain object describes a single NT or Active Directory domain. Each nadDomain object holds a DirXML association with the DirXML driver that controls the domain. |

## Management Utilities

We recommend that you set up and configure DirXML using Novell iManager 2.0. iManager includes several DirXML wizards to help you quickly complete tasks such as creating a new rule, creating a new driver, or exporting existing driver configurations. It also gives you a graphical view of DirXML objects and their relationships to each other.

**Figure 3 Novell iManager 2.0**



1 Driver Set(s) found in: driverset.novell

Driver Set: driverset.novell Activation required by: August 28, 2003

**NOTE:** If iManager is not an option for your environment, DirXML can be managed using ConsoleOne®. Information about using ConsoleOne to manage DirXML is available in the *DirXML 1.1 Administration Guide* (http://www.novell.com/documentation/lg/dirxml11/dirxml/data/hgcbnee7.html).

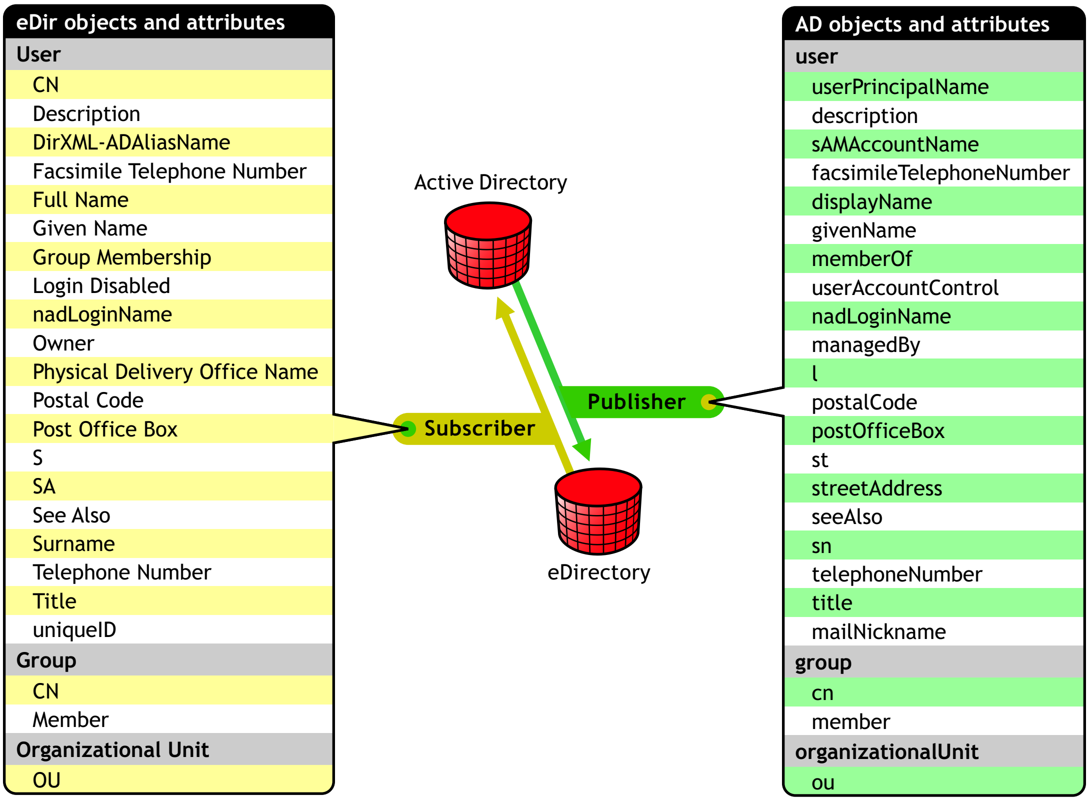
# Default Data Flow

You can modify default driver settings when you first configure the driver or later if your business policies or data exchange requirements change.

## Default Driver Settings for Active Directory

During driver configuration, you specify whether Active Directory or eDirectory will be the authoritative source for object data. You can also choose to make both systems equally responsible for object data by specifying bi-directional synchronization as shown in the following illustration:

**Figure 4 Default Data Flow for Active Directory**



## Event Processing

How the events in one directory are handled in the other directory depends on which system you designate as the authoritative source.

- **If you specify Active Directory as the authoritative source**, any Active Directory add, delete, and modify events are synchronized to eDirectory; eDirectory events are not synchronized back to Active Directory. This means that an object deletion in Active Directory results in an object deletion in eDirectory, but an object deletion in eDirectory does not have any impact on the associated Active Directory object. Further, the next time that the Active Directory object is modified, it is re-created in eDirectory.
- **If you specify eDirectory as the authoritative source**, any eDirectory add, delete, and modify events are synchronized to Active Directory; Active Directory events are not synchronized back to eDirectory. This means that an object deletion in eDirectory results in an object deletion in Active Directory, but an object deletion in Active Directory does not have any impact on the associated eDirectory object. Further, the next time that eDirectory object is modified, it is re-created in Active Directory.
- **If you specify both directories as the authoritative source**, any Active Directory add, delete, and modify events are synchronized to eDirectory, and any eDirectory add, delete, and modify events are synchronized to Active Directory. This means that an object deletion in Active Directory results in an object deletion in eDirectory, and an object deletion in eDirectory results in an object deletion in Active Directory.

You can customize rules and style sheets to specify that Active Directory is the authoritative source for specific events and specific attributes and that eDirectory is the authoritative source for other events and other attributes.

### Naming Conventions

Active Directory users might log on with either a pre-Windows 2000 user logon name (the sAMAccountName) or a Windows 2000 logon name (the user principal name, UPN). User object names are generated as follows:

- If the user object is created in Active Directory, the corresponding user object in eDirectory is named after the UPN. For example, an Active Directory UPN of rprice@acme.com generates an eDirectory user object with CN rprice.
- If the user object is created in eDirectory, the corresponding user object in Active Directory is named after the Full Name. For example, a user object created in eDirectory with a CN of rprice and a Full Name of Richard Price creates an Active Directory user object with cn=Richard Price and a UPN/sAMAccountName=rprice.

### Object Placement

During configuration, you also specify object placement. For synchronization with Active Directory, you have the following placement options:

**Mirrored:** You specify a base container in the target directory, then the hierarchy from the source directory is mirrored inside the base container of the target directory. The structure of the synchronized object's source DN is reflected inside the base container in the target directory.

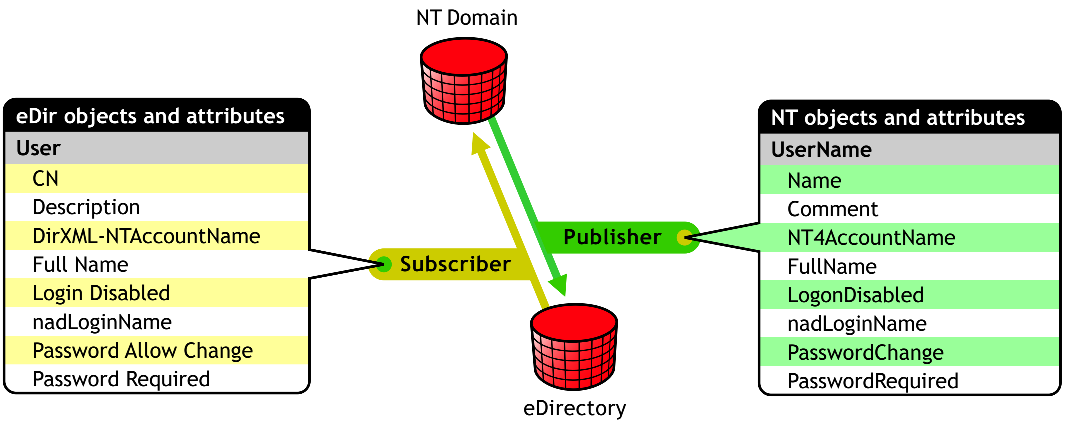
**Flat:** You specify a base container for User objects and a base container for Group objects. All synchronized User objects are placed directly in the base container for users, and all synchronized Group objects are placed directly in the base container for groups.

If these placement options don't meet the needs of your organization, you can create customized style sheets or rules to handle placement.

## Default Driver Settings for NT Domain

During driver configuration, you specify whether NT Domain or eDirectory will be the authoritative source for object data. You can also choose to make both systems equally responsible for object data by specifying bi-directional synchronization as shown in the following illustration:

**Figure 5 Default Data Flow for NT Domain**



### Event Processing

How the events in one directory are handled in the other directory depends on which system you designate as the authoritative source.

- **If you specify NT as the authoritative source**, any NT add, delete, and modify events are synchronized to eDirectory; eDirectory events are not synchronized back to NT. This means that an object deletion in NT results in an object deletion in eDirectory, but an object deletion in eDirectory does not have any impact on the associated NT object. Further, the next time that NT object is modified, it is re-created in eDirectory.
- **If you specify eDirectory as the authoritative source**, any eDirectory add, delete, and modify events are synchronized to NT; NT events are not synchronized back to eDirectory. This means that an object deletion in eDirectory results in an object deletion in NT, but an object deletion in NT does not have any impact on the associated eDirectory object. Further, the next time that eDirectory object is modified, it is re-created in NT.
- **If you specify both directories as the authoritative source**, any NT add, delete, and modify events are synchronized to eDirectory, and any eDirectory add, delete, and modify events are synchronized to NT. This means that an object deletion in NT results in an object deletion in eDirectory, and an object deletion in eDirectory results in an object deletion in NT.

You can customize rules and style sheets to specify that NT is the authoritative source for specific events and specific attributes and that eDirectory is the authoritative source for other events and other attributes.

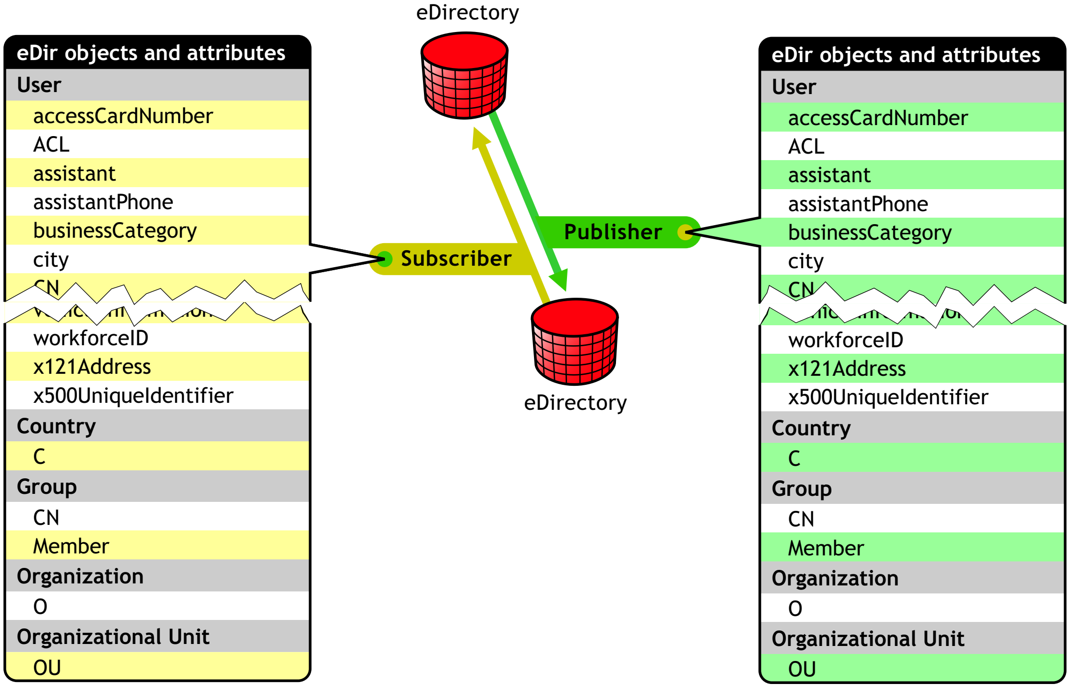
### Object Placement

NT Domain object data is stored in a flat database. eDirectory object data is stored in a hierarchical tree structure. The default configuration for NT specifies that new objects created in NT Domain and synchronized to eDirectory are placed in a single container that you specify during driver configuration; however, you can use customized style sheets to define hierarchical placement. Associated objects (existing objects found to be a match) retain their hierarchical placement in eDirectory.

## Default Driver Settings for eDirectory

The default driver filters for eDirectory allow for synchronization of a large number of attributes, regardless of their class. During driver configuration, you specify whether the local or remote tree is the authoritative source for object data. You can also choose to make both trees equally responsible for object data by specifying bi-directional synchronization as shown in the following illustration:

**Figure 6** Default Data Flow for eDirectory



## Event Processing

How the events in one directory are handled in the other directory depends on which system you designate as the authoritative source.

- **If you specify a single directory, such as Directory 1, as the authoritative source**, any Directory 1 add, delete, and modify events are synchronized to Directory 2; Directory 2 events are not synchronized back to Directory 1. So an object deletion in Directory 1 results in an object deletion in Directory 2, but an object deletion in Directory 2 does not have any impact on the associated Directory 1 object. Further, the next time that Directory 1 object is modified, it is re-created in Directory 2.

  The opposite would be true if you specify Directory 2 as the authoritative source.

- **If you specify both directories as the authoritative source**, any add, delete, and modify events are synchronized in both directories. This means that an object deletion in Directory 1 results in an object deletion in Directory 2. An object deletion in Directory 2 results in an object deletion in Directory 1.

You can customize rules and style sheets to specify that NT is the authoritative source for specific events and specific attributes and that eDirectory is the authoritative source for other events and other attributes.

## Object Placement

During configuration, you also specify object placement. For synchronization with eDirectory, you have the following placement options:

**Mirrored:** You specify a base container on the target tree, then the hierarchy from the source tree is mirrored inside the base container of the target tree. The structure of the synchronized object's source DN will be reflected inside the base container of the target tree.

**Flat:** You specify a base container for User objects and a base container for Group objects. All synchronized User objects are placed directly in the base container for users, and all synchronized Group objects are placed directly in the base container for groups.

**Department:** You specify a base container on the target tree, then a synchronized object and its parent OU object are synchronized to the target base container. For example, JBrown.Sales.Tree1Org would be synchronized into the target tree as JBrown.Sales.*BaseContainer*.Tree2Org.

## Account Management Scenario

The following examples illustrate the account management functionality provided by the DirXML Starter Pack. These examples are based on an installation configured to synchronize account data between eDirectory and Active Directory when both directories are considered authoritative.

### New Employee, John Brown, Is Hired

An administrator creates a user account for John in Active Directory using a template that requires John to change his password when he logs in for the first time. Account creation is necessary only once.

- DirXML checks to see if John already has an eDirectory account. Because John is new, he does not have an account.
- DirXML then checks to see if there is enough Active Directory data to create an account in eDirectory. John's account has the minimum data requirements for user object creation, Given Name and Surname.

  DirXML creates an eDirectory account for John.
- John logs on to Active Directory and sets his password. The password is captured by the PasswordSync Filter, delivered to the PasswordSync Agent, and synchronized into eDirectory.

### John Accepts an Assignment in a New Division of the Company

John's new assignment requires him to move from the Los Angeles office to the New York office. An administrator updates the contact information for John's user object in eDirectory.

- DirXML is notified that John's user object has been modified.
- DirXML updates John's Active Directory account with the new address and phone number information.

### John Changes His Active Directory Password

Company policy dictates that passwords be changed every 90 days. Just days after John has settled into his new office, he is prompted to change his Active Directory password.

- John resets his password when he logs on to Active Directory.
- The PasswordSync Filter captures John's password change and delivers it to the PasswordSync Agent.
- The agent notifies eDirectory and John's eDirectory password is updated.

### John Leaves the Company

John takes a position in a partner company. The eDirectory administrator disables John’s eDirectory account.

- DirXML is notified of the change and deletes John’s Active Directory account.

# 2 Planning Your Installation

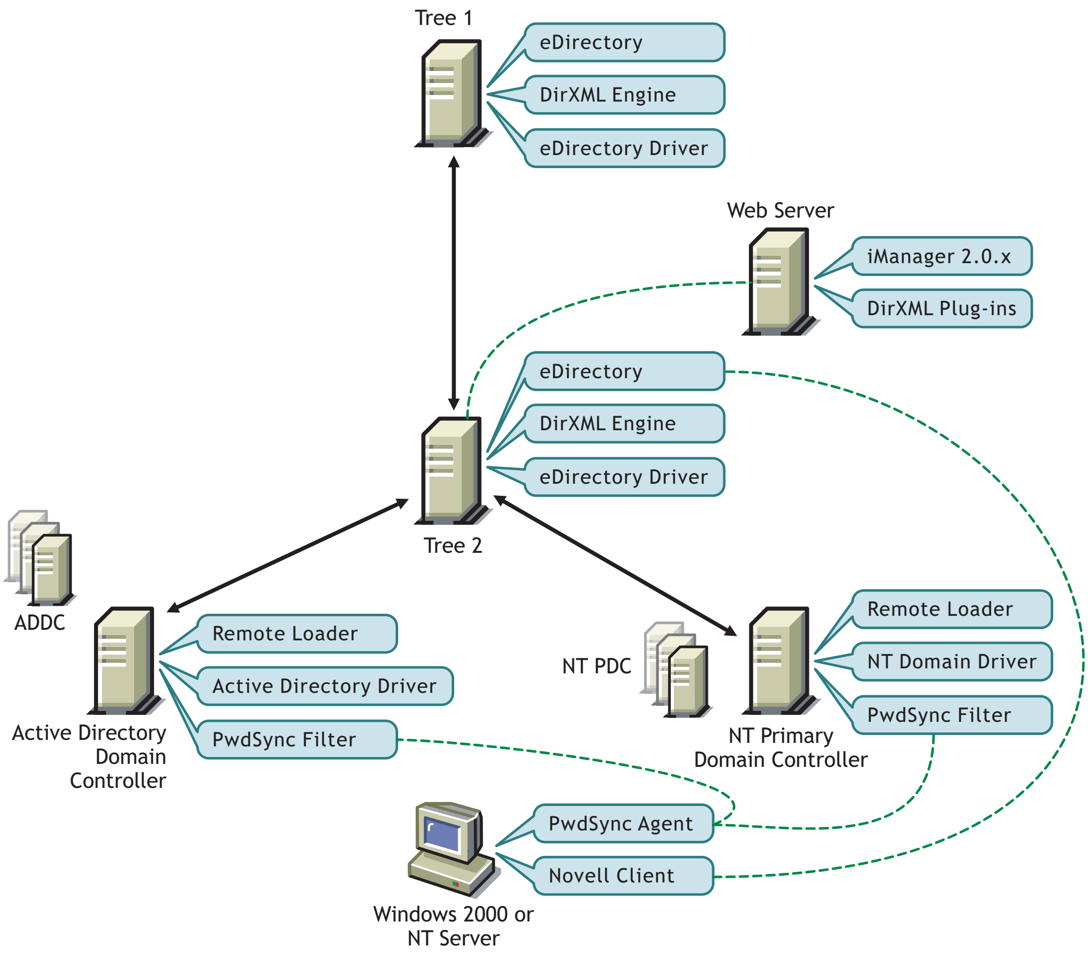
This section includes the following planning topics:

- "Where to Install DirXML Components" on page 21
- "Additional Considerations" on page 23
- "Active Directory Considerations" on page 24

## Where to Install DirXML Components

DirXML® is a distributed system consisting of an engine, drivers, and management tools. This guide describes only one of several options for installation locations. This installation scenario is illustrated in Figure 7 and explained in the following sections.

**Figure 7 Default Installation**



- **DirXML engine and DirXML driver for eDirectory**: Because data in two Novell® eDirectory™ trees is being synchronized in this scenario, the engine and the eDirectory driver are installed on two separate Linux, Windows, or NetWare® servers in two separate trees. The engine always needs to be on a server holding a replica of the data you will be synchronizing.
- **iManager and the plug-ins for DirXML**: Although iManager can be installed on the same Linux server that is hosting the DirXML engine, you might want to install iManager on a separate server to insulate administration functions. The configuration described in this document assumes separate servers.
- **DirXML driver for Active Directory and Remote Loader**: The Active Directory driver is installed on your Linux server, but runs remotely on a Windows computer. Because the driver is being installed on a computer separate from the engine, the Remote Loader service is installed with the driver. In this example, we've installed the driver and Remote Loader on the Active Directory domain controller. The driver doesn't need to be installed on the domain controller. Additional installation options are explained in the *Implementation Guide* for the Active Directory driver  (http://www.novell.com/documentation/lg/dirxmldrivers/ad/data/agdyjgz.html).
- **DirXML driver for NT 4 Domain and Remote Loader**: The NT driver can be installed on any Member Server, Backup Domain Controller, or even the Primary Domain Controller. Because the driver is being installed on a computer separate from the engine, the Remote Loader service must be installed with the driver. In this example, we've installed the driver and the Remote Loader on the Primary Domain Controller (PDC). Additional installation options are explained in the *Implementation Guide* for the NT driver (http://www.novell.com/documentation/lg/dirxmldrivers/nt/data/ageixcu.html).
- **Multiple domains**: If you have multiple domains, you'll need to install and configure a driver for each domain. The setup in this example doesn't describe installing the drivers for multiple domains. However, you can simply repeat the process used to set up the first domain for additional domains. No additional licenses are required for additional instances of the drivers when they are installed in the same eDirectory tree.
- **PasswordSync Agents**: Agents can be installed on any Windows 2000/NT server or on any Windows 2000/NT workstation that is continuously available. There is no requirement to place an agent on a controller or on the same computer as eDirectory or DirXML; however, the computer where the agent is installed must have the latest Novell Client™ installed. If you are synchronizing password data in more than one eDirectory tree, you need to install an agent for each tree.
- **PwdSync Filters**: PasswordSync Filters must be installed on all domain controllers. Every NT PDC, every Backup Domain Controller that might be promoted to a PDC, and every Active Directory Domain Controller requires a filter and an association with at least one PasswordSync Agent. The more agents that service a given domain controller, the greater redundancy you achieve.

## Additional Considerations

As part of your planning, you need to make sure that certain Novell eDirectory objects are replicated on servers where you want to run DirXML drivers.

You can use filtered replicas, as long as all of the objects and attributes that the driver needs are included in the filtered replica.

Keep in mind that you must give the DirXML Driver object sufficient eDirectory rights to any objects it is to synchronize with connected systems, either by explicitly granting rights to the Driver object, or by making it security equivalent to an object that has the desired rights.

An eDirectory server that is running a DirXML driver (or that the driver refers to, if you are using Remote Loader) must hold a master or read/write replica of the following:

- The DirXML Driver Set object for that server.

  You should have one Driver Set object for each server that is running DirXML. Unless you have specific needs, don't associate more than one server with the same Driver Set object.

  **NOTE:** When creating a Driver Set object, the default setting is to create a separate partition, but this is not required.

- The Server object for that server.

  The Server object is necessary because it allows the driver to generate key pairs for objects. It also is important for Remote Loader authentication.

- The objects that you want this instance of the driver to synchronize.

  A DirXML driver can't synchronize objects unless a replica of those objects is on the same eDirectory server as the Driver object. In fact, a driver will synchronize the objects in *all* the containers that are replicated on the server unless you create rules to specify otherwise (rules for scope filtering).

  If you want a driver to synchronize all user objects, for example, the simplest way is to use one instance of the driver on a server that holds a master or read/write replica of all your users.

  However, many environments don't have a single server that contains a replica of all the users. Instead, the complete set of users is spread across multiple servers. In this case, you have two choices:

  - **Aggregate users onto a single server.** You can create a single server that holds all users by adding replicas to an existing server. Filtered replicas can be used to reduce the size of the eDirectory database if desired, as long as the necessary user objects and attributes are part of the filtered replica.

  - **Use multiple instances of the driver on multiple servers, with scope filtering.** If you *don't* want to aggregate users onto a single server, you will need to determine which set of servers holds all the users, and set up one instance of the DirXML driver on each of those servers.

    To prevent separate instances of a driver from trying to synchronize the same users, you need to use scope filtering to define which users each instance of the driver should synchronize. Scope filtering means that you add rules to each driver to limit the scope of the driver's management to specific containers. For more information, see Managing Users on Different Servers Using Scope Filtering (http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/am361a8.html#alw2n7d).

- Any additional containers you want the DirXML driver to use for managing users.

To move an object, DirXML must have both the source container and the destination container replicated on the same server.

For example, if you have created a container named Inactive Users to hold user accounts that have been disabled, you must have a master or read/write replica of that container on the server where the driver is running.

**NOTE:** If you are using read/write replicas instead of master replicas, we recommend you set up the Move Proxy driver to facilitate moves from one container to another. This driver and instructions are available from Novell Support (http://support.novell.com/cgi-bin/search/searchtid.cgi?/2964749.htm).

- The Template objects you want the driver to use when creating users, if you choose to use templates.

  DirXML drivers do not require you to specify eDirectory Template objects for creating users. But if you specify that a driver should use a template when creating users in eDirectory, the Template object must be replicated on the server where the driver is running.

- Any other objects that the driver needs to refer to.

# Active Directory Considerations

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

A simple prescription for managing security is not possible because the security profile available from Windows 2000 varies with service pack, DNS server infrastructure, domain policy, and local policy settings on the Windows 2000 servers. Security choices for the DirXML driver for Active Directory are covered in the following sections. Various combinations of these choices are discussed in Recommended Security Configurations (http://www.novell.com/documentation/lg/dirxmldrivers/ad/data/agdyjgz.html#agdyjgz) in the *Implementation Guide* for the Active Directory driver.

## Security Parameters

You can set the following parameters during installation or later, in the Driver Parameters page. Understanding how the parameters work together and work with the operating system will help you define your approach to security for DirXML data synchronization.

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

| Username | Format |
|---|---|
| User Principal Name | user@domain.com |
| Domain name | user |
| Fully Qualified Domain name | domain\user |

  If the driver is installed on the Domain Controller and LSA access to Active Directory has not been restricted, you don't have to set an Authentication ID; the driver will use its local identity for authentication.

- **Application Password:** This is the password for the Authentication ID account. Set a password whenever you use an Authentication ID.
- **Authentication Context:** This is an LDAP URL that encodes the DNS name of the Active Directory domain controller. For example: LDAP://mycontroller.mydomain.com.

  To configure secure communication using SSL, add the LDAP SSL port number to the DNS server hostname (for example: LDAP://mycontroller.mydomain.com:636). Be aware that SSL will only work if you have set up a Certificate infrastructure and have imported certificates to your Windows 2000 servers. See the Microsoft documentation for Certificate Services for more detail.

  If the driver is running on the Domain Controller and you don't specify an authentication context, the driver will address its connection to the local machine.
- **Use Secure Authentication:** When this option is set to Yes, the driver will negotiate Kerberos or NTLM authentication to Active Directory.

  When this option is set to No, the driver uses an LDAP simple bind. Simple bind is usually unacceptable because it transmits passwords in clear text on the wire. However if you have configured SSL secure communication, then the password is sent on an SSL encrypted pipe and is secure.
- **Use SSL:** This parameter controls encryption if you connect to Active Directory using the LDAP SSL port number. By default the parameter is set to No, which means the SSL secure communication will drop out after simple bind authentication completes. Communication after authentication will use clear text.

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

  This parameter is configurable through the Driver Parameters page after the driver has been imported.
- **Use Signing / Sealing:** This flag enables signing and sealing of the Active Directory connection if you are not using the LDAP SSL port. Signing ensures that a malicious computer is not intercepting data. Sealing encrypts the data so that it cannot be viewed by a network monitor.

  This setting is effective *only* if you are running the Windows 2000 Security Rollout Package SP1 (SRP1) or Windows 2000 SP3, with Internet Explorer 5.5 SP2 installed on both Windows 2000 servers, and will enable signing and encryption on a Kerberos or NTLM authenticated connection.

  Like SSL mode, this parameter is not available on initial import; it is set through the Driver Parameters page after installation is complete.
- **Keep Credentials:** This parameter instructs the driver to use an updated authentication method to maintain its connection to Active Directory. The updated method is important on systems that have upgraded to Windows 2000 Security Rollout Package 1 (SRP1) or Windows 2000 SP3. If you are using an earlier release of Windows and are not experiencing connection problems, set this parameter to No.

## Authentication Options

The three authentication methods used by the driver are listed below. If you have installed a different security package into the Microsoft Security Service Provider Interface (SSPI) infrastructure, you will have additional options.

- **Use Process Identity:** This mode is selected when you leave the Authentication ID blank. Typically, eDirectory runs as a service and you will receive Local Service Account (LSA) rights to Active Directory. Unless policy or local Active Directory security settings disallow access for the LSA, this level of rights works when you are running the driver on your Active Directory server. This only works if the driver is running on the Domain Controller.
- **Simple Bind:** Passes the user name and password in clear text. This option should only be used with SSL.
- **Kerberos / NTLM authentication:** NTLM is the standard Domain authentication used on Windows NT 4. It is weaker than Kerberos because key lengths might not be as long and it does not support mutual authentication. However, NTLM has been used for years with Domain authentication and is acceptable for most uses.

  Kerberos is the new Windows 2000 authentication and is the preferred method for future authentications with Microsoft. It implements a third-party mutual authentication scheme and is generally stronger than NTLM. The driver is not notified which authentication scheme is being used.

# 3 Installing the Novell DirXML Starter Pack

This section explains how to install the DirXML® engine and iManager plug-ins for DirXML.

Depending on your system configuration, you might need to run the DirXML installation program several times to install other DirXML components on the appropriate systems.

For example, you could install DirXML components on the following systems:

- eDirectory™ Server: DirXML engine and DirXML drivers
- iManager Server: iManager plug-ins for DirXML and driver configuration files
- Application Server: Remote Loader service, DirXML drivers, and management utilities

The system configuration described in this guide assumes that DirXML is installed on a server separate from the server hosting iManager, as shown in Figure 7, "Default Installation," on page 21.

Use the steps in the following sections to help you complete setup of DirXML components.

- "Installing DirXML" on page 27
- "Setting Up iManager" on page 28

## Installing DirXML

### Prerequisites

❑ Supported Operating System

The DirXML engine can be installed on a Linux, Windows, or NetWare server that holds a master or read/write replica of the data you will be synchronizing.

DirXML requires one of the following operating systems:

- Red Hat Enterprise Linux AS 2.1, Red Hat Enterprise Linux ES 2.1, or SuSE Linux Enterprise Server 8.0.
- NetWare® 5.1., NetWare 6, or NetWare 6.5 with the latest support pack.
- Windows NT with Service Pack 5 or higher, or Windows 2000 Professional or Server with the latest service pack.

❑ eDirectory 8.6.1 or later.

## Installing the DirXML Engine

If you choose to install the DirXML engine on a Linux server, you already installed it during the the NNLS product installation.

For instructions on how to install the DirXML engine on Windows or NetWare, refer to the DirXML online documentation.

- Installing DirXML on Windows (http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/abaa35l.html)
- Installing DirXML on NetWare (http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/abaa2oj.html#abaa2oj)

Continue with the next section, “Setting Up iManager” on page 28.

# Setting Up iManager

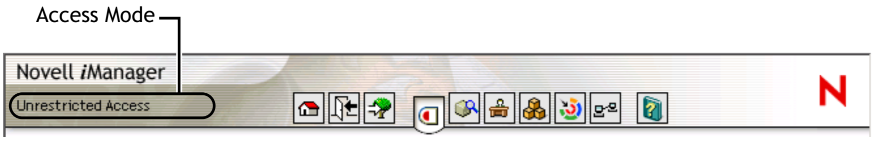
## Prerequisites

❑ Novell iManager 2.0

iManager should be installed and configured before you install the plug-ins for DirXML.

You can configure iManager to run in various modes. Before you install the plug-ins for DirXML, determine which mode you use by checking the type of access displayed in the top left corner.

**Figure 8 iManager Access Mode**



For more information about installing iManager, see Installing Novell iManager (http://www.novell.com/documentation/lg/imanager20/index.html) in the *Novell iManager 2.0 Administration Guide*.

## Installing the iManager Plug-Ins for DirXML and the Driver Configurations

The iManager plug-ins and DirXML driver configurations are installed as part of the NNLS installation. If, however, you are running iManager on a Windows or NetWare server, you need to run the appropriate installation program on that server.

1. On the server where iManager is installed, insert the DirXML CD into the CD drive and run the installation program.
2. On the DirXML Product Installation page, click Next.
3. Read the license agreement; if you agree to the terms, click I Accept.
4. On the Components page, mark the following items, then click Next.
   - DirXML Preconfigured Drivers
   - Novell iManager Plug-ins for DirXML

**5** Verify that all the preconfigured driver files are selected, then click Next.

**6** Read the Summary page, then click Finish.

If you are presented with an LDAP warning message, verify that no conflicts exist, then click OK.

Plug-ins and preconfigured drivers are copied to the Tomcat directory (typically, sys:tomcat\4\webapps\nps\portal\modules\plugins and sys:tomcat\4\webapps\nps\DirXML.Drivers) for use during iManager and driver configuration. The file copy might take a few minutes.

**7** At the message directing you to restart your Web services, click OK.

**8** After the Installation Complete dialog box is displayed, click Close.

**9** Restart your Web services using the following sequence:

**9a** To stop Tomcat, at the System Console prompt, type **`tc4stop`**, then press Enter.

Verify that this service is stopped by going to the Logger screen and finding the message `Bootstrap exited successfully`.

**9b** To restart Tomcat, at the System Console prompt, type **`tomcat4`**, then press Enter.

Verify that this service is started by going to the Logger screen and finding the message `Jk running...`.

**10** Launch iManager by going to http://*serveripaddress*/nps/iManager.html.

**IMPORTANT:** This URL is case sensitive.

**11** (Conditional) If you are using Assigned Access or Collection Owner Access, make DirXML roles available by using the iManager Configuration Wizard as explained in the steps that follow.

**11a** Launch iManager by going to http://*serveripaddress*/nps/iManager.html.

**IMPORTANT:** This URL is case sensitive.

**11b** Click the Configure button, then click RBS Configuration > Configure iManager.

**11c** Select either Create a New Collection or Upgrade Collections, then click Next.

**NOTE:** Fewer collections will improve iManager performance.

**11d** Select the collections to be updated, then click Next.

**11e** Select DirXML Utilities and assign a Scope.

**TIP:** Assign the Scope high enough in the tree to allow access to all DirXML objects including the server object representing the server where DirXML is installed,

**11f** If you are configuring multiple collections, click Next to assign a Scope for each collection.

**11g** If you are configuring only one collection, or if this is the final collection that will be configured, click Start to launch the wizard.

iManager RBS collections are updated.

**11h** Upon notice of completion, click Close, click Roles and Tasks, then verify that the following DirXML roles are present:

- DirXML Management
- DirXML Planning

**12** Continue with DirXML setup as explained in Chapter 4, “Setting Up Participating Systems,” on page 31.

# 4 Setting Up Participating Systems

After the DirXML® engine and Novell® iManager have been installed, you install DirXML drivers and configure systems participating in data synchronization. Use the following sections to help with system setup and configuration. These systems can be set up in any order.

- "Setting Up Active Directory" on page 31
- "Setting Up eDirectory" on page 44
- "Setting Up NT Domain" on page 49
- "Configuring the DirXML Drivers" on page 57
- "Migrating Existing Data" on page 61

After setting up participating systems, you can set up and configure password synchronization as explained in Chapter 5, "Setting Up Password Synchronization," on page 63.

## Setting Up Active Directory

For the default NNLS setup, the driver for Active Directory is installed on the Domain Controller. Additional installation options are explained in Planning Your Installation (http://www.novell.com/documentation/lg/dirxmldrivers/ad/data/agdyjgz.html) in the *Implementation Guide* for the Active Directory Driver.

To synchronize account information for Active Directory users, complete the following sections:

- "Prerequisites" on page 31
- "Collecting Configuration Information" on page 32
- "Creating an Admin User" on page 40
- "Identifying the Active Directory Domain GUID" on page 41
- "Installing and Configuring the Remote Loader and Driver" on page 42

### Prerequisites

The computer where you will install the Remote Loader and the driver must be running the following software:

❑ Windows 2000 Server or Windows 2000 Professional (Support Pack 1)

❑ Internet Explorer 5.5 or later

❑ The server must be a member of the Active Directory tree

## Collecting Configuration Information

You'll need to provide a number of system-specific details when you install and configure the DirXML driver for Active Directory. Some of these details can be collected before you complete the following procedures, and others will be defined during the process.

- "Required Driver Configuration Information for Active Directory" on page 32 provides you with a place to record configuration data for later use.
- Figure 9, "Active Directory Configuration Form," on page 34 is provided for reference; it shows the Active Directory configuration form as it appears in iManager. You will see this form when you configure the DirXML drivers.

During the configuration process, you will also need to provide the container names for placement of synchronized objects. For more information about Active Directory placement options, see "Default Driver Settings for Active Directory" on page 14.

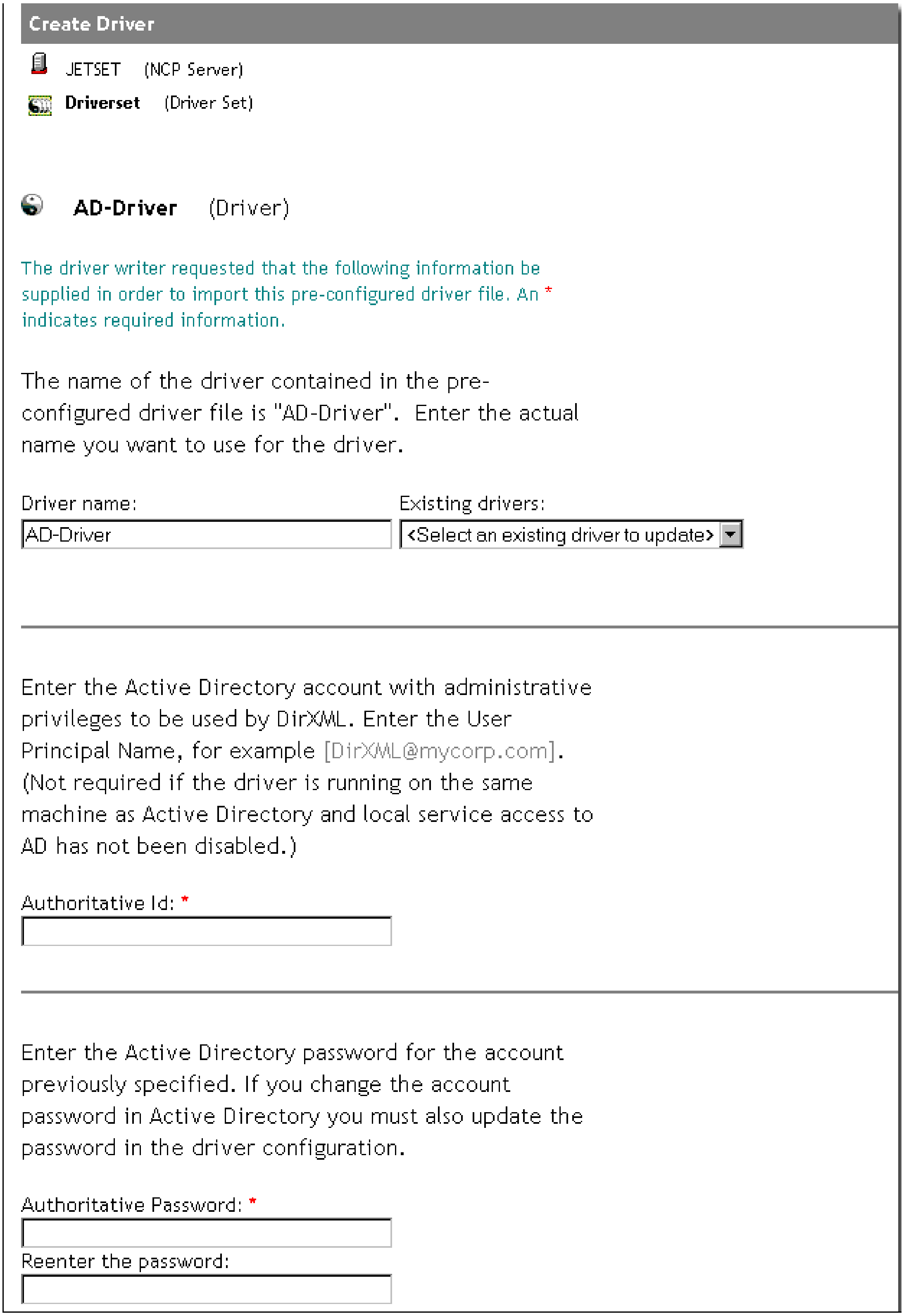
### Required Driver Configuration Information for Active Directory

**IMPORTANT:** The data you supply during configuration is used to build DirXML rules. Often, case is significant to a rule. Mirror case when entering the requested data.

| System | Value |
|---|---|
| Authoritative ID<br>(example: DirXML@mycorp.com)<br>Used by the driver to access objects necessary for data synchronization. To create this user, see "Creating an Admin User" on page 40. | |
| Authoritative Password<br>Password for the above user. Can be set when "Creating an Admin User" on page 40. | |
| Authentication Server<br>(example: LDAP://mycontroller.domain.mycorm.com)<br>The DNS name for the Domain Controller. You might need to ask the Active Directory administrator for this information. | |
| Domain GUID<br>This data can be automatically collected and stored in a text file using the ADShimDiscorveryTool. See "Identifying the Active Directory Domain GUID" on page 41. | ADShimData.txt |
| Base Container in Active Directory<br>(example: CN=Users,DC=MyDomain,DC=com)<br>The Active Directory container holding objects to synchronize with eDirectory. If this container does not exist, you must create it before starting the driver. | |
| Base Container in eDirectory<br>(example: Users.MyOrganization)<br>The eDirectory container holding objects to synchronize with Active Directory. If this container does not exist, you must create it before starting the driver. | |

| System | Value |
|---|---|
| Remote Host Name and Port<br>Specify the port when "Installing and Configuring the Remote Loader and Driver" on page 42. | |
| Driver Password<br>Specify the password when "Installing and Configuring the Remote Loader and Driver" on page 42. | |
| Remote Password<br>Specify the password when "Installing and Configuring the Remote Loader and Driver" on page 42. | |
| Default Exchange Server<br>To synchronize Exchange 2000 information, you will need to provide values for this and the following prompts.<br>This data can be automatically collected and stored in a text file using the ADShimDiscoveryTool. See "Identifying the Active Directory Domain GUID" on page 41. | ADShimData.txt |
| Default Exchange DN<br>This data can be automatically collected and stored in a text file using the ADShimDiscoveryTool. See "Identifying the Active Directory Domain GUID" on page 41. | ADShimData.txt |
| Default Exchange MTA<br>This data can be automatically collected and stored in a text file using the ADShimDiscoveryTool. See "Identifying the Active Directory Domain GUID" on page 41. | ADShimData.txt |
| Default Exchange MDB<br>This data can be automatically collected and stored in a text file using the ADShimDiscoveryTool. See "Identifying the Active Directory Domain GUID" on page 41. | ADShimData.txt |

**Figure 9 Active Directory Configuration Form**



Create Driver

JETSET (NCP Server)

**Driverset** (Driver Set)

**AD-Driver** (Driver)

The driver writer requested that the following information be supplied in order to import this pre-configured driver file. An * indicates required information.

The name of the driver contained in the pre-configured driver file is "AD-Driver". Enter the actual name you want to use for the driver.

Driver name: AD-Driver

Existing drivers: <Select an existing driver to update>

Enter the Active Directory account with administrative privileges to be used by DirXML. Enter the User Principal Name, for example [DirXML@mycorp.com]. (Not required if the driver is running on the same machine as Active Directory and local service access to AD has not been disabled.)

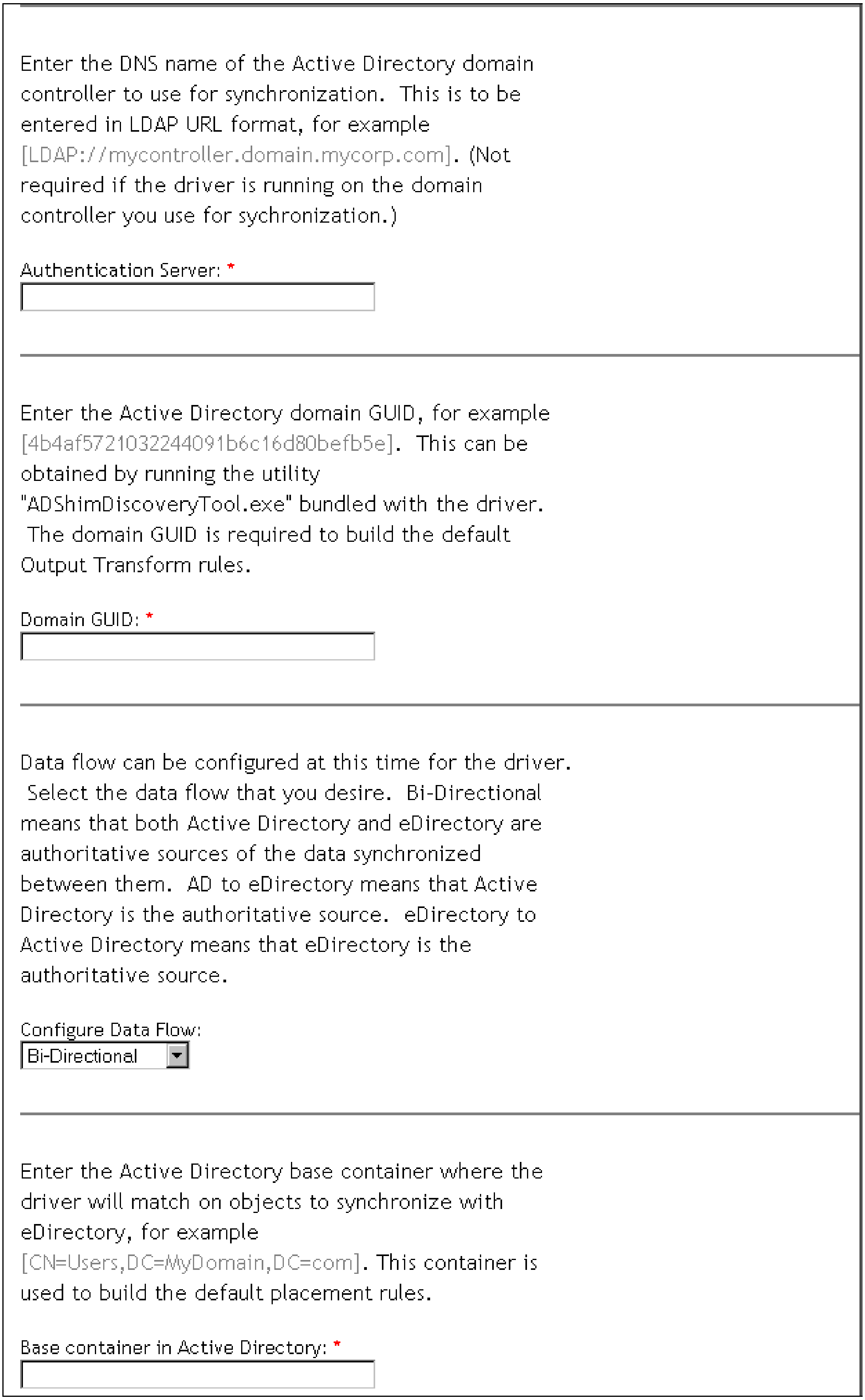
Authoritative Id: *

Enter the Active Directory password for the account previously specified. If you change the account password in Active Directory you must also update the password in the driver configuration.

Authoritative Password: *

Reenter the password:

Description: Active Directory Configuration Form (continued)



Enter the DNS name of the Active Directory domain controller to use for synchronization. This is to be entered in LDAP URL format, for example [LDAP://mycontroller.domain.mycorp.com]. (Not required if the driver is running on the domain controller you use for sychronization.)

Authentication Server: *

Enter the Active Directory domain GUID, for example [4b4af5721032244091b6c16d80befb5e]. This can be obtained by running the utility "ADShimDiscoveryTool.exe" bundled with the driver. The domain GUID is required to build the default Output Transform rules.

Domain GUID: *

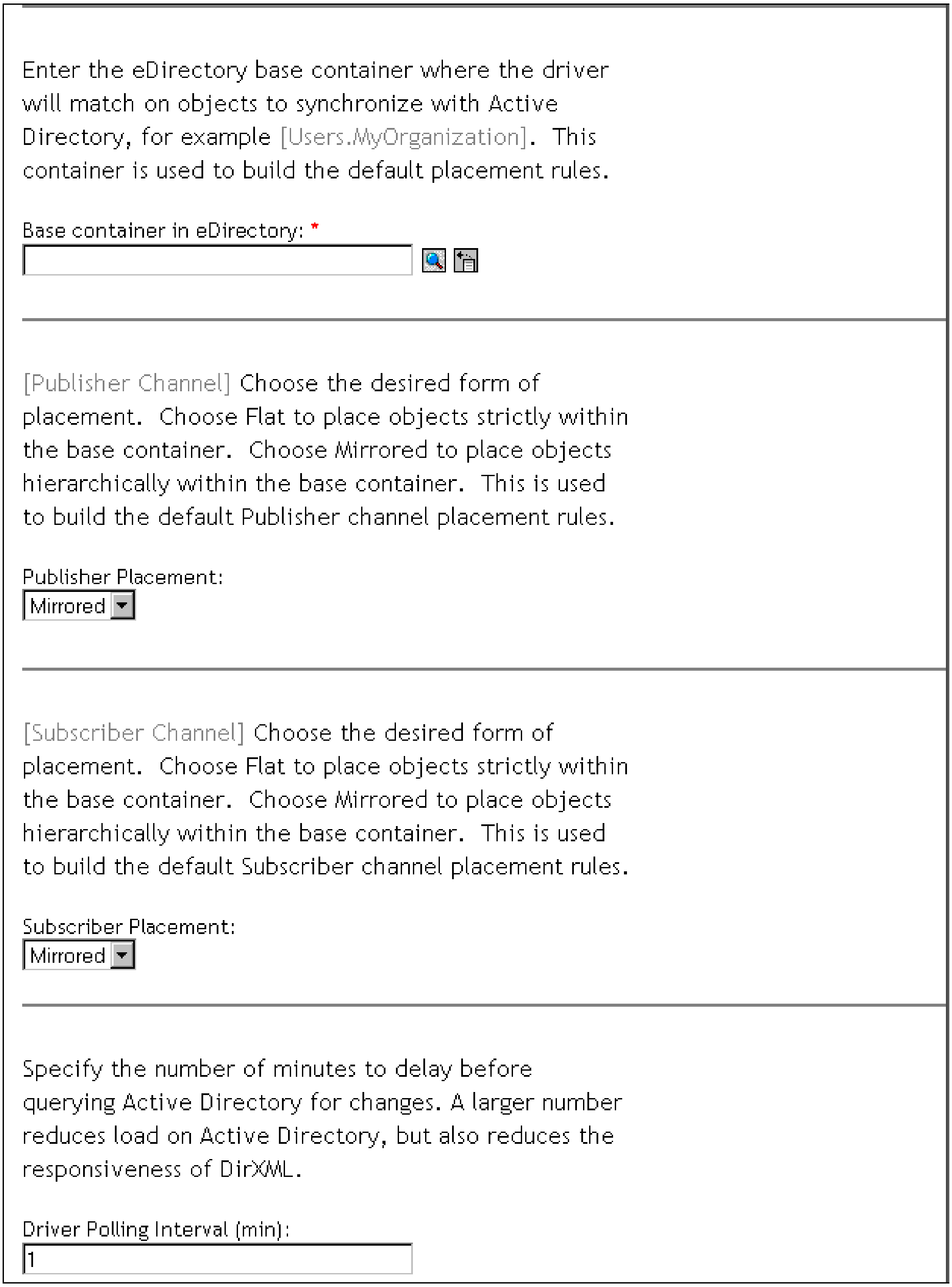
Data flow can be configured at this time for the driver. Select the data flow that you desire. Bi-Directional means that both Active Directory and eDirectory are authoritative sources of the data synchronized between them. AD to eDirectory means that Active Directory is the authoritative source. eDirectory to Active Directory means that eDirectory is the authoritative source.

Configure Data Flow: Bi-Directional

Enter the Active Directory base container where the driver will match on objects to synchronize with eDirectory, for example [CN=Users,DC=MyDomain,DC=com]. This container is used to build the default placement rules.

Base container in Active Directory: *

Description: Active Directory Configuration Form (continued)



Enter the eDirectory base container where the driver will match on objects to synchronize with Active Directory, for example [Users.MyOrganization]. This container is used to build the default placement rules.

Base container in eDirectory: *

---

[Publisher Channel] Choose the desired form of placement. Choose Flat to place objects strictly within the base container. Choose Mirrored to place objects hierarchically within the base container. This is used to build the default Publisher channel placement rules.

Publisher Placement: Mirrored

---

[Subscriber Channel] Choose the desired form of placement. Choose Flat to place objects strictly within the base container. Choose Mirrored to place objects hierarchically within the base container. This is used to build the default Subscriber channel placement rules.

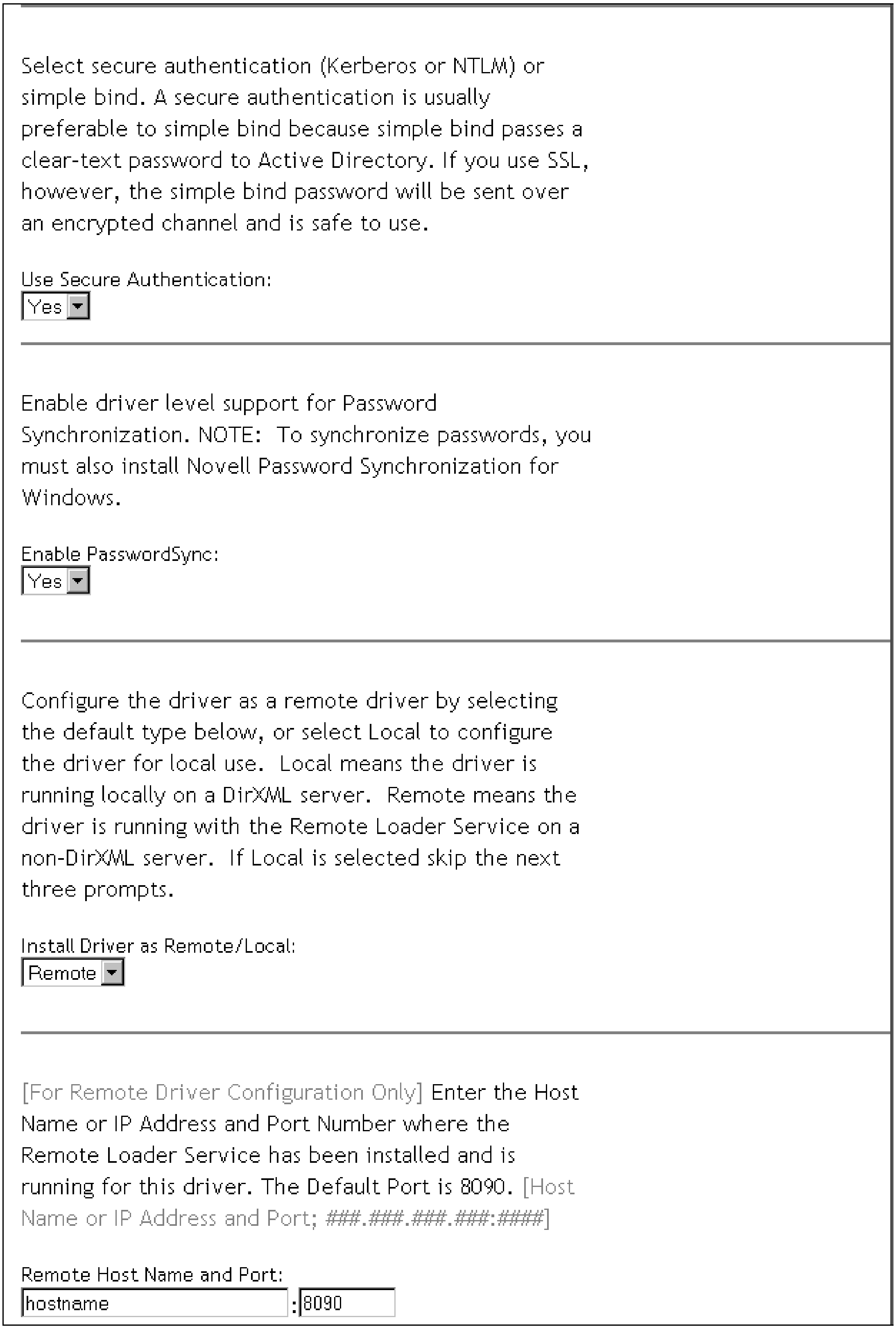
Subscriber Placement: Mirrored

---

Specify the number of minutes to delay before querying Active Directory for changes. A larger number reduces load on Active Directory, but also reduces the responsiveness of DirXML.

Driver Polling Interval (min): 1

Description: Active Directory Configuration Form (continued)



Select secure authentication (Kerberos or NTLM) or simple bind. A secure authentication is usually preferable to simple bind because simple bind passes a clear-text password to Active Directory. If you use SSL, however, the simple bind password will be sent over an encrypted channel and is safe to use.

Use Secure Authentication:
Yes

Enable driver level support for Password Synchronization. NOTE:  To synchronize passwords, you must also install Novell Password Synchronization for Windows.

Enable PasswordSync:
Yes

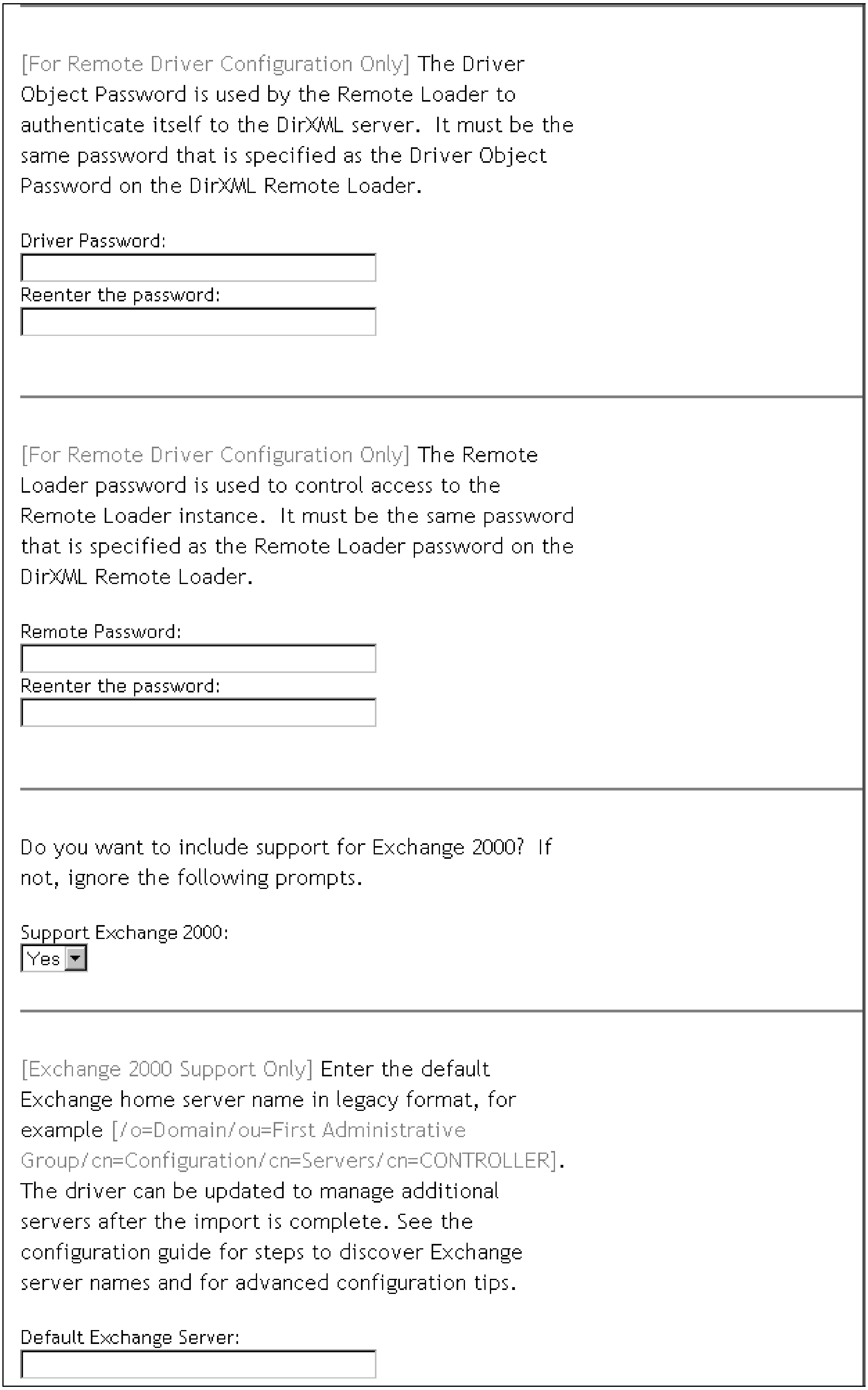
Configure the driver as a remote driver by selecting the default type below, or select Local to configure the driver for local use.  Local means the driver is running locally on a DirXML server.  Remote means the driver is running with the Remote Loader Service on a non-DirXML server.  If Local is selected skip the next three prompts.

Install Driver as Remote/Local:
Remote

[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. [Host Name or IP Address and Port; ###.###.###.###:####]

Remote Host Name and Port:
hostname : 8090

## Description: Active Directory Configuration Form (continued)



[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.

Driver Password:

Reenter the 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.

Remote Password:

Reenter the password:

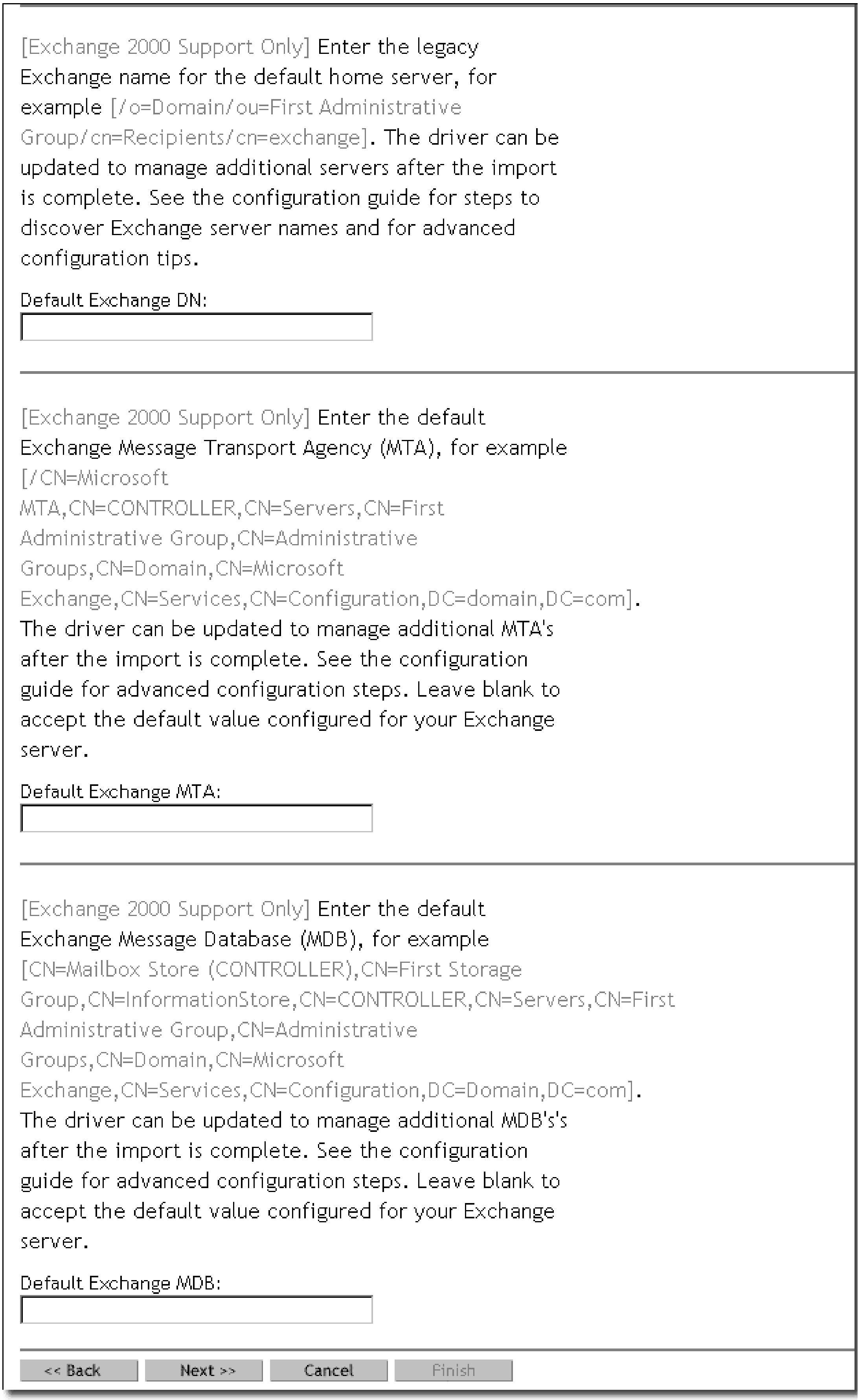
Do you want to include support for Exchange 2000? If not, ignore the following prompts.

Support Exchange 2000: Yes

[Exchange 2000 Support Only] Enter the default Exchange home server name in legacy format, for example [/o=Domain/ou=First Administrative Group/cn=Configuration/cn=Servers/cn=CONTROLLER]. The driver can be updated to manage additional servers after the import is complete. See the configuration guide for steps to discover Exchange server names and for advanced configuration tips.

Default Exchange Server:

Description: Active Directory Configuration Form (continued)



[Exchange 2000 Support Only] Enter the legacy Exchange name for the default home server, for example [/o=Domain/ou=First Administrative Group/cn=Recipients/cn=exchange]. The driver can be updated to manage additional servers after the import is complete. See the configuration guide for steps to discover Exchange server names and for advanced configuration tips.

Default Exchange DN:

[Exchange 2000 Support Only] Enter the default Exchange Message Transport Agency (MTA), for example [/CN=Microsoft MTA,CN=CONTROLLER,CN=Servers,CN=First Administrative Group,CN=Administrative Groups,CN=Domain,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=domain,DC=com]. The driver can be updated to manage additional MTA's after the import is complete. See the configuration guide for advanced configuration steps. Leave blank to accept the default value configured for your Exchange server.

Default Exchange MTA:

[Exchange 2000 Support Only] Enter the default Exchange Message Database (MDB), for example [CN=Mailbox Store (CONTROLLER),CN=First Storage Group,CN=InformationStore,CN=CONTROLLER,CN=Servers,CN=First Administrative Group,CN=Administrative Groups,CN=Domain,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=Domain,DC=com]. The driver can be updated to manage additional MDB's's after the import is complete. See the configuration guide for advanced configuration steps. Leave blank to accept the default value configured for your Exchange server.

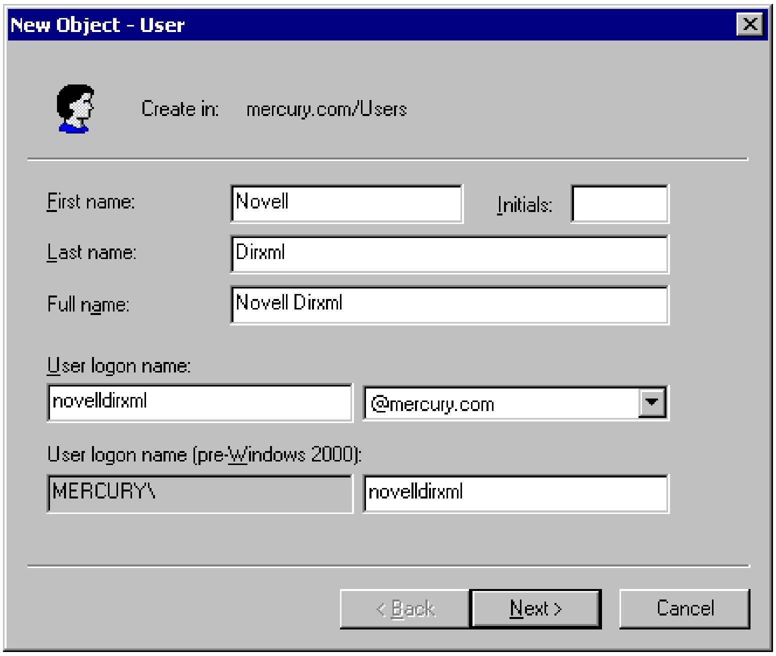
Default Exchange MDB:

## Creating an Admin User

Create a user with administrative privileges to be exclusively used by the driver to authenticate into Active Directory. Doing this keeps the DirXML Admin account isolated from changes to other Admin accounts.

1. Click Start > Programs > Administrative Tools > Active Directory Users and Computers.
2. From Active Directory Users and Computers, select the container where you want to add the user, then choose Action > New > User.
3. Enter the Full Name, which is the AD user object name, and enter the User logon name, which is the AD authentication name.

**Figure 10 Creating an Active Directory User for the Driver**



New Object - User

Create in: mercury.com/Users

First name: Novell

Initials:

Last name: Dirxml

Full name: Novell Dirxml

User logon name: novelldirxml @mercury.com

User logon name (pre-Windows 2000): MERCURY\ novelldirxml

Record the logon name plus the domain as the Authentication ID in the table under "Required Driver Configuration Information for Active Directory" on page 32. For example, record novelldirxml@mercury.com. This information will be required later during driver parameter configuration.

4. Click Next, then set the password for the new user. Mark Password Never Expires so that a password policy won't disable the driver unexpectedly.

   Record the password in the table under "Required Driver Configuration Information for Active Directory" on page 32. This information will be required later during driver parameter configuration.

5. Click Next, review the summary, then click Finish.
6. In the Tree view, select Builtin, then right-click Administrators. Select Properties, click Members, then click Add.

   **NOTE:** In this scenario, the Builtin Administrators assignment covers the broadest set of possible configurations, but this assignment isn't always necessary. Depending on where you install the driver and how your environment is configured, you might be able to use the Domain Admins group or another administrator equivalent.

7. Select the full name of the user you created, click Add, then click OK twice.
8. Close the Active Directory Users and Computers window.
9. In the Administrative Tools window (Start > Programs > Administrative Tools), select Domain Controller Security Policy.
10. In the Tree View, select Security Settings > Local Policies > User Rights Assignment.
11. Open Log On As a Service, then click Add.

    **NOTE:** The admin user must log on as a service only when the driver is installed on the domain controller, as is the case in this scenario. If the driver is installed on a member server, logging on as a service is not required.
12. Click Browse and select the user you created. Click Add, then click OK three times to return to the Domain Controller Security Policy window.
13. Close the Domain Controller Security Policy.
14. Update the machine policy for the domain controller.

    You can do this either by rebooting the domain controller or by running the following command at the domain controller command prompt:
    secedit /refreshpolicy machine_policy /enforce
15. Continue with the next section, "Identifying the Active Directory Domain GUID" on page 41.

## Identifying the Active Directory Domain GUID

Use the ADShimDiscoveryTool utility to expedite data gathering required for driver configuration.

1. At the computer where you will access iManager and administer DirXML, insert the DirXML CD. When the installation program launches, click Cancel.
2. From the DirXML CD, run utilities\ad_disc\ADShimDiscoveryTool.exe.
3. Enter the Administrator password in the LDAP User Password field.
4. Enter the IP address of the AD domain controller that will be synchronizing data through DirXML.
5. Leave the default setting in the Port field.
6. Click Discover.

   Active Directory configuration information is displayed.
7. Click Paste to File to copy the following values to a configuration information to a text file on the desktop for later use:
   - Active Directory Domain GUID
   - Default Naming Context (Authentication Server)
   - DNS Host Name
   - Default Exchange Server
   - Default Legacy Exchange DN
   - Default Exchange MTA
   - Default Exchange MDB
8. Click Exit, then continue with the next section, "Installing and Configuring the Remote Loader and Driver" on page 42.

## Installing and Configuring the Remote Loader and Driver

The Remote Loader allows you to run the driver on a computer other than the server hosting the DirXML engine.

1. At the AD computer that will host the driver, insert the DirXML CD into the CD drive. The CD may take a moment to load. Then, at the Welcome page, click Next.
2. Read the license agreement; if you agree to the terms, click I Accept.
3. On the Components page, select DirXML Remote Loader and Drivers, then click Next.
4. Accept the default installation path for the Remote Loader, then click Next.
5. Mark the following items, then click Next.
   - DirXML Remote Loader Service
   - DirXML Driver for Active Directory
6. Review the Product Summary, then click Finish to install Remote Loader files.

   If you are presented with an LDAP warning message, verify that no conflicts exist, then click OK.
7. When prompted, create a shortcut.
8. On the Installation Complete page, click Close.
9. Run the DirXML Remote Loader Configuration Wizard from your desktop.
10. On the Welcome page, click Next.
11. Keep the default Command Port number, then click Next.
12. Keep the default Configuration File Name, then click Next.
13. On the DirXML Driver page, mark Native, ensure that the addriver.dll file is selected in the drop-down list, then click Next.
14. On the Connection to DirXML page, leave the default Port settings and Addresses.
15. If appropriate for your environment, mark Use SSL and browse to the Trusted Root Certificate.

    Using SSL with Remote Loader encrypts the communication between the Remote Loader and the DirXML engine. It does not address communication between Active Directory and DirXML. See "Active Directory Considerations" on page 24 for more information about secure communication between Active Directory and DirXML.

    You can create a Server Certificate object and then export a self-signed root certificate from your Organizational CA as explained in Exporting the Organizational CA's Self-Signed Certificate (http://www.novell.com/documentation/lg/crt252/crtadmin/data/a2ebop8.html#a2ppx57). Save the certificate file in base64 format and copy it to a local directory on the computer hosting the Remote Loader.

    **IMPORTANT:** If you use SSL, then *after* the driver configuration is imported you must:<br>
     - Use iManager to edit the Authentication section of the Driver Parameters. In the Remote Loader Connection Parameters add a reference to the certificate as shown in the following example: hostname=192.168.0.1 port=8090 kmo=servernamecert.<br>
     - Re-enter the application and the Remote Loader passwords.
16. Record the port number in the table under "Required Driver Configuration Information for Active Directory" on page 32, then click Next.

    This information will be required later during driver parameter configuration.

**17** Set Trace Level to 3 so that you'll get adequate tracking data from the Remote Loader for troubleshooting.

Trace information can include general state information, event information, warning messages, error messages, etc.

| Trace Level | Information |
|---|---|
| 0 | No information display or tracking |
| 1 | General informational messages about processing |
| 2 | Displays messages from level 1 plus the XML documents that are passed between the engine and driver |
| 3 | Displays messages from level 2 plus documents sent and received between the Remote Loader and the DirXML engine |
| 4 | Displays messages from level 3 plus information about the connection between the Remote Loader and the DirXML engine |

**18** Specify a location and filename for the trace file, then click Next.

The default location is c:\Novell\RemoteLoader.

**WARNING:** The trace file is a tool to help you monitor events during startup or when you are troubleshooting. Messages will be logged to this file continuously, making it grow until it fills the available disk space. Ensure that the location of this file is appropriate for your environment.

After you're satisfied that the driver is running as expected, you can reset the Trace Level to 0. Then use the Windows Event Viewer found under Administrative Tools or the eDirectory Report and Notification Service (http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/afae8bz.html) to monitor events on an ongoing basis.

Ensure that the path you enter actually exists. If the path does not exist, messages will not be logged.

If the path to the trace file includes spaces, enclose the path in quotes. For example, type "c:\documents and settings\Adminstrator\My Documents". If the trace level is greater than 0, trace messages will be written to the log file even if the trace window is not open.

If you are running multiple Remote Loader sessions on a single computer, you should create separate trace files for each session.

**19** Mark Install the Remote Loader Instance as a Service, then click Next.

Installing Remote Loader as a service allows the Remote Loader to continue to run, even when you log off.

**20** Set Remote Loader and Driver Object passwords.

We recommend keeping remote passwords and driver passwords the same across systems and changing them later when you go to production.

Record the passwords in the table under "Required Driver Configuration Information for Active Directory" on page 32. This information will be required later during driver parameter configuration.

**21** Review the summary, then click Finish.

**22** When prompted, start the service.

You will see the Trace screen with messages indicating that Remote Loader is waiting for a DirXML connection.

**NOTE:** If you close the Trace screen and then want to open it again, you can do so at a command prompt by entering `dirxml_remote -window on`.

To stop or start the service, locate DirXML Loader in Microsoft Services (Start > Settings > Control Panel > Administrative Tools > Services).

The Active Directory system is prepared to synchronize data. Complete preparation of other participating systems and then proceed to "Configuring the DirXML Drivers" on page 57.

# Setting Up eDirectory

The Novell eDirectory™ system requires a DirXML driver to be installed and configured on each tree for which you will synchronize data. In Chapter 3, "Installing the Novell DirXML Starter Pack," on page 27, you should have installed the first DirXML driver for eDirectory. You will configure that driver later in this chapter.

This section explains how to install and configure the second DirXML driver for eDirectory.

To set up synchronization for the second eDirectory tree, complete each of the following sections:

- "Prerequisites" on page 44
- "Collecting Configuration Information" on page 45
- "Installing DirXML and the DirXML Driver for eDirectory on Tree 1" on page 48
- "Configuring the DirXML Driver for eDirectory" on page 48

## Prerequisites

❑ JVM* 1.4

You can download JVM 1.4. on Novell Software Downloads (http://www.novell.com/download/index.html). The ConsoleOne® DirXML snap-ins require this version.

❑ NICI 2.4 or later

You can download NICI 2.4 or later from Novell Software Downloads (http://www.novell.com/download/index.html).

❑ Novell eDirectory 8.6.2 or later

You can download eDirectory 8.6.2 or later from Novell Software Downloads (http://www.novell.com/download/index.html).

❑ If you plan to use ConsoleOne, ConsoleOne 1.3.3 or later

You can install ConsoleOne 1.3.3 or later and the latest ConsoleOne DirXML snap-ins at the root of the product CD or from Novell Software Downloads (http://www.novell.com/download/index.html).

**NOTE:** If you are managing DirXML on an eDirectory 8.6.x system, you should use ConsoleOne 1.3.3. There are DClient issues specific to this version of eDirectory.

If you want to manage DirXML using ConsoleOne 1.3.4 and eDirectory 8.6.x, you should install ConsoleOne on a system where eDirectory is not installed.

## Collecting Configuration Information

You'll need to provide a number of system-specific details when you install and configure the DirXML driver for eDirectory. Some of these details can be collected before you complete the following procedures, and others will be defined during the process.

- "Required Driver Configuration Information for eDirectory" on page 45 provides you with a place to record configuration data for later use.
- Figure 11, "eDirectory Configuration Form," on page 46 is provided for reference; it shows the eDirectory configuration form as it appears in iManager. You will see this form when you configure the DirXML drivers.

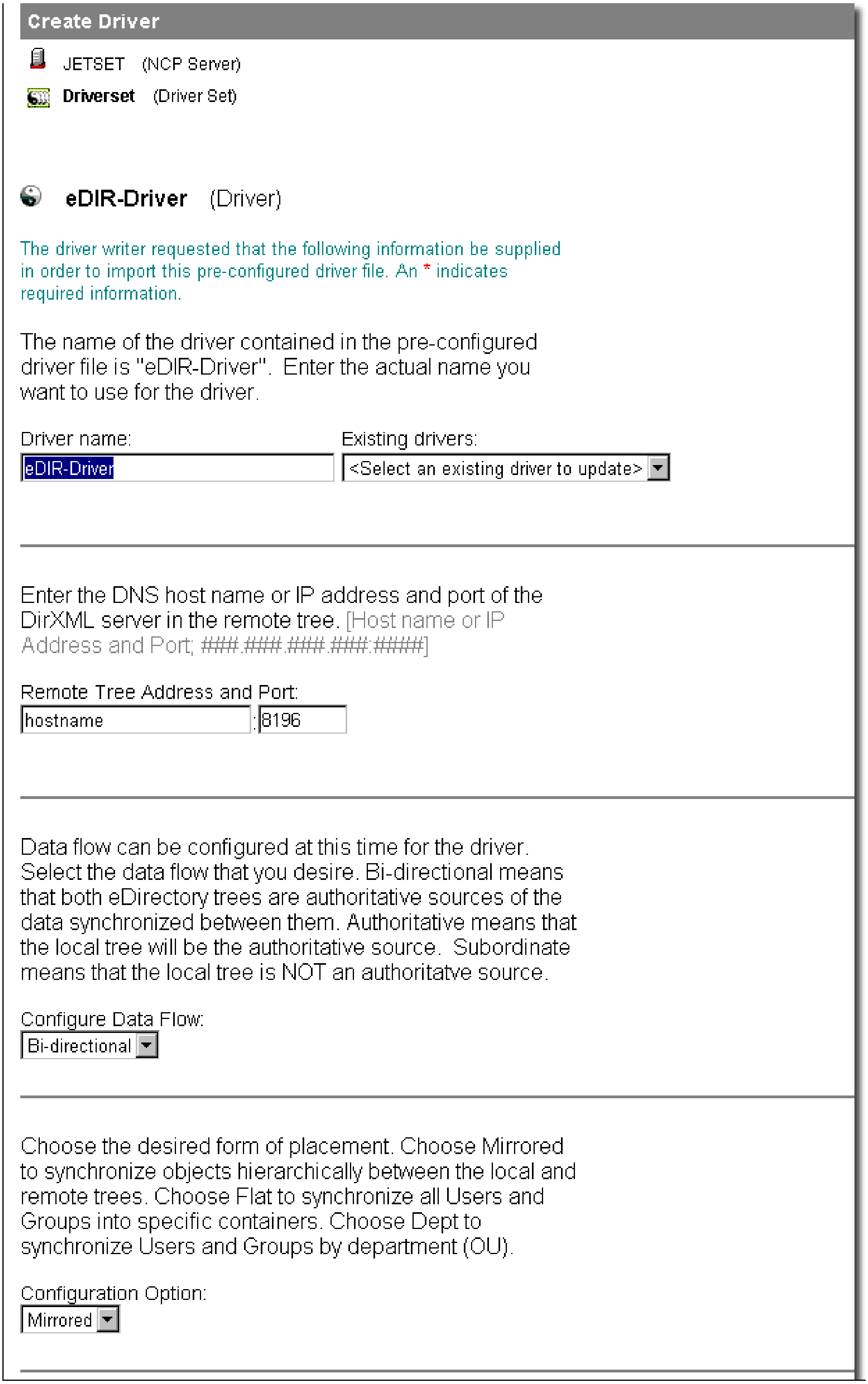
During the configuration process, you will need to provide the container names for placement of synchronized objects. For more information about eDirectory placement options, see "Default Driver Settings for eDirectory" on page 17.

### Required Driver Configuration Information for eDirectory

**IMPORTANT:** The data you supply during configuration is used to build DirXML rules. Often, case is significant to a rule. Mirror case when entering the requested data.

| System | Value |
|---|---|
| Remote Tree Address and Port<br>IP address and port for Tree 1 | |
| Remote Base Container<br>Base container for Tree 1<br>If this container does not exist, you must create it before starting the driver. | |
| Base Container<br>Base Container for groups in Tree 2<br>(If you choose the Flat placement option, you need two base containers: one for users and one for groups. For more information about placement options, see "Default Driver Settings for eDirectory" on page 17.) | |

**Figure 11 eDirectory Configuration Form**



Create Driver

JETSET (NCP Server)

Driverset (Driver Set)

eDIR-Driver (Driver)

The driver writer requested that the following information be supplied in order to import this pre-configured driver file. An * indicates required information.

The name of the driver contained in the pre-configured driver file is "eDIR-Driver". Enter the actual name you want to use for the driver.

Driver name: eDIR-Driver

Existing drivers: <Select an existing driver to update>

Enter the DNS host name or IP address and port of the DirXML server in the remote tree. [Host name or IP Address and Port; ###.###.###.###:####]

Remote Tree Address and Port: hostname : 8196

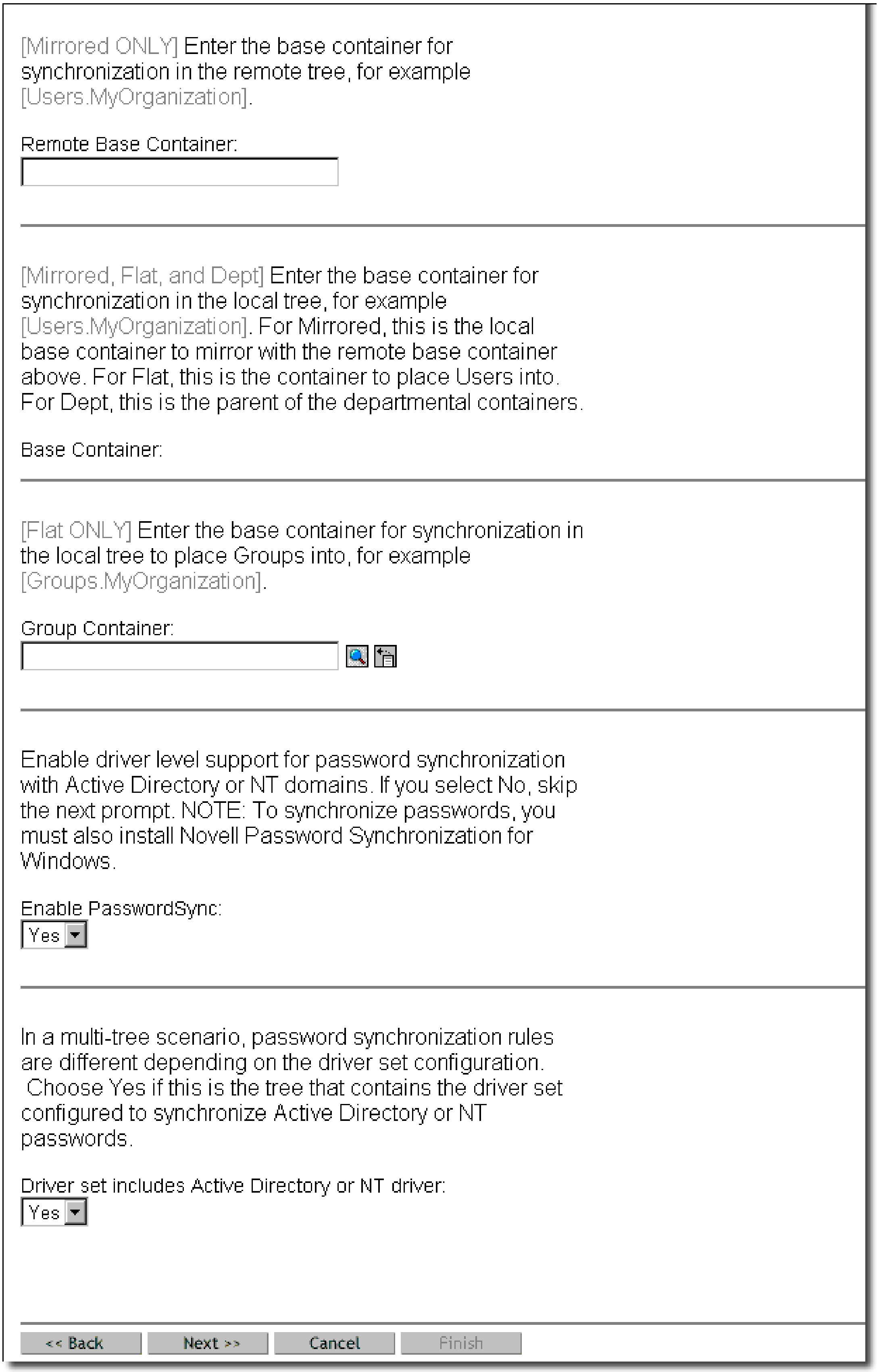
Data flow can be configured at this time for the driver. Select the data flow that you desire. Bi-directional means that both eDirectory trees are authoritative sources of the data synchronized between them. Authoritative means that the local tree will be the authoritative source. Subordinate means that the local tree is NOT an authoritatve source.

Configure Data Flow: Bi-directional

Choose the desired form of placement. Choose Mirrored to synchronize objects hierarchically between the local and remote trees. Choose Flat to synchronize all Users and Groups into specific containers. Choose Dept to synchronize Users and Groups by department (OU).

Configuration Option: Mirrored

Description:  eDirectory Configuration Form (continued)



[Mirrored ONLY] Enter the base container for synchronization in the remote tree, for example [Users.MyOrganization].

Remote Base Container:

[Mirrored, Flat, and Dept] Enter the base container for synchronization in the local tree, for example [Users.MyOrganization]. For Mirrored, this is the local base container to mirror with the remote base container above. For Flat, this is the container to place Users into. For Dept, this is the parent of the departmental containers.

Base Container:

[Flat ONLY] Enter the base container for synchronization in the local tree to place Groups into, for example [Groups.MyOrganization].

Group Container:

Enable driver level support for password synchronization with Active Directory or NT domains. If you select No, skip the next prompt. NOTE: To synchronize passwords, you must also install Novell Password Synchronization for Windows.

Enable PasswordSync: Yes

In a multi-tree scenario, password synchronization rules are different depending on the driver set configuration. Choose Yes if this is the tree that contains the driver set configured to synchronize Active Directory or NT passwords.

Driver set includes Active Directory or NT driver: Yes

## Installing DirXML and the DirXML Driver for eDirectory on Tree 1

1. At the server for your first tree, insert the DirXML CD into the CD drive. Run the installation program.
2. Read the license agreement; if you agree to the terms, click I Accept.
3. On the Components page, select the following items, then click Next.
   - DirXML Engine and Drivers
   - Driver Preconfiguration Files
4. In the Schema Extension page, specify the following:
   - **User Name:** Specify the context of a user who has rights to extend the schema, for example, CN=admin.O=hq.
   - **User Password:** Specify the password for the admin or equivalent user you specified.
5. Select the DirXML Driver for eDirectory, then click Next.
6. Select the driver configuration (XML files) for eDirectory, then click Next.
7. Read the Summary page, then click Finish.

   The file copy might take a few minutes.
8. After the installation completes and displays the Installation Complete dialog box, click Close.
9. Continue with the next section, "Configuring the DirXML Driver for eDirectory" on page 48.

## Configuring the DirXML Driver for eDirectory

This section explains how to configure the eDirectory driver for the first tree. Configuring the eDirectory driver for the second tree, along with the drivers for Active Directory and NT, is explained in "Configuring the DirXML Drivers" on page 57.

1. From your administrative workstation, launch iManager by going to http://*serveripaddress*/nps/iManager.html.

   **IMPORTANT:** This URL is case sensitive.
2. Authenticate to the first tree.
3. Click DirXML Management > Create Driver.
4. Mark In a New Driver Set, then click Next.
5. Specify a driver set name, browse to the context where you want the driver set object to be created, then browse to the server object representing the server where you installed DirXML.
6. Leave Create a New Partition checked, then click Next.
7. Mark Import a Preconfigured Driver from the Server, select eDir-Driver.xml, then click Next.
8. Using the configuration information you collected earlier, fill in the prompts for information required by the driver.
9. Click Define Security Equivalence, add Admin, then click OK.

   Drivers need rights to read and update data in eDirectory. Assigning a security equivalent is a quick way to provide necessary rights assignments. This option does not provide access to data in the other eDirectory tree.

**10** Click Exclude Administrative Roles, add Admin, click OK, then click Next.

These objects will not be replicated to the other eDirectory tree. We recommend that you add all objects that represent an administrative role (for example, the Admin object) to this list. These objects typically have no function outside of the directory tree that they were created in. Maintaining these objects in only one directory prevents potentially disruptive changes, such as access control or password changes, from causing problems.

**11** Click Finish with Overview.

**12** The eDirectory driver for Tree 1 is prepared to synchronize data. Complete preparation of other participating systems, then proceed to "Configuring the DirXML Drivers" on page 57.

# Setting Up NT Domain

For the default setup, the driver for NT is installed on the Primary Domain Controller.

**NOTE:** Additional installation options are explained in Planning Considerations (http://www.novell.com/documentation/lg/dirxmldrivers/nt/data/ageixcu.html) in the *Implementation Guide* for the NT Driver.

To synchronize account information for NT Domain users, complete the following sections:

- "Prerequisites" on page 49
- "Collecting Configuration Information" on page 49
- "Creating an Authoritative User" on page 54
- "Granting Rights to the Driver" on page 54
- "Installing and Configuring the Remote Loader and Driver" on page 54

## Prerequisites

The computer where you will install the Remote Loader and the driver must be running Windows NT* 4 with Service Pack 6a or later.

## Collecting Configuration Information

You'll need to provide a number of system-specific details when you configure the DirXML driver for NT Domain. Some of these details can be collected before you complete the following procedures, and others will be defined during the process.

- "Required Driver Configuration Information for NT Domain" on page 50 provides you with a place to record configuration data for later use.
- Figure 12, "NT Configuration Form," on page 51 is provided for reference; it shows the NT configuration form as it appears in iManager. You will see this form when you configure the DirXML drivers.

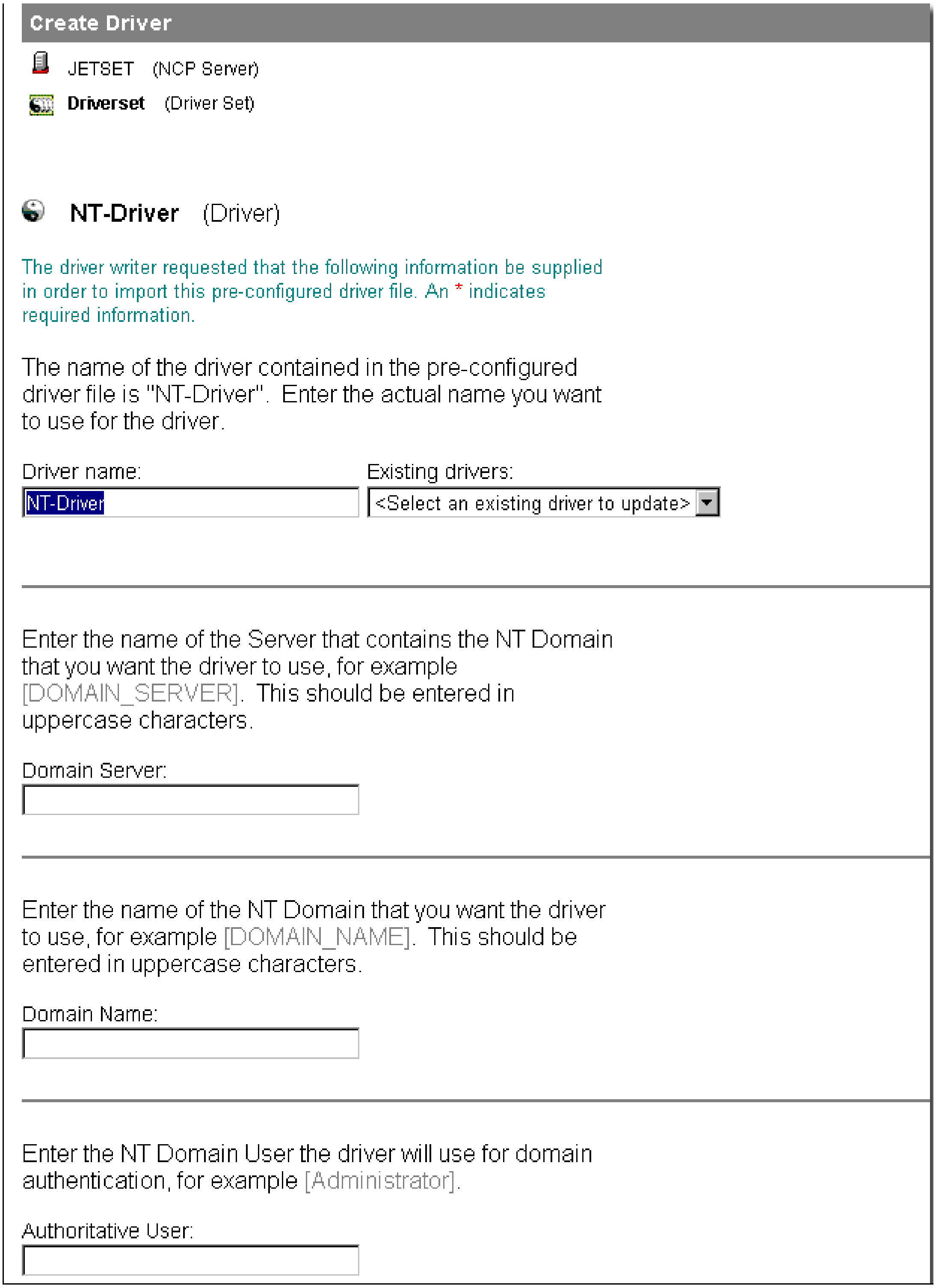
During the configuration process, you will need to provide the container names for placement of synchronized objects. For more information about NT placement options, see "Default Driver Settings for NT Domain" on page 16.

### Required Driver Configuration Information for NT Domain

**IMPORTANT:** The data you supply during configuration is used to build DirXML rules. Often case is significant to a rule. Mirror case when entering the requested data.

| System | Value |
|---|---|
| Domain Server<br>(example: DOMAIN_SERVER)<br>If necessary, ask the NT Administrator for this information. | |
| Domain Name<br>(example: DOMAIN_NAME)<br>If necessary, ask the NT Administrator for this information. | |
| Authoritative User<br>Used by the driver to access objects necessary for data synchronization. To create this user, see "Creating an Authoritative User" on page 54. | |
| Authoritative Password<br>Password for the above user. Can be set when "Creating an Authoritative User" on page 54. | |
| eDirectory Container<br>(example: Users.MyOrganization)<br>The container holding objects to synchronize with NT. If this container does not exist, you must create it before starting the driver. | |
| Remote Host and Port<br>(Specify the port when "Installing and Configuring the Remote Loader and Driver" on page 54.) | |
| Driver Password<br>Specify the password when "Installing and Configuring the Remote Loader and Driver" on page 54. | |
| Remote Password<br>Specify the password when "Installing and Configuring the Remote Loader and Driver" on page 54. | |

Figure 12 NT Configuration Form



Create Driver

JETSET (NCP Server)

**Driverset** (Driver Set)

**NT-Driver** (Driver)

The driver writer requested that the following information be supplied in order to import this pre-configured driver file. An * indicates required information.

The name of the driver contained in the pre-configured driver file is "NT-Driver". Enter the actual name you want to use for the driver.

Driver name: NT-Driver

Existing drivers: <Select an existing driver to update>

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 Server:

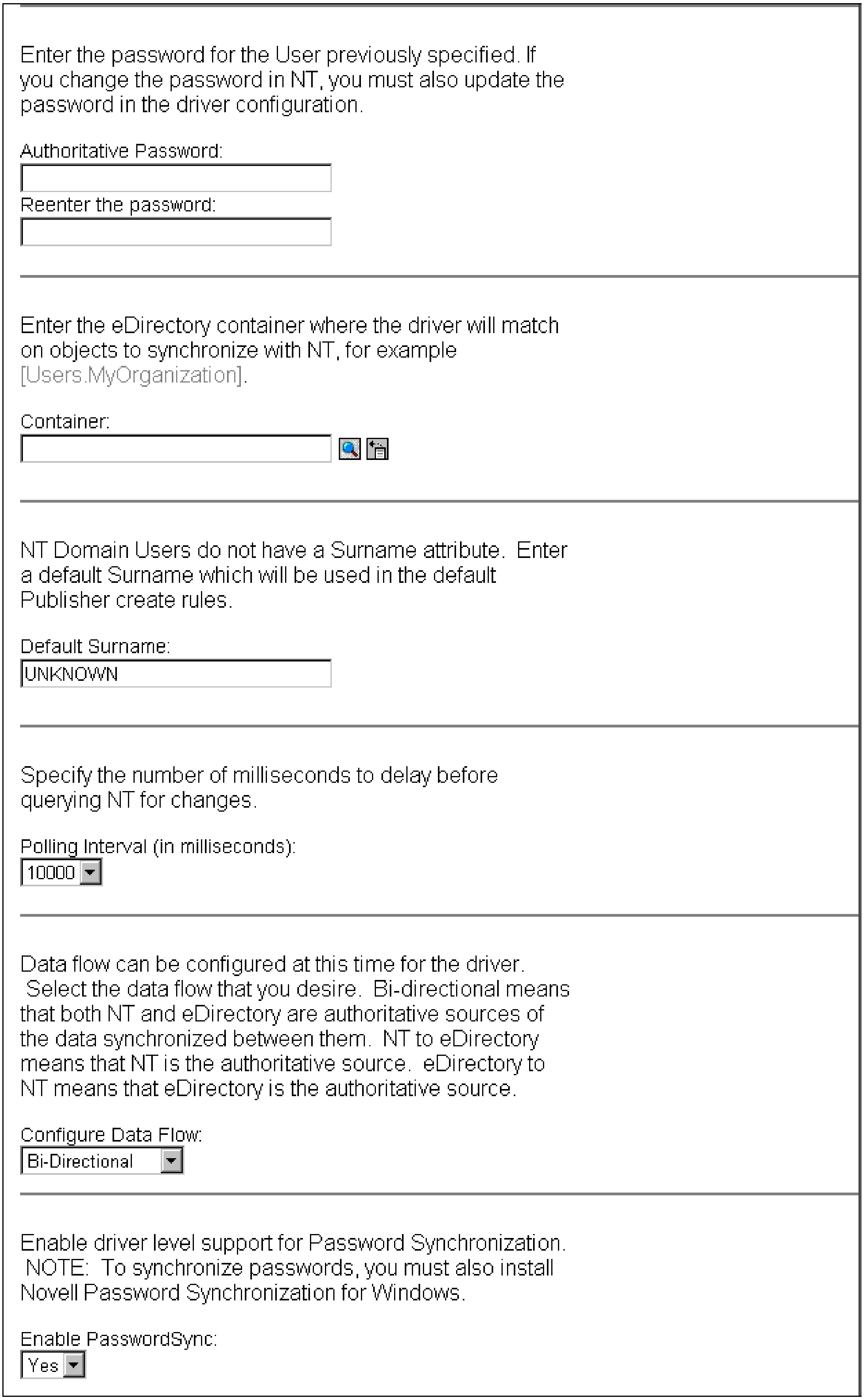
Enter the name of the NT Domain that you want the driver to use, for example [DOMAIN_NAME]. This should be entered in uppercase characters.

Domain Name:

Enter the NT Domain User the driver will use for domain authentication, for example [Administrator].

Authoritative User:

## Description: NT Configuration Form (continued)



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.

Authoritative Password:

Reenter the password:

Enter the eDirectory container where the driver will match on objects to synchronize with NT, for example [Users.MyOrganization].

Container:

NT Domain Users do not have a Surname attribute. Enter a default Surname which will be used in the default Publisher create rules.

Default Surname: UNKNOWN

Specify the number of milliseconds to delay before querying NT for changes.

Polling Interval (in milliseconds): 10000

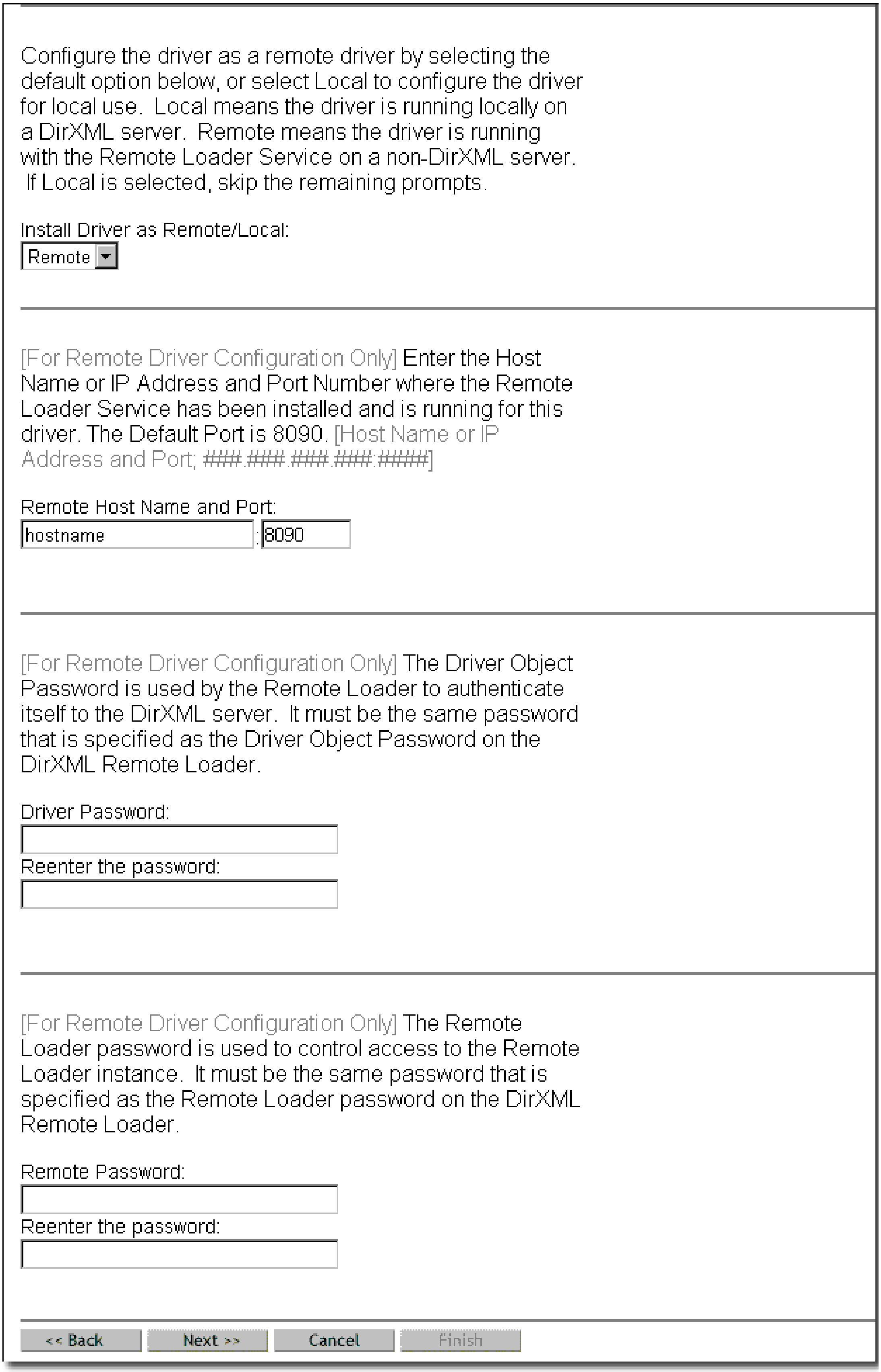
Data flow can be configured at this time for the driver. Select the data flow that you desire. Bi-directional means that both NT and eDirectory are authoritative sources of the data synchronized between them. NT to eDirectory means that NT is the authoritative source. eDirectory to NT means that eDirectory is the authoritative source.

Configure Data Flow: Bi-Directional

Enable driver level support for Password Synchronization. NOTE: To synchronize passwords, you must also install Novell Password Synchronization for Windows.

Enable PasswordSync: Yes

## Description: NT Configuration Form (continued)



Configure the driver as a remote driver by selecting the default option below, or select Local to configure the driver for local use.  Local means the driver is running locally on a DirXML server.  Remote means the driver is running with the Remote Loader Service on a non-DirXML server.  If Local is selected, skip the remaining prompts.

Install Driver as Remote/Local: Remote

[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. [Host Name or IP Address and Port; ###.###.###.###:####]

Remote Host Name and Port: hostname : 8090

[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.

Driver Password:

Reenter the 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.

Remote Password:

Reenter the password:

## Creating an Authoritative User

The driver needs Read/Write rights to the domain. You can configure the driver to use any existing account with the appropriate rights. However, to ease future management, we recommend that you create a new account to be used exclusively by the driver.

1. Click Start > Programs > Administrative Tools (Common) > UserManager for Domains.
2. In the User Manager dialog box, select User > New User.
3. Specify a username and password.

   Record the Authoritative user information in the table under "Required Driver Configuration Information for NT Domain" on page 50.
4. Unmark User Must Change Password at Next Logon, then mark Password Never Expires so that a password policy won't disable the driver unexpectedly.
5. Click Groups, then move Domain Admins to the Member of list.
6. Click Set, then click OK.
7. Click Add, then close the New User dialog box.
8. Continue with the next section, "Granting Rights to the Driver" on page 54.

## Granting Rights to the Driver

You need to grant rights to the authoritative user that the driver uses so that it can access the SAM keys in the registry of the server that has the domain you want to use.

Creating a user equivalent to Administrator for the driver 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.

1. Log in to NT as Administrator.
2. Run regedt32.
3. Select the HKEY_LOCAL_MACHINE window.
4. Select the SAM key, then go to the Security menu and select Permissions.
5. Mark Replace Permission on Existing Subkeys.
6. Give Full Control permission to Administrators, then click OK.
7. Click Yes to replace the permission on all existing subkeys within the SAM.
8. Close the registry and continue with the next section, "Installing and Configuring the Remote Loader and Driver" on page 54.

## Installing and Configuring the Remote Loader and Driver

The Remote Loader allows you to run the driver on a computer other than the server hosting the DirXML engine.

1. At the NT computer that will host the driver, insert the DirXML CD into the CD drive. The CD may take a moment to load. Then, at the Welcome page, click Next.
2. Read the license agreement; if you agree to the terms, click I Accept.
3. On the Components page, select DirXML Remote Loader and Drivers, then click Next.

4. Accept the default installation path for the Remote Loader, then click Next.
5. Mark the following items, then click Next.
   - DirXML Remote Loader Service
   - DirXML Driver for NT Domain
6. Review the Product Summary, then click Finish to install the Remote Loader files.
7. When prompted, create a shortcut.
8. On the Installation Complete page, click Close.
9. Run the DirXML Remote Loader Configuration Wizard from your desktop.
10. On the Welcome page, click Next.
11. Keep the default Command Port number, then click Next.
12. Keep the default Configuration File Name, then click Next.
13. On the DirXML Driver page, mark Native, browse to and select the NT Domain driver (c:\Novell\Remoteloader\NTDomainShim.dll) then click Next.
14. On the Connection to DirXML page, leave the default Port settings and Addresses.
15. If appropriate for your environment, mark Use SSL and browse to the Trusted Root Certificate.

    Using SSL with Remote Loader encrypts the communication between the Remote Loader and the DirXML engine.

    You can create a Server Certificate object and then export a self-signed root certificate from your Organizational CA as explained in Exporting the Organizational CA's Self-Signed Certificate (http://www.novell.com/documentation/lg/crt252/crtadmin/data/a2ebop8.html#a2ppx57). Save the certificate file in base64 format and copy it to a local directory on the computer hosting the Remote Loader.

    **IMPORTANT:** If you use SSL, then *after* the driver configuration is imported you must:
    - Use iManager to edit the Authentication section of the Driver Parameters. In the Remote Loader Connection Parameters add a reference to the certificate as shown in the following example: hostname=192.168.0.1 port=8090 kmo=servernamecert.
    - Re-enter the application and the Remote Loader passwords.
16. Record the port number in the table under "Required Driver Configuration Information for NT Domain" on page 50, then click Next. This information will be required later during driver parameter configuration.
17. Set Trace Level to 3 so that you'll get adequate tracking data from the Remote Loader for troubleshooting.

    Trace information can include general state information, event information, warning messages, error messages, etc.

| Trace Level | Information |
|---|---|
| 0 | No information display or tracking |
| 1 | General informational messages about processing |
| 2 | Displays messages from level 1 plus the XML documents that are passed between the engine and driver |
| 3 | Displays messages from level 2 plus documents sent and received between the Remote Loader and the DirXML engine |

| Trace Level | Information |
|---|---|
| 4 | Displays messages from level 3 plus information about the connection between the Remote Loader and the DirXML engine |

**18** Specify a location and filename for the trace file, then click Next.

The default location is c:\Novell\RemoteLoader.

**IMPORTANT:** The trace file is a tool to help you monitor events during startup or when you are troubleshooting. Messages will be logged to this file continuously, making it grow until it fills the available disk space. Ensure the location of this file is appropriate for your environment.

After you're satisfied that the driver is running as expected, you can reset the Trace Level to 0. Then use the Windows Event Viewer found under Administrative Tools or the eDirectory Report and Notification Service (http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/afae8bz.html) to monitor events on an ongoing basis.

Ensure that this path exists. If the path does not exist, messages will not be logged.

If the path to the trace file includes spaces, enclose the path in quotes. For example, type "c:\documents and settings\Adminstrator\My Documents." If the trace level is greater than 0, trace messages will be written to the log file even if the trace window is not open.

If you are running multiple Remote Loader sessions on a single computer, you should create separate trace files for each session.

**19** Mark Install the Remote Loader Instance as a Service, then click Next.

Installing Remote Loader as a service allows the Remote Loader to continue to run, even when you log off.

**20** Set Remote Loader and Driver Object passwords.

We recommend keeping remote passwords and driver passwords the same across systems and changing them later when you go to production.

Record the passwords in the table under "Required Driver Configuration Information for NT Domain" on page 50. This information will be required later during driver parameter configuration.

**21** Review the summary, then click Finish.

**22** When prompted, start the service.

You will see the Trace screen with messages indicating that Remote Loader is waiting for a DirXML connection.

**NOTE:** If you close the Trace screen and then want to open it again, you can do so at a command prompt by entering **`dirxml_remote -window on`**.

To stop or start the service, locate DirXML Loader in Microsoft Services (Start > Settings > Control Panel > Administrative Tools > Services).

The NT system is prepared to synchronize data. Complete preparation of other participating systems and then proceed to "Configuring the DirXML Drivers" on page 57.

# Configuring the DirXML Drivers

After the systems hosting DirXML drivers have been set up, you will configure the drivers by importing driver preconfiguration files and then testing data synchronization. These tasks can be completed using Novell iManager 2.0 plug-ins, which were installed when you completed the section, "Setting Up iManager" on page 28.

**NOTE:** ConsoleOne can also be used to configure DirXML drivers. For ConsoleOne information, see DirXML Administration (http://www.novell.com/documentation/lg/dirxml10/dirxml/data/hgcbnee7.html).

To configure the drivers, complete the steps in the following sections:

- "Importing the Preconfigured Drivers" on page 57
- "Configuring Secure Data Transfers for the DirXML Driver for eDirectory" on page 58
- "Testing Data Synchronization" on page 59

## Importing the Preconfigured Drivers

Using application information that you provide, the Import Drivers Wizard completes configuration for the DirXML drivers.

You'll need the data you collected and recorded in the Configuration Information tables at the beginning of each system's setup.

1. Launch iManager by going to http://*serveripaddress*/nps/iManager.html.

   **IMPORTANT:** This URL is case sensitive.

2. Authenticate to the second tree.
3. Click DirXML Management > Import Drivers.
4. Mark In a New Driver Set, then click Next.
5. Specify a driver set name, browse to the context where you want the driver set object to be created, then browse to the server object representing the server where you installed DirXML.
6. Leave Create a New Partition checked, then click Next.
7. Select the appropriate driver configuration files for your installation.

   Driver configuration files are available for drivers licensed with this release (eDirectory, Active Directory, and NT Domain) and for evaluation drivers.

8. Click Next, then fill in the prompts for application information using the data you recorded in Configuration Information tables.

   You will be presented with a page of information prompts for each driver you selected.

   **IMPORTANT:** Scroll to the bottom of the page to see all the prompts. If you quit before configuring all of the drivers, the drivers will not have enough information to function properly.

9. Click Define Security Equivalence, add Admin, then click OK.

   Drivers need rights to read and update data in eDirectory. Assigning a security equivalent is a quick way to provide necessary rights assignments. This option does not provide access to data in the target application. Access to the target application is provided through other driver parameters.

10. Click Exclude Administrative Roles, add Admin, click OK, then click Next.

These objects will not be replicated to the application. We recommend that you add all objects that represent an administrative role (for example, the Admin object) to this list. These objects typically have no function outside of the directory that they were created in. Maintaining these objects in only one directory prevents potentially disruptive changes, such as access control or password changes, from causing problems.

11 After providing all the required information, click Finish with Overview.

Setup of the DirXML Starter Pack is complete.

12 If you are synchronizing data between two eDirectory trees, continue with the next section, "Configuring Secure Data Transfers for the DirXML Driver for eDirectory" on page 58.

or

If you are not synchronizing data between two eDirectory trees, continue with "Testing Data Synchronization" on page 59.

## Configuring Secure Data Transfers for the DirXML Driver for eDirectory

The DirXML driver for eDirectory requires Novell Certificate Server™ and a Certificate Authority (CA) to ensure data security. All transactions between trees must be secured through an SSL connection. We recommend that you use the Certificate Authority from the tree containing the driver to issue the certificates used for SSL.

For more information about Novell Certificate Server, see Understanding the Novell Certificate Server (http://www.novell.com/documentation/lg/edir87/edir87/data/a7elxuq.html).

### Run the Certificate Wizard

1 Launch iManager by going to http://*serveripaddress*/nps/iManager.html.

**IMPORTANT:** This URL is case sensitive.

2 Authenticate to the second eDirectory tree hosted on the server.

3 Click DirXML Management > NDS2NDS Driver Certificates.

4 On the Welcome page, enter the requested information for the first tree.

Default values are provided using objects in the tree that you authenticated to when you launched iManager. You must enter or confirm the following information:

- Driver DN: Use the distinguished name of the eDirectory driver, such as EDir-Driver.DriverSet.Services.YourOrganization.
- The tree name: Enter the IP address for the first tree.
- A username for an account with administrative rights, such as Admin.
- The password for the administrative user.
- The user's context, such as Services.YourOrganization.

5 Click Next.

The wizard uses the information you entered to authenticate to the first tree, verify the driver DN, and verify that the driver is associated with a server.

6 Enter or confirm the following information for the second tree:

- Driver DN: Use the distinguished name of the eDirectory driver, such as EP-EDir-Account.DriverSet.YourOrganization.

- The tree name: Enter the IP address for second tree.
- A username for an account with administrative rights, such as Admin.
- The password for the administrative user.
- The user's context, such as HQ.YourOrganization.

7 Click Next.

The wizard uses the information you entered to authenticate to the second tree, verify the driver DN, and verify that the driver is associated with a server.

8 Review the information on the Summary Page, then click Finish.

If Key Material Objects (KMOs) already exist for these trees, the wizard deletes them and then does the following:

- Exports the trusted root of the CA in the first tree
- Creates KMO objects
- Issues a certificate signing request
- Places certificate key pair names in the drivers' Authentication ID

9 Configuration for secure data synchronization is complete. Continue with the next section, "Testing Data Synchronization" on page 59.

## Testing Data Synchronization

After participating systems are set up and their drivers have been configured, use the following procedures to verify that data is synchronized correctly.

### Start Each Driver

Start one driver at a time to validate proper DirXML configuration. By default, drivers are set for Manual startup.

**NOTE:** After you have a driver configuration that works in your environment, use iManager to change the startup option to Auto Start. Auto Start will re-start the driver whenever eDirectory is re-started.

1 Ensure that the Remote Loader service is running on the systems where you set it up and that you can view the trace screen for the Remote Loader.

**NOTE:** To open the Trace Screen: at a command prompt enter **`dirxml_remote -window on`**.

2 Open a DSTrace screen on the computer where the DirXML engine is installed by typing **`dstrace on screen on file off`** at the console prompt.

To configure dstrace.nlm to display only DirXML trace messages, enter **`dstrace -all +dxml +dvrs`**.

To include message tags and time stamps, enter **`dstrace -all +dxml +dvrs +tags +time`**.

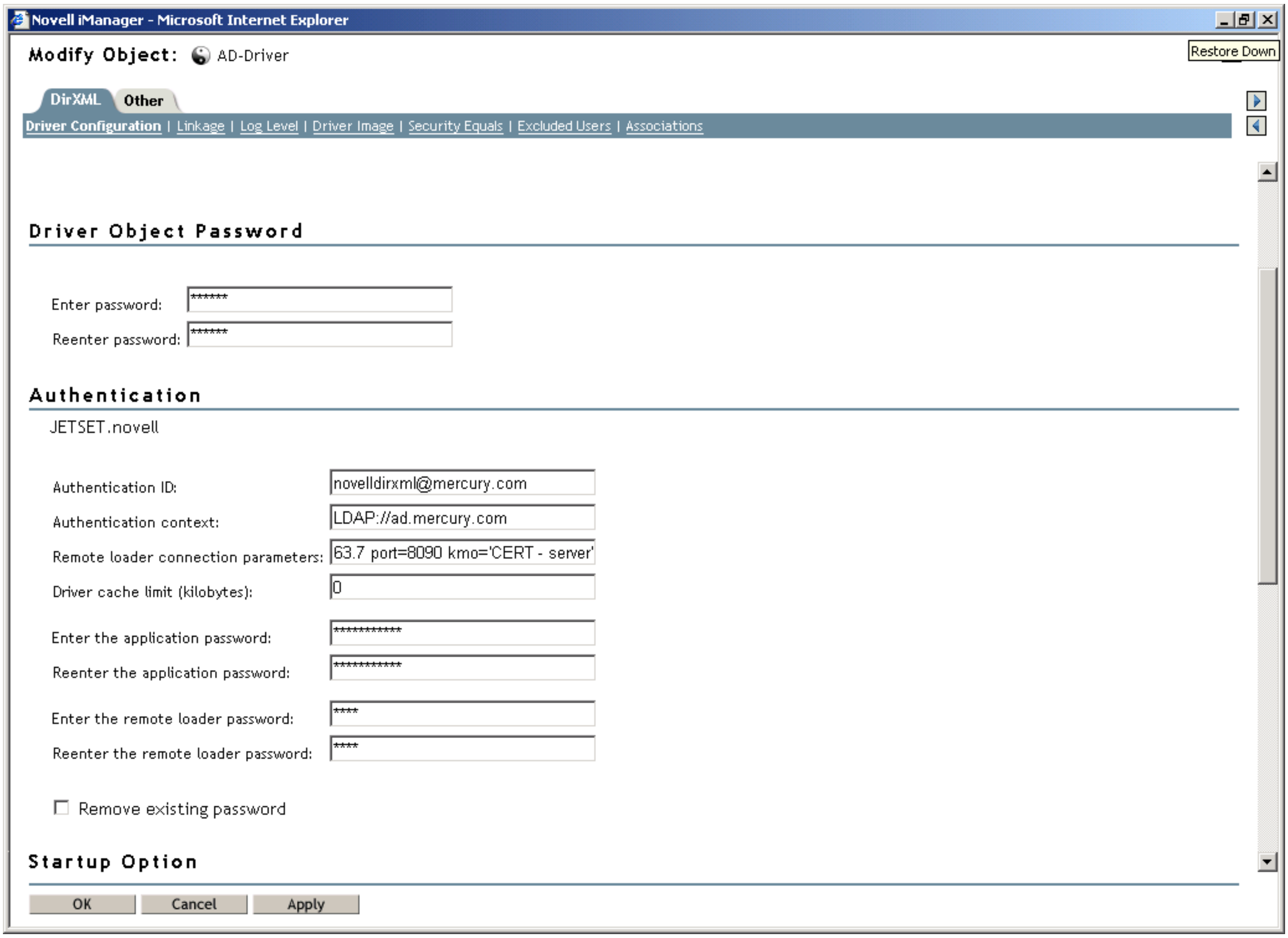
3 In iManager, select DirXML Management > Overview.

4 Browse to the DirXML driver set.

5 (Conditional) If you configured the Remote Loader Service to use SSL, before you start the drivers, you must edit the Authentication section of the Driver Parameters and re-enter passwords.

Add a reference to the certificate as shown in the following example.
hostname=192.168.0.1 port=8090 kmo=servernamecert

**Figure 13 Referencing the KMO**



Novell iManager - Microsoft Internet Explorer
Restore Down
DirXML
Other
Driver Configuration | Linkage | Log Level | Driver Image | Security Equals | Excluded Users | Associations
OK
Cancel
Apply

Modify Object: AD-Driver

Driver Object Password

Enter password: ******

Reenter password: ******

Authentication

JETSET.novell

Authentication ID: novelldirxml@mercury.com

Authentication context: LDAP://ad.mercury.com

Remote loader connection parameters: 63.7 port=8090 kmo='CERT - server'

Driver cache limit (kilobytes): 0

Enter the application password: ************

Reenter the application password: ************

Enter the remote loader password: ****

Reenter the remote loader password: ****

□ Remove existing password

Startup Option

6 Click the status icon in the upper right corner of the driver's icon, then click Start Driver.

7 Review the messages in the DSTrace screen and the remote trace screen to verify successful driver start.

**NOTE:** See Novell AppNotes, Effectively Reading a DirXML Trace File (http://developer.novell.com/research/appnotes/2002/october/06/a021006.pdf) for in-depth information about using DSTrace with DirXML.

8 After all drivers are running, add a new user as described in the following Data Synchronization Tests.

### Data Synchronization Tests

- ❑ **Add a New User:** In any of your participating systems, create new user. Verify that an account was created for the new user in each of the participating systems. Log in to each system as the new user.
- ❑ **Modify User Information**: Log in as administrator on any of the participating systems. Modify an attribute that is synchronized on the new user object. Verify data synchronization in participating systems.
- ❑ **Delete a User:** Delete the new user account. Verify that the account was removed from all participating systems.

## Migrating Existing 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.

The issues to consider before migration vary depending on the system you are synchronizing. For system-specific information, see the following documents:

- For migration of NT data, see Migrating and Resynchronizing Data (http://www.novell.com/documentation/lg/dirxmldrivers/nt/data/acacizx.html#ageis08) in the *Implementation Guide* for NT.
- For migration of Active Directory data, see Migrating and Resynchronizing Data (http://www.novell.com/documentation/lg/dirxmldrivers/ad/data/agdyl3s.html#ageis08) in the *Implementation Guide* for Active Directory.

To use one of the options explained above:

1. In iManager, select DirXML Management > Overview.
2. Locate the driver representing the system that you are synchronizing, then double-click the driver icon.
3. Click the appropriate migration button.

# 5 Setting Up Password Synchronization

Password Synchronization allows passwords to be securely, consistently, and automatically shared across Novell® eDirectory™, Microsoft* NT domains, and Microsoft Active Directory.

With PasswordSync, a user can log in to any of these systems using the same password. Administrators can manage passwords in the system of their choice. Any time a password is changed in one of these environments, it will be updated in all of them.

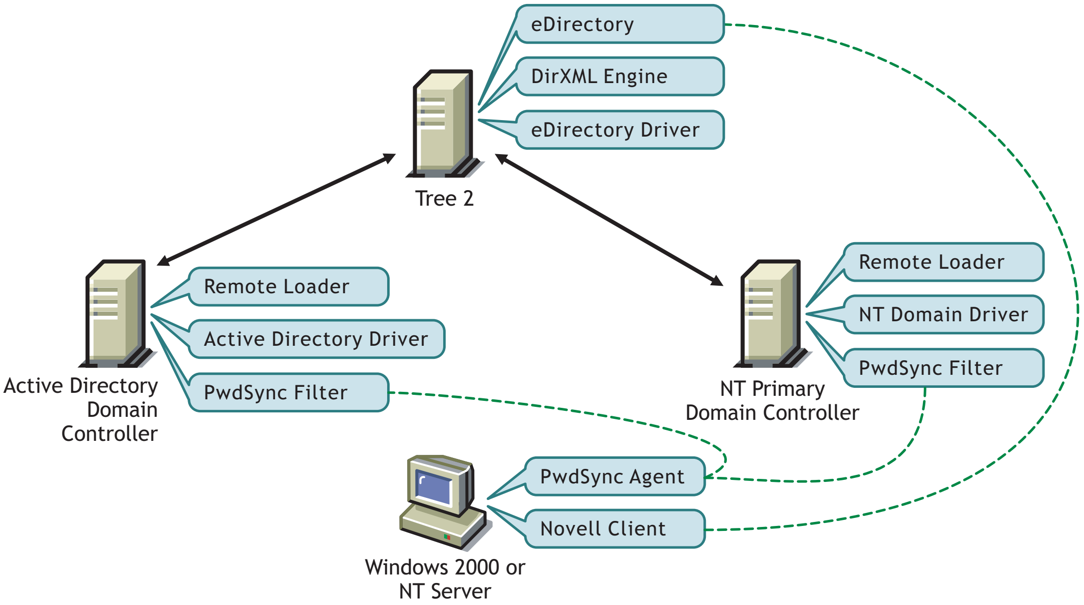
This section explains how to install Password Synchronization and begin synchronizing passwords. It includes the following topics:

For more conceptual information about Password Synchronization, see Understanding PasswordSync (http://www.novell.com/documentation/lg/pwdsync10/passsync/data/adtyhxw.html).

## Where to Install PasswordSync

As shown in Figure 14, PasswordSync is a distributed application that requires DirXML® drivers and includes PasswordSync Agents and PasswordSync Filters. Installation of the DirXML drivers is explained in the previous chapter, Chapter 4, "Setting Up Participating Systems," on page 31. Agent and filter installation options are discussed in the sections that follow.

Figure 14 PasswordSync Agents and Filters



### PasswordSync Agents

A PasswordSync Agent can be installed on any Windows 2000/NT server or on any Windows 2000/NT workstation that is continuously available. The computer where the agent is installed must have the latest Novell Client™ installed.

There is no requirement to place an agent on a controller or on the same computer as Novell® eDirectory™ or DirXML.

Agents are configured and maintained on the computer where they run, so easy access to the computer, either physically or through terminal services, is one of the most important considerations.

Install PasswordSync Agents on as many computers as necessary to address topology issues and satisfy redundancy requirements for your environment.

### PasswordSync Filters

PasswordSync Filters must be installed on all domain controllers, even if the domain controllers are already hosting DirXML drivers. Filters can be installed as part of the agent installation or installed separately as changes to your network may require.

Every NT Primary Domain Controller (PDC), every Backup Domain Controller that might be promoted to a PDC, and every Active Directory Domain Controller requires a filter and an association with at least one PasswordSync Agent. The more agents that service a given domain controller, the greater redundancy you achieve.

## Installing PasswordSync

You can configure password synchronization for either a single-tree network or a multi-tree network.

- **Single-tree network:** Complete the steps in "Installing PasswordSync Into a Single-Tree Network" on page 65.

- **Multi-tree network:** First, complete the steps in "Installing PasswordSync Into a Single-Tree Network" on page 65, then continue with "Installing PasswordSync Into a Multi-Tree Network" on page 68.

## Installing PasswordSync Into a Single-Tree Network

### Prerequisites

- The computer hosting the PasswordSync Agent must have one of the following Novell Clients installed.
  - 4.83 SP1 or later for Windows NT/2000
  - 4.82 or later for Windows XP
- Computers used to generate any eDirectory password changes must have one of the following Novell Clients installed.
  - 4.81 or later for Windows NT/2000
  - 3.31 or later for Windows 95/98
  - 4.82 or later for Windows XP
- If you are synchronizing with a domain outside of the tree where the agent is installed, then the computer hosting the agent must be configured to use WINS or DNS.

  **TIP:** To see whether you need to use WINS or DNS, you can use Windows Explorer to navigate through network neighborhood. If you can't see all domain controllers, then you need to use WINS or DNS.
- All domain controllers hosting filters and computers hosting agents must use the same Windows Service Packs; otherwise, passwords are encrypted and decrypted in different ways and password synchronization will fail.

### Installing an Agent and Filter

1. Authenticate to the eDirectory Tree.
2. At the Windows computer that will host the agent, insert the DirXML CD into the CD drive.

   The CD may take a moment to load.
3. At the Welcome screen, click Next.
4. Read the license agreement; if you agree to the terms, click I Accept.
5. At the Components page, mark PasswordSync Agent, then click Next. A summary screen is displayed.
6. Click Finish, then at notice of completion, click Close.

   If Microsoft DLL files required for PasswordSync are out of date, the installation program will copy them to the system directory and you will be prompted to reboot.
7. In Control Panel, click Password Synchronization.
8. Specify the tree name, then click OK.
9. In the PasswordSync Setup dialog box, select the domain that will participate in password synchronization and its associated DirXML driver.

   **NT Domains:** If you type the name of an NT 4 domain rather than browse to it, you must enter the name in uppercase. This requirement is for NT 4 domain names only; Active Directory domain names are not required to be uppercase.

**10** Click OK, then specify the name for the new PasswordSync object and the context where it should be placed.

The default object name is the name of the server where you are installing PasswordSync, followed by -pwdsync.

The default context is that of the container holding the DirXML Driver Set object.

**11** Click OK, then select the container for which PasswordSync will be assigned as a trustee.

The PasswordSync Agent needs the rights to manage passwords in eDirectory and to read the DirXML drivers that control the domains being synchronized.

Select a container high enough in the tree to span all objects that the agent needs to access, including user objects, the domain object, the DirXML driver object, and the server object for the server hosting the DirXML engine.

If you want to make narrower rights assignments, make the following trustee assignments:

- For users participating in password synchronization:

| Trustee | Attribute | Rights |
|---|---|---|
| nadPwdSync object | Password Expiration Interval | compare, read |
| nadPwdSync object | Password Management | compare, read, write |
| nadPwdSync object | Password Expiration Time | write |
| [Public] | [Entry Rights] | browse |
| [Public] | nadLoginName | compare, read |

- For nadDomain objects:

| Trustee | Attribute | Rights |
|---|---|---|
| nadPwdSync object | Server | compare, read |
| [Public] | [Entry Rights] | browse |
| [Public] | nadPasswordSync | compare, read |

- For server objects holding the PwdSync index (by default, this is the server where DirXML is installed):

| Trustee | Attribute | Rights |
|---|---|---|
| nadPwdSync object | Index Definition | compare, read |
| nadPwdSync object | [Entry Rights] | browse |

**12** When prompted, click Yes to install a PasswordSync Filter. Select domain controllers from those listed, then click Add.

*Remote domain controllers will be automatically rebooted when installation is complete.* You must manually reboot the local domain controller after installation is complete.

**IMPORTANT:** Because any domain controller can process a password change request, a filter must be installed on each Active Directory Domain Controller and each NT Primary Domain Controller. You should also install a filter on each NT Backup Domain Controller that could be promoted to a Primary Domain Controller.

If you have several domain controllers, we recommend that you install filters on a few controllers at a time. This will minimize the impact of rebooting many domain controllers at once and will expedite your initial installation. To install filters to domain controllers after initial installation, see "Installing Additional Filters" on page 67.

**13** Click Close, then click Close.

PasswordSync installation is complete for the domain and driver you selected. To synchronize passwords for existing user accounts in this domain, see "Synchronizing Passwords for Existing Accounts" on page 75.

If you have additional DirXML NT Domain or Active Directory drivers, or if you need to provide additional PasswordSync coverage, complete the additional installation processes described in the following table:

| Condition | Additional Installation |
|---|---|
| A single agent can service many domains; however, additional agents provide redundancy and address network topology issues.<br>For example, to synchronize a domain that is on one end of a WAN link, you can install a PasswordSync Agent on that side of the WAN for more efficient network traffic. | Install additional PasswordSync Agents on another workstation by repeating the steps in Installing PasswordSync Into a Single-Tree Network. |
| The PasswordSync installation program allows you to install filters on all domain controllers in a single domain.<br>Install additional filters if you:<br>◆ Didn't install filters on all domain controllers<br>◆ Have additional domains you want to synchronize | See "Installing Additional Filters" on page 67. |

### Installing Additional Filters

Installing a PasswordSync Filter on a domain controller creates an association between a PasswordSync Agent and the domain controller. If the domain controller is already associated with an agent, installing a filter just updates the filter's list of available PasswordSync Agents.

If this is the first time the domain controller has participated in password synchronization, it has no association with any agent. In this case, the installation will require rebooting the domain controller. You might want to perform this procedure after hours, or select only one domain controller at a time.

**NOTE:** Remote domain controllers will be rebooted automatically; a local domain controller must be rebooted manually.

**1** At the computer where the Password Synchronization service is installed, click Start > Settings > Control Panel.

**2** Click Password Synchronization.

**3** Select a domain, then click Filters.

4 Select a domain controller, then click Add.

5 Click Close. The domain now has a PasswordSync Filter.

6 Verify that the filter is running by checking the event log on the domain controller.

To access the event log, choose Start > Settings > Control Panel > Administrative Tools > Event Viewer. For Windows 2000, the log is called PwdSync. For NT, messages are logged in the Application log with a source reference of PwdSync.

## Installing PasswordSync Into a Multi-Tree Network

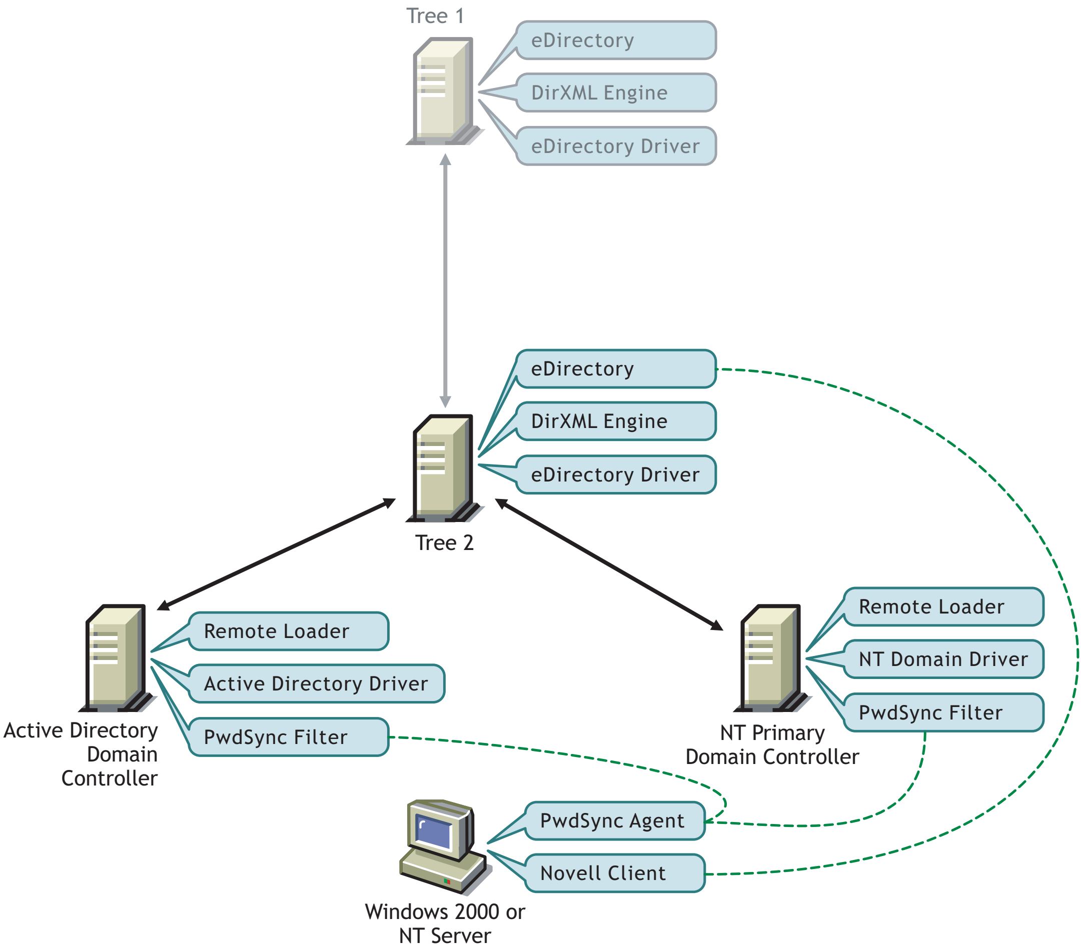
### Understanding the Process

In the following sections, the two eDirectory trees are labeled Tree 1 and Tree 2. As shown in Figure 15, Tree 2 is configured to synchronize account information using the Active Directory and NT drivers.

To synchronize passwords in an environment with multiple eDirectory trees,

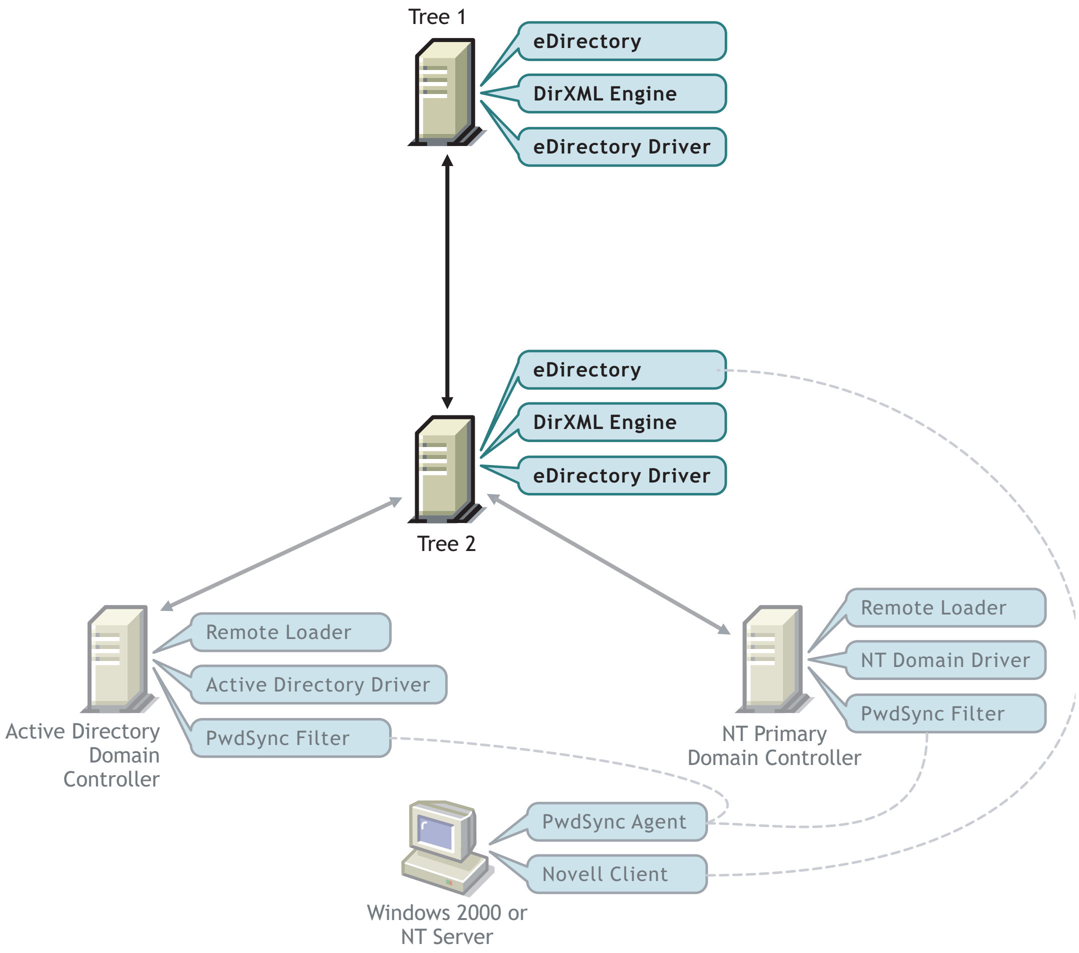
- First you set up password synchronization in Tree 2 as explained in "Installing PasswordSync Into a Single-Tree Network" on page 65. This step should already be completed.

**Figure 15 Single-Tree Password Synchronization**



- Then, you migrate object information required by PasswordSync from Tree 2 to Tree 1. This step is explained in "Migrating PasswordSync Data" on page 70.

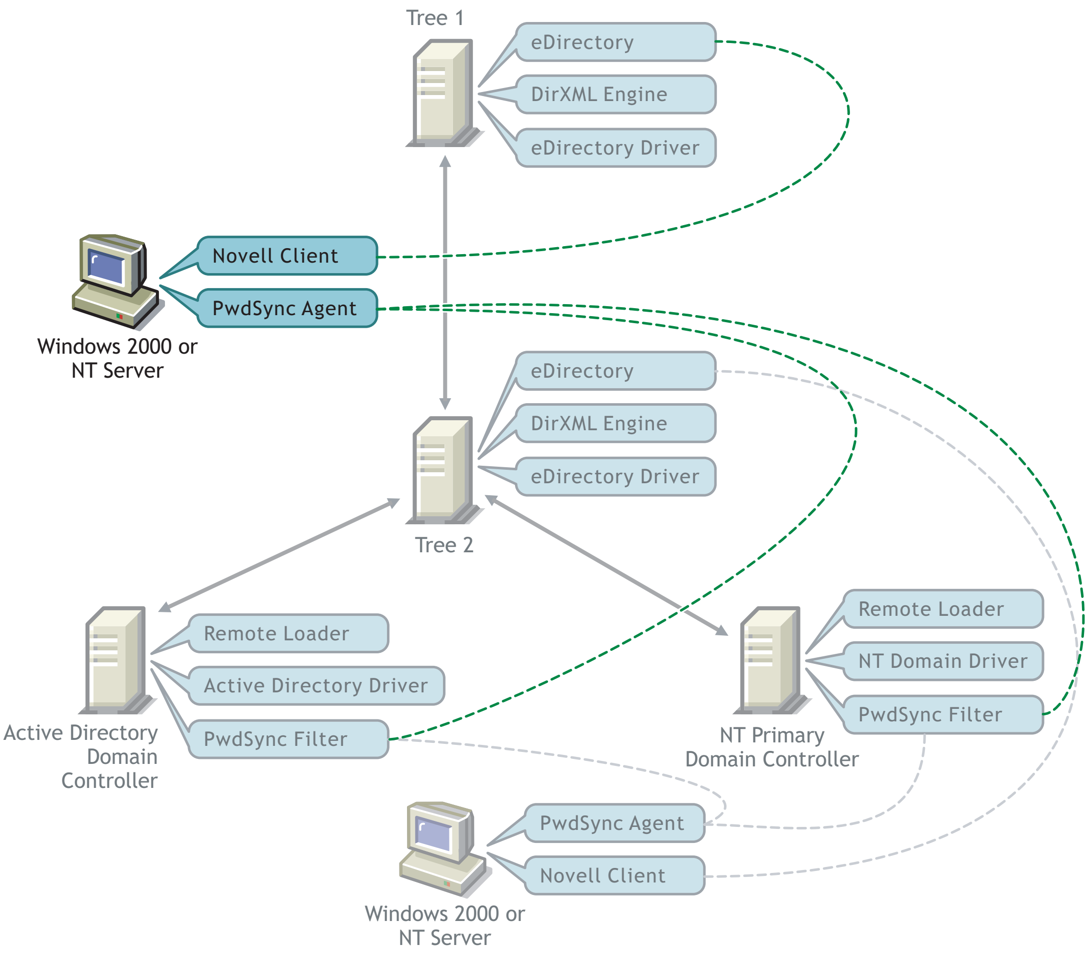
**Figure 16 eDirectory Driver Configuration for PasswordSync**



- Finally, you install a PasswordSync Agent into Tree 1 to communicate password changes between this tree and participating domains. This step is explained in "Installing a PasswordSync Agent for Tree 1" on page 71.

  Without this PasswordSync setup, password changes made in Tree 1 would be synchronized to Tree 2, but would not be synchronized with Active Directory or NT.

Figure 17 **PasswordSync Agent for Tree 1**



**TIP:** To keep these trees straight in the procedures that follow, you might want to label Figure 17 with the actual tree names for the trees you are synchronizing, then reference this graphic as you complete the setup process.

To allow Tree 1 to participate fully in password synchronization, complete the following procedures:

❑ "Migrating PasswordSync Data" on page 70

❑ "Installing a PasswordSync Agent for Tree 1" on page 71

## Migrating PasswordSync Data

The nadDomain objects from Tree 2 must be migrated to Tree 1. Additionally, you should force an update of the Tree 2 user objects that are participating in password synchronization.

To migrate PasswordSync data from the Tree 2 to Tree 1:

**1** Launch iManager by going to http://*serveripaddress*/nps/iManager.html.

**IMPORTANT:** This URL is case sensitive.

**2** Authenticate to Tree 2, then click DirXML Management > Overview.

**3** Locate the DirXML eDirectory driver.

4. In the Driver Overview page for the eDirectory driver, click Migrate from eDirectory, then click Add.
5. Select the nadDomain object representing the domain already participating in password synchronization, then click OK.

   This object will be inside the driver object that is participating in password synchronization.
6. Click Add.
7. Select the container holding all the users whose account data is already being synchronized by the AD or NT driver, then click OK.

Tree 1 is updated with information necessary for the PasswordSync service to run. Continue with Installing a PasswordSync Agent for Tree 1.

## Installing a PasswordSync Agent for Tree 1

You need to install a PasswordSync Agent to direct password communication between Tree 1 and Active Directory or NT Domains.

### Prerequisites

The PasswordSync Agent should be installed on a computer running Windows 2000 or Windows NT4 SP6. This computer cannot already host an agent.

This computer does not need to be host eDirectory, but must have at least Novell Client 4.83 SP1 or later and connectivity to both the Active Directory or NT domains and the corporate tree between which passwords will be synchronized.

If you are synchronizing with a domain outside of the tree where the agent is installed, then the computer hosting the agent must be configured to use WINS or DNS.

### Installation

1. Log in to Tree 1 as Administrator or equivalent.
2. Log in to the domain as Administrator or equivalent.
3. At the Windows computer where the agent will be installed, insert the DirXML CD into the CD drive. The CD may take a moment to load.
4. At the Welcome screen, click Next.
5. Read the license agreement; if you agree to the terms, click I Accept.
6. At the Components page, mark PasswordSync Agent, then click Next. A summary screen is displayed.
7. Click Finish, then at notice of completion, click Close.
8. In Control Panel, click Password Synchronization.
9. Specify the tree name for Tree 1, then click Ok.
10. In the PasswordSync Setup dialog box, select a domain and its associated DirXML driver; in this case, the DirXML driver for eDirectory.

    If the domain is in another tree or forest, the computer on which the PasswordSync Agent is being installed must be configured with the address of a WINS server in the target tree or forest.

**NT Domains:** If you type the name of an NT 4 domain rather than browse to it, you must enter the name in uppercase. This requirement is for NT 4 domain names only; Active Directory domain names are not required to be uppercase.

**11** Click OK, then specify the name for the new PasswordSync object and the context where it should be placed.

The default object name is the name of the server where you are installing PasswordSync, followed by -pwdsync.

The default context is that of the container holding the DirXML Driver Set object.

**12** Select the container for which PasswordSync will be assigned as a trustee.

The PasswordSync Agent needs the rights to manage passwords in eDirectory and to read the DirXML drivers that control the domains being synchronized.

**IMPORTANT:** Select a container high enough in the tree to span all objects that the agent needs to access, including user objects, the domain object, the DirXML driver object, and the server object for the server hosting the DirXML engine.

If you want to make narrower rights assignments, make the following trustee assignments:

- For users participating in password synchronization:

| Trustee | Attribute | Rights |
|---|---|---|
| nadPwdSync object | Password Expiration Interval | compare, read |
| nadPwdSync object | Password Management | compare, read, write |
| nadPwdSync object | Password Expiration Time | write |
| [Public] | [Entry Rights] | browse |
| [Public] | nadLoginName | compare, read |

- For nadDomain objects:

| Trustee | Attribute | Rights |
|---|---|---|
| nadPwdSync object | Server | compare, read |
| [Public] | [Entry Rights] | browse |
| [Public] | nadPasswordSync | compare, read |

- For server objects holding the PwdSync index (by default, this is the server where DirXML is installed):

| Trustee | Attribute | Rights |
|---|---|---|
| nadPwdSync object | Index Definition | compare, read |
| nadPwdSync object | [Entry Rights] | browse |

**13** When prompted, click Yes to install a PasswordSync Filter. Select domain controllers from those listed, then click Add.

**IMPORTANT:** Even if Password Filters have been installed on the domain controllers when the PasswordSync Agent was installed in Tree 2, these Password Filters must be updated by the PasswordSync Agent servicing Tree 1 because configuration information is written to eDirectory during this process.

Because any domain controller can process a password change request, a filter must be installed on each Active Directory Domain Controller and each NT Primary Domain Controller. You should also install a filter on each NT Backup Domain Controller that could be promoted to a Primary Domain Controller.

If you have several domain controllers, we recommend that you install filters on a few controllers at a time. This will minimize the impact of rebooting many domain controllers at once and will expedite your initial installation. To install filters to domain controllers after initial installation, see Install a Password Filter (http://www.novell.com/documentation/lg/pwdsync10/passsync/data/ae8udjf.html#ae8udjf).

Remote domain controllers will be rebooted automatically when installation is complete. You must reboot the local domain controller manually after installation is complete.

**14** Click Yes, then click Close twice.

PasswordSync installation is complete.

**15** Check to see that your configuration is successful by completing the steps in "Validating Password Synchronization" on page 73.

## Validating Password Synchronization

After PasswordSync is set up, check to make sure that a password change in your eDirectory tree is synchronized to Active Directory and vise versa.

**1** Create an Active Directory or NT user.

**2** Verify that you can log in to eDirectory as that user.

**3** Change the user's eDirectory password.

For successful synchronization, eDirectory password changes must be made on a computer running the correct version of the Novell Client. For more information about required client versions, see "Prerequisites" on page 65. For more information about the role of the client in password synchronization, see "Sample Password Scenarios" on page 77.

**4** Verify that you can log in to Active Directory or NT as the new user.

You can view PasswordSync transactions in the PwdSync event log. The agent and filters log messages there.

To access the event log, choose Start > Settings > Control Panel > Administrative Tools > Event Viewer. For Windows 2000, the log is called PwdSync. For NT, messages are logged in the Application log with a source reference of PwdSync.

The following section lists common log messages:

| Message | Explanation |
|---|---|
| The password synchronization service has started.<br>The password synchronization service has stopped.<br>Loaded password provider %1 for directory %2.<br>Unloaded password provider %1 for directory %2. | Informational messages that occur when the agent is started or stopped. |
| The password for user %2 in directory %1 has been successfully changed by %3. | Informational message indicating that a password was successfully synchronized. |
| The password filter has been fully initialized. Domain Name = %2, Computer Name = %1, Host Name = %3. | Informational message indicating that the filter is fully operational for a given domain and domain controller. |
| The Cryptographic Service Provider has defaulted to %1. Encryption will be downgraded to the standards of this provider. Execution of the password synchronization server will not be affected. If higher encryption standards are required, please contact your network administrator. | Warning message reported at start up indicating that the cryptography being used by the agent isn't as strong as it could be. |
| The user %1 in directory %2 could not be mapped to a user in directory %3. The error code is in the data.<br>or<br>The password for user %1 in directory %2 was not synchronized because the password change timed out. | Warning message indicating that the agent could not map an NT or Active Directory user to the corresponding eDirectory user. This message will only occur for password changes originating in Active Directory or NT.<br>This is most likely to occur when the nadLoginName attribute isn't populated or the agent doesn't have proper rights to read the information necessary to perform the mapping.<br>The mapping for nadLoginName is found by searching against an index of the nadLoginName attribute held on an eDirectory server. The reference to the eDirectory server is held in the nadDomain object that represents the Active Directory or NT domain.<br>The agent may have been unable to find the eDirectory server holding the index. Ensure that<br>◆ The nadDomain object references the eDirectory server.<br>◆ The eDirectory server holds an index of the nadLoginName attribute.<br>◆ The PwdSync object has Browse, Compare, and Read rights to the nadDomain object and the server’s indexDefinition attribute.<br>The agent might have searched the index, but has been unable to find the nadLoginName attribute that matched the search criteria. Ensure that<br>◆ The eDirectory user object has a corresponding nadLoginName.<br>◆ The eDirectory user object exists in a replica on the server referenced by the nadDomain object. |

| Message | Explanation |
|---|---|
| The password synchronization service failed to load. The error code is in the data. | Error message indicating that the agent was not able to start.<br>The Novell Client might not have been able to find an eDirectory server holding a replica of the partition containing the PwdSync object.<br>Add the following information to the registry on the computer that is hosting the agent:<br>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PWDSYNC\Parameters<br>Value name: eDir Server IP Address<br>Value type: REG_SZ<br>Value data: *xxx.xxx.xxx.xx IP Address Here*<br>**WARNING:** If you use Registry Editor incorrectly, you might cause serious problems that might require you to reinstall your operating system. |
| A password change request was made by directory %1. No password provider exists for this directory. | Error message indicating that there is no provider available to service a password change request for a given directory and user.<br>The PasswordSync Agent uses providers to hold platform-specific information required for synchronization. Providers are represented by nadPwdProvider objects subordinate to the PwdSync objects. Typically, two nadPwdProvider objects should exist under the PwdSync object, one for the eDirectory tree and one for the Active Directory or NT domain.<br>If the eDirectory provider is missing, PasswordSync must be re-installed. If the Active Directory or NT provider is missing, it can be added through the Password Synchronization applet in the Control Panel on the computer where the agent is installed.<br>If both providers are present, ensure that the PwdSync object has Browse, Compare, Read, Write, and Add Self rights to the nadPwdProvider objects. |
| The password for user %1 in directory %2 could not be decrypted. The error code is in the data. | Error message indicating that password data could not be decrypted.<br>This most likely indicates an encryption level mismatch. Ensure that Service Pack levels match across domains participating in password synchronization. |

## Synchronizing Passwords for Existing Accounts

Existing user accounts are synchronized when the DirXML driver reports a change in an application. Using iManager, you can force DirXML to resynchronize data on all accounts at once. Doing so allows users to begin participating in password synchronization as soon as they make their next password change.

**IMPORTANT:** If you have a large number of objects to synchronize (typically greater than 1000), you might need to adjust some policy settings for Active Directory. For more information, see Migrating A Large Number of Objects (http://www.novell.com/documentation/lg/dirxmldrivers/ad/data/agdyl3s.html#alf3ioz) in the *DirXML Driver for Active Directory Implementation Guide*.

1. Launch iManager by going to http://*serveripaddress*/nps/iManager.html.

   **IMPORTANT:** This URL is case sensitive.

2. Authenticate to the tree on which you just installed password synchronization, then click DirXML Management > Overview.
3. Locate the DirXML driver that you just updated, then click Migrate from eDirectory.

   You can check the success of the migration by verifying that a migrated user object now has the nadLoginName attribute.

Individual passwords will be synchronized as soon as a user makes a password change in NT, Active Directory, or eDirectory.

# Setting Passwords for New Accounts

You have several options for setting an initial password for a new account. Setting a password happens early in the account creation process, and PasswordSync will respond to new passwords differently depending upon where and how you set the initial password.

## Setting Passwords with DirXML

DirXML allows you to generate an initial password for an account based on the account's attributes or other information available through Java* services. For instance, you can generate a password based on a user's Surname plus a four-digit number. Generating an initial password requires driver customization, but is a good way to manage passwords.

If you choose to set the initial password through a DirXML customized style sheet, you should also ensure that the user will be prompted to change the initial password upon login. After the initial password is changed, passwords will be synchronized.

## Setting Passwords with ConsoleOne or iManager

ConsoleOne and iManager let you set an initial password when creating a user account. In this case, the password is set before an account is associated in NT or Active Directory, thus preventing the initial password from being synchronized. Passwords will be synchronized only after the first password change.

To avoid this delay, you have several alternatives:

- Do not assign an initial password during user creation and assign the password later. A brief delay will allow account associations to be completed.
- Select Prompt User on First Login so that setting a password is delayed until the account is actually used.
- Go ahead and set the password during account creation, but inform users that passwords will not be synchronized until the eDirectory password is changed using the Novell Client.

### Setting Passwords with Microsoft Management Console

Microsoft Management Console (MMC) lets you set an initial password on a user account simply by typing the password at account creation. The password is set before PasswordSync is able to associate an eDirectory account with the NT or Active Directory account, so the PasswordSync service is not able to update the eDirectory account immediately. However, the service will retry the password update and the account will be properly updated within several minutes.

## Maintaining Password Synchronization

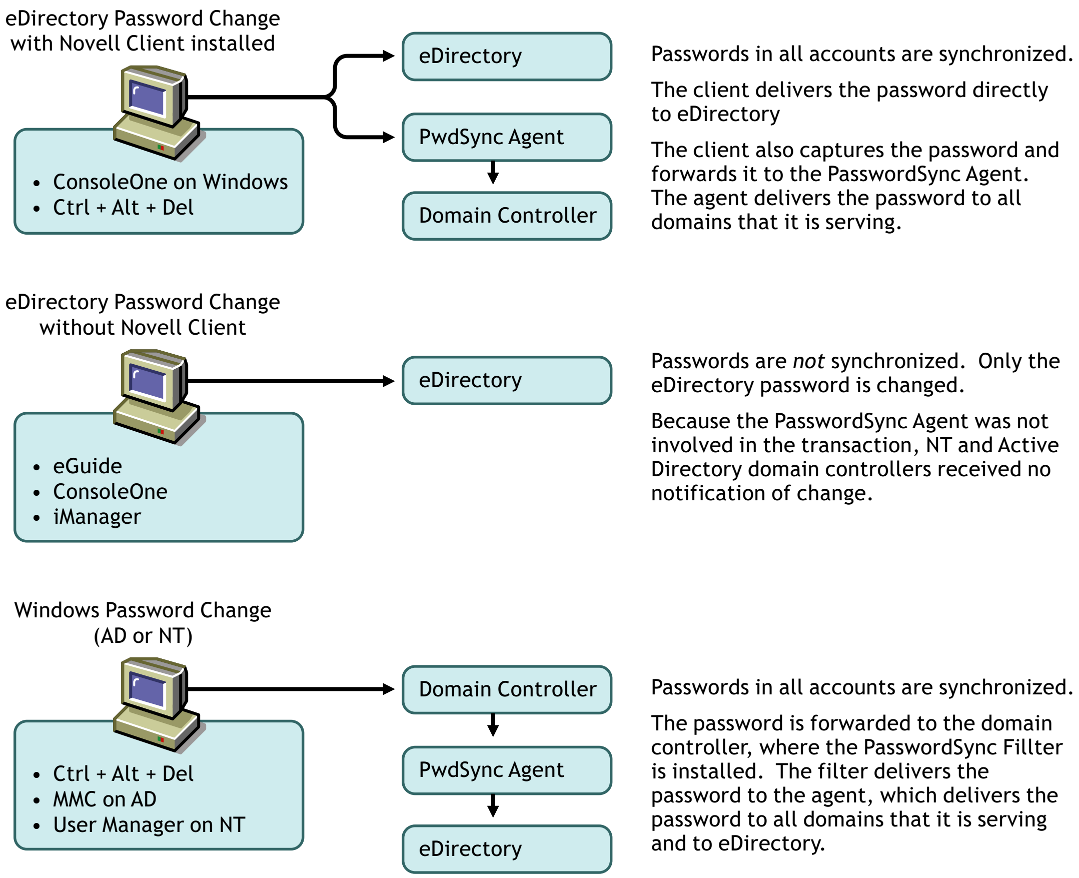
To keep passwords synchronized when your network changes, you might need to make changes to your PasswordSync configuration. For example, if you add a domain controller, you must install a PasswordSync Filter on that domain controller.

For more maintenance and configuration information, refer to Configuring and Maintaining PasswordSync (http://www.novell.com/documentation/lg/pwdsync10/passsync/data/ae8b8m9.html).

## Sample Password Scenarios

Passwords can be changed in any number of places. The following graphic outlines several password change scenarios:

**Figure 18 Password Change Scenarios**



Passwords in all accounts are synchronized.

The client delivers the password directly to eDirectory

The client also captures the password and forwards it to the PasswordSync Agent. The agent delivers the password to all domains that it is serving.

Passwords are *not* synchronized. Only the eDirectory password is changed.

Because the PasswordSync Agent was not involved in the transaction, NT and Active Directory domain controllers received no notification of change.

Passwords in all accounts are synchronized.

The password is forwarded to the domain controller, where the PasswordSync Fillter is installed. The filter delivers the password to the agent, which delivers the password to all domains that it is serving and to eDirectory.

# Uninstalling Password Synchronization

You can uninstall any of the following PasswordSync components:

- "Uninstalling a PasswordSync Filter" on page 78
- "Uninstalling a PasswordSync Agent" on page 78

## Uninstalling a PasswordSync Filter

Uninstalling a filter from a domain controller removes the association between the domain controller and a PasswordSync Agent. If the domain controller is associated with *only one* PasswordSync Agent and you remove the filter, then the domain controller must be rebooted to complete the process.

**NOTE:** Remote domain controllers will be rebooted automatically; a local domain controller must be rebooted manually.

1. On the Windows task bar, click Start > Settings > Control Panel.
2. Click Password Synchronization.
3. Select a domain.
4. Click Filters.
5. Select a domain controller > click Remove.

   **NOTE:** If you disassociate the domain controller from all agents, password changes in this domain will not be synchronized.

6. Click Close.

## Uninstalling a PasswordSync Agent

1. Log in to the local workstation as Administrator or equivalent and log in to eDirectory as Administrator.
2. From Control Panel > Add/Remove Programs, select Novell DirXML Password Synchronization for Windows NT/2000.
3. Click Change/Remove.
4. From the InstallShield Wizard's Welcome dialog box, select Remove and click Next.
5. In the PasswordSync dialog box, select all domains listed and click Remove > Close.

# A Activating Novell DirXML Products

The following information explains how activation works for products based on DirXML®. To activate your products you must:

- Generate a Product Activation Request
- Submit the Product Activation Request
- Install the Product Activation Credential received from Novell

DirXML and DirXML drivers must be activated within 90 days of installation, otherwise they will shut down. At any time during the 90 days, or afterward, you can choose to activate DirXML products.

If you are installing a DirXML product on multiple trees, as would be the case if you use the DirXML driver for eDirectory, you must install a unique Product Activation Credential on each tree. You use the same license to get both Product Activation Credentials.

**NOTE:** Activating a driver does not change your current configuration or install a newer version of the driver shim. It simply changes the driver to an activated state.

Activation procedures are the same regardless of the DirXML products you purchase. The following examples describe various activation scenarios you might encounter:

- You get a license for the DirXML Starter Pack with your purchase of NNLS. This license entitles you to activate the DirXML engine and the drivers for Novell® eDirectory™, Active Directory, and NT Domain, as well as Password Synchronization.
- You purchase a license for an individual driver, as would be the case if you decided to use one of the DirXML drivers not included as part of the DirXML Starter Pack, for example, the JDBC* driver. This license entitles you to activate the purchased driver and the DirXML engine.
- You purchase a license to use a non-Novell driver. This license entitles you to activate the customized or third-party driver and the DirXML engine.

After you complete the activation procedures, you can view your current DirXML activations through Novell iManager. For more information, refer to "Viewing Product Activations for DirXML and DirXML Drivers" on page 84.

For more information about activation, refer to Activation Basics (http://www.novell.com/partners/partnerplace/epd/product_activation_basics.html) and Activation Troubleshooting (http://www.novell.com/partners/partnerplace/epd/troubleshooting_activation.html).

# Generating a Product Activation Request

You will use your Customer ID to generate a Product Activation Request. When you purchase your DirXML product, Novell will send an e-mail to your company's primary contact (the person who purchased the product license) that includes a customer ID.

Novell Nterprise Linux Service customers will receive their customer ID as outlined in the following table:

| If | Then |
|---|---|
| You purchased a new license or upgraded an existing license directly from Novell or through a Novell license program such as an MLA license | Novell will e-mail your customer ID to your company's primary contact. |
| You do not have any licensing agreement with Novell and you purchased the physical product from a distributor or retailer | The customer ID is on a printed card inside the product package. |

If you do not remember or do not receive your Customer ID, please call the Novell Activation Center at 1-800-418-8373 in the U.S. In all other locations, call 1-801-861-8373. (If applicable, you will be charged long distance fees for calls made using the 801 area code.)

**NOTE:** The individual who purchases the product license will receive an e-mail containing the Customer ID. If your company uses its purchasing agent to handle this transaction, you might need to check with this individual to obtain your Customer ID.

You should create a Driver Set object before you generate a Product Activation Request to activate DirXML.

**1** Launch iManager by going to http://*serveripaddress*/nps/iManager.html.

**2** Click DirXML Management > Activation Request.

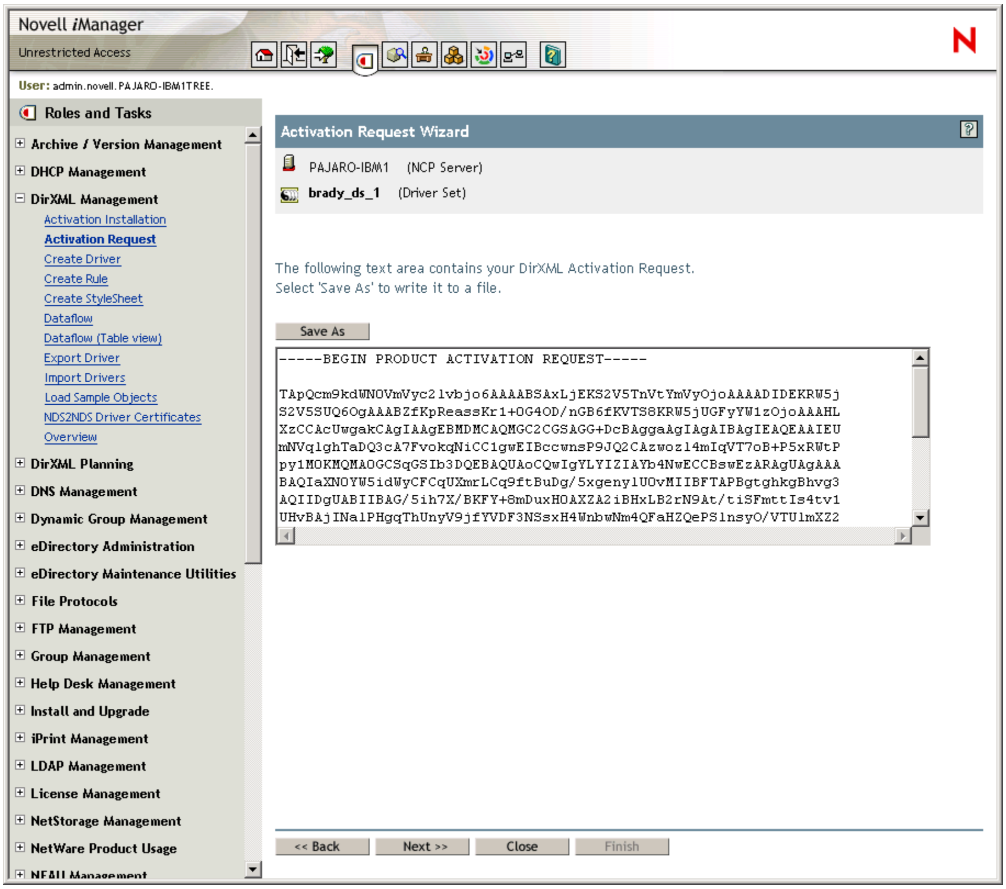
**3** Browse to the driver set that you want to activate > click Next.

**NOTE:** If the driver set is not associated with a server or is associated with multiple servers, you will be prompted to select a server to associate with a driver set.

**4** Enter your Novell Customer ID, then click Next to build your Activation Request file.

Your customer ID and identifying information about the server's tree are stored in the Product Activation Request.

**Figure 19 Activation Request**



PAJARO-IBM1 (NCP Server)

brady_ds_1 (Driver Set)

The following text area contains your DirXML Activation Request.
Select 'Save As' to write it to a file.

```
-----BEGIN PRODUCT ACTIVATION REQUEST-----

TApQcm9kdWNOVmVyc2lvbjo6AAAABSAxLjEKS2V5TnVtYmVyOjoAAAADIDEKRW5j
S2V5SUQ6OgAAABZfKpReassKr1+OG4OD/nGB6fKVTS8KRW5jUGFyYW1zOjoAAAHL
XzCCAcUwgakCAgIAAgEBMDMCAQMGC2CGSAGG+DcBAggaAgIAgAIBAgIEAQEAAIEU
mNVqlghTaDQ3cA7FvokqNiCC1gwEIBccwnsP9JQ2CAzwozl4mIqVT7oB+P5xRWtP
py1MOKMQMAOGCSqGSIb3DQEBAQUAoCQwIgYLYIZIAYb4NwECCBswEzARAgUAgAAA
BAQIaXNOYW5idWyCFCqUXmrLCq9ftBuDg/5xgenylUOvMIIBFTAPBgtghkgBhvg3
AQIIDgUABIIBAG/5ih7X/BKFY+8mDuxHOAXZA2iBHxLB2rN9At/tiSFmttIs4tv1
UHvBAjINalPHgqThUnyV9jfYVDF3NSsxH4WnbwNm4QFaHZQePSlnsyO/VTUlmXZ2
```

5. Copy the Product Activation Request that is in the text area to the clipboard or save the request directly to a file, then click Next.

   You will need this information later at the Novell Product Activation Web site.

   **IMPORTANT:** Do not edit the content of the Product Activation Request.

6. Click the hyperlink to launch the Novell Product Activation Web site (http://www.novell.com/products/activation).

   or

   Click Finish to return to the main menu of iManager.

**NOTE:** To continue the activation process, you need to submit this Product Activation Request to Novell at the Novell Product Activation Web site (http://www.novell.com/products/activation). For information, see "Submitting a Product Activation Request" on page 81.

## Submitting a Product Activation Request

After you create a Product Activation Request, you submit it to Novell through the Novell Product Activation Web site (http://www.novell.com/products/activation). Novell will then send an e-mail containing a Product Activation Credential. Use this credential to activate the driver.

1. Go the Product Activation Web site (http://www.novell.com/products/activation) site, then click DirXML 1.1x and drivers.

**2** Follow through the introductory screens, then when prompted, log in to your MyNovell account.

You must have a MyNovell account to access the Product Activation Web site. If you don't already have an account, you can create this free account when you visit the Product Activation site.

**3** Click Browse to specify the path to the Product Activation Request file or paste the text of the Product Activation Request into the text area.

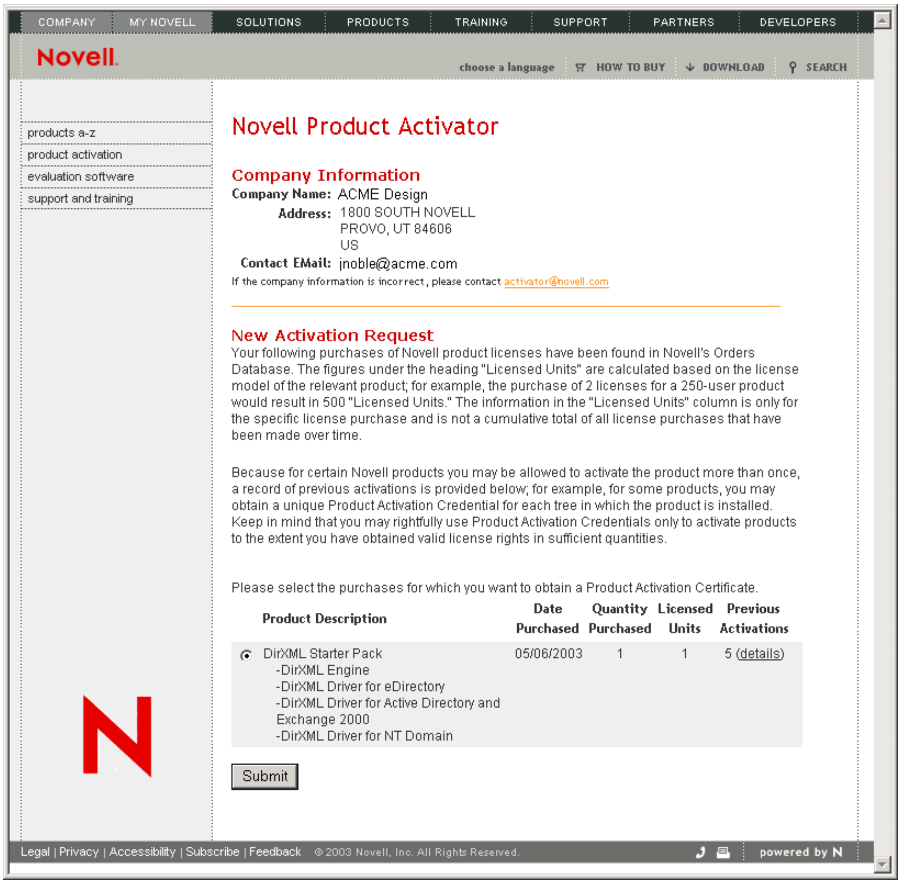
If you copied the Product Activation Request to a diskette, make sure you have the request available on the computer you are working on.

**IMPORTANT:** Do not edit the content of the Product Activation Request.

**4** Click Submit.

Your product purchases available for activation are displayed.

**Figure 20 Products Available for Activation**



Novell Product Activator

Company Information

**Company Name:** ACME Design
**Address:** 1800 SOUTH NOVELL
PROVO, UT 84606
US
**Contact EMail:** jnoble@acme.com

If the company information is incorrect, please contact activator@novell.com

New Activation Request

Your following purchases of Novell product licenses have been found in Novell's Orders Database. The figures under the heading "Licensed Units" are calculated based on the license model of the relevant product; for example, the purchase of 2 licenses for a 250-user product would result in 500 "Licensed Units." The information in the "Licensed Units" column is only for the specific license purchase and is not a cumulative total of all license purchases that have been made over time.

Because for certain Novell products you may be allowed to activate the product more than once, a record of previous activations is provided below; for example, for some products, you may obtain a unique Product Activation Credential for each tree in which the product is installed. Keep in mind that you may rightfully use Product Activation Credentials only to activate products to the extent you have obtained valid license rights in sufficient quantities.

Please select the purchases for which you want to obtain a Product Activation Certificate.

| | Product Description | Date Purchased | Quantity Purchased | Licensed Units | Previous Activations |
|---|---|---|---|---|---|
| ● | DirXML Starter Pack<br>-DirXML Engine<br>-DirXML Driver for eDirectory<br>-DirXML Driver for Active Directory and Exchange 2000<br>-DirXML Driver for NT Domain | 05/06/2003 | 1 | 1 | 5 (details) |

Submit

**5** Mark the product purchase you are activating.

You can activate only one purchase at a time. Mark the purchase you are currently activating. If you need to activate any of the other products listed and they will be used in the same tree, submit the Product Activation Request again. If they will be used in a different tree, you must create a new Product Activation Request and submit that request to obtain a credential.

**6** Click Submit.

Novell Nterprise Linux Service customers might also be prompted to enter the product serial number located on the Novell Nterprise Linux Service license diskette.

Novell generates a Product Activation Credential based on the Product Activation Request you submitted and sends that credential to you via e-mail. A copy of the credential will be sent to the primary contact as well.

**NOTE:** Some companies limit the list of employees authorized to receive credentials. You might not have rights to use the customer ID. In this case, after you click Submit, a notification is sent to the primary contact. The primary contact must approve your usage of the customer ID before you will receive the credential by e-mail.

## Installing a Product Activation Credential

You should install the Product Activation Credential via iManager. The following procedures explain how to install the Product Activation Credential.

1. Open the Novell e-mail that contains the Product Activation Credential.
2. Do one of these steps:
   - Save the Product Activation Credential file.

     or

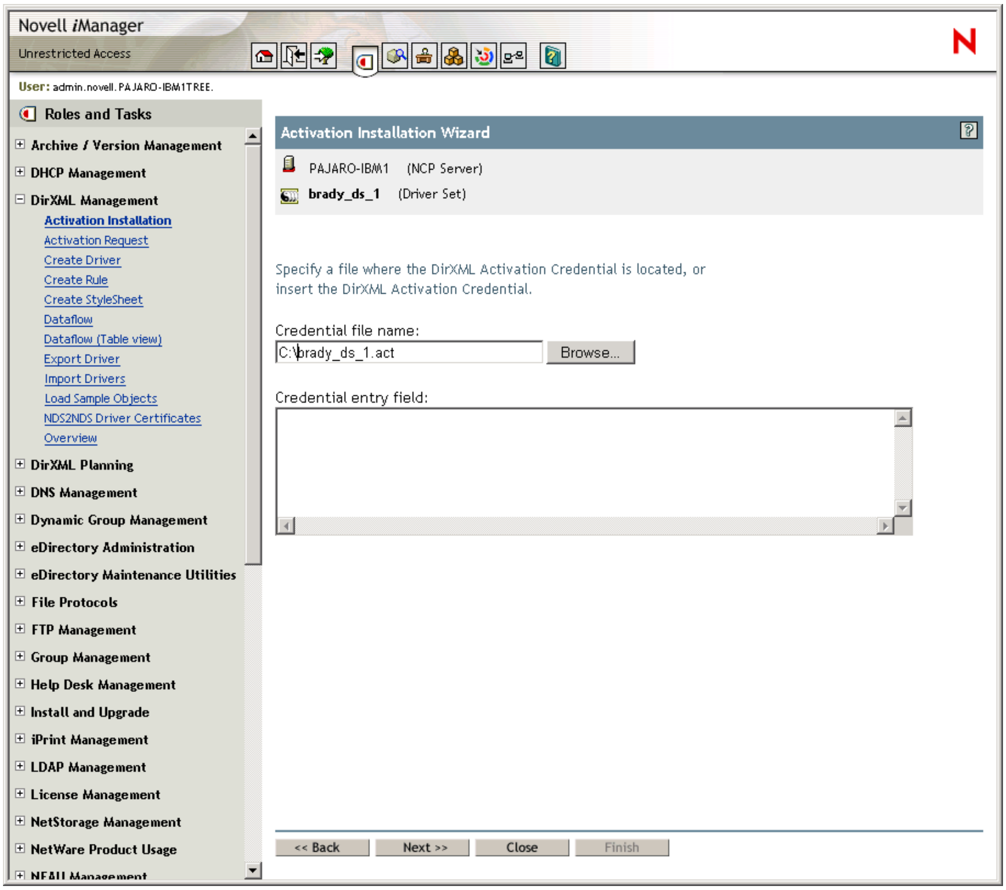
   - Open the Product Activation Credential file > copy the contents of the Product Activation Credential to your clipboard.

     **IMPORTANT:** Do not edit the contents of the Product Activation Credential.
3. Open iManager.
4. Choose DirXML Management > Activation Installation.
5. Select the driver set or browse to a driver set > click Next.

   **IMPORTANT:** Make sure you choose a driver set that is in the same tree that the Product Activation Request was created from initially.
6. If the driver set is not associated with a server or is associated with multiple servers, select a server to associate with a driver set > click Next.

   The installation dialog box appears:

**Figure 21 Installation Dialog Box**



User: admin.novell.PAJARO-IBM1TREE.

PAJARO-IBM1 (NCP Server)

brady_ds_1 (Driver Set)

Specify a file where the DirXML Activation Credential is located, or insert the DirXML Activation Credential.

Credential file name: C:\brady_ds_1.act

Credential entry field:

**7** Do one of these steps:

- Specify where you saved the DirXML Activation Credential > click Next.

  or

- Paste the contents of the DirXML Activation Credential into the text area > click Next.

**8** Click Finish.

**NOTE:** You need to activate each driver set that has a driver. You can use the same Product Activation Credential to activate other driver sets as long as the driver sets are in the same tree. A Product Activation Credential can only be used in the tree from which the Product Activation Request was created.

# Viewing Product Activations for DirXML and DirXML Drivers

For each of your DirXML driver sets, you can see the Product Activation Credentials you have installed for the DirXML Engine and drivers. To view Product Activation Credentials:

**1** Open iManager.

**2** Click eDirectory Administration > Modify Object.

**3** Enter the driver set or the driver you want to view activation information for in the object name field.

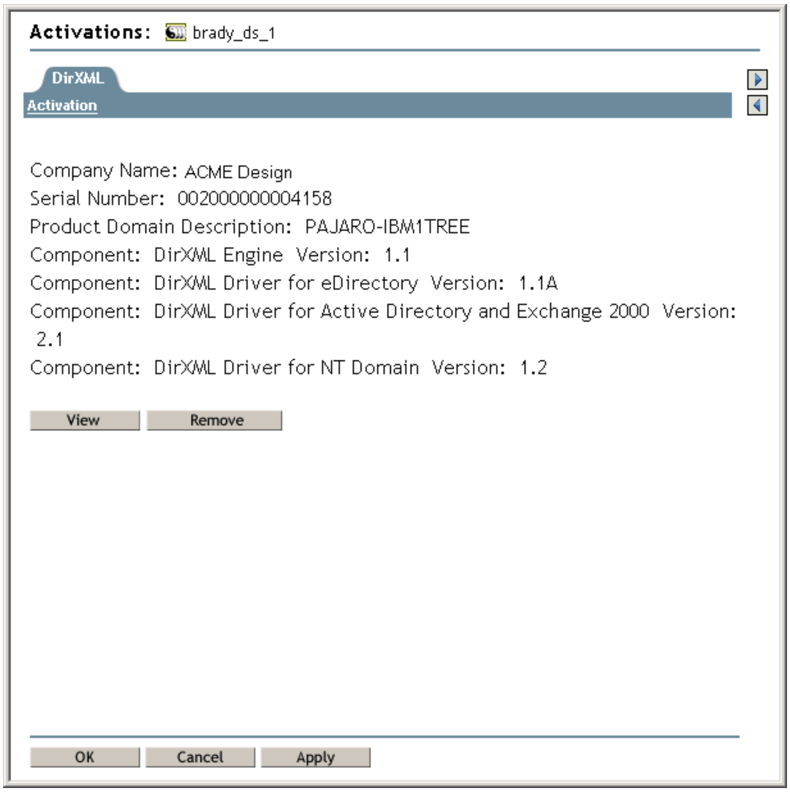
or

Browse to the driver set or the driver you want to view activation information on.

**4** From the DirXML tab, select Activation.

DirXML and DirXML Driver activation credentials display on this page.

**Figure 22 Activation Credentials**



Activations: brady_ds_1

Company Name: ACME Design
Serial Number: 002000000004158
Product Domain Description: PAJARO-IBM1TREE
Component: DirXML Engine Version: 1.1
Component: DirXML Driver for eDirectory Version: 1.1A
Component: DirXML Driver for Active Directory and Exchange 2000 Version: 2.1
Component: DirXML Driver for NT Domain Version: 1.2

You can view the text of the activation credential or, if an error is reported, you can remove an activation credential.

**NOTE:** After installing a valid Product Activation Credential for a driver set, you might still see “Activation Required” next to the driver name. If this is the case, restart the driver and the message should then disappear.