Novell DirXML® Starter Pack

www.novell.com

DEPLOYMENT GUIDE

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. Patents Pending.

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

www.novell.com

Deployment Guide
April 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

ConsoleOne is a registered trademark of Novell, Inc. in the United States or other countries.
eDirectory is a trademark of Novell, Inc.
DirXML is a registered trademark of Novell, Inc. in the United States and other countries.
NetWare is a registered trademark of Novell, Inc., in the United States and other countries.
Novell is a registered trademark of Novell, Inc., in the United States and other countries.
Novell Certificate Server is a trademark of Novell, Inc.
Novell Client is a trademark of Novell, Inc.

Third-Party Trademarks

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

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 NetWare® 6.5 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 rules 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 bundle's architecture and default data flow.

- Chapter 2, "Planning Your Installation," on page 19

  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 21

  The DirXML engine and Novell iManager plug-ins for DirXML are the foundation for any DirXML installation. This section explains how to install these key components.

- Chapter 4, "Setting Up Participating Systems," on page 25

  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 53

  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 69

  Novell 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 this Deployment Guide, see the NetWare 6.5 Documentation Web Site (http://www.novell.com/documentation/beta/nw65/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 NetWare® 6.5 provides licensed synchronization of information held in NT Domains, Active Directory, and eDirectory. When data from one system changes, DirXML detects and propagates these changes to other connected systems based on the business rules 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 need to manage passwords in only one place.

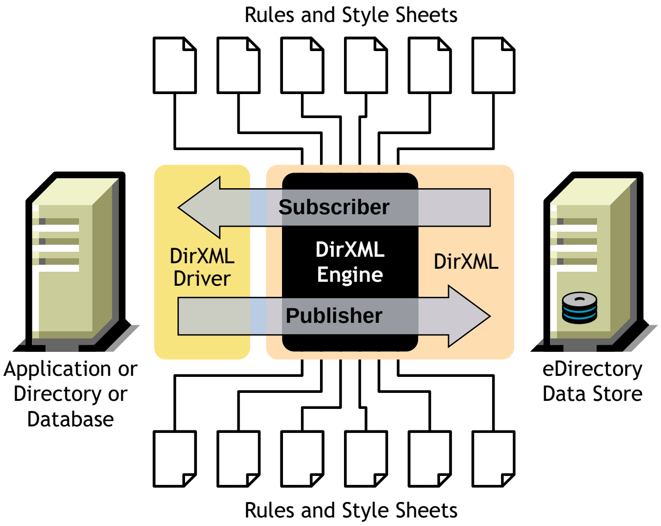
This section contains information on the DirXML data sharing model, and the data flow and object placement between eDirectory and other applications:

- "The DirXML Data Sharing Model" on page 9
- "Default Data Flow and Object Placement" on page 13

The DirXML Data Sharing Model

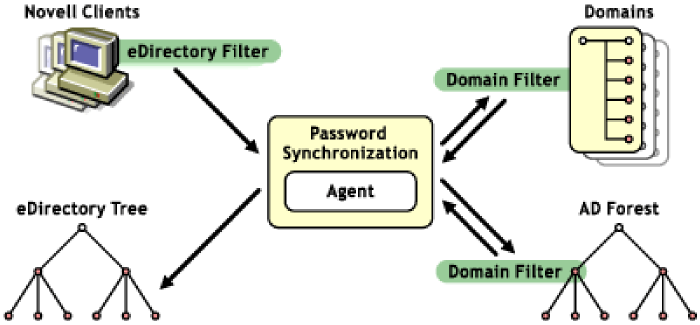
In simplest terms, DirXML delivers application-specific drivers and a data transformation engine to communicate data changes between applications and eDirectory. DirXML drivers take their direction for what data to manage and how to manage it from DirXML rules and style sheets. You customize these rules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

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 an eDirectory event into an XML document and uses rules to determine how the modification is sent to the application. It ensures consistent processing methods for disparate data.

DirXML Driver for Active Directory

This driver runs on a Windows* workstation or server and is designed to synchronize data between Active Directory and eDirectory. It comes with a configuration file to help you set up initial data processing rules and driver behavior.

DirXML Driver for NT Domain

This driver runs on a Windows workstation or server and is designed to synchronized data between an NT 4 domain and eDirectory. It comes with a configuration file to help you set up initial data processing rules and driver behavior.

DirXML Driver for eDirectory

This driver runs on an eDirectory server (a NetWare 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.

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 can be pushed to the application, and the *Publisher* filter, which determines the objects and attributes that can be 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 password change notification to PasswordSync Agents. These filters run on domain controllers (and as part of the Novell Client™). Each domain participating in password synchronization must have a filter installed on the domain controller.

The PasswordSync Agent is a service that runs on a Windows computer. It communicates password change notifications sent by the filters to participating systems. You can install agents on several workstations to improve performance when network topology issues arise and to provide redundancy for fault tolerance.

DirXML Objects in eDirectory

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

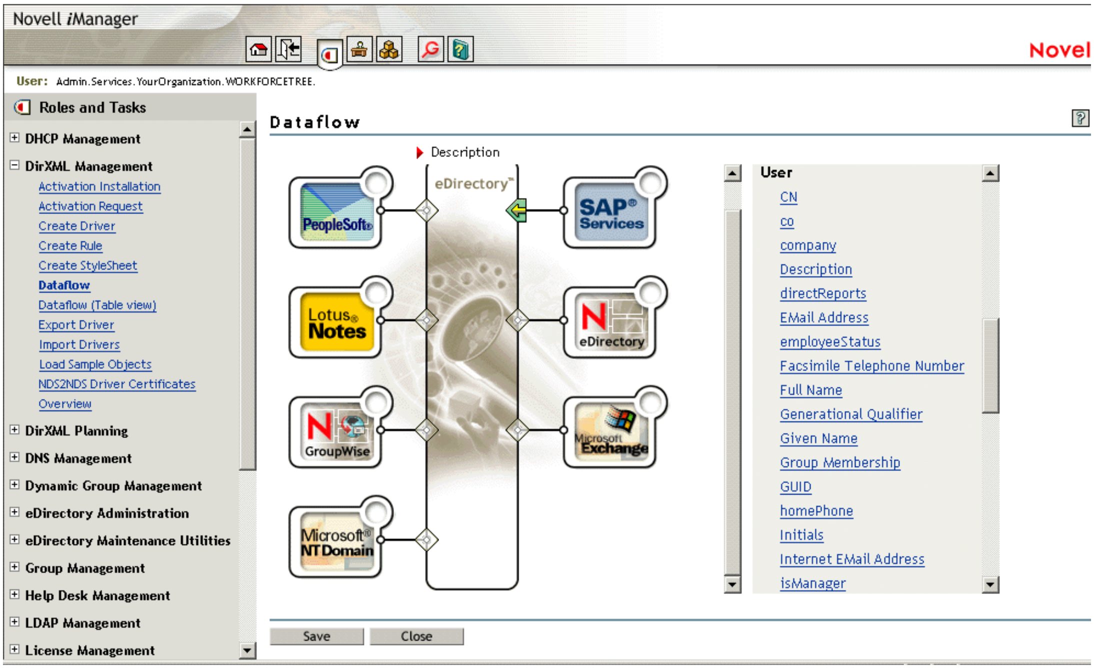
Table 1 DirXML Objects in eDirectory

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: ◆ Matching Rule: Specifies what constitutes a match when objects already exist in both eDirectory and the target application ◆ Creation Rule: Determines the requirements for object creation ◆ Placement Rule: determines object placement ◆ Schema Mapping Rule: Establishes the mapping between objects and attributes in the target application and those in eDirectory 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 is 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



NOTE: The initial release of iManager 2.0 runs only on NetWare 6.5. 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).

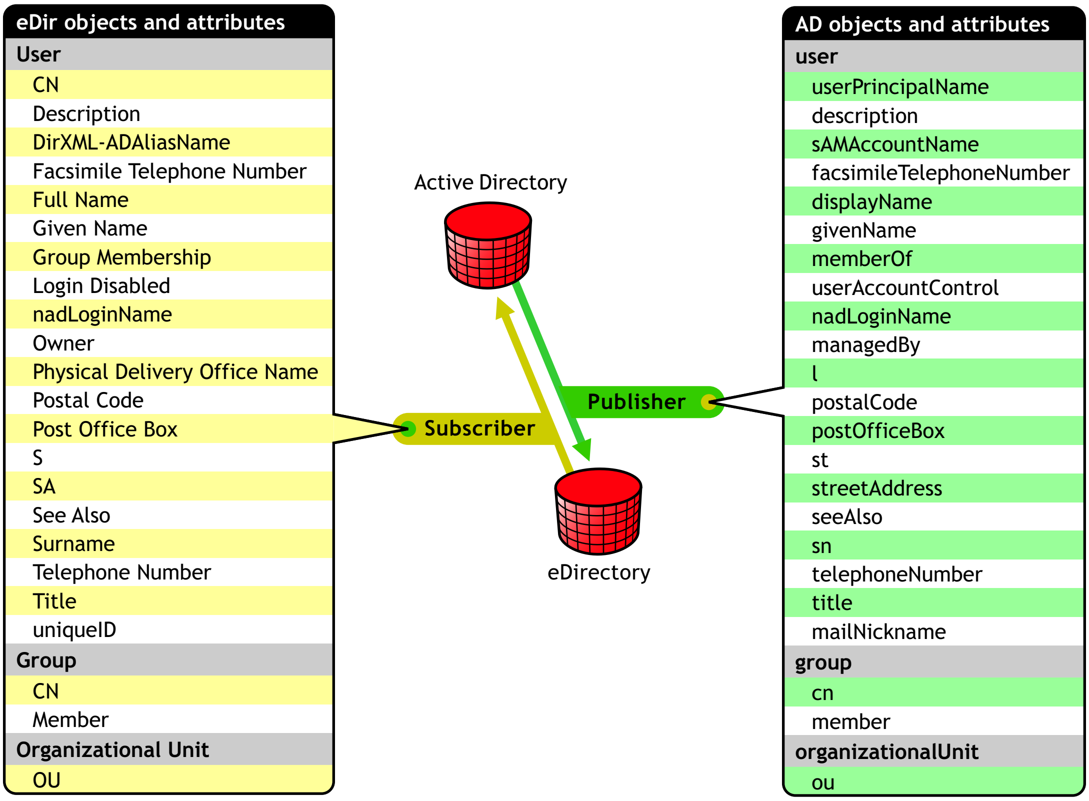
Default Data Flow and Object Placement

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



eDir objects and attributes

User
- CN
- Description
- DirXML-ADAliasName
- Facsimile Telephone Number
- Full Name
- Given Name
- Group Membership
- Login Disabled
- nadLoginName
- Owner
- Physical Delivery Office Name
- Postal Code
- Post Office Box
- S
- SA
- See Also
- Surname
- Telephone Number
- Title
- uniqueID

Group
- CN
- Member

Organizational Unit
- OU

AD objects and attributes

user
- userPrincipalName
- description
- sAMAccountName
- facsimileTelephoneNumber
- displayName
- givenName
- memberOf
- userAccountControl
- nadLoginName
- managedBy
- l
- postalCode
- postOfficeBox
- st
- streetAddress
- seeAlso
- sn
- telephoneNumber
- title
- mailNickname

group
- cn
- member

organizationalUnit
- ou

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

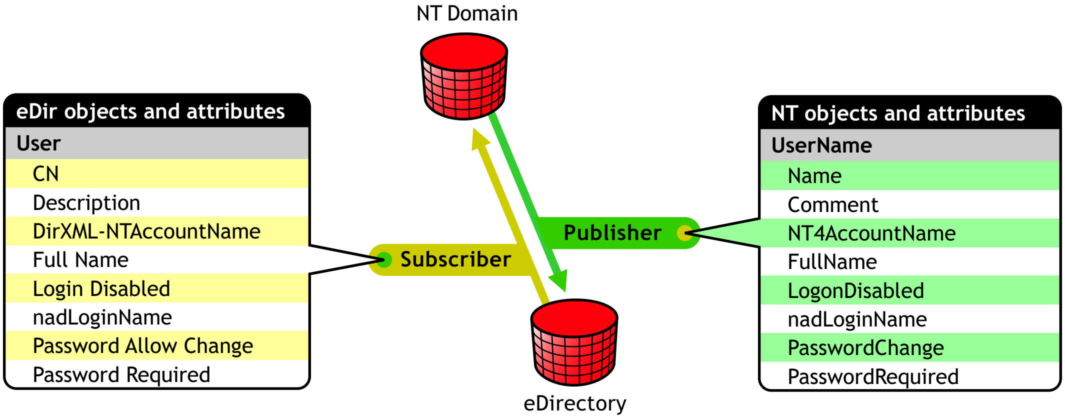
Mirrored: You specify a base container in the target directory, then the hierarchy from the source directory is mirrored inside the base container of the target directory. The structure of the synchronized object's source DN will be reflected inside the base container in the target directory.

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.

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

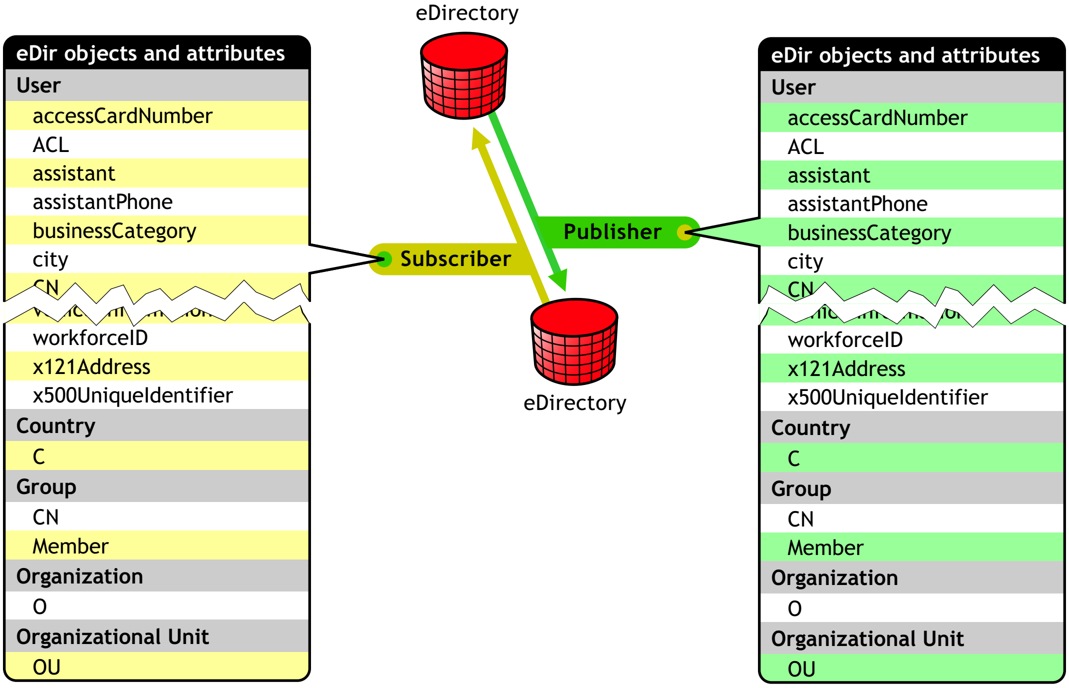


NT Domain object data is stored in a flat database. eDirectory object data is stored in a hierarchical tree structure. The default configuration for NT specifies that new objects created in NT Domain and synchronized to eDirectory are placed in a single container that you specify during driver configuration. 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



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.

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.

- The driver for Active Directory checks to see if John already has an eDirectory account. Because John is new, he does not have an account.
- The driver 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.

  The driver 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.

- The driver for Active Directory is notified that John's user object has been modified.
- The driver 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 partner company. The eDirectory administrator disables John’s eDirectory account.

- The driver for Active Directory is notified of the change and deletes John’s Active Directory account.

2 Planning Your Installation

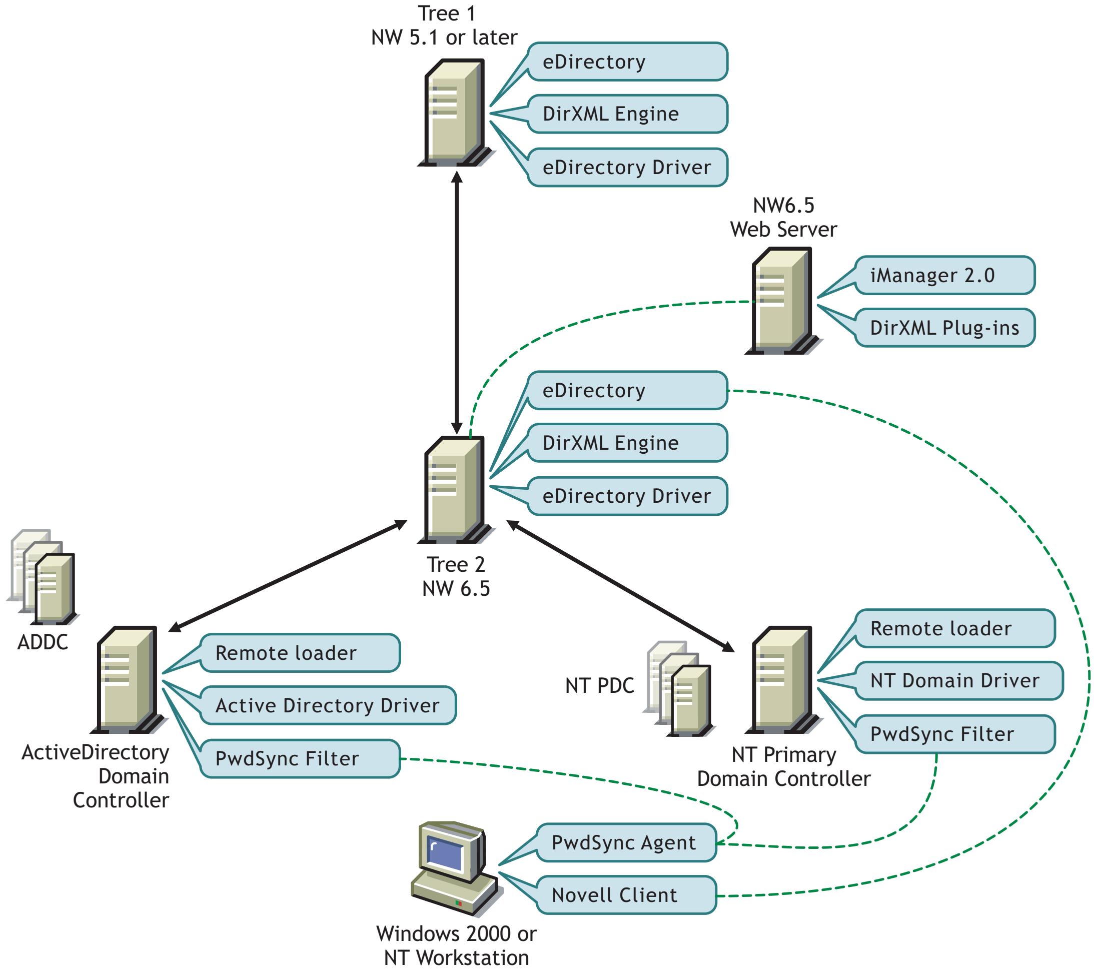
This section includes the following planning topics:

- "Where to Install" on page 19
-

Where to Install

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 are being synchronized in this scenario, the engine and the eDirectory driver are installed on two separate 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 NetWare server that is hosting the DirXML engine, for performance reasons you may want to install iManager on a separate server. The configuration described in this document assumes separate servers.
- **DirXML driver for Active Directory and Remote Loader**: The Active Directory driver must run on a Windows 2000 computer. 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 document, we've installed the driver and Remote Loader on the Active Directory domain controller. The driver doesn't have 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 must run on an NT domain computer. 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 document, we've installed the driver and the Remote Loader on the Primary Domain Controller (PDC). The driver doesn't need to be installed on the domain controller. 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 document doesn't describe installing the drivers for multiple domains. However, you can just 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.

3 Installing the Novell DirXML Starter Pack

This section explains how to install the DirXML® engine and iManager plug-ins for DirXML. These components must be installed on NetWare 6.5 servers.

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

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

- NetWare eDirectory Server: DirXML engine, DirXML drivers, ConsoleOne® snap-ins, and driver configuration files
- NetWare 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 19.

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

- "Installing DirXML" on page 21
- "Setting Up iManager" on page 22

Installing DirXML

Prerequisites

❑ NetWare 6.5

The DirXML engine must be installed on a NetWare 6.5 server that holds a replica of the data you will be synchronizing.

Installing the DirXML Engine

1. At the NetWare 6.5 server, insert the DirXML CD into the CD drive. At the system console, enter **`CDROM`**.
2. From the GUI server console, click Novell > Install > Add.

   If the GUI server console isn't running, launch it by entering **STARTX** at the console.
3. In the Path to Install From field, browse to nw\product.ni on the DirXML CD, then click OK twice.
4. In the DirXML Product Installation page, click Next.
5. Read the license agreement; if you agree to the terms, click I Accept.

6. On the Components page, mark DirXML Engine and Drivers, then click Next.
7. On the Schema Extension page, enter the following information, then click Next:
   - **User Name:** Enter the context of a user who has rights to extend the schema, for example, admin.hq
   - **User Password:** Enter the password for the admin or equivalent user you specified.
8. If you will be synchronizing data between this eDirectory tree and another tree, select the DirXML Driver 1.1a for eDirectory; otherwise, leave all the items unmarked. Click Next.

   NOTE: This screen lists all DirXML drivers. Drivers that aren't licensed in this bundle, but that can run on NetWare, are labeled Evaluation. Evaluation drivers require a separate purchase and activation within 90 days of their installation. (If you test the Evaluation drivers and choose not to activate them, you must undo any changes you made using these drivers.)
9. Read the Summary page, then click Finish.

   The file copy might take a few minutes.
10. After the Installation Complete dialog box is displayed, click Close.
11. Continue with the next section, "Setting Up iManager" on page 22.

Setting Up iManager

Prerequisites

❑ Novell iManager 2.0

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

See <xref to iManager manual>.

Installing the iManager Plug-Ins for DirXML

1. At the NetWare 6.5 server where iManager is installed, insert the DirXML CD into the CD drive. The CD may take a moment to load. Then, at the system console, enter **`CDROM`**.
2. From the GUI server console, click Novell > Install > Add.

   If the GUI server console isn't running, launch it by entering **`STARTX`** at the console.
3. In the Path to Install From field, browse to nw\product.ni on the DirXML CD, then click OK twice.
4. On the DirXML Product Installation page, click Next.
5. Read the license agreement; if you agree to the terms, click I Accept.
6. On the Components page, mark the following items, then click Next.
   - DirXML Preconfigured Drivers
   - Novell iManager Plug-ins for DirXML

   Plug-ins and preconfigured drivers are copied to the Tomcat directory for use during iManager and driver configuration.

7 On the Schema Extension page, enter the following information, then click Next:

- **User Name:** Enter the context of a user who has rights to extend the schema, for example, admin.hq
- **User Password:** Enter the password for the admin or equivalent user you specified.

8 Select the preconfigured driver files for the drivers you will be using, then click Next.

9 Read the Summary page, then click Finish.

The file copy might take a few minutes.

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

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

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

12 Restart your Web services using the following sequence:

12a To stop Tomcat, type **`tc4stop`**, then press Enter.

12b To restart Tomcat, type **`tomcat4`**, then press Enter.

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

IMPORTANT: This URL is case sensitive.

14 Verify that the DirXML Management and DirXML Planning tasks are available.

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 25
- "Setting Up eDirectory" on page 36
- "Setting Up NT Domain" on page 42
- "Configuring the DirXML Drivers" on page 49

After setting up participating systems, you need to set up and configure password synchronization as explained in Chapter 5, "Setting Up Password Synchronization," on page 53.

Setting Up Active Directory

For the default NetWare 6.5 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 25
- "Collecting Configuration Information" on page 26
- "Creating an Admin User" on page 33
- "Installing and Configuring the Remote Loader and Driver" on page 34

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

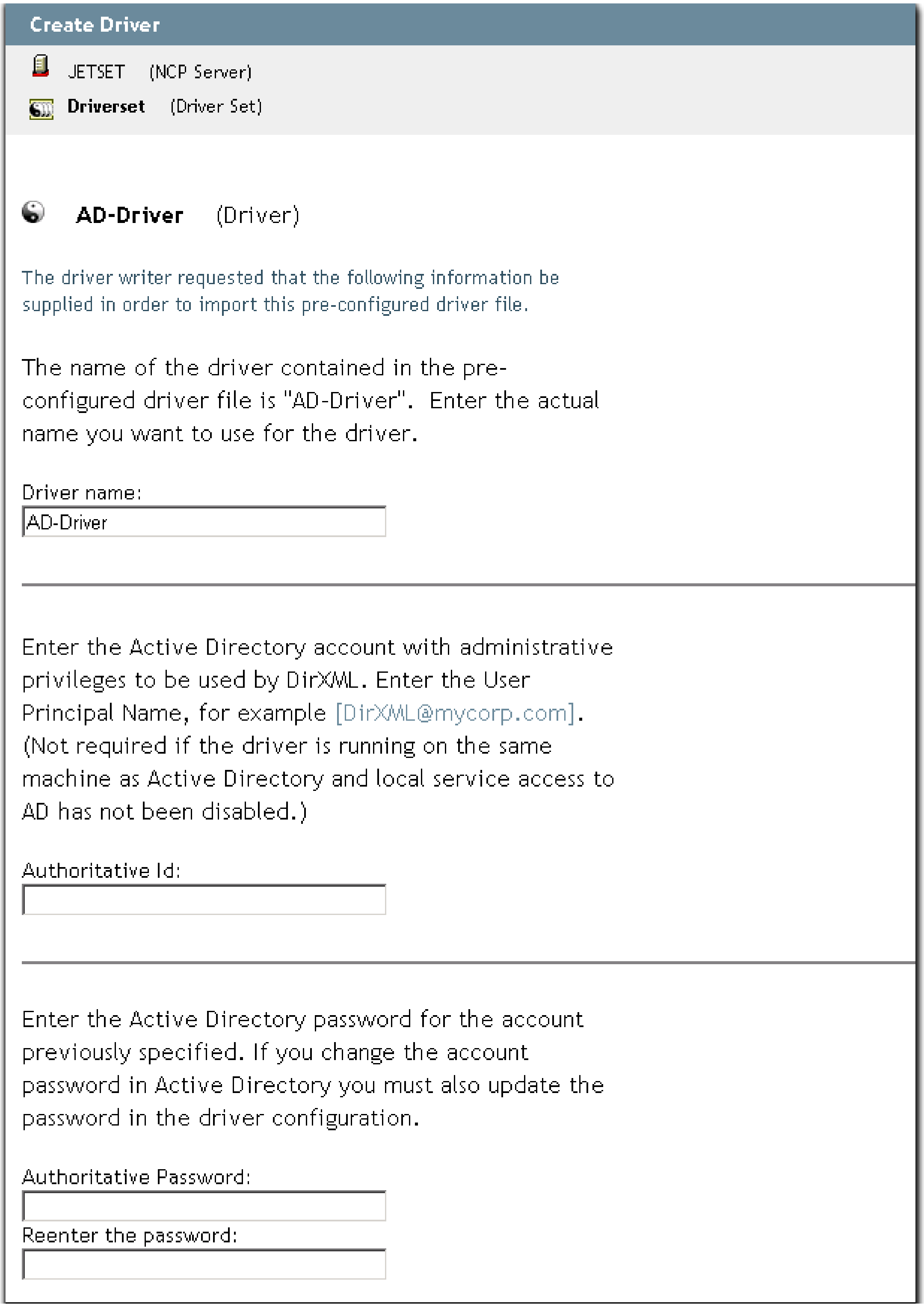
Collecting Configuration Information

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.

- Figure 8, “Active Directory Configuration Form,” on page 27 shows the Active Directory configuration form as it appears in iManager.
- Table 2, “Active Directory Configuration Information,” on page 32 provides you with a place to record configuration data for later reference.

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 13.

Figure 8 Active Directory Configuration Form



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.

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

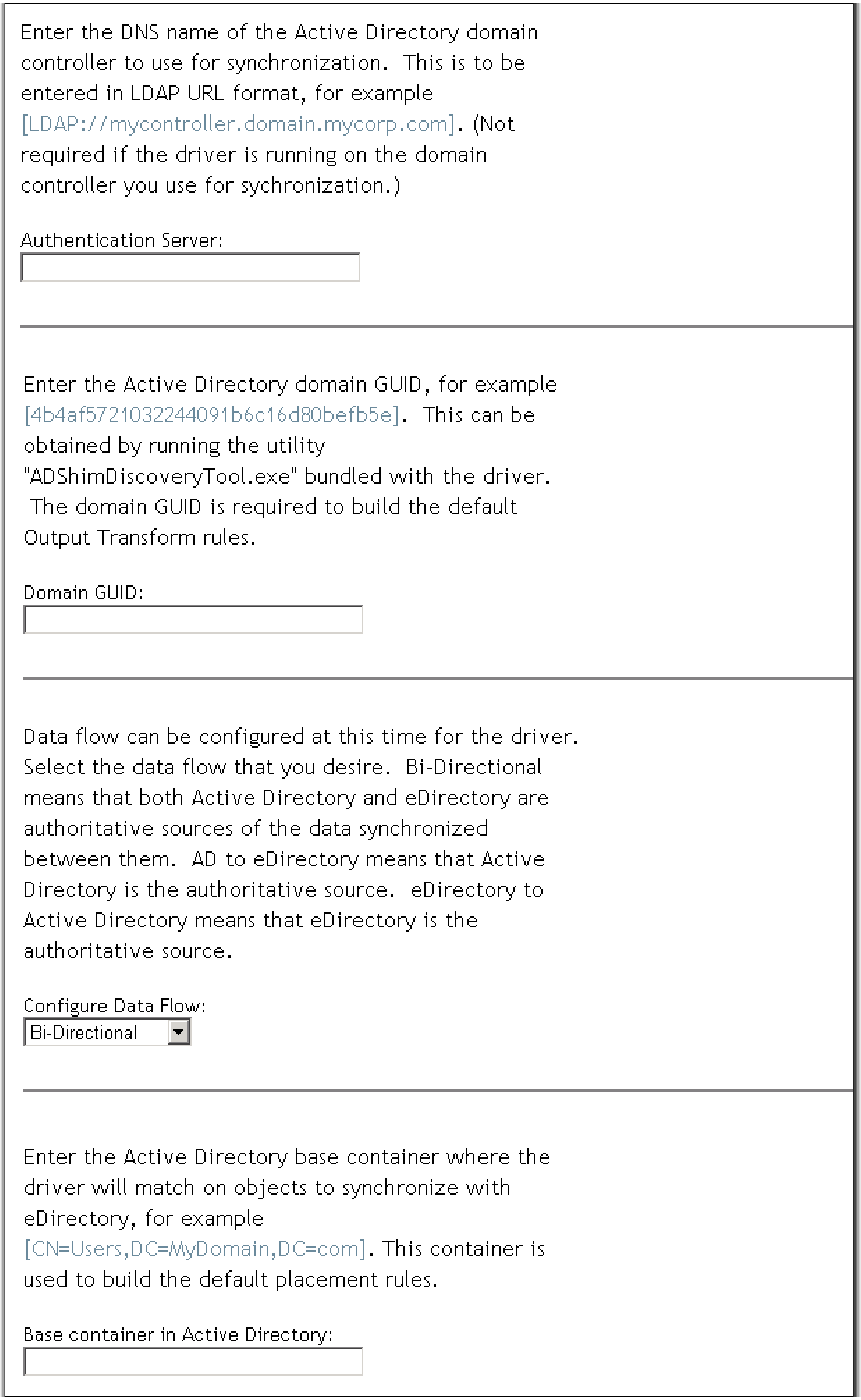
Enter the Active Directory account with administrative privileges to be used by DirXML. Enter the User Principal Name, for example [DirXML@mycorp.com]. (Not required if the driver is running on the same machine as Active Directory and local service access to AD has not been disabled.)

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:



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.

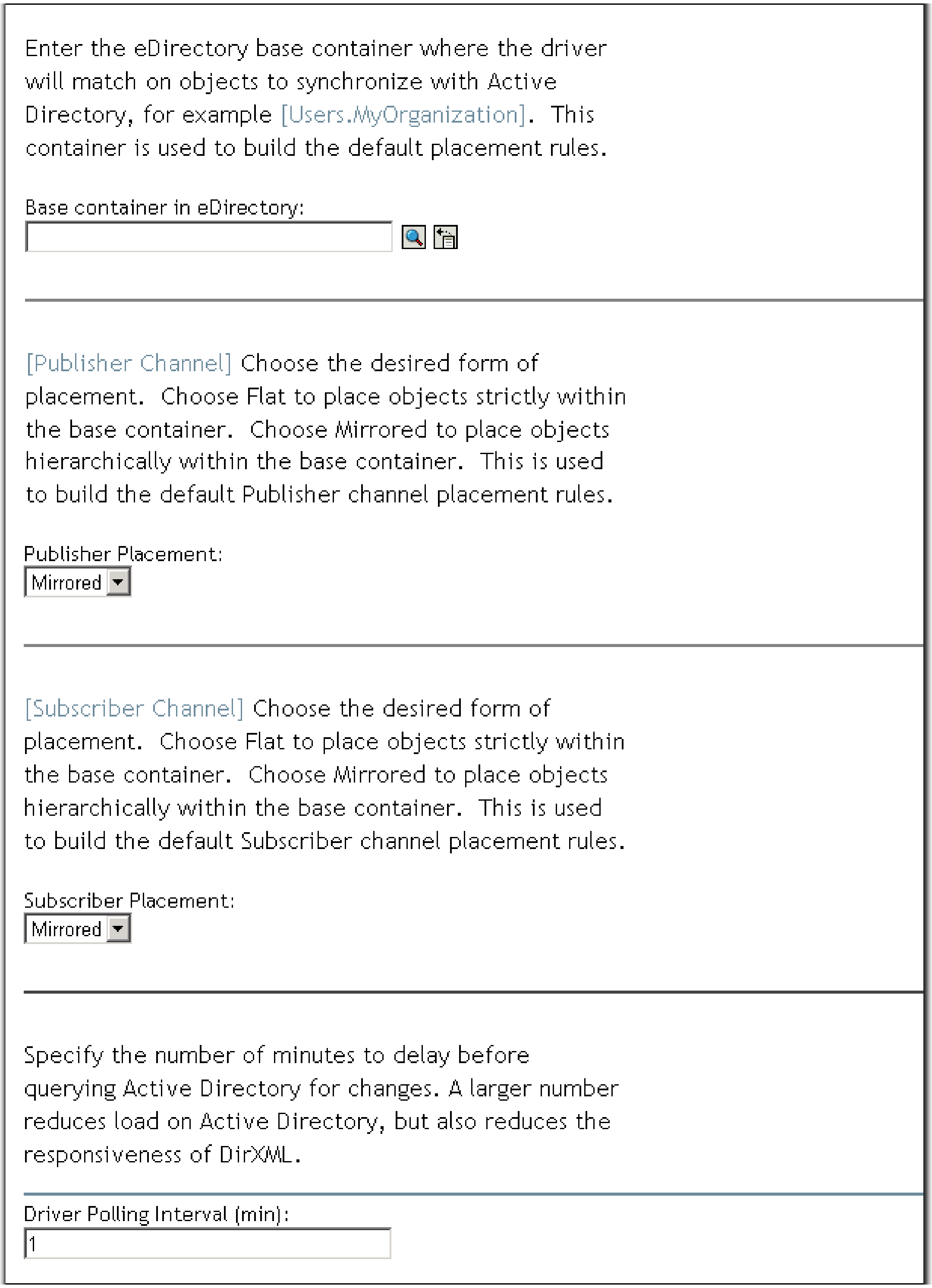
Domain GUID:

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:



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.

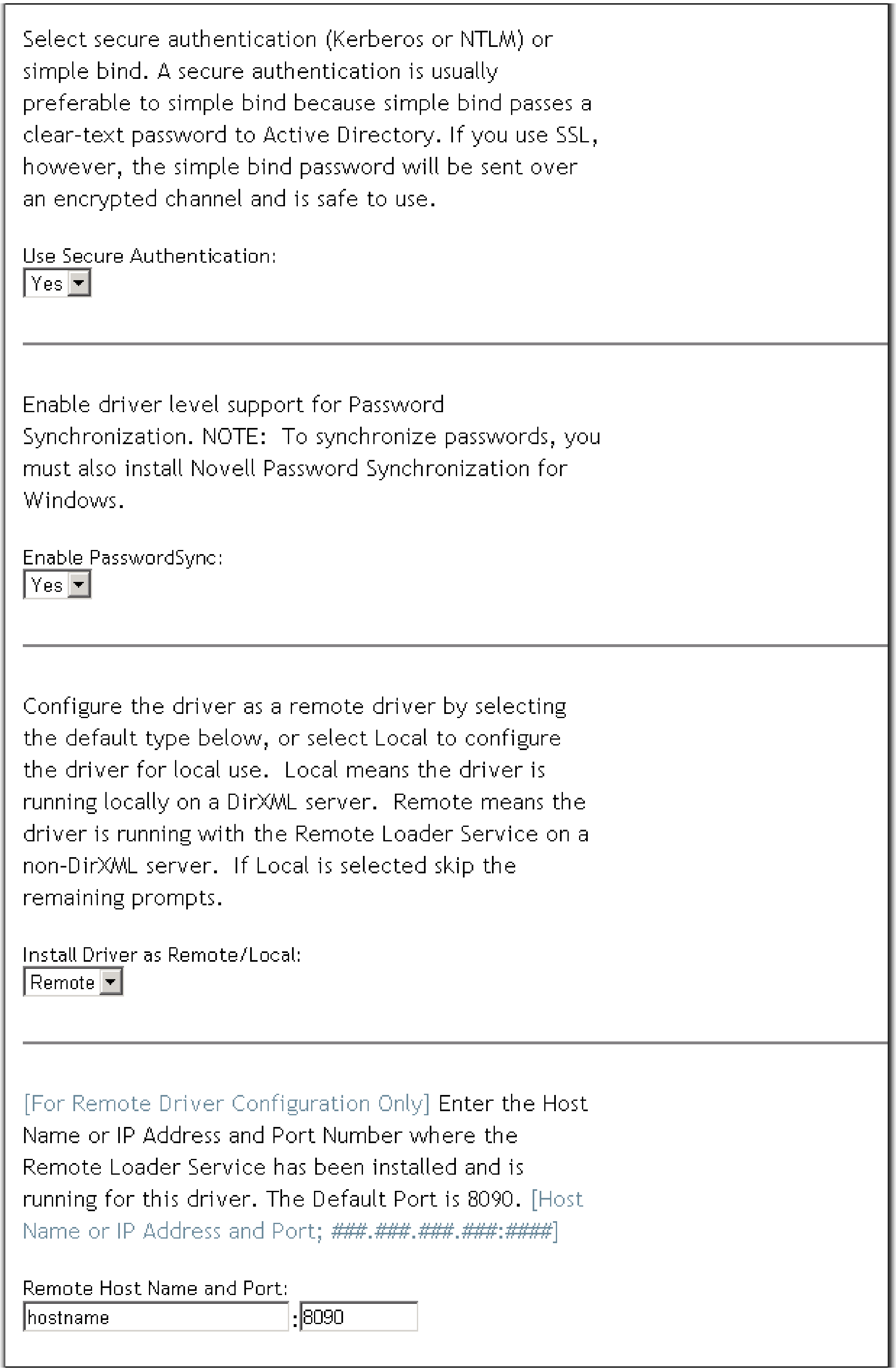
Publisher Placement: Mirrored

[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



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.

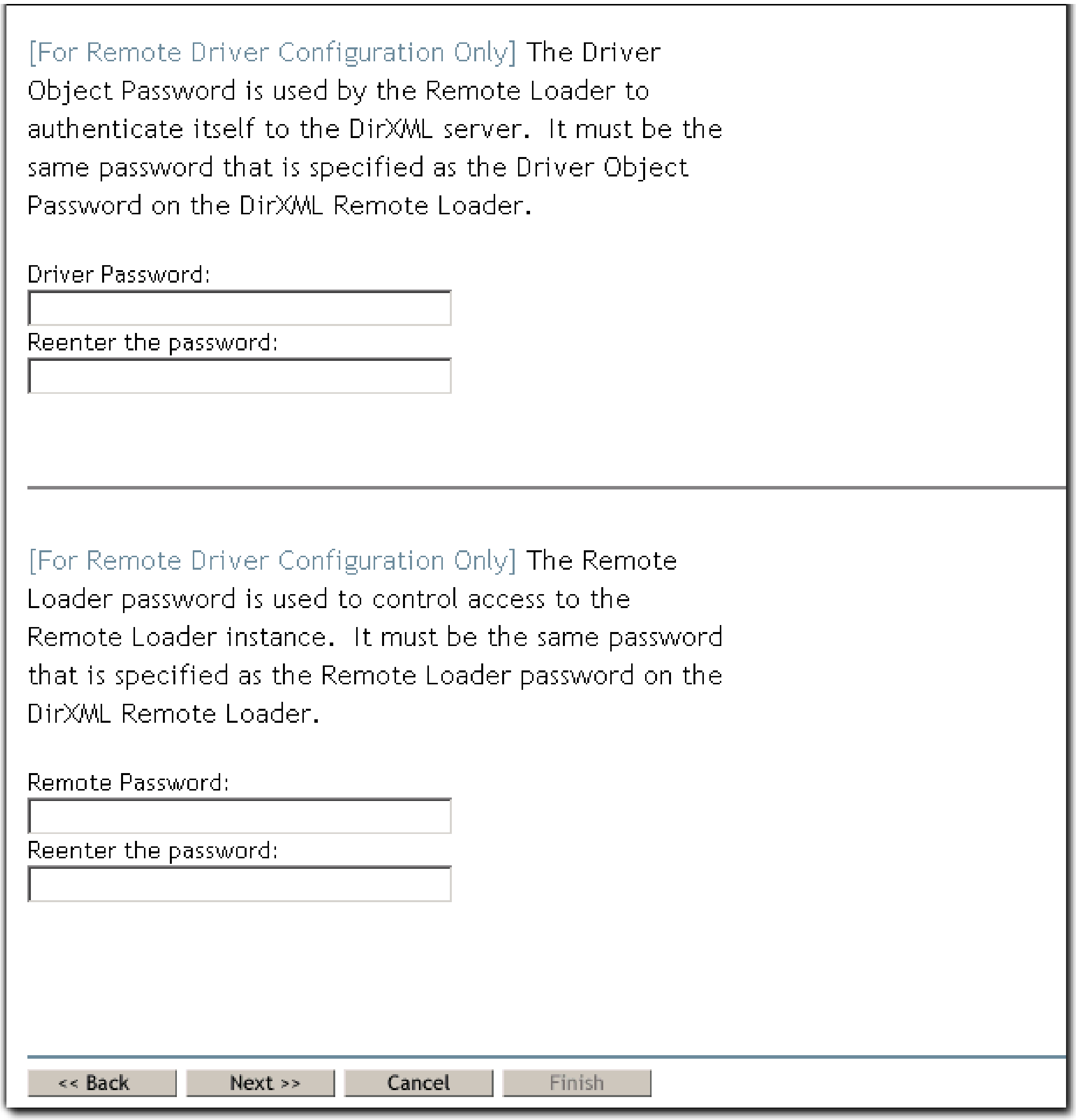
Enable PasswordSync:
Yes ▾

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 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:

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.

Table 2   Active Directory Configuration Information

System	Value
Authentication ID (Used by the driver to access objects necessary for data synchronization. To create this user, see "Creating an Admin User" on page 33.)	
Authentication Password (Password for the above user. Can be set when "Creating an Admin User" on page 33.)	
The DNS name for the Domain Controller (You might need to ask the AD administrator for this information.)	
The GUID for the Domain Controller (To get this information, see "Identifying the Active Directory Domain GUID" on page 34.)	
The Active Directory container holding objects to synchronize with eDirectory. If this container does not exist, you must create it before starting the driver.	
The eDirectory container holding objects to synchronize with Active Directory. If this container does not exist, you must create it before starting the driver.	
IP Address and Port Number for the Remote Loader (Default Port number is 8090) (Specify the port when "Installing and Configuring the Remote Loader and Driver" on page 34.)	
Driver Object Password (Specify the password when "Installing and Configuring the Remote Loader and Driver" on page 34.)	

System	Value
Remote Loader Password (Specify the password when “Installing and Configuring the Remote Loader and Driver” on page 34.)	

Creating an Admin User

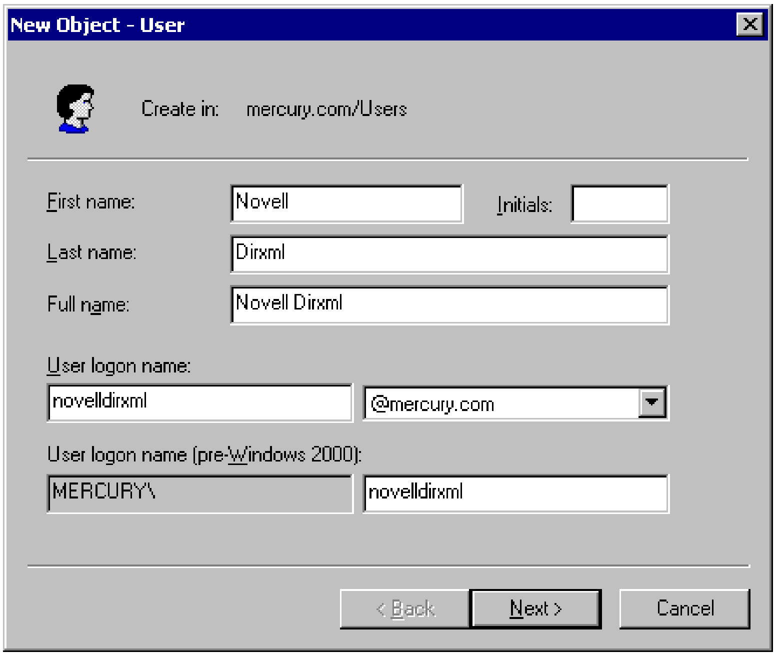
Create a user with Admin privileges to be exclusively used by the driver to authenticate into Active Directory. Doing this keeps DirXML Admin account isolated from changes to other Admin accounts.

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 Fullname, which is the AD user object name, and enter the User logon name, which is the AD authentication name.

Figure 9 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 “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 “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.

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, 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.

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 Reboot the system to make these changes effective in Active Directory.

15 Continue with the next section, "Installing and Configuring the Remote Loader and Driver" on page 34.

Identifying the Active Directory Domain GUID

The Active Directory Domain GUID is required for password synchronization.

1 At the computer where you will run iManager, 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 Copy the Active Directory Domain GUID to a text file for use during driver configuration.

8 Note the filename or GUID in the table under "Driver Configuration Information for Active Directory" on page 32. Then click Exit.

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 Service, 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 ensure that Use SSL is unchecked.
15. Record the port number in the table under "Driver Configuration Information for Active Directory" on page 32, then click Next. This information will be required later during driver parameter configuration.
16. Set Trace Level to 3 so that you'll get adequate tracking data from the Remote Loader for troubleshooting, specify a location and filename for the trace file, then click Next.

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

17. Mark Install the Remote Loader Instance as a Service, then click Next.
18. 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 "Driver Configuration Information for Active Directory" on page 32. This information will be required later during driver parameter configuration.

19. Review the summary, then click Finish.
20. When prompted, start the service.

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

    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 49.

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 21, 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. The procedures in this section assume a NetWare 5.1 server. Later versions of NetWare could also be used. The steps to launch the DirXML installation program will vary depending on which version of NetWare you are running.

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

- "Prerequisites" on page 36
- "Collecting Configuration Information" on page 37
- "Installing DirXML and the DirXML Driver for eDirectory on Tree 1" on page 40
- "Configuring the DirXML Driver for eDirectory" on page 40

Prerequisites

❑ NetWare 5.1 SP6 or later, NetWare 6.0 SP3 or later, or NetWare 6.5

❑ JVM* 1.4.0.

You can download JVM 1.4.0 from the NetWare section 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.

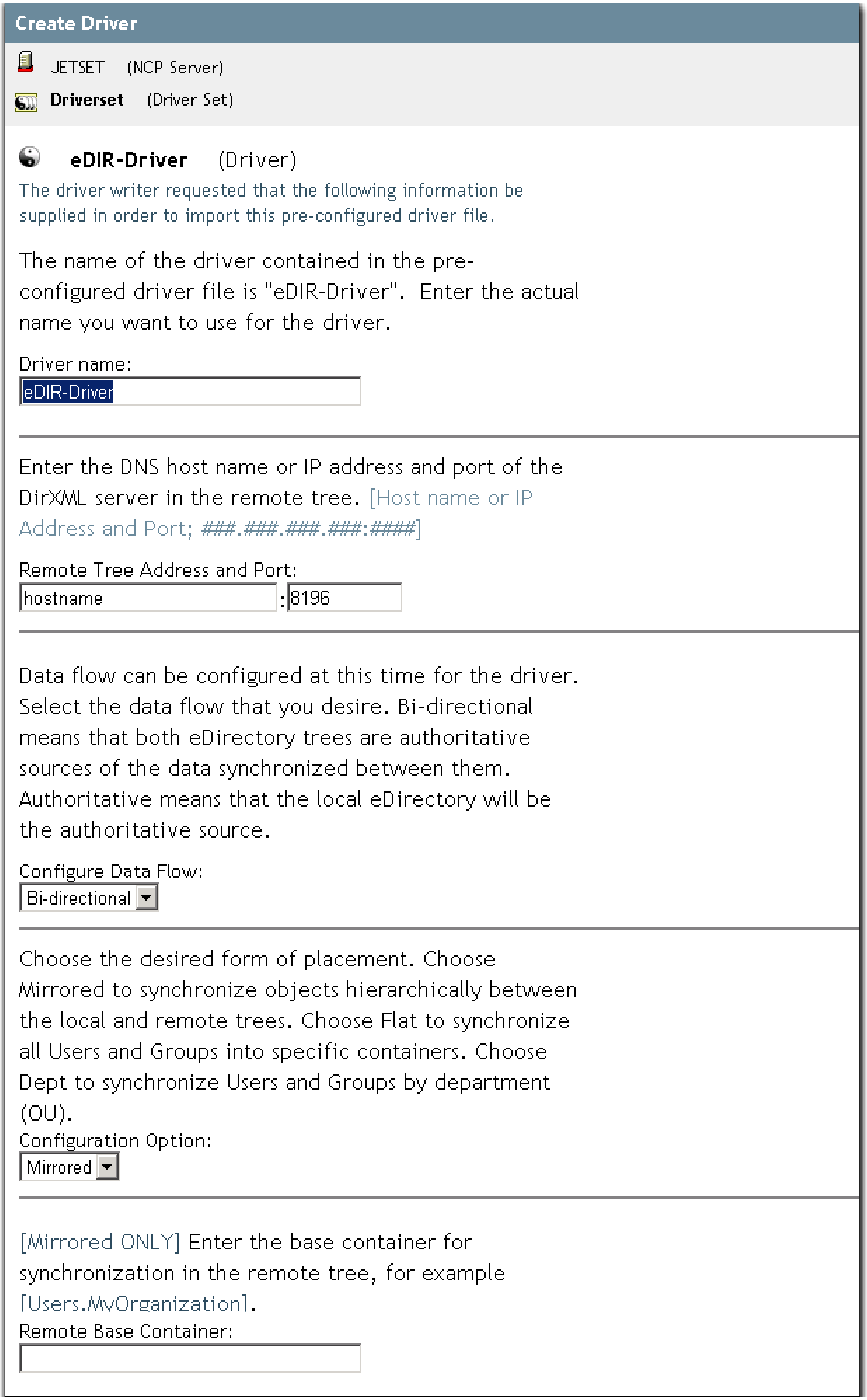
Collecting Configuration Information

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.

- Figure 10, "eDirectory Configuration Form," on page 38 shows the eDirectory configuration form as it appears in iManager.
- Table 3, "eDirectory Configuration Information," on page 39 provides you with a place to record configuration data for later reference.

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 15.

Figure 10 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.

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

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 eDirectory will be the authoritative source.

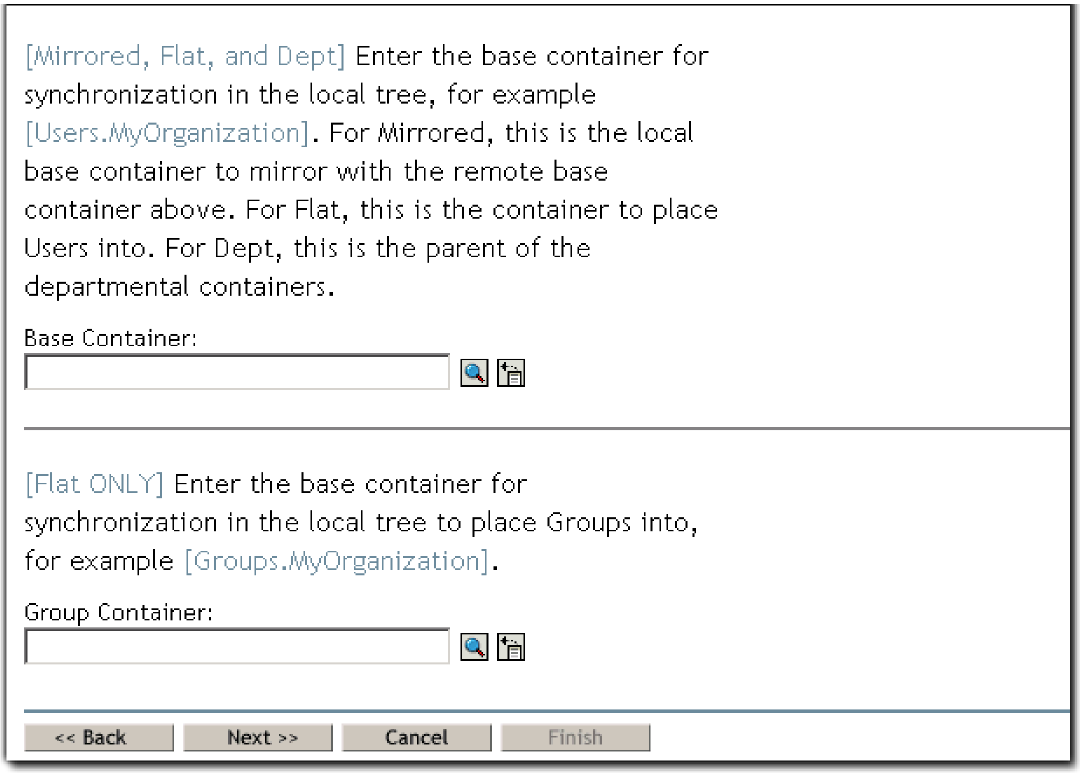
Configure Data Flow:
Bi-directional

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

[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:

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.

Table 3 eDirectory Configuration Information

System	Value
IP Address and port for the remote tree, Tree 1 The default port is 8196.	
Base Container for the remote tree, Tree 1 If this container does not exist, you must create it before starting the driver.	
Base Container for the local tree, Tree 2 If this container does not exist, you must create it before starting the driver. (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 15.)	

Installing DirXML and the DirXML Driver for eDirectory on Tree 1

1. At the NetWare 5.1 server, insert the DirXML CD into the CD drive. At the system console, enter **`CDROM`**.
2. Enter **`NWCONFIG`**.
3. Select Product Options > Install a Product Not Listed.
4. Press F3 (F4 if you're using RCONSOLE), then specify the path to the DirXML NetWare installation files on the DirXML CD, for example, *volume_name*:nw.

   The graphical installation utility will start after a few moments.
5. Click Next. After the files have finished copying, the DirXML Welcome Screen will appear. Click Next to begin the installation.
6. Read the license agreement; if you agree to the terms, click I Accept.
7. On the Components page, select the following items, then click Next.
   - DirXML Engine and Drivers
   - Driver Preconfiguration Files
   - (If you plan to use ConsoleOne) ConsoleOne Snap-ins
8. In the Schema Extension screen, 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.
9. Select the DirXML Driver for eDirectory, then click Next.
10. Select the driver configuration (XML files) for eDirectory, then click Next.
11. Read the Summary page, then click Finish.

    The file copy might take a few minutes.

    If you are presented with an LDAP warning message, verify that no conflicts exist, then click OK.
12. After the installation completes and displays the Installation Complete dialog box, click Close.
13. Continue with the next section, "Configuring the DirXML Driver for eDirectory" on page 40.

Configuring the DirXML Driver for eDirectory

This section explains how to configure the eDirectory driver for the NetWare 5.1 tree (Tree 1). Configuring the eDirectory driver for the NetWare 6.5 tree (Tree 2), along with the drivers for Active Directory and NT, is explained later in this document.

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 NetWare 5.1 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.
10. Click Exclude Administrative Roles, add Admin, click OK, then click Next.
11. Click Finish with Overview.
12. Start the driver by clicking the status indicator in the upper-right corner of the driver icon.

    DirXML reports driver events, such as starting a driver, through DSTrace. If the driver status indicator doesn't change to running within the polling period you specified during configuration, review the DirXML messages in DSTrace for troubleshooting information.
13. The eDirectory driver for Tree 1 is prepared to synchronize data. Complete preparation of other participating systems and then proceed to "Configuring the DirXML Drivers" on page 49.

Setting Up NT Domain

For the default NetWare® 6.5 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 42
- "Collecting Configuration Information" on page 42
- "Creating an Authoritative User" on page 47
- "Granting Rights to the Driver" on page 48
- "Installing and Configuring the Remote Loader and Driver" on page 48

Prerequisites

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

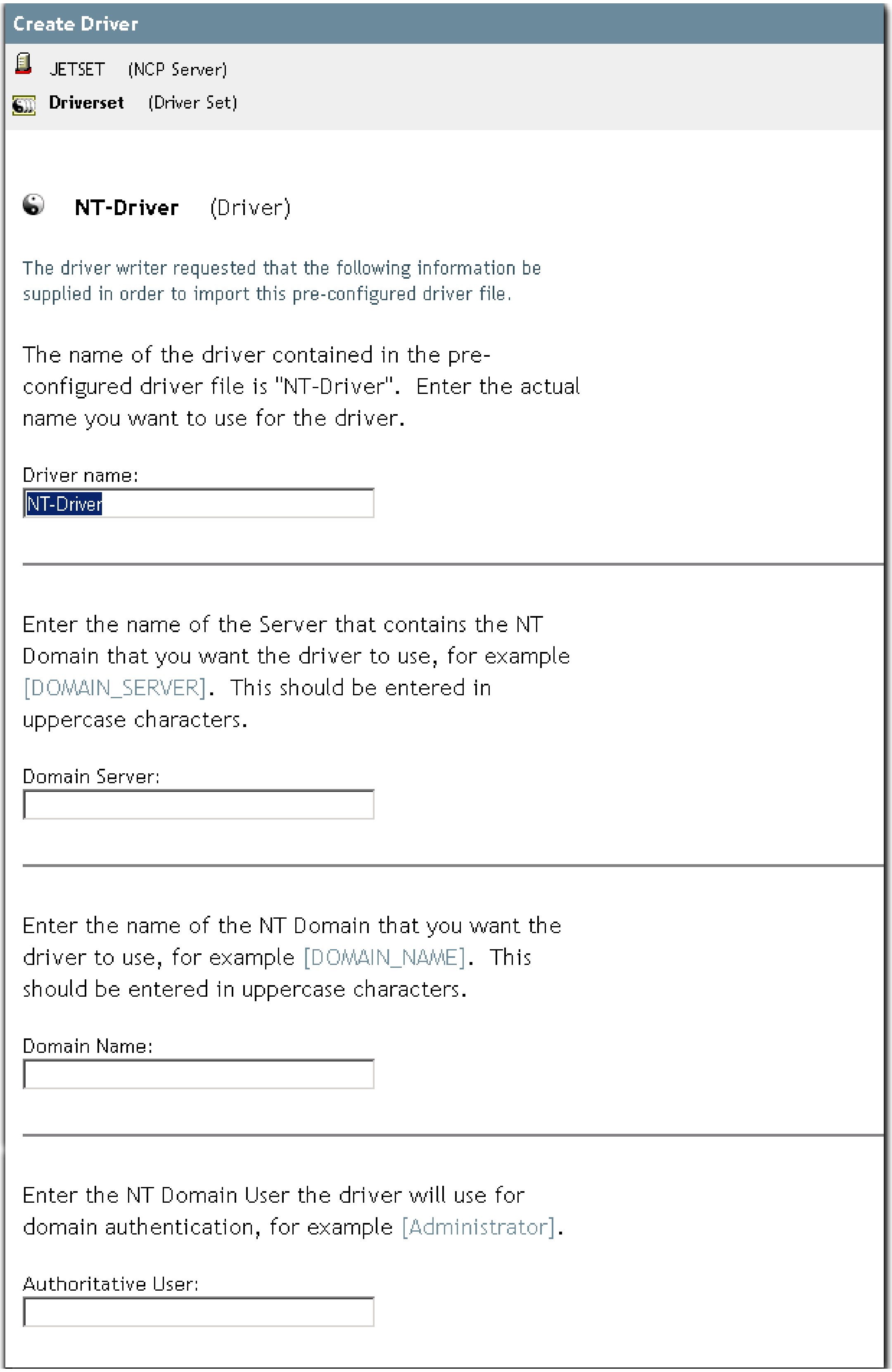
- Windows NT* 4 with Service Pack 6a or later

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.

- Figure 11, "NT Configuration Form," on page 43 shows the NT Domain configuration form as it appears in iManager.
- Table 4, "NT Configuration Information," on page 46 provides you with a place to record configuration data for later reference.

Figure 11 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.

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

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.

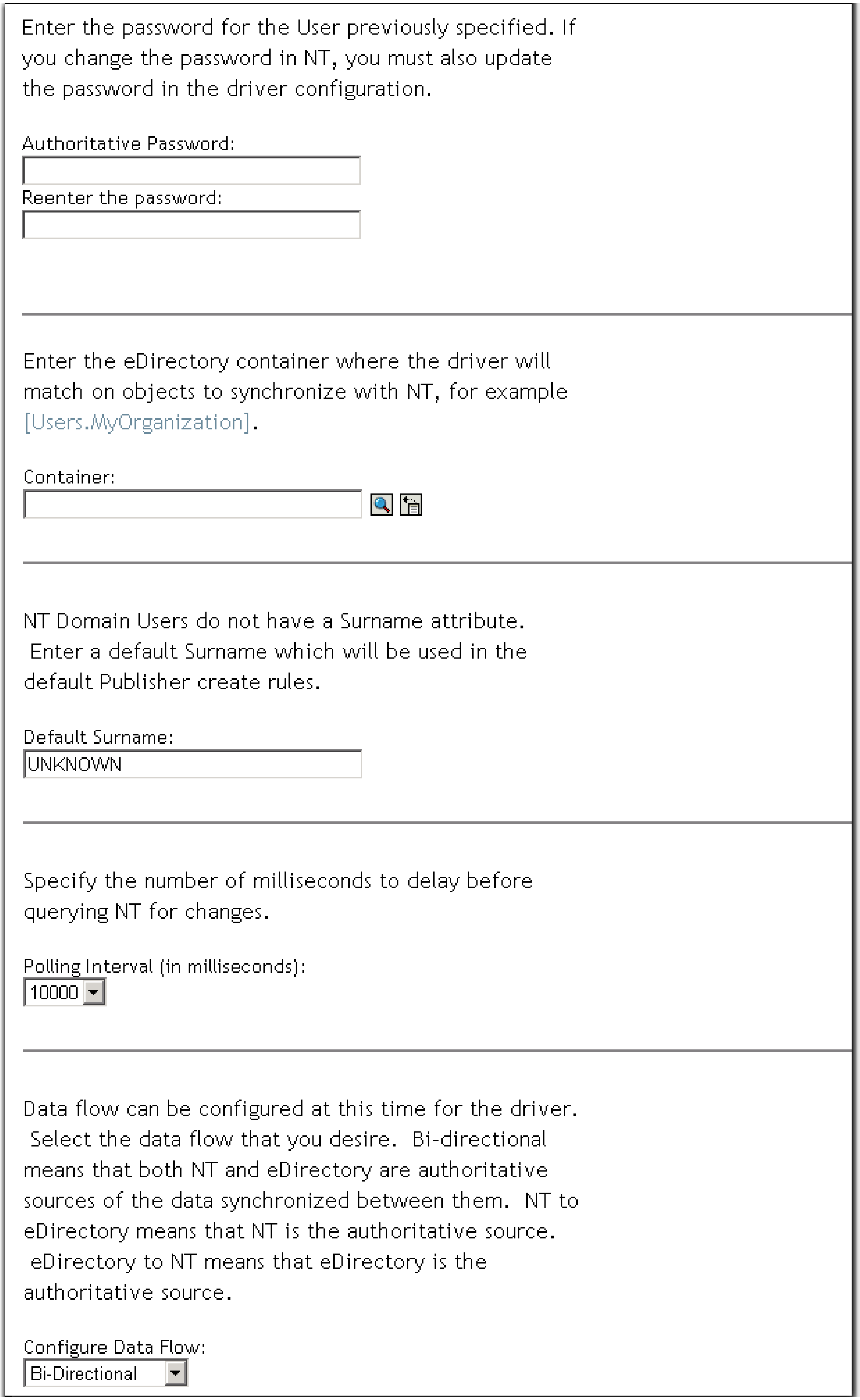
Domain Server:

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:



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.

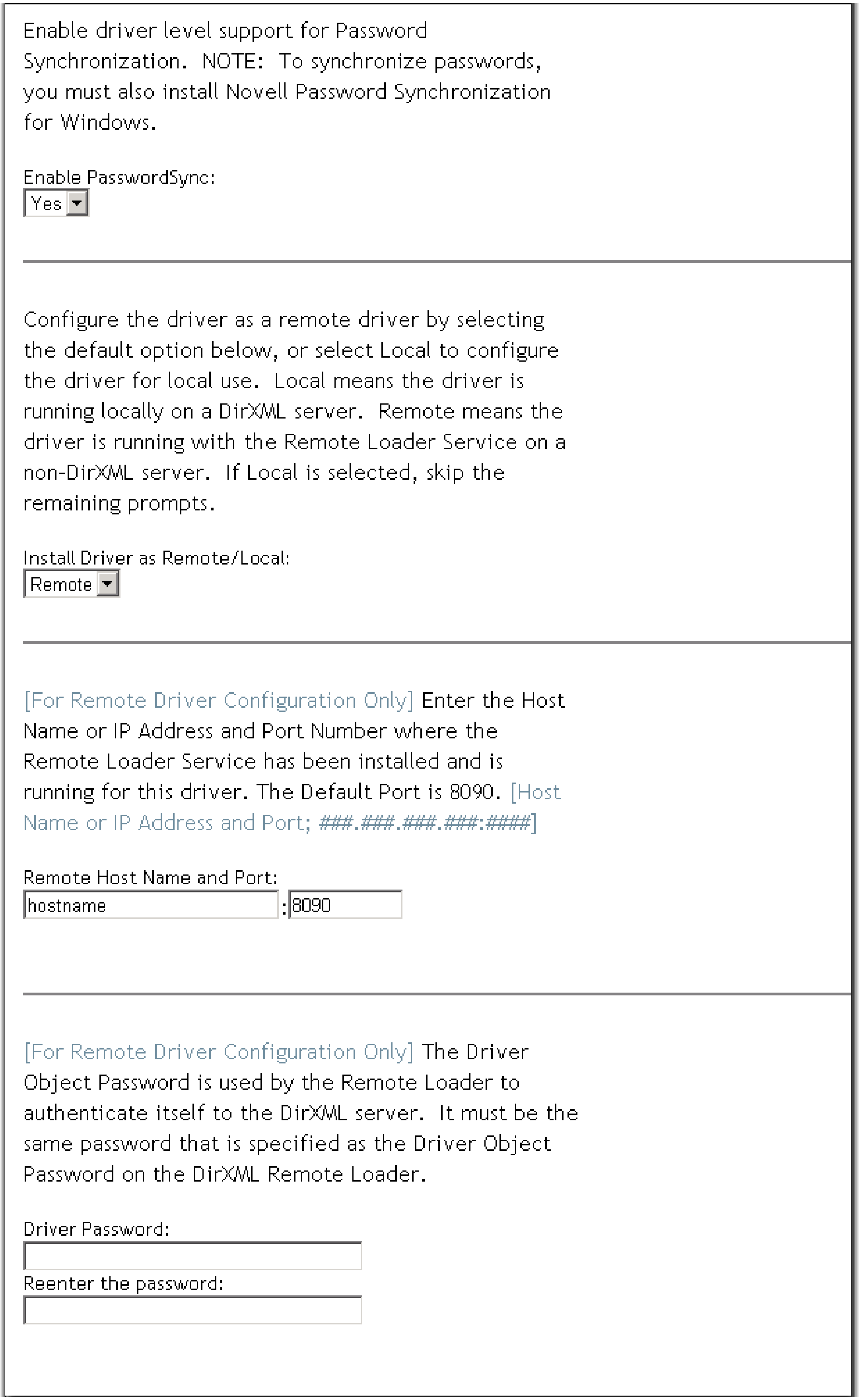
Default Surname: UNKNOWN

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

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

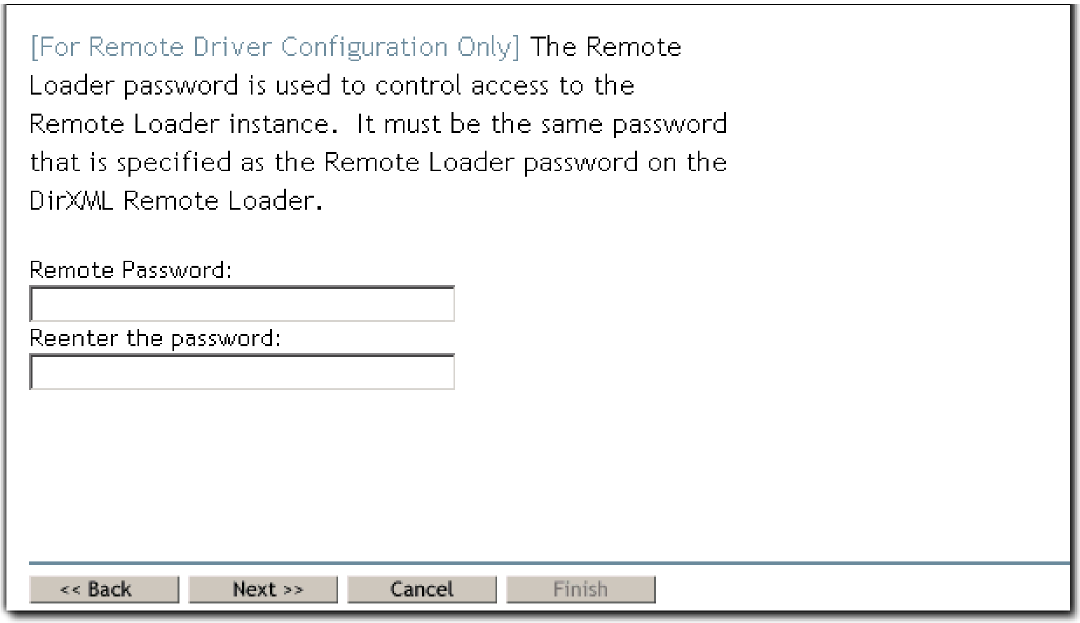
[For Remote Driver Configuration Only] Enter the Host Name or IP Address and Port Number where the Remote Loader Service has been installed and is running for this driver. The Default Port is 8090. [Host Name or IP Address and Port; ###.###.###.###:####]

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:

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 14.

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.

Table 4 NT Configuration Information

System	Value
Domain Server (You might need to ask the NT Administrator for this information.)	
Domain Name (You might need to ask the NT Administrator for this information.)	
Authoritative User (Used by the driver to access objects necessary for data synchronization. To create this user, see "Creating an Authoritative User" on page 47.)	
Authoritative Password (Password for the above user. Can be set when "Creating an Authoritative User" on page 47.)	

System	Value
eDirectory Container (The container holding objects to synchronize with NT. If this container does not exist, you must create it before starting the driver.)	
IP Address and Port Number the for Remote Loader (Default Port number is 8090) (Specify the port when "Installing and Configuring the Remote Loader and Driver" on page 48.)	
Driver Object Password (Specify the password when "Installing and Configuring the Remote Loader and Driver" on page 48.)	
Remote Loader Password (Specify the password when "Installing and Configuring the Remote Loader and Driver" on page 48.)	

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 Choose Start > Programs > Administrative Tools (Common) > UserManager for Domains.

2 In the User Manager dialog box, choose User > New User.

3 Enter a username and password.

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 Record the Authoritative user information in the table under "Driver Configuration Information for NT Domain" on page 46.

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.

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 Service, 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 ensure that Use SSL is unchecked.

15. Record the port number in the table under "Driver Configuration Information for NT Domain" on page 46, then click Next. This information will be required later during driver parameter configuration.

16. Set Trace Level to 3 so that you'll get adequate tracking data from the Remote Loader for troubleshooting, specify a location and filename for the trace file, then click Next.

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

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

18. 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 "Driver Configuration Information for NT Domain" on page 46. This information will be required later during driver parameter configuration.

19. Review the summary, then click Finish.

20. When prompted, start the service.

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

    The NT system is prepared to synchronize data. Complete preparation of other participating systems and then proceed to "Configuring the DirXML Drivers" on page 49.

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.

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 49
- "Configuring Secure Data Transfers for the DirXML Driver for eDirectory" on page 50
- "Testing Data Synchronization" on page 51

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 NetWare 6.5 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.
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. Scroll to the bottom of the page to see all the prompts.

   If you quit before configuring all of the drivers, none of the drivers will be added to the driver set.
9. Click Define Security Equivalence, add Admin, then click OK.
10. Click Exclude Administrative Roles, add Admin, click OK, then click Next.
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 50.

    or

    If you are not synchronizing data between two eDirectory trees, continue with "Testing Data Synchronization" on page 51.

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 SSL technology. 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 eDirectory tree hosted on the NetWare 6.5 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 51.

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.

1 On each system, ensure that the Remote Loader service is running and that you can view the trace screen for the Remote Loader.

2 Open a DSTrace screen on the computer where the DirXML engine is installed.

3 In iManager, select DirXML Management > Overview.

4 Browse to the DirXML driver set.

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

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

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

Data Synchronization Checklist

- ❑ **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.

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 only one place. Any time a password is changed in one of these environments it will be updated in all of them.

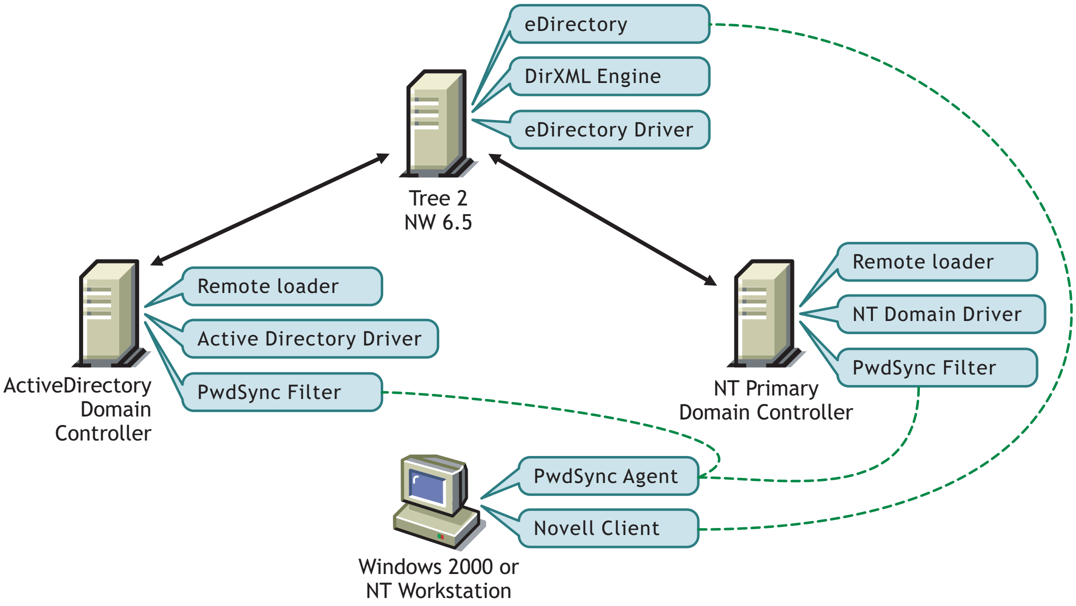
This section explains how to install Password Synchronization and begin synchronizing passwords. It includes the following topics:

For more conceptual information about Password Synchronization, see Password Synchronization for Windows (http://www.novell.com/documentation/lg/pwdsync10/index.html)

Where to Install PasswordSync

As shown in Figure 12, 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 25. Agent and filter installation options are discussed in the sections that follow.

Figure 12 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 55.
- **Multi-tree network:** First, complete the steps in "Installing PasswordSync Into a Single-Tree Network" on page 55, then continue with "Installing PasswordSync Into a Multi-Tree Network" on page 58.

Installing PasswordSync Into a Single-Tree Network

Prerequisites

The computer hosting the PasswordSync Agent 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.

Installing an Agent and Filter

1. Authenticate to the eDirectory Tree.
2. At the Windows computer that will host the agent, insert the Novell DirXML Starter Pack 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, 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, add the agent's nadPwdSync object as a trustee with rights as outlined in the following table:

Object	Attribute	Rights
User objects participating in password synchronization	Password Expiration Interval	compare, read
User objects participating in password synchronization	Password Management	compare, read, write
User objects participating in password synchronization	Password Expiration Time	write
nadDomain object	Server	compare, read
Server object holding the PwdSync index (by default, this is the server where DirXML is installed)	Index Definition	compare, read

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

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 57.

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

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 66.

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
Each domain controller must be serviced by at least one agent. A single agent can service many domains; however, additional agents provide redundancy and address network topology issues. 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. Install additional filters if you: ◆ Didn't install filters on all domain controllers ◆ Have additional domains you want to synchronize	See "Installing Additional Filters" on page 57.

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.

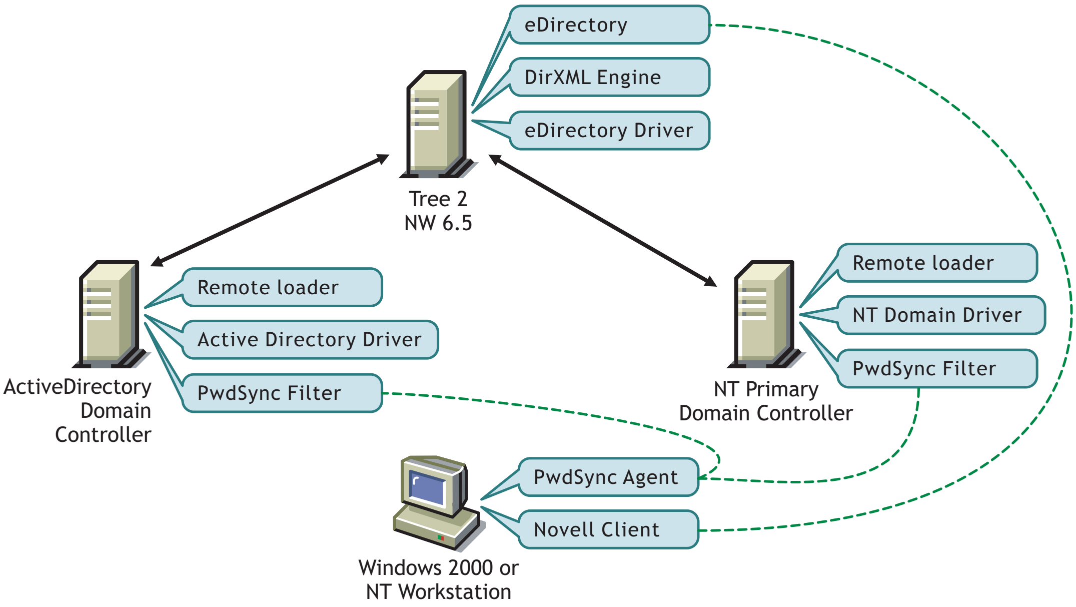
Installing PasswordSync Into a Multi-Tree Network

Understanding the Process

In the following sections, the two eDirectory trees are labeled Tree 1 and Tree 2. As shown in Figure 13, Tree 2 holds the driver set that includes the PasswordSync-enabled Active Directory and NT drivers.

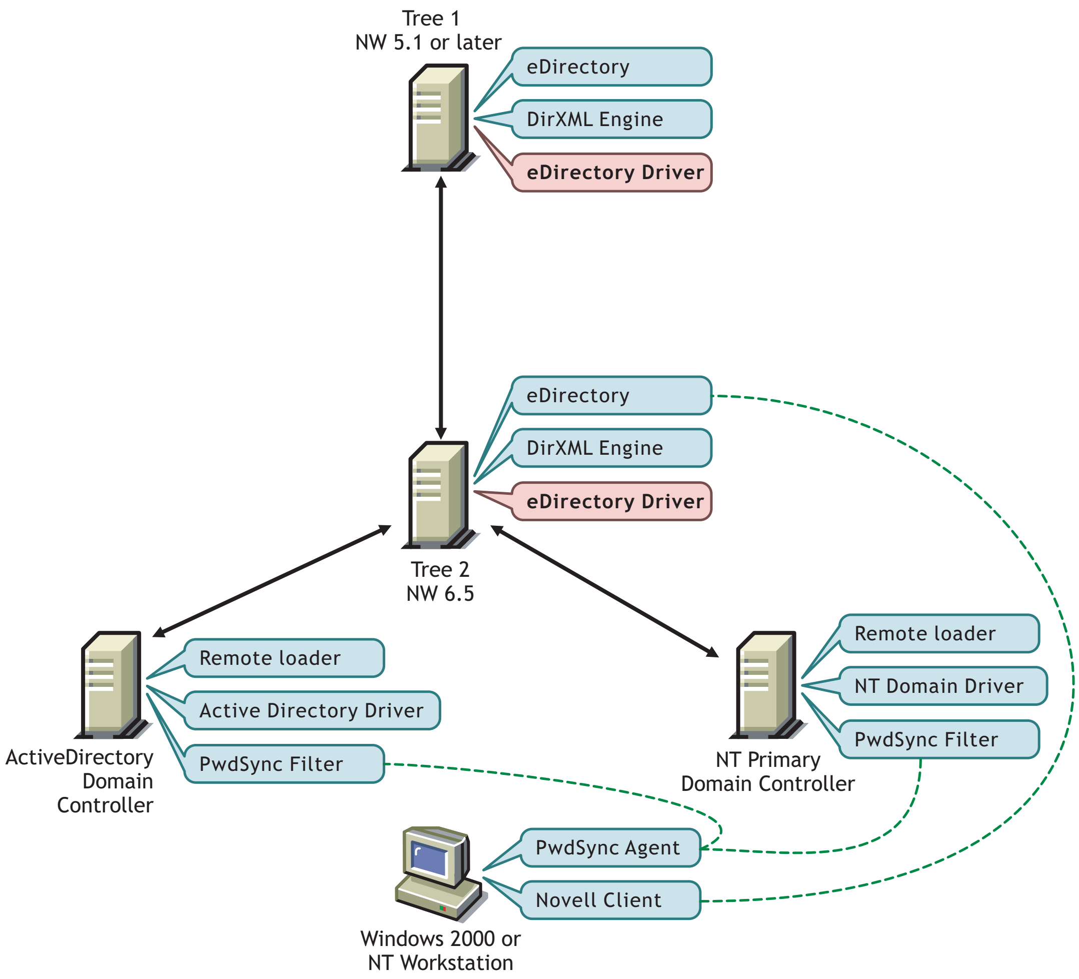
To synchronize passwords in an environment with multiple eDirectory trees, first you set up password synchronization in Tree 2 as explained in "Installing PasswordSync Into a Single-Tree Network" on page 55. This step should already be completed.

Figure 13 Single-Tree Password Synchronization



Then, you configure the eDirectory drivers to populate Tree 1 with the information needed for PasswordSync. This step is explained in the following sections.

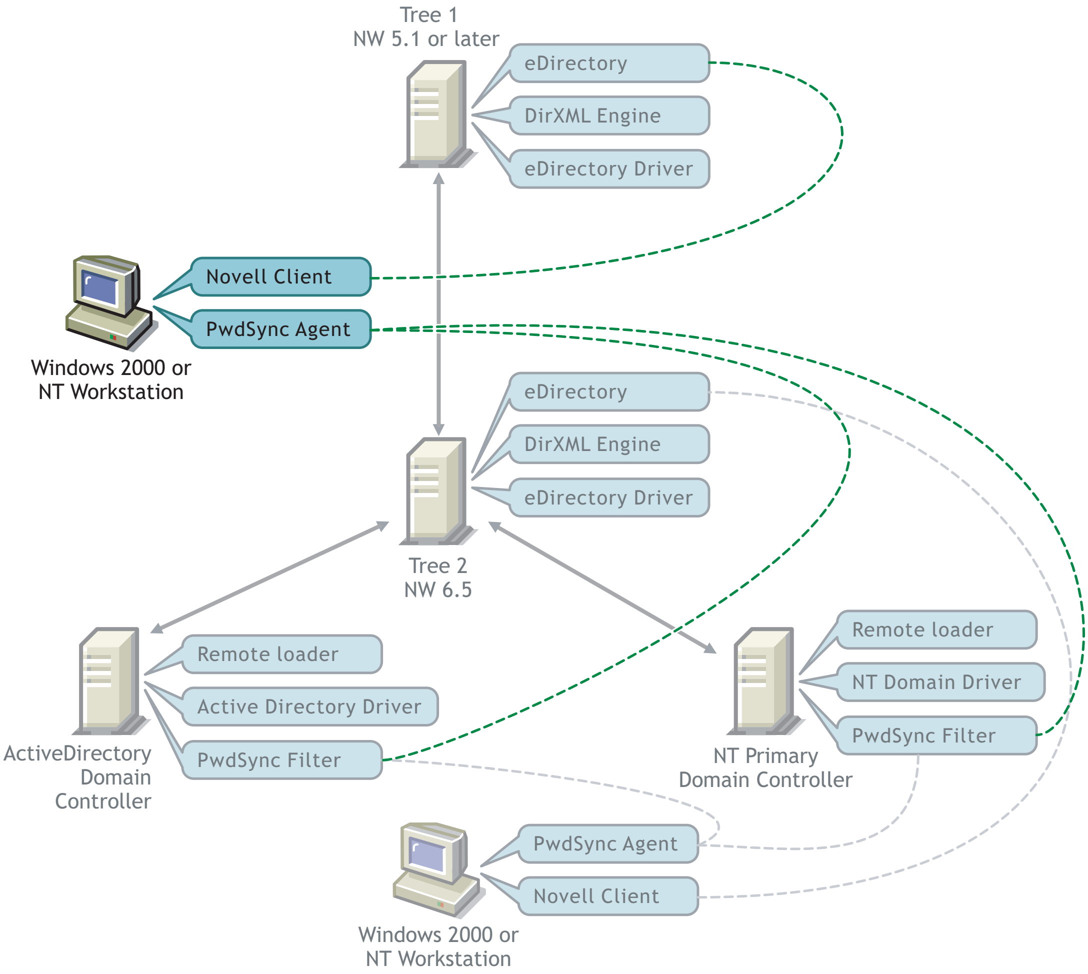
Figure 14 eDirectory Driver Configuration for PasswordSync



Finally, you install a PasswordSync Agent into Tree 1 to communicate password changes between this tree and participating domains. This step is explained in the following sections.

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 15 PasswordSync Agent for Tree 1



HINT: To keep these trees straight in the procedures that follow, you might want to label Figure 15 with the actual tree names for the trees you are synchronizing.

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

❑ "Extending the Schema for Password Synchronization" on page 61

❑ "Configuring the eDirectory Drivers for Password Synchronization" on page 61

❑ "Migrating PasswordSync Data" on page 63

❑ "Installing a PasswordSync Agent for Tree 1" on page 63

Extending the Schema for Password Synchronization

As explained in "Management Utilities" on page 12, PasswordSync requires the addition of three objects in your eDirectory schema: nadPwdSync, nadPwdProvider, and nadDomain. These objects already exist in Tree 2. The Tree 1 schema must be extended to include these objects.

1. Copy pwdsync.sch from the nt\dirxml\schema directory on the DirXML Starter Pack CD to a network directory.
2. At the NetWare server, load NWCONFIG.
3. Choose Directory Options.
4. Choose Extend Schema, then authenticate to Tree 1.
5. Press F3 and type the path to where you copied the schema extension file.

   For example, type SYS:\TMP\pwdsync.sch.
6. Press Enter to complete the process, then close the configuration utility.

The objects necessary for password synchronization are now available for use by the DirXML drivers. Continue with the next section, Configuring the eDirectory Drivers for Password Synchronization.

Configuring the eDirectory Drivers for Password Synchronization

To exchange password synchronization data, you need to modify the filters and rules for the eDirectory drivers as explained in the following steps.

Editing the eDirectory Driver on Tree 2

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

   IMPORTANT: This URL is case sensitive.
2. Authenticate to Tree 2.
3. Click DirXML Management > Overview.
4. Locate the DirXML eDirectory driver.
5. Click the driver icon to open the Driver Overview page.
6. Edit the driver's subscriber filter as follows:

   6a In the Driver Overview, click the Subscriber Filter, then click User.

   You might need to scroll to see User.

   6b In the Attributes column on the right, mark Show All Attributes from All Classes, then mark nadLoginName.

   6c In the Classes column on the left, mark nadDomain.

   Other classes will be selected. Leave them marked.

   6d In the Attributes column, mark dc, then click OK.

   At the bottom of the list, the filter should show nadLoginName (in addition to any other attributes you are synchronizing) under User. The dc attribute should display under nadDomain.
7. Click OK.

The eDirectory driver for Tree 2 is ready to support multi-tree password synchronization. Continue with Editing the eDirectory Driver on Tree 1.

Editing the eDirectory Driver on Tree 1

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

IMPORTANT: This URL is case sensitive.

2 Authenticate to Tree 1.

3 Click DirXML Management > Overview.

4 Locate the DirXML eDirectory driver.

5 Click the driver icon to open the Driver Overview page.

6 Edit the driver's publisher filter as follows:

6a In the Driver Overview, click the Publisher Filter, then click User.

6b In the Attributes column on the right, mark Show All Attributes from All Classes, then mark nadLoginName.

6c In the Classes column on the left, mark nadDomain.

6d In the Attributes column, mark dc, then click OK.

At the bottom of the list, the filter should show nadLoginName (in addition to any other attributes you are synchronizing) under User. The dc attribute should display under nadDomain.

6e Click OK.

7 Append a new Creation rule on the Publisher channel as follows:

7a Click the Creation rule on the Publisher channel, the mark Create a New Rule.

7b Enter a rule name, such as PasswordSync, then click OK.

7c Click Append New Rule.

7d Enter a rule description, such as nadDomain, then click Next.

7e From the drop-down list, select nadDomain, then click Next.

7f Do not match any attributes. Click Next.

7g Add dc to the Required Attributes List, then click Next.

7h Do not enter a template DN. Click Finish, then click OK.

8 Append a new Placement rule on the Publisher channel as follows:

8a Open the existing Placement rule on the Publisher channel.

8b Click Append New Rule.

8c Enter a rule name, such as PasswordSync, then click Next.

8d Select nadDomain from the Additional class list, then click Next.

8e Do not match path prefixes. Click Next.

8f Do not match attributes. Click Next.

8g Click Append New Item, then select Data and enter the full name of the Tree 1 eDirectory driver followed by a slash.

For example, type

```
\TREE1\MyOrg\DirXML\DriverSet\eDirDriver\
```

8h Click OK.

8i Click Append New Item, then deselect Data; in the Copy section below, select Name.

8j Click OK, then click Finish.

9 Click OK.

The eDirectory driver for Tree 1 is ready for password synchronization. Continue with Migrating PasswordSync Data.

Migrating PasswordSync Data

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

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, or the objects representing, 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 Novell DirXML Starter Pack 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.

    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, use ConsoleOne to add the agent's eDirectory object as a trustee with rights as outlined in the following table:

Object	Attribute	Rights
User Objects participating in password synchronization	Password Expiration Interval	compare, read
User objects participating in password synchronization	Password Management	compare, read, write

Object	Attribute	Rights
User Objects participating in password synchronization	Password Expiration Time	write
nadDomain object	Server	compare, read
Server object holding the PwdSync index (by default, this is the server where DirXML is installed)	Index Definition	compare, read

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 65.

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

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.

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.

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 by marking the Assign NDS Password check box and then selecting the Prompt During Creation option. 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:

- Unmark Assign NDS Password during user creation and assign the password later. A brief delay will allow account associations to be completed. (This works for ConsoleOne only.)
- 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

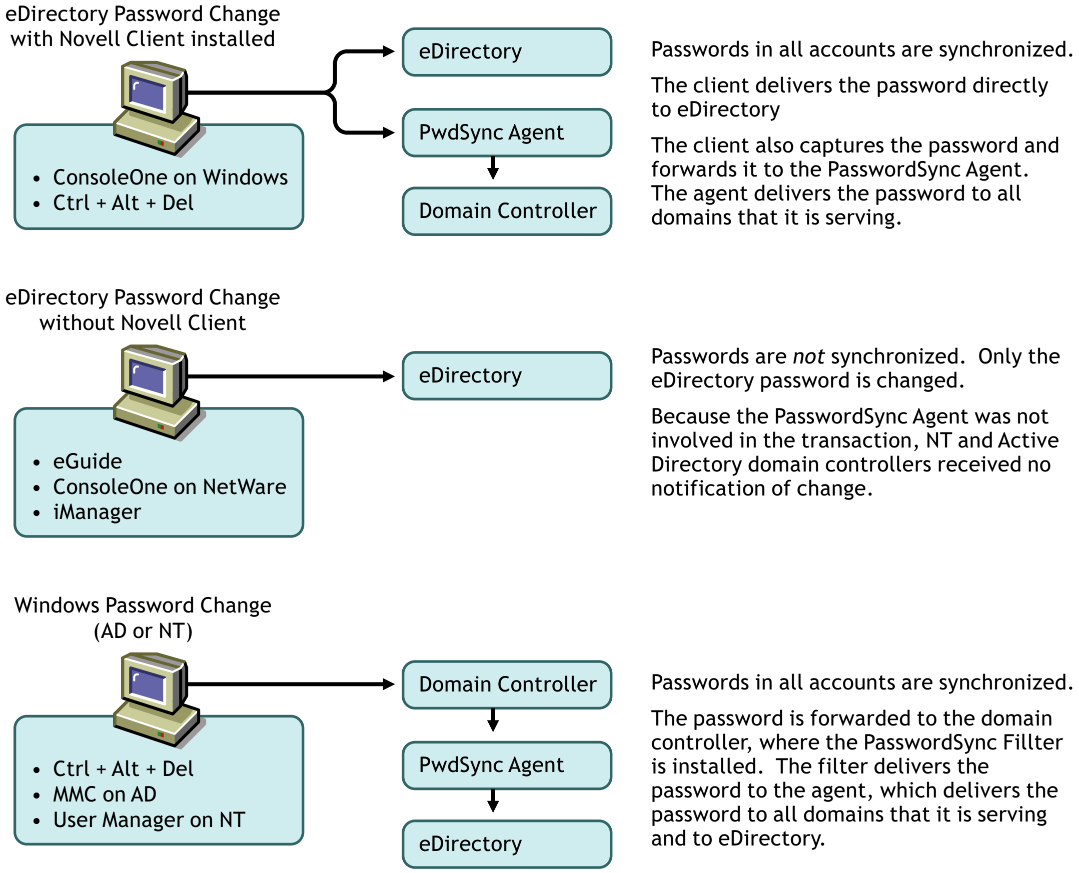
To keep passwords synchronized when your network changes, you might need to make changes to your PasswordSync configuration. For example, if you add a domain controller, you must install a PasswordSync Filter on that domain controller.

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 16 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.

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 to a fully licensed state.

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 NetWare 6.5. This license includes the activation of the DirXML engine and the drivers for 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 includes the activation of a single driver and the DirXML engine.
- You purchase a license to use a non-Novell driver. This includes the activation of a 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 71.

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

When you purchase NetWare 6.5, you recieve a customer ID. If you received the RedBox product, the ID is ?? If you downloaded the product, the

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 will use your Customer ID to generate a Product Activation Request in Novell iManager. 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 Wizard.
3. Browse to the driver set where you want the driver to be activated > click Next.
4. 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.
5. Enter your Novell Customer ID > 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.
6. Copy the Activation Request file into the text area to the clipboard > click Next.

   You will need to paste the contents of this file in a text area at the Novell Product Activator Web site.

   IMPORTANT: Do not edit the content of the Product Activation Request.
7. Click the hyperlink to launch the Novell Product Activator Web site (http://www.novell.com/activator).

   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 Activator Web site (http://www.novell.com/activator). For information, see "Submitting an Activation Request" on page 70.

Submitting an Activation Request

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

1. Log in at the Product Product Activator Web site (http://www.novell.com/activator).

   You must have an eLogin account to access the Product Activator Web site. If you don't already have an eLogin account, you can create this free account when you visit the Product Activator site.
2. 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.

3 Click Submit.

4 Mark the product you are activating.

All the DirXML products that you have purchased are listed. You can activate only one product at a time. Mark the product you are currently activating. If you need to activate any of the other products listed, submit the Product Activation Request again.

5 Click Submit.

Novell generates a Product Activation Credential based on the Product Activation Request you submitted and sends that credential to you via 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 file to your clipboard.

  IMPORTANT: Do not edit the contents of the Product Activation Credential file.

3 Open iManager.

4 Choose DirXML Management > Activation Installation Wizard.

5 Select the driver set or browse to a driver set > click Next.

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.

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, but you can use the same Product Activation Credential to activate each driver set (in the same tree that corresponds to your acquired license). Make sure you install the Product Activation Credential on the same tree where you generated the Product Activation Request.

Viewing Product Activations for DirXML and DirXML Drivers

For each of your DirXML license purchases, you can see the Product Activations you have installed for those licenses. To view Product Activations:

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 activations display on this page. You can view the activation text or, if the activation reports an error, remove an invalid activation from DirXML or from any driver.

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.