

Novell Identity Manager Driver for Legacy NDS®

1.0

www.novell.com

IMPLEMENTATION GUIDE

October 21, 2005



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.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to www.novell.com/info/exports/ for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2005 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.novell.com/company/legal/patents/> and one or more additional patents or pending patent applications in the U.S. and in other countries.

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

www.novell.com

Identity Manager Driver for Legacy NDS: Implementation Guide

[October 19, 2005](#)

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

Novell Trademarks

eDirectory is a trademark of Novell, Inc.

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

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

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

NetWare Loadable Module is a trademark of Novell, Inc.

NLM is a trademark of Novell, Inc.

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

Third-Party Materials

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

Contents

- About This Guide** **7**

- 1 Overview** **9**
 - Key Terms 9
 - Identity Manager 9
 - DirXML Engine 9
 - NDS Driver 9
 - Driver Shim 10
 - Driver Agent. 10
 - Subscriber and Publisher Channels 11
 - Filter. 11
 - Base Container 12
 - Associations. 12
 - SSL Configuration 12
 - Using Rules. 13

- 2 Configuring SSL** **15**
 - Configuring SSL on NDS Platforms 15
 - Configuring SSL on eDirectory Platforms. 16
 - Create a Keystore File 16
 - Store the Certificate. 18
 - View the *ndsagent* Keystore 18

- 3 Installing the Identity Manager Driver for Legacy NDS** **19**
 - Supported NDS Platforms 19
 - Supported NDS Versions. 19
 - Installation Prerequisites 20
 - Installing the NDS Driver Shim 20
 - Installing on Windows, Linux, Solarix, AIX, or NetWare 6.x. 20
 - Installing the Driver Agent 23
 - Activating the Driver 24

- 4 Configuring the Identity Manager Driver for Legacy NDS** **25**
 - Configuring the NDS Agent. 25
 - Configuring the NDS Agent without SSL 25
 - Configuring the NDS Agent with SSL. 25
 - Configuring the Driver 26
 - Adding the NDS Driver 26
 - Configuring Driver Startup 29
 - Starting or Stopping the Driver 30
 - Starting or Stopping the NDS Agent 30

- 5 Troubleshooting Common Problems** **31**
 - Troubleshooting 31
 - Error Codes. 31

- A Documentation Updates** **33**
 - October 21, 2005. 33

About This Guide

- ◆ Chapter 1, “Overview,” on page 9
- ◆ Chapter 2, “Configuring SSL,” on page 15
- ◆ Chapter 3, “Installing the Identity Manager Driver for Legacy NDS,” on page 19
- ◆ Chapter 4, “Configuring the Identity Manager Driver for Legacy NDS,” on page 25
- ◆ Chapter 5, “Troubleshooting Common Problems,” on page 31

Audience

This guide is for Novell® eDirectory™ and Identity Manager administrators who are using the Identity Manager Driver for Legacy NDS®.

Feedback

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

Documentation Updates

For the most recent version of this document, see the [Novell documentation Web site \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Additional Documentation

For documentation on using Identity Manager and the other Identity Manager drivers, see Identity Manager documentation on the [Novell Web site \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Documentation Conventions

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

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

1

Overview

The Identity Manager Driver for Legacy NDS[®] is designed for bidirectional synchronization of data between eDirectory[™] and NDS servers. The driver allows you to integrate NDS servers with cross-platform eDirectory.

The driver provides the following:

- ◆ Bidirectional synchronization of Create, Modify, Delete, Move, and Rename events for user and group accounts between eDirectory and NDS.
- ◆ Bidirectional synchronization of Create, Modify, and Delete events for containers between eDirectory and NDS.

Rename and Move operations are not supported on Container objects. We strongly recommend that you do not use the Rename and Move operations on Container objects because the synchronization of the objects under the Container object fails.

- ◆ Bidirectional synchronization of user passwords between eDirectory and NDS.
- ◆ Migration and resynchronization between NDS and eDirectory.

Key Terms

Identity Manager

Novell[®] Identity Manager is a service that synchronizes data among servers by using a robust set of configurable policies. Identity Manager uses eDirectory to store shared information, and uses the DirXML[®] engine for policy-based management of the information as it changes in eDirectory.

DirXML Engine

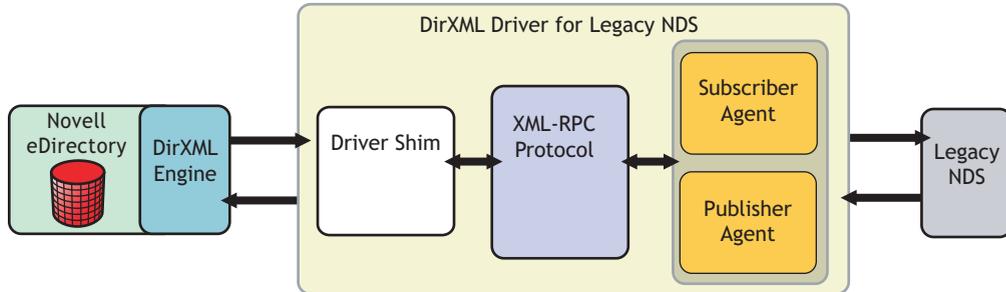
The DirXML engine is the core server that implements the event management and policies of Identity Manager. The engine runs on the Java^{*} Virtual Machine in eDirectory.

NDS Driver

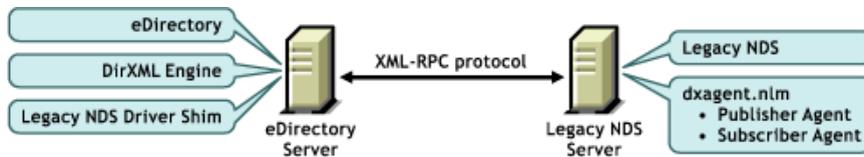
The NDS driver implements the data sharing policy. You control the driver's actions by using iManager to define the filters and policy. The following figure illustrates the NDS driver icon in iManager.



The following figure illustrates the driver's components.



As the following figure illustrates, the driver shim runs on an eDirectory server. The Subscriber Agent and Publisher Agent reside in dxagent.nlm, a driver agent that runs on the NetWare® 4.x or NetWare 5.x server. The driver shim communicates with the driver agent (Publisher Agent and Subscriber Agent) by using the XML-RPC protocol.



Driver Shim

The NDS driver contains a driver shim. The shim converts the XML-based Identity Manager command and event language (XDS) to the protocols and API calls needed to interact with the NDS driver agent. The shim is called to execute commands on the driver agent after the Output Transform has been run.

Commands are usually generated on the Subscriber channel, but can be generated by command write-back on the Publisher channel. The driver agent captures events from NDS on the NetWare server and passes them to the Input Transform of Identity Manager.

The shim for NDS is called LegacyNDSDriverShim.jar. It is implemented in Java.

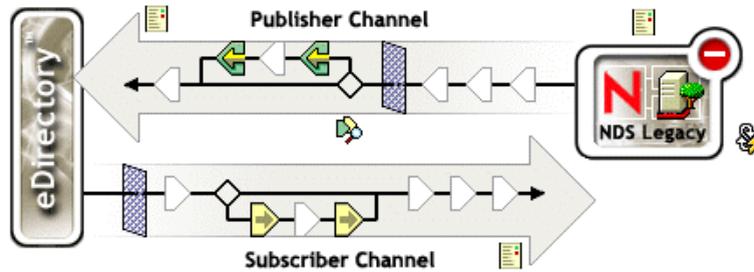
Driver Agent

The driver agent is a NetWare Loadable Module™, dxagent.nlm, which runs on the NetWare server. It is implemented in C.

WARNING: Do not run dxagent.nlm with NDS maintenance tools (for example, dsrepair.nlm or dsmerge.nlm). Before running these tools, unload dxagent.nlm.

Subscriber and Publisher Channels

The driver interfaces with Identity Manager and NDS by using two channels: the Publisher channel and the Subscriber channel.



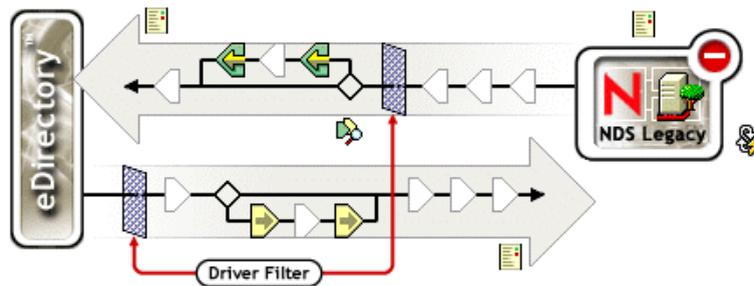
The `dxagent.nlm` captures the events of the NDS system and temporarily places them in a cache file (`sys:/netware/dxagent. tao`). `NotesDriverShim.jar` periodically requests the data from this cache file, based on a polling interval, pushes the changes through the transformation Publisher channel, and then updates eDirectory.

The Subscriber channel receives events from eDirectory and then updates NDS.

The updates are events related to the following:

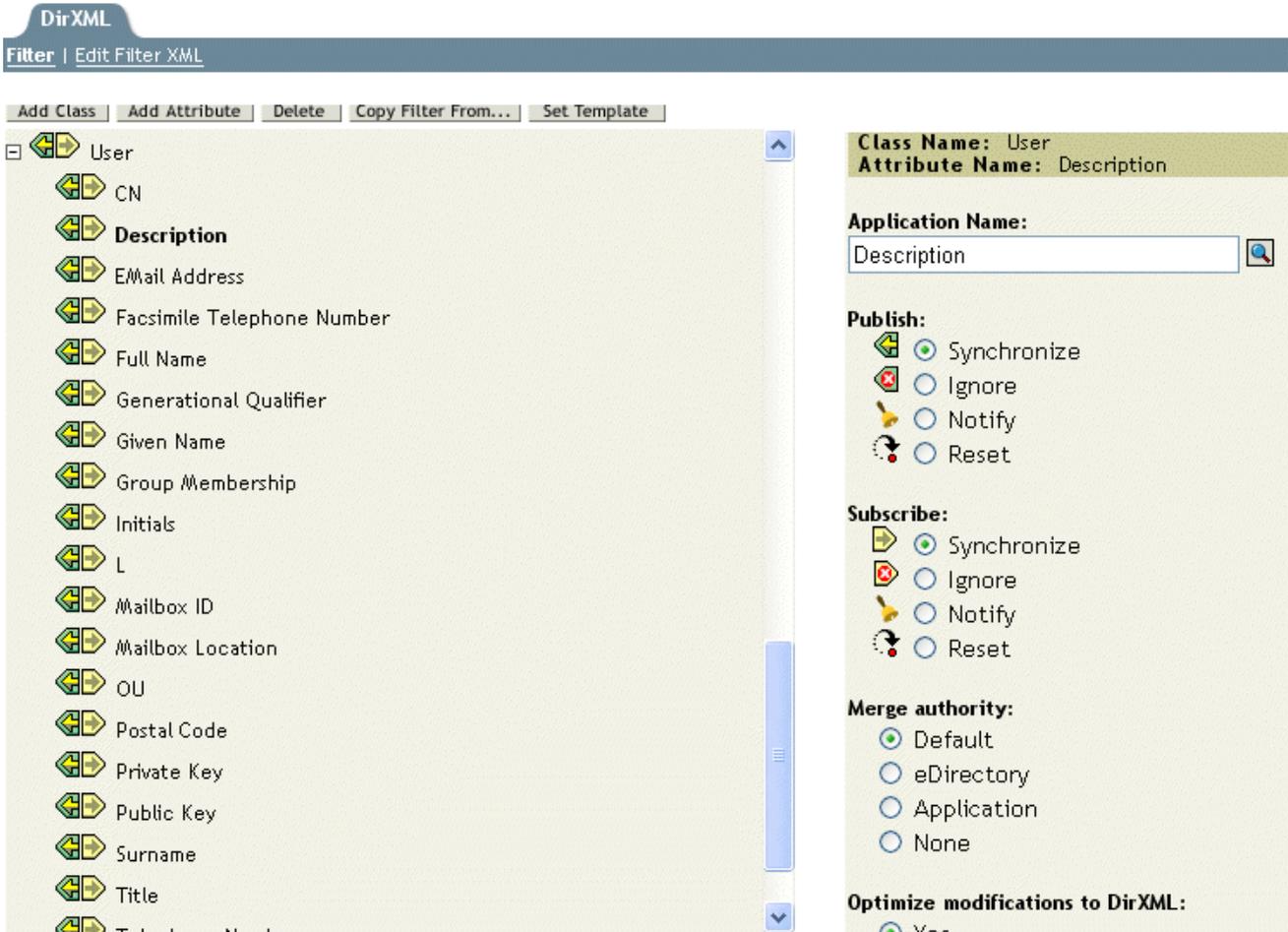
- ♦ Adding, modifying, deleting, renaming, and moving objects in eDirectory
- ♦ Changing passwords
- ♦ Migration and resynchronization of objects based on the search criteria

Filter



The filters on the Publisher and Subscriber channels are used to control the data changes that eDirectory sends to NDS or changes that NDS sends to eDirectory.

The driver filter represents the default classes and attributes that the driver is configured to use. The following figure illustrates attributes found in the User class:



Base Container

A base container is a starting-point container in a directory tree. For example, when you select or specify a base container for synchronization, the base container and all containers below it are synchronized.

Associations

The driver uses the DN of the NDS object to create an association in eDirectory. When the DN of an object is modified in NDS, the association of this object is modified in eDirectory.

SSL Configuration

The Identity Manager Driver for Legacy NDS optionally uses a secure channel for communication. The driver supports SSL to provide secure network connection. The driver uses OpenSSL on NDS platforms and pure Java SSL on eDirectory platforms for secure connection. See [Chapter 2, “Configuring SSL,” on page 15](#) and [“Configuring the NDS Agent with SSL” on page 25](#).

Using Rules

The NDS driver uses the following policies:

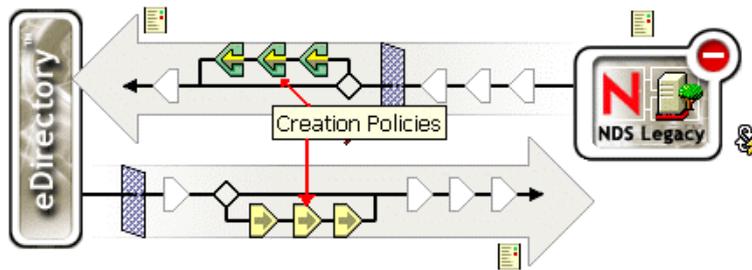
- ◆ Creation
- ◆ Matching
- ◆ Placement

These rules apply to the configuration type (Mirrored, Flat, or Department) that you select.

Usage of the Creation, Matching, and Placement policies varies, depending on the configuration. After you install the driver, you can view the policy sets and edit these policies by clicking the icons for each policy set. The following figure illustrates icons for the Creation policies:

DirXML Driver Overview

Driver: LegacyNDS.hraun_set.Delgna

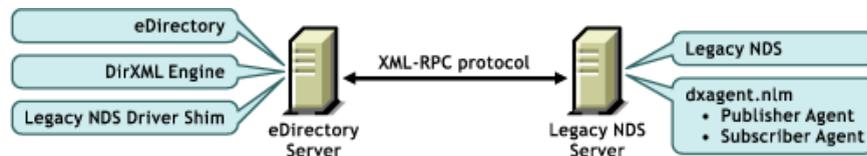


2 Configuring SSL

- ♦ “Configuring SSL on NDS Platforms” on page 15
- ♦ “Configuring SSL on eDirectory Platforms” on page 16

Configuring SSL on NDS Platforms

The Identity Manager Driver for Legacy NDS[®] supports the Secure Sockets Layer (SSL) protocol. The XML-RPC protocol can be an SSL connection.



If you want an SSL connection, configure SSL on both the NDS and eDirectory™ platforms.

NOTE: Ensure that you use the same eDirectory tree CA to configure SSL on both the NDS and eDirectory platforms.

- 1** On a machine that has OpenSSL, generate the private key and the Certificate Signing Request (CSR) by executing the following command:

```
openssl req -new -keyout key.pem -out csrreq.pem -days 365
```

- 2** Follow the prompts to generate the key.pem file and the csrreq.pem file.

The PEM passphrase refers to the password of the private key that is to be used while configuring the NDS agent in [Step 4 on page 25](#).

The key.pem file contains the private key. The csrreq.pem file contains the CSR.

- 3** Transfer the csrreq.pem file to the system that has eDirectory installed.
- 4** Have the CSR signed by eDirectory:
 - 4a** In iManager, log in to eDirectory as an administrator with the appropriate rights.
 - 4b** From the Roles and Tasks menu, click Novell Certificate Server > Issue Certificate.
 - 4c** Specify the path to the csrreq.pem file, or browse to select it, then click Next.
 - 4d** Select SSL or TLS as the key type, then click Next.
 - 4e** Verify the certificate parameters, then click Next.
 - 4f** Select File in Base64 format as the file format to which the certificate is to be saved.
 - 4g** Click Next to view the parameters of the issued certificate.

4h Click Download the Issued Certificate as Pubkey.pem, then specify the path to which the certificate is to be saved.

4i Click Close.

The file that you saved is the public key certificate file.

5 Export the self-signed certificate of the eDirectory CA as rootcert.pem.

5a To open the Modify Object page, from the Roles and Tasks menu, click eDirectory Administration > Modify Object.

5b Use the Object selector icon to browse to the Organizational CA, then click OK.

The Organizational CA is present under the Security container at the top level of the tree.

5c Select the Certificates tab and then select Self Signed Certificate.

5d Click Export.

5e When you are prompted to export the private key along with the certificate, select No, then click Next

5f Select File in Base64 format as the file format to which the certificate is to be saved, then click Next.

5g Save the issued certificate as rootcert.pem by clicking Save the Exported Certificate to a File.

This is the root certificate file.

6 Transfer the private key file (key.pem), public key certificate file (pubkey.pem), and the root certificate file (rootcert.pem) to the NDS machine.

The private key and public key are in pem format.

Configuring SSL on eDirectory Platforms

Prerequisite

- ♦ Java 1.3 or later

Create a Keystore File

To configure SSL on eDirectory, create a keystore file:

1 Export the eDirectory CA trusted root certificate.

1a From the Roles and Tasks menu, click eDirectory Administration > Modify Object to open the Modify Object page.

1b Use the Object selector icon to browse to the Organizational CA, then click OK.

The Organizational CA is present under the Security container at the top level of the tree.

1c Select the Certificates tab, then select Self Signed Certificate.

1d Click Export.

1e When you are prompted to export the private key along with the certificate, select No, then click Next.

1f Select File in Base64 format as the file format to which the certificate is to be saved, then click Next.

1g Click Save the Exported Certificate to a File to save the issued certificate as *NOVELLCASELFSIGNEDCERT.B64*.

2 Import this certificate into the Java trusted-certificate keystore by executing the following command:

```
java-home/jre/bin/keytool -import -alias novellca -file  
NOVELLCASELFSIGNEDCERT.B64 -keystore java-home/jre/lib/  
security/cacerts -storepass changeit
```

The Java keytool comes with the Java installation. You use the keytool to build a keystore file, which contains encrypted passwords.

3 Type Yes when prompted to trust a certificate.

4 Import the exported certificate into a new keystore file by executing the following command:

```
java-home/jre/bin/keytool -import -alias novellca -file  
NOVELLCASELFSIGNEDCERT.B64 -keystore java-home/jre/lib/  
security/ndsagentcert -storepass novell1
```

java-home/jre/lib/security/ndsagentcert is referred as the client's keystore in the subsequent steps.

5 When prompted to trust a certificate, type Yes.

6 Generate the public and private key pair for the agent in the client's keystore file by executing the following command:

```
java-home/jre/bin/keytool -genkey -alias ndsagent -keyalg RSA  
-dname "CN=137.65.146.24, OU=DirXML, O=Novell, L=Provo, S=Utah,  
C=US" -keypass novell1 -keystore javahome/jre/lib/security/  
ndsagentcert -storepass novell1
```

NOTE: The keypass and storepass must be the same.

7 Generate a Certificate Signing Request (CSR) in the *novellagent.csr* file.

To guarantee the identity of the client, a certificate is needed to authenticate the key pair ownership. To do this, generate a Certificate Signing Request (CSR) in the *novellagent.csr* file by executing the following command:

```
java-home/jre/bin/keytool -certreq -alias ndsagent -file  
novellagent.csr -keypass novell1 -keystore javahome/jre/lib/  
security/ndsagentcert -storepass novell1
```

8 In iManager, log in to eDirectory as an administrator with the appropriate rights.

9 From the Roles and Tasks menu, click Novell Certificate Server > Issue Certificate.

10 Enter *novellagent.csr* as the filename or browse to select it, then click Next.

11 Select SSL or TLS as the key type, then click Next.

12 Verify the certificate parameters, then click Next.

13 Select File in Binary DER Format as the file format to which the certificate is to be saved.

14 Click Next to view the parameters of the issued certificate.

15 Click Download the Issued Certificate, save the certificate as *issuedcertificate.der*, then click Close.

Store the Certificate

The certificate now needs to be stored in the *ndsagentcert* keystore with the key pair.

- 1 Execute the following command:

```
java-home/jre/bin/keytool -import -trustcacerts -alias  
ndsagent -file ISSUEDCERTIFICATE.DER -keypass novell1 -keystore  
java-home/jre/lib/security/ndsagentcert -storepass novell1
```

- 2 When prompted to trust a certificate, type Yes.

At this point, your *ndsagentcert* keystore consists of the client's CA selfsigned certificate and your key, and a Certificate Authority has signed it.

View the *ndsagent* Keystore

The file should contain at least two entries, which are keys. It might also contain objects.

Your key entry should show "Certificate chain length: 2". The first certificate is your key; the second certificate is the CA that signed it.

```
java-home/jre/bin/keytool -list -v -keystore java-home/jre/lib/  
security/ndsagentcert -storepass novell1
```

NOTE: *Ndsagentcert* is the keystore file that is to be used with a full directory path while configuring SSL for the driver.

3

Installing the Identity Manager Driver for Legacy NDS

The Identity Manager Driver for Legacy NDS[®] runs on NetWare[®], Windows*, Linux*, Solaris*, and AIX*.

- ♦ [“Supported NDS Platforms” on page 19](#)
- ♦ [“Installation Prerequisites” on page 20](#)
- ♦ [“Installing the NDS Driver Shim” on page 20](#)
- ♦ [“Activating the Driver” on page 24](#)

Supported NDS Platforms

- ♦ NetWare 4.11 with Support Pack 9 or later
- ♦ NetWare 4.2 with Support Pack 9 or later
- ♦ NetWare 5.0 with Support Pack 6a or later
- ♦ NetWare 5.1 with Support Pack 7 or later
- ♦ NDS 6.21 on NetWare 4.x
- ♦ NDS 7.62c or later (but not eDirectory™ version 8) on NetWare 5.x

You can install the Legacy NDS driver shim into any environment where Identity Manager 2 and the DirXML[®] engine are installed.

The Legacy NDS driver doesn't support Universal Password functionality. The driver can synchronize the key pairs but not the Universal Password.

The driver supports Publisher channel synchronization only from the local replica (master replica) on which the driver agent is installed.

Supported NDS Versions

- ♦ NDS 6.21 or later on NetWare 4.x
- ♦ NDS 7.62c or later (but not eDirectory version 8) on NetWare 5.x

Installation Prerequisites

- ◆ Identity Manager 2
- ◆ DSLOADFX patch

This patch is for NetWare 4.x only. You can load this patch by executing the command

```
pmload dsloadfx
```

- ◆ Winsock files on NDS platforms

Installing the NDS Driver Shim

WARNING: Do not run dxagent.nlm with NDS maintenance tools (for example, dsrepair.nlm or dsmerge.nlm). Before running these tools, unload dxagent.nlm.

The driver installation consists of:

- ◆ Installing the driver shim on the Novell® eDirectory platform.
- ◆ Installing the Agent on the NDS platform.

The installation file (NDSInst.zip or NDSInst.jar) includes the following files:

General Files

- ◆ LegacyNDS.xml
- ◆ A license file (for example, dirxmllicense.txt or dirxmllicense_fr.txt)
- ◆ dxagent.cfg
- ◆ LegacyNDSDriverShim.jar
- ◆ Readme.html

NetWare 4 Files

- ◆ dsloadfx.nlm
- ◆ dxagent.nlm

NetWare 5 Files

- ◆ dxagent.nlm

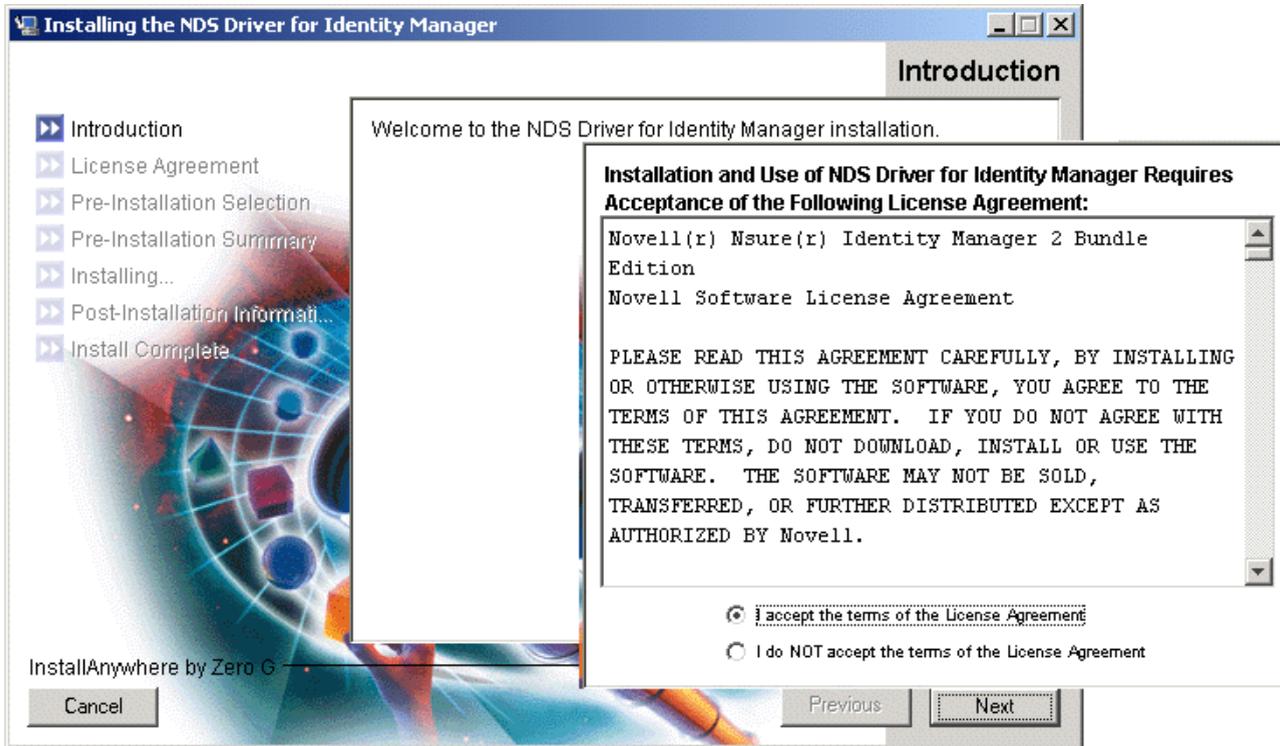
Installing on Windows, Linux, Solarix, AIX, or NetWare 6.x

- 1 Run the installation program from the Identity Manger download image or CD.

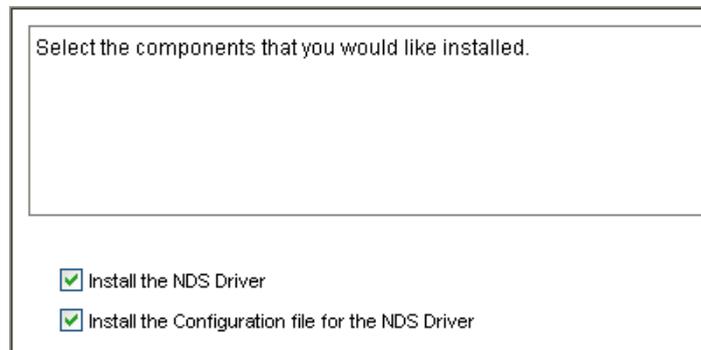
| Platform | Installation Program |
|-------------|------------------------|
| Windows | NDSInstall_Windows.exe |
| Linux | NDSInstall_Linux.bin |
| Solaris | NDSInstall_Solaris.bin |
| AIX | NDSInstall_AIX.bin |
| NetWare 6.x | NDSInstall_NetWare.jar |

Downloads are available from the [Novell download Web site \(http://download.novell.com/index.jsp\)](http://download.novell.com/index.jsp).

- 2 View the Welcome (Introduction) page, then accept the license agreement.



- 3 Select whether to install the NDS driver, the driver configuration file, or both.



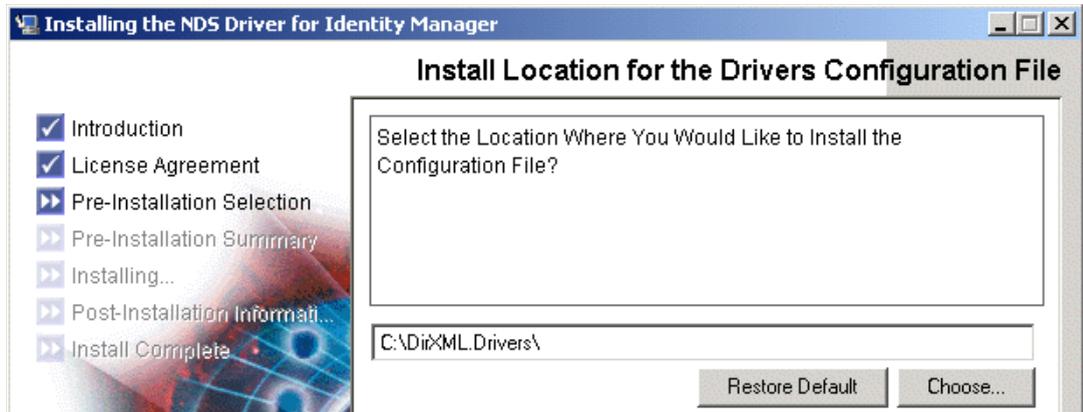
If you are installing on a server, select to install the NDS driver and the configuration file.

If you are installing on a connected system, select to install the NDS driver.

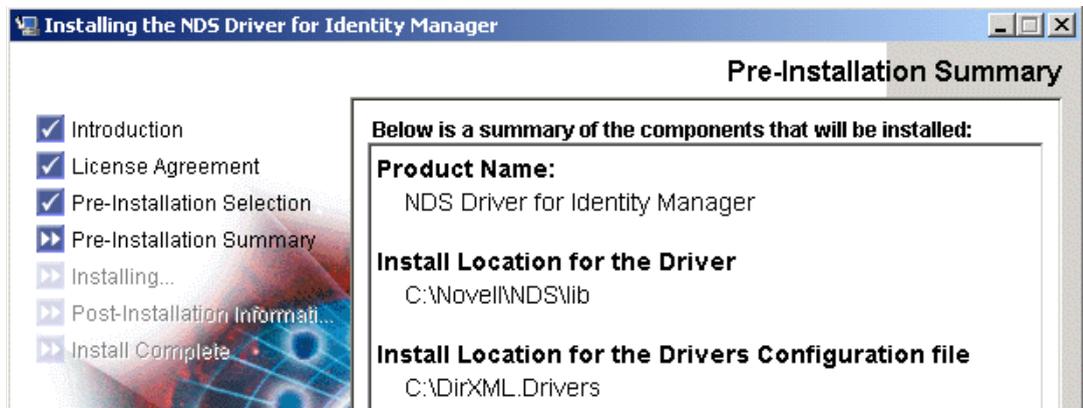
- 4 Select or create a path for installing the driver.

For example, type `/usr/lib/dirxml/classes` for Linux, or select `c:\novell\nds\lib` for Windows.

- 5 Select a path for installing the sample configuration file.



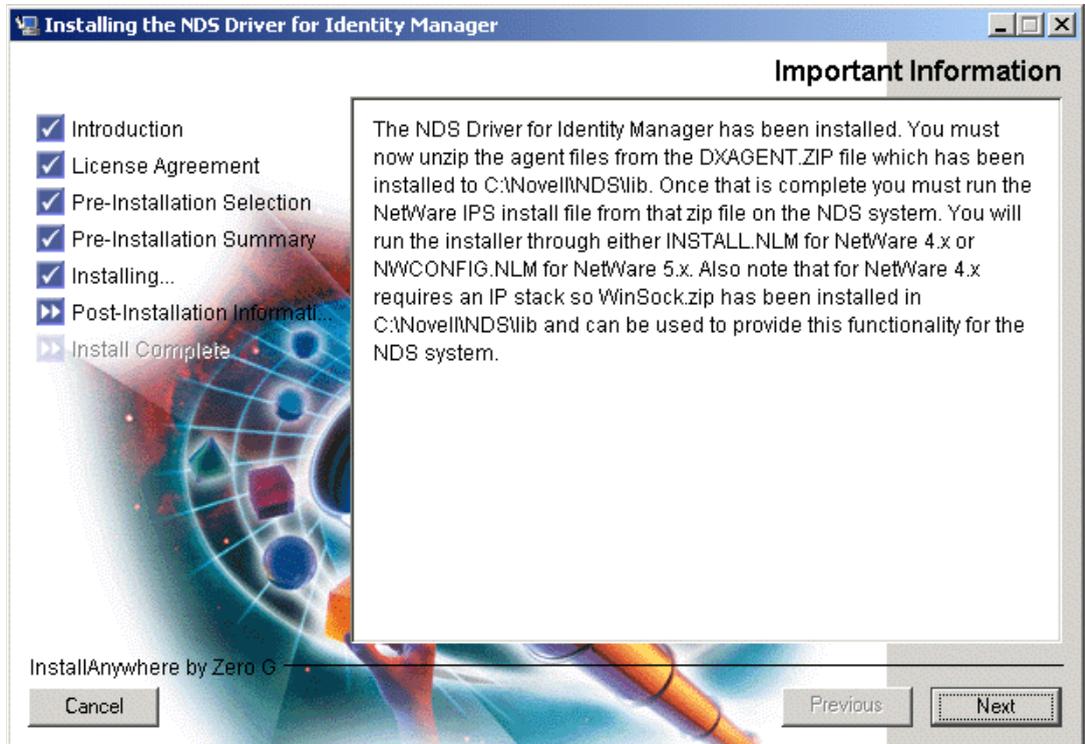
6 Review components that you selected.



7 Click Install.

8 Review post-install information.

The installation program installs the NDS Agent component (dxagent.nlm) in a .zip file. Follow the prompts to install the components. See [“Installing the Driver Agent” on page 23](#).



- 9** Select to restart eDirectory, then click Next.

eDirectory can't recognize the Driver for Legacy NDS until eDirectory is restarted. Of course, you can select No, then restart eDirectory later.

- 10** Click Done.

Installing the Driver Agent

- 1** On the NetWare 4.x or Netware 5.x server where you want to install the NDS driver agent, unzip the agent files from the dxagent.zip file.
- 2** Run the NDSInst.ips install.

| Platform | Task |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------|
| NetWare 4.x | Use install.nlm. Ensure that the server has an IP stack. You can use c:\novell\nds\lib\WinSock.zip to provide this functionality. |
| NetWare 5.x | Use nwconfig.nlm. |

Activating the Driver

The Identity Manager Driver for Legacy NDS must be activated within 90 days of installation. Otherwise, it will shut down.

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

4

Configuring the Identity Manager Driver for Legacy NDS

- ◆ [“Configuring the NDS Agent” on page 25](#)
- ◆ [“Configuring the Driver” on page 26](#)
- ◆ [“Starting or Stopping the Driver” on page 30](#)
- ◆ [“Starting or Stopping the NDS Agent” on page 30](#)

Configuring the NDS Agent

The driver configuration consists of:

- ◆ Configuring the agent on the NDS[®] platform.
- ◆ Configuring the driver on an eDirectory[™] platform.

IMPORTANT: Password Synchronization is not supported if SSL is not configured.

To configure the agent, edit the `sys:\etc\dxagent.cfg` file. This file contains information about the port that the agent starts listening on and also information about the SSL configuration (optional).

Lines starting with the `#` character are ignored.

- ◆ [“Configuring the NDS Agent without SSL” on page 25](#)
- ◆ [“Configuring the NDS Agent with SSL” on page 25](#)

Configuring the NDS Agent without SSL

To configure the agent on NDS platforms, edit the `dxagent.cfg` file to specify the port on which the NDS agent starts listening.

Configuring the NDS Agent with SSL

To configure the agent on NDS platforms, edit the `dxagent.cfg` file to specify the following:

- 1** Specify the port on which the NDS agent starts listening.
- 2** Specify the path to the root certificate file.
- 3** Specify the path to the private key file.
- 4** Specify the password of the private key file.
- 5** Specify the format of the private key.
- 6** Specify the path to the public key certificate file.
- 7** Specify the format of the public key.

NOTE: For more information on obtaining the above specified files, refer to [“Configuring SSL on NDS Platforms” on page 15](#).

Configuring the Driver

In this section:

- ◆ “Adding the NDS Driver” on page 26
- ◆ “Configuring Driver Startup” on page 29

Adding the NDS Driver

Novell® provides a sample configuration file (LegacyNDS.xml). You can use this file to add the NDS driver to your driver set.

- 1 In Novell iManager, select DirXML Utilities > Overview.
- 2 Browse to and select the driver set, then click Search.
- 3 Click Add Driver, select In an Existing Driver Set, then click Next.
- 4 Click Import a Driver Configuration from the Client (.XML File), browse to and select the LegacyNDS.xml file, then click Next.

Import or create a new Application Driver for this driver set.

- Import a driver configuration from the server (.XML file)

ActiveDirectory.xml

- Import a driver configuration from the client (.XML file)

File:

- Create a new driver

Name:

<< Back

Next >>

Cancel

Finish

- 5 Name the driver, specify user account information, and provide information about the NDS system.

The wizard provides help so that you can set these parameters.

- 6 Configure data flow.

The Data Flow setting controls whether the Publisher channel filter and the Subscriber channel filter are synchronized or ignored. The setting determines whether data flows from both NDS and eDirectory™ or either NDS or eDirectory. The Data Flow settings use policies to control the flow of data.

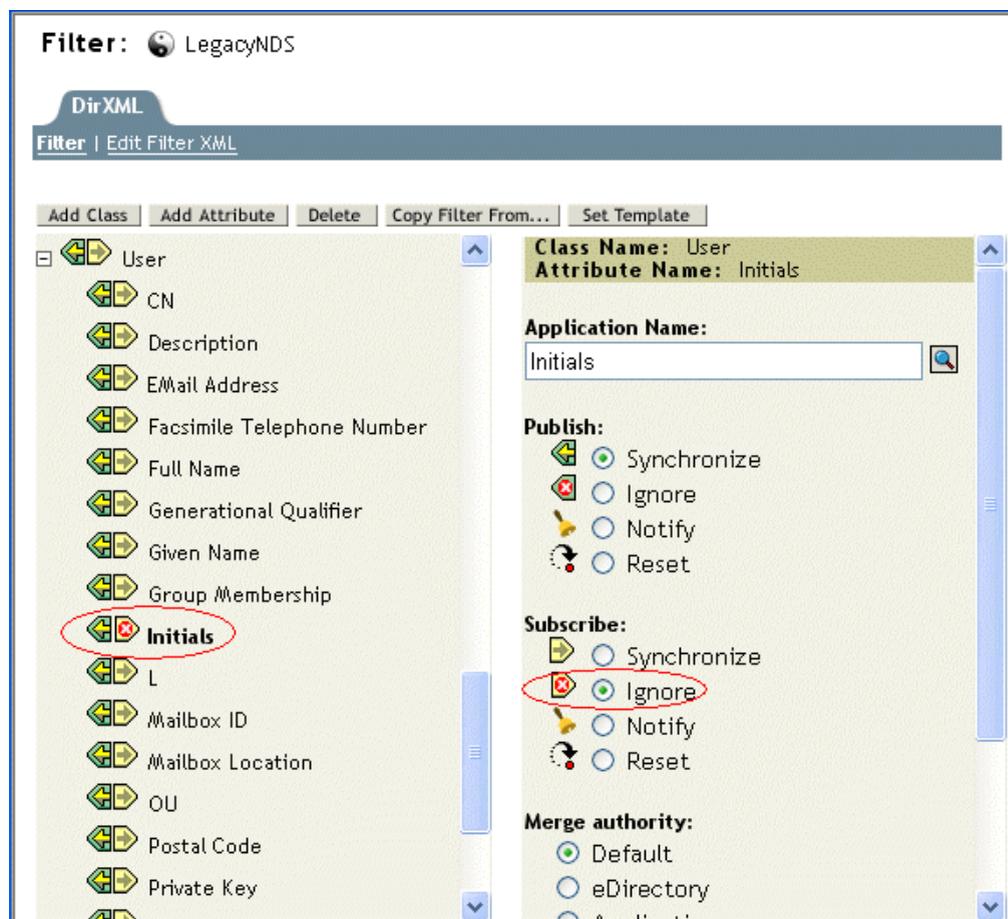
Configure Data Flow:

Bi-directional

Bi-directional
Authoritative
Subordinate

| Data Flow Setting | Description |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bi-directional | Typically, both the Legacy NDS tree and eDirectory are authoritative sources. The Publisher and Subscriber channels fully synchronize objects and attributes. |
| Authoritative | The NDS tree is the authoritative source. Only the Publisher channel (NDS) synchronizes objects and attributes. The Subscriber filter is empty. |
| Subordinate | eDirectory is the authoritative source. Only the Subscriber channel (eDirectory) synchronizes attributes. The Publisher filter is empty. |

The following figure illustrates filter settings. In this example, all attributes except Initials are set for bidirectional data flow. On the Initials attribute, the Publisher channel synchronizes data. Because the Subscriber channel is set to Ignore, NDS is the authoritative source.



7 Select how to place synchronized objects.

Configuration Option:



- ◆ **Mirrored:** Synchronizes objects hierarchically between the NDS tree and eDirectory.
This option in the driver configuration synchronizes User, Group, Organization, Country, and Organizational Unit objects. It also mirrors the structure of a subtree in another tree.
When new User objects are created in one directory, they are placed in the matching hierarchical level of the mirrored container in the other directory.
The Mirrored option doesn't require a Create rule.
- ◆ **Flat:** Synchronizes User and Group objects into specific containers.
Regardless of where synchronization begins or where objects appear in the NDS tree, this option places all users in one container and all groups in another container in eDirectory. A similar process occurs from eDirectory to the NDS tree. The user and group containers are the same in both the NDS tree and eDirectory.
With this configuration, you must specify a container for User objects (to hold all new User objects) and a separate container for Group objects (to hold all new Group objects). This option doesn't create the containers that hold the users and groups. You must create the containers manually.
Any changes in a user or group container in one system appear in the user or group container in the other system. The Placement policy places the objects and makes changes appropriately.
The Create rule for the Flat option requires users to have a given name and a surname, so that users are unique when they appear in the other system.
- ◆ **Department:** Synchronizes users and groups by department (OU).
This option synchronizes User and Group objects and places all users and groups in a container based on the Department field in your management console.
On either side, you define a container where all User objects are placed. You also define a department that the users belong to.
A department (OU) attribute must already exist in the appropriate base container.
This option doesn't create the containers for each department. You must create the containers manually. There must be the same as the container specified when you add or import the driver.
The Create rule for the Department option requires a given name, surname, and OU.

Scenario: Using Department Containers

At the DigitalAirlines company, a Department container exists in the NDS tree. The network administrator has created (in the Department container) subdirectories named after departments that people belong to: R&D, Marketing, Corporate Sales, and Human Resources. Upon creating a user, the administrator assigns the user to a department name. Through the NDS driver, the Department attribute is created in the correct container in eDirectory.

- 8 Configure the base container, remote base container, Publisher channel, and (optionally) the keystore file and password.

| Parameter | Description |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Base Container | Specifies the container in eDirectory where objects are placed and synchronized. <ul style="list-style-type: none">♦ If using with Mirrored: The local base container to mirror with the remote base container.♦ If using with Flat: The container to place users and groups into.♦ If using with Department: The parent of the departmental containers. |
| Remote Base Container | Specifies the base container for synchronization in NDS. |
| Enable Publisher Channel | Enables or disables the Publisher channel of the driver shim. |
| Keystore File | An optional encrypted file. Required for an SSL connection between the NDS driver shim and dsagent.nlm, but not required otherwise. Specifies a file where SSL client passwords are stored. |
| Keystore Password | Unlocks the keystore file. |

- 9 Click Next, then specify a polling interval.
- 10 (Conditional) If you selected the Flat placement, specify a Local Group Container in eDirectory.

This is the base container for synchronization in eDirectory. Groups are placed here.
- 11 Click Next.
- 12 Define a security-equivalent user.

Click Define Security Equivalences, then browse to and add a user.
- 13 Click Exclude Administrative Roles, then browse to and add a user who is to be excluded from administrative roles.
- 14 Click Next, review settings, then click Finish.

Configuring Driver Startup

- 1 In iManager, select DirXML Management > Overview.
- 2 Select the driver set containing the driver, then click Search.
- 3 Click the driver icon to see the driver overview, then click the driver icon again to display the Modify Object page.
- 4 Click Driver Configuration at the top of the page, then select one of the three options listed under Startup Option.

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

- ♦ **Automatic:** Whenever the DirXML engine starts, the driver starts automatically. After you have configured the driver, you should use this option.

- ♦ **Manual:** Starts the driver manually. This option is often used during driver modification and testing cycles. The engine buffers the changes to be processed when the driver starts.
- ♦ **Disabled:** If you use this option, Identity Manager does not cache events. Data changes made in eDirectory during the time a driver is disabled are not synchronized upon driver startup.

5 Click OK.

For more information, refer to the [DirXML \(Identity Manager\) Administration Guide \(http://www.novell.com/documentation/dirxml20/index.html\)](http://www.novell.com/documentation/dirxml20/index.html).

Starting or Stopping the Driver

1 In iManager, select DirXML Management > Overview.

2 Browse to the driver whose status you want to change.

The status is shown in the top right corner of the driver icon.

3 Click the driver to stop, start, or get the driver's status.

Starting or Stopping the NDS Agent

To start the NDS agent:

1 At the server console prompt, enter

```
load sys:/system/dxagent.nlm sys:/etc/dxagent.cfg
```

To stop the NDS agent:

1 At the server console prompt, enter

```
unload dxagent.nlm
```

5

Troubleshooting Common Problems

This section contains information for troubleshooting common problems you might encounter using the Identity Manager Driver for Legacy NDS[®].

- ♦ “Troubleshooting” on page 31
- ♦ “Error Codes” on page 31

Troubleshooting

- ♦ Ensure that the driver admin DN and the DN used to perform operations on NDS are different.
- ♦ If you make Publisher filter changes, the driver must be restarted for the changes to take effect.

Error Codes

When NDS returns an error code, the driver logs the error code in the status log. For more information, refer to *NDS Error Codes* (http://www.novell.com/documentation/lg/ndsam/errorcodes/list_of_nds_error_codes.htm).

A

Documentation Updates

This section contains new or updated information on installing and managing the Identity Manager Driver for Legacy NDS[®].

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

If you need to know whether a copy of the PDF documentation you are using is the most recent, check the date that the PDF file was published. The date is on the title page.

New or updated documentation was published on the following dates:



October 21, 2005

| Location | Change |
|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| “Supported NDS Platforms” on page 19 | Updated the list of supported platforms. |
| “Installing the NDS Driver Shim” on page 20 | Deleted a topic on installing on NetWare 4.x or Netware 5.x. The necessary information is in “Installing the Driver Agent” on page 23 . |

