Novell Identity Manager Driver for eDirectory™

3.0

www.novell.com

IMPLEMENTATION GUIDE

June 25, 2007

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.

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

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

Novell Trademarks

For a list of Novell trademarks, see Trademarks (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

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

Contents

About This Guide

This guide explains how to install and configure the Identity Manager Driver for eDirectory™.

Audience

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

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. 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 *Identity Manager Driver for eDirectory* in the Identity Manager Drivers section on the Novell Documentation Web site (http://www.novell.com/documentation).

Additional Documentation

For information on Identity Manager and other Identity Manager drivers, see the Novell Documentation Web site (http://www.novell.com/documentation).

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.

Overview

1

The Identity Manager Driver for eDirectory™ synchronizes objects and attributes between different eDirectory trees.

This driver is unique among all other Identity Manager drivers. 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.

For example, the Publisher channel in TreeA communicates with the Subscriber channel in TreeB; and conversely, the Publisher in TreeB communicates with the Subscriber channel in TreeA. Therefore, the installation and configuration of the driver must be completed twice—once for the eDirectory driver in TreeA and once for the driver in TreeB.

For information on what's new in Identity Manager, see "What's New in Identity Manager?" in the *Identity Manager 3.0.1 Installation Guide*.

1.1 Changes in Terminology

The following terms have changed from earlier releases:

Table 1-1 *Changes in Terminology*

Earlier Terms	New Terms
DirXML®	Identity Manager
DirXML Server	Metadirectory server
DirXML engine	Metadirectory engine
eDirectory	Identity Vault (except when referring to eDirectory attributes or classes)

1.2 Key Terms

Driver shim. A Java file (`NdsToNds.jar`) loaded directly by Identity Manager. Communicates event changes to be sent from the Identity Manager Driver for eDirectory to an Identity Vault, communicates changes from the Identity Vault to the Identity Manager Driver for eDirectory, and operates as the link that connects the Identity Vault and the Identity Vault Driver object.

Driver. A set of policies, filters, and objects that act as the connector between an Identity Vault and the driver shim.

This software enables an application to publish events from an application to the directory, enables an application to subscribe to events from the directory, and synchronizes data between the directory and applications.

To establish a connection between the Metadirectory engine and an Identity Vault, you specify the driver's configuration and connection parameters, policies, and filter values.

Driver object. A collection of channels, policies, rules, and filters that connect an application to an Identity Vault that is running Identity Manager.

Each driver performs different tasks. Policies, rules, and filters tell the driver how to manipulate the data to perform those tasks.

The Driver object displays information about the driver's configuration, policies, and filters. This object enables you to manage the driver and provide eDirectory management of the driver shim parameters.

Identity Vault. A hub, with applications and directories publishing their changes to it. The Identity Vault then sends changes to the applications and directories that have subscribed for them. This results in two main flows of data: the Publisher channel and the Subscriber channel.

Installing the Identity Manager Driver for eDirectory

2

2.1 Where to Install the Driver Shim

You install Identity Manager and the eDirectory™ driver shim on both of the Novell® eDirectory servers and in the trees that you want to synchronize. This driver does not use the Remote Loader technology because the driver in one tree communicates directly with the driver in the other tree.

The driver uses Novell Certificate Server™ and a Certificate Authority (CA) to ensure data security. All transactions between trees will be secured through SSL technology. For information on data security, see Section 4.2, “Configuring Secure Identity Manager Data Transfers,” on page 25.

2.2 Driver Prerequisites

- ❑ Requirements for Identity Manager. See the *Identity Manager 3.0.1 Installation Guide*.
- ❑ The Novell Certificate Server running on each server that hosts the eDirectory driver.
- ❑ A Certificate Authority (CA) so that SSL encryption can work.

2.3 Upgrading to Identity Manager 3

During an Identity Manager installation, you can install the Driver for eDirectory (along with other Identity Manager drivers) at the same time that the Metadirectory engine is installed. See the *Identity Manager 3.0.1 Installation Guide*. You can upgrade from DirXML 1.1a or Identity Manager 2 to Identity Manager 3.

2.4 Installing the Driver Shim

You can install the Identity Manager Driver for eDirectory shim (along with other Identity Manager drivers) at the same time that the Metadirectory engine is installed.

You can also install the driver separately, after the Metadirectory engine is installed.This section assumes that you have already installed the Metadirectory engine (and, most likely, other drivers) on the server and need to install the eDirectory driver only.

If you don’t have a CD, download the file that you need for your platform (for example, `Identity_Manager_3_Linux_NW_Win.iso`) and create one. Downloads are available from Novell Downloads (http://download.novell.com/index.jsp).

IMPORTANT: Because you are installing the driver on two separate Identity Vault (eDirectory) servers, you must complete procedures for each server.

During the installation, `NdsToNds.jar` is copied to the appropriate directory. The following table shows these locations per platform:

Operating System	Directory
Linux*, Solaris*, or AIX*	`/usr/lib/dirxml/classes` (For eDirectory 8.8: `opt/novell/eDirectory/lib/dirxml/classes`)
NetWare®	`sys:system\lib`
Windows* NT*/2000	The default is `novell\nds`, but you can specify any directory.

After the installation program ends, configure security as explained in Section 4.2, "Configuring Secure Identity Manager Data Transfers," on page 25.

2.4.1 Installing to Windows

1. Run the installation program from the Identity Manager CD.

   If the installation program doesn't autolaunch, you can run `\nt\install.exe`.
2. In the Welcome dialog box, click *Next*, then accept the license agreement.
3. In the first Identity Manager Overview dialog box, review the information, then click *Next*.

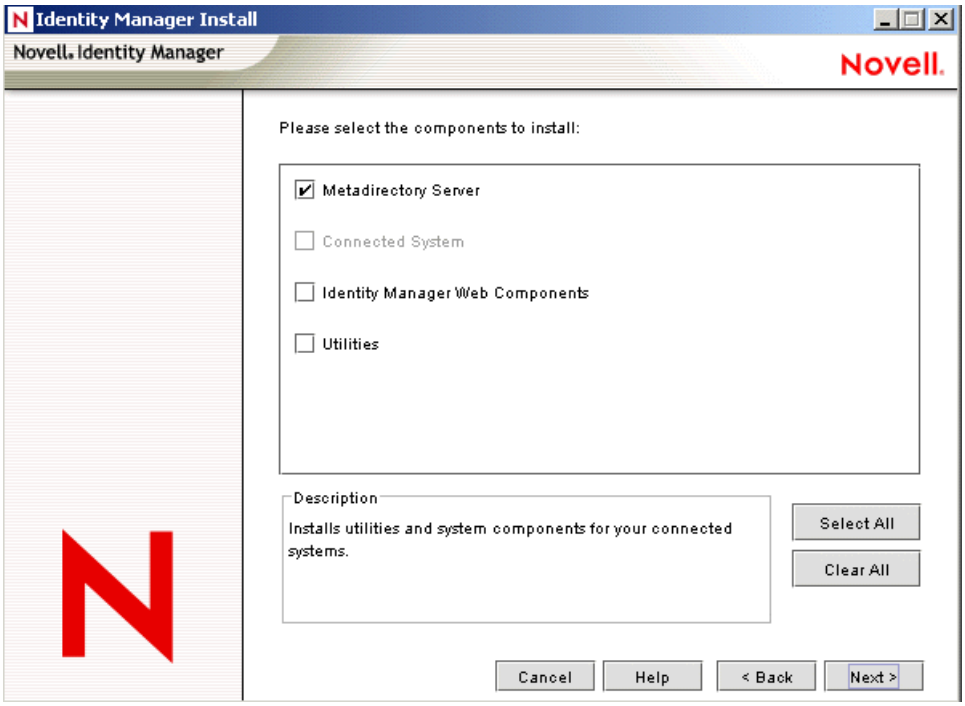
   The dialog box provides information on the following:

   - A Metadirectory server
   - A connected server system
4. In the second Identity Manager Overview dialog box, review information, then click *Next*.

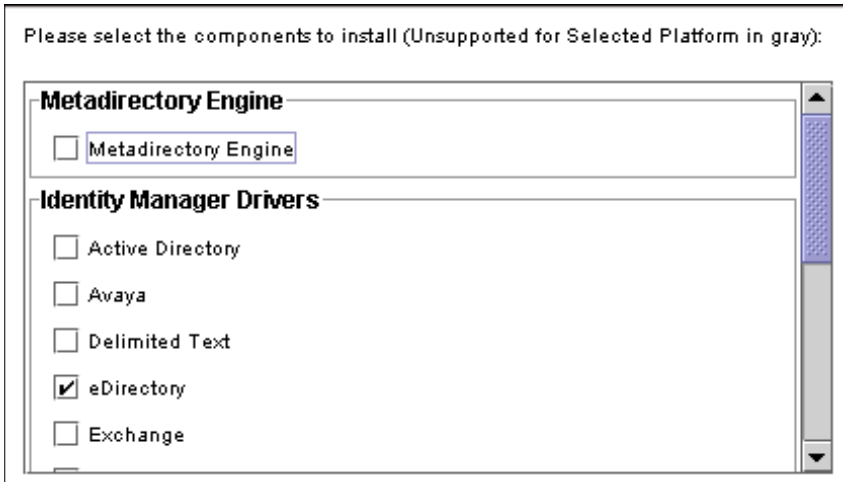
   The dialog box provides information on the following:

   - A Web-based administration server
   - Identity Manager utilities

5 In the Please Select the Components to Install dialog box, select only *Metadirectory Server*, then click *Next*.



6 In the Select Drivers for Engine Install dialog box, select only *eDirectory*, then click *Next*.



7 In the Identity Manager Upgrade Warning dialog box, click *OK*.

8 In the Summary dialog box, review the selected options, then click *Finish*.

9 In the Installation Complete dialog box, click *Close*.

After installation, configure the driver as explained in "Configuring the Driver" on page 31.

2.4.2 Installing to NetWare

1 At the NetWare server, insert the Identity Manager CD and mount the CD as a volume.

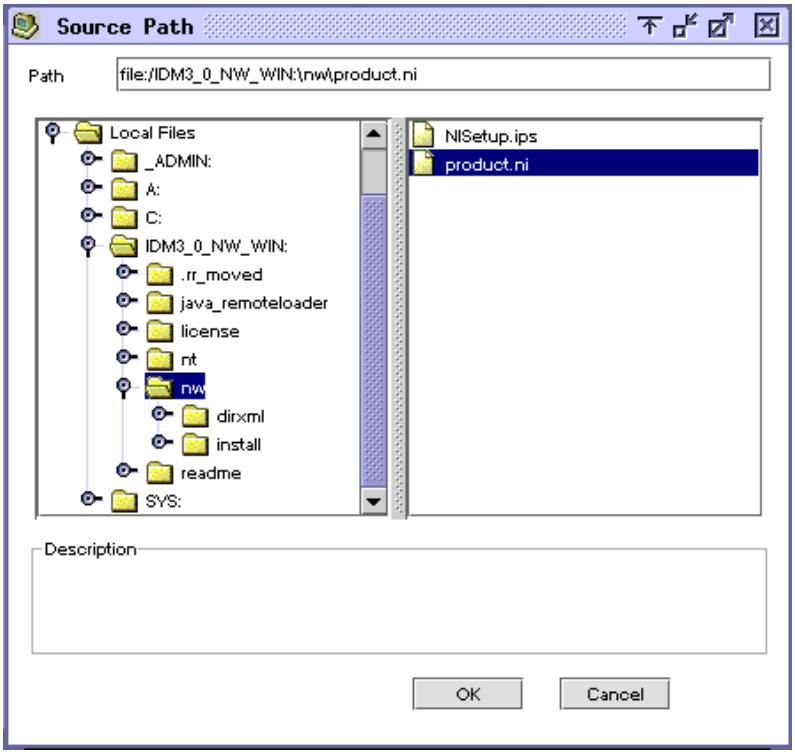
To mount the CD, enter `m cdrom`.

2 (Conditional) If the graphical utility isn't loaded, load it by entering `startx`.

3 In the graphical utility, click the *Novell* icon, then click *Install*.

4 In the Installed Products dialog box, click *Add*.

5 In the Source Path dialog box, browse to and select the `product.ni` file.

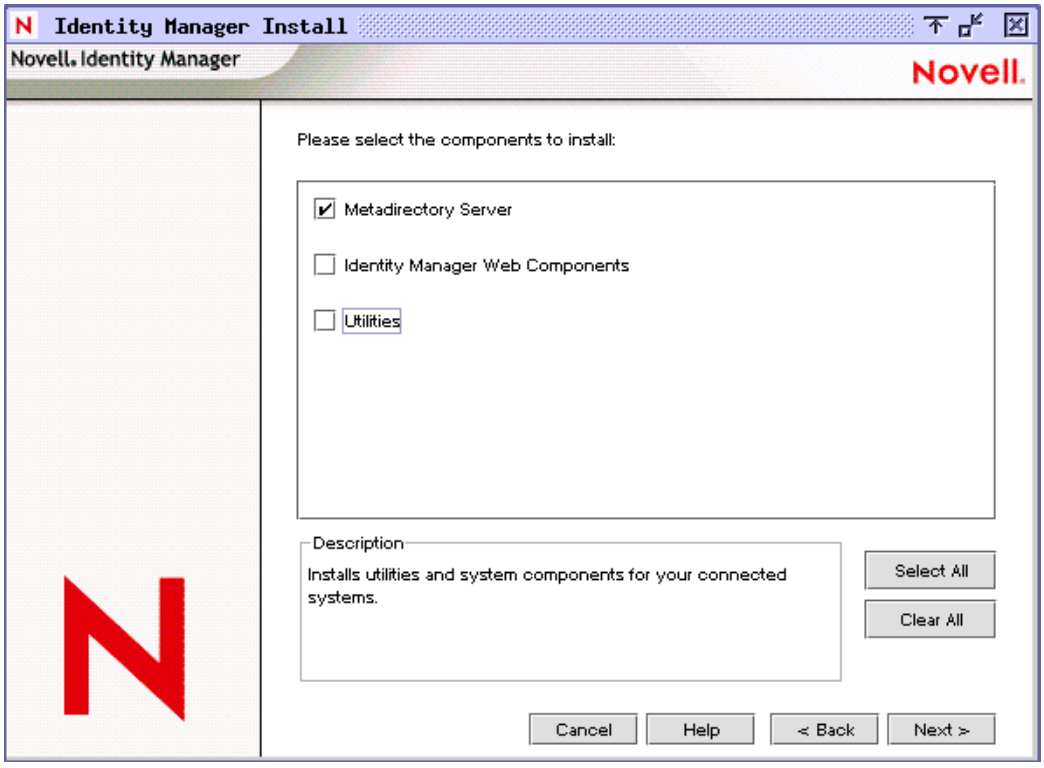


5a Browse to and expand the CD volume (`Identity_Manager_3_Linux_NW_WIN`) that you mounted earlier.

5b Expand the *nw* directory, select *product.ni*, then click *OK* twice.

6 In the Welcome to the Novell Identity Manager Installation dialog box, click *Next*, then accept the license agreement.

7 In the Identity Manager Install dialog box, select only *Metadirectory Server*.

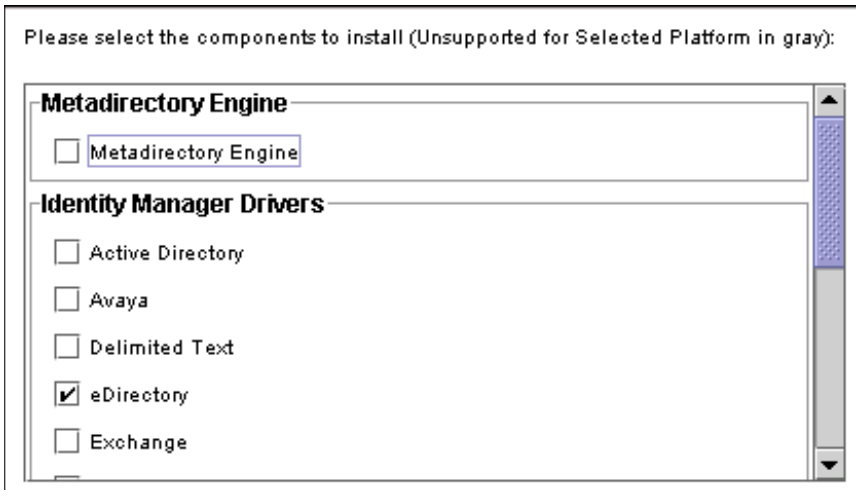


Deselect the following:

- Identity Manager Web Components
- Utilities

8 Click *Next*.

9 In the Select Drivers for Engine Install dialog box, select only *eDirectory*.



Deselect the following:

- *Metadirectory Engine*

- All drivers except eDirectory

10 In the Identity Manager Upgrade Warning dialog box, click *OK*.

The dialog box advises you to activate a license for the driver within 90 days.

11 In the Summary page, review the selected options, then click *Finish*.

12 Click *Close*.

After installation, configure the driver as explained in "Configuring the Driver" on page 31.

2.4.3 Installing to Linux, Solaris, or AIX

By default, the Identity Manager Driver for eDirectory is installed when you install the Metadirectory engine. If the driver wasn't installed at that time, this section helps you install it.

As you move through the installation program, you can return to a previous section (screen) by entering `previous`.

1 In a terminal session, log in as root.

2 Insert the Identity Manager CD and mount it.

Typically, the CD is automatically mounted. The following table lists examples for manually mounting the CD. The actual commands that you enter depend on how your system is configured and the operating system:

Platform	What to Type
AIX* or Red Hat*	`mount /mnt/cdrom`, then press Enter
Solaris	`mount /cdrom`, then press Enter
SUSE®	`mount /media/cdrom`, then press Enter, or `mount /media/dvd`, then press Enter

3 Change to the setup directory.

For example, change to *mount point*/*platform*/`setup`

- *mount point* is wherever the cd/dvd is mounted.
- *platform* is the name of the platform (`solaris`, `linux`, or `aix`).

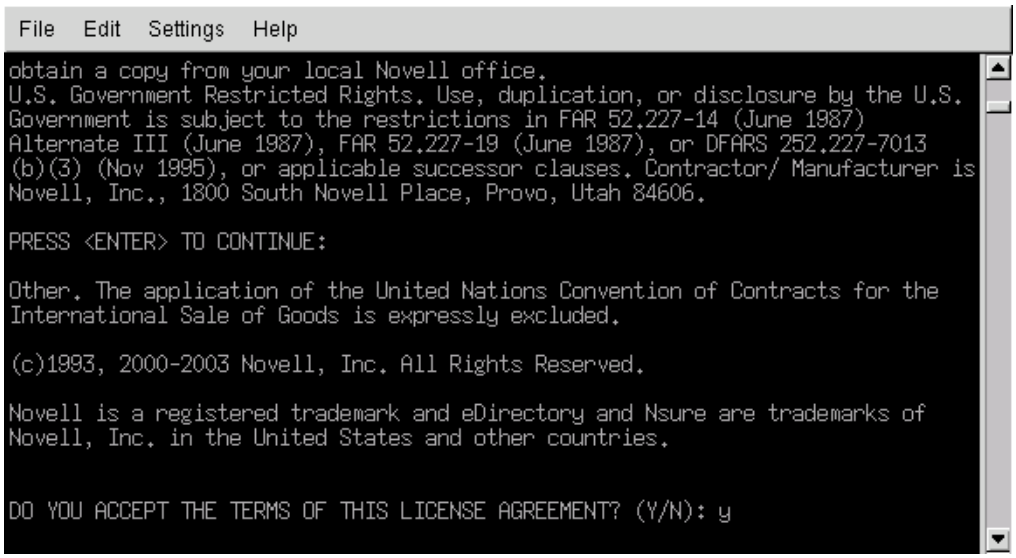
4 Run the installation program.

For example, for Linux type `./dirxml_linux.bin`.

5 In the Introduction section, press Enter.

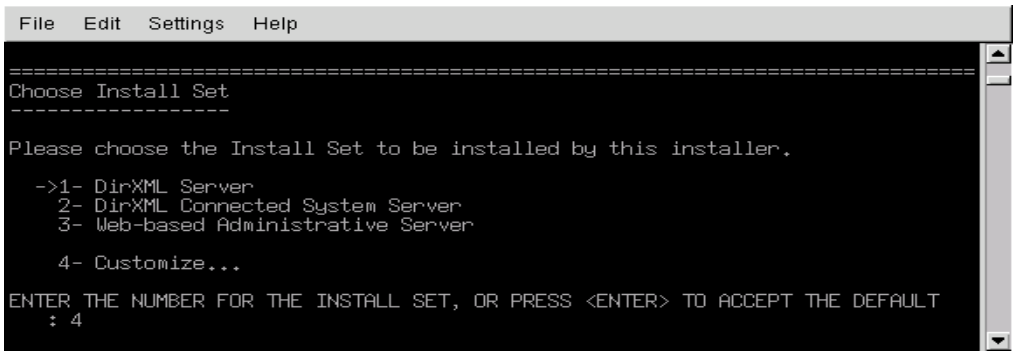
6 Accept the license agreement.

Press Enter until you reach *DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT*, type `y`, then press Enter.



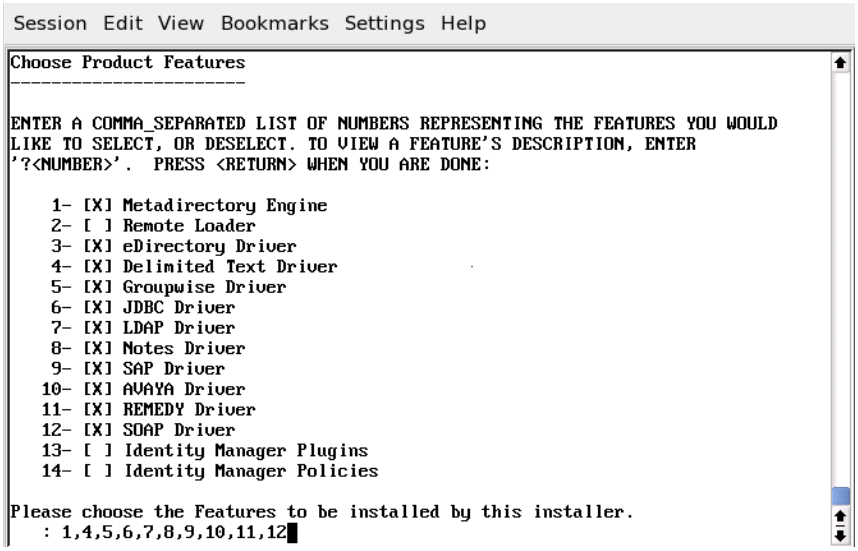
7 In the *Choose Install Set* section, select the *Customize* option.

Type `4`, then press Enter.

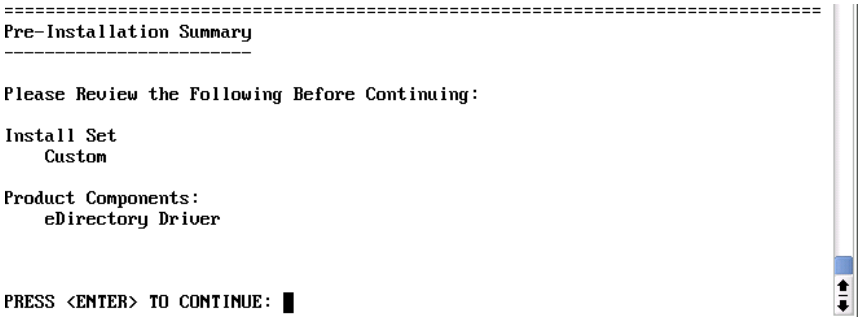


8 In the *Choose Product Features* section, deselect all features except *eDirectory*, then press Enter.

To deselect a feature, type its number. Type a comma between additional features that you deselect.



9 In the *Pre-Installation Summary* section, review options.



To return to a previous section, type `previous`, then press Enter.

To continue, press Enter.

10 After the installation is complete, exit the installation by pressing Enter.

After installation, configure the driver as explained in "Configuring the Driver" on page 31.

2.5 Activating the Driver

Activate the driver within 90 days of installation. Otherwise, the driver will stop running.

For information on activation, refer to "Activating Novell Identity Manager Products" in the *Identity Manager 3.0.1 Installation Guide*.

Upgrading the Identity Manager Driver for eDirectory

3

3.1 Preparing to Upgrade

Make sure you have reviewed all TIDs and Product Updates for the version of the driver you are using.

The new driver shim is intended to work with your existing driver configuration with no changes, assuming that your driver shim and configuration have the latest fixes.

3.2 Upgrading the Driver Shim

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

   To help minimize upgrade issues, we recommend that you complete this step on all drivers.

2. Install the new driver shim.

   You can do this at the same time that you install the Metadirectory engine, or you can do it after the engine is installed. See “Installing the Driver Shim” on page 11.

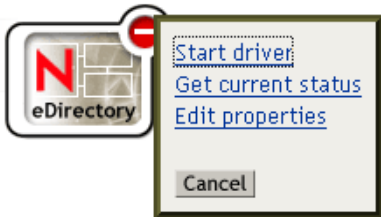
   When you upgrade, the new driver shim replaces the previous driver shim but keeps the previous driver’s configuration.

3. After the shim is installed, restart the driver.

   3a. In iManager, select *Identity Manager* > *Identity Manager Overview*.

   3b. Browse to the driver set where the driver exists.

   3c. Select the driver that you want to restart, click the status icon, then select *Start Driver*.



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

   You activate only once per driver set, not for each driver. Most likely, you have already activated the driver set and can skip this step.

For information on activation, see "Activating Novell Identity Manager Products" in the *Identity Manager 3.0.1 Installation Guide*.

After you install the driver shim, upgrade the driver configuration. See "Upgrading the Driver Configuration" on page 20.

3.3 Upgrading the Driver Configuration

IMPORTANT: This section applies to upgrading from DirXML® 1.*x* only.

Because you are upgrading the driver on two separate Identity Vault servers, you must complete the upgrade procedures for each server.

Installing the driver shim does not change your existing configuration. Your existing configuration continues to work with the new driver shim.

However, to take advantage of new features, you must upgrade your driver configuration, either by replacing your driver configuration with the new sample configuration or by converting your existing configuration to Identity Manager 3 format and adding policies to it.

- To replace your existing configuration, import the new sample configuration for your existing driver objects.

  The sample configuration contains all the newer features, such as support for Identity Manager Password Synchronization and Role-Based Entitlements.
- To convert an existing driver configuration so that you can edit it with the new Identity Manager plug-ins, see "Upgrading a Driver Configuration from DirXML 1.1a to Identity Manager Format" in *Novell Identity Manager 3.0.1 Administration Guide*.
- To add Identity Manager Password Synchronization functionality to an existing driver configuration, see "Upgrading Existing Driver Configurations to Support Password Synchronization" in *Novell Identity Manager 3.0.1 Administration Guide*.

  The new policies for password synchronization are intended to support Universal Password and Distribution Password. If you are planning to synchronize only the NDS® Password, these policies should not be added to the driver configuration. NDS Password is synchronized by using Public Key and Private Key attributes instead of these policies.

3.4 Upgrade Issues for the eDirectory Driver

IMPORTANT: This section applies to upgrading from DirXML 1.*x* only.

If you are upgrading Identity Manager and the eDirectory driver, you might encounter data synchronization errors if your certificates have expired (or if one of the two certificates has expired).

If you create a user on the server that holds a valid certificate, the user won't be synchronized to the server containing the invalid certificate. Also, you might see the following error in DSTrace:

```
SSL handshake failed, X509_V_CERT_HAS_EXPIRED
SSL handshake failed, SSL_ERROR_ZERO_RETURN,
```

If you create a user on the server that holds an expired certificate, the user is still synchronized to the server containing a valid certificate. Also, you might see the following error in DSTrace:

```
Error: 14094415: SSL Routines: SSL_READ_BYTES: sslv3 alert certificate
expired.
```

To fix this issue, create new certificates.

The Sample Driver Configuration File

4

4.1 Importing the Sample Driver Configuration

4.1.1 Importing by Using iManager

1. Create a new driver or import the configuration `eDirectory.xml` onto an existing driver.

   In Novell iManager, select Identity Manager Utilities, then use one of the tasks as described in “Managing Identity Manager Drivers” in *Novell Identity Manager 3.0.1 Administration Guide*.
2. Configure the driver by following the instructions in Section 4.2, “Configuring Secure Identity Manager Data Transfers,” on page 25.

The wizard prompts you to provide the following information:

Item	Description
Driver name	You can use the default name *eDirectory Driver*, or change the name.
R*emote Tree Address and Port*	Specify the DNS host name or IP address and port of the Identity Manager server in the remote tree. For example: 151.155.144.23:8196 hostname:8196
Configure Data Flow	**Bidirectional:** Both eDirectory™ trees are authoritative sources of the data synchronized between them. **Authoritative:** The local tree is the authoritative source. **Subordinate:** The local tree is not an authoritative source.

Item	Description
Configuration Option	**Mirrored:** Synchronizes objects hierarchically between the local and remote trees. If you choose this option, use the same option for configuring both eDirectory trees you are synchronizing. This option in the driver configuration synchronizes User, Group, Organization, Country, and Organizational Unit objects. It also mirrors the structure of a subtree in the other tree. **Flat:** Synchronizes all Users and Groups into specific containers. This option synchronizes User and Group objects and places all users in one container and all groups in another container. This option is typically used in conjunction with the Department option (or a similar configuration) in the other tree. This option doesn't create the containers that hold the users and groups. You must create those manually. **Department:** Synchronize 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. This configuration is typically used in conjunction with the Flat option (or a similar configuration) in the other tree. This option doesn't create the containers for each department. You must create those manually. They must be the same as the container specified during import.
Remote Base Container	Used for Mirrored option only. Specify the base container for synchronization in the remote tree, for example Users.MyOrganization.
Base Container	Used for Mirrored, Flat, and Department options. Specify the base container for synchronization in the local tree, for example Users.MyOrganization. **If using with Mirrored:** The local base container to mirror with the Remote Base Container above. **If using with Flat:** The container to place Users into. **If using with Department:** The parent of the departmental containers.
Group Container	Used for Flat only. Specify the base container for synchronization in the local tree to place Groups into, for example Groups.MyOrganization.
Password Sync Version	The default is 1.0. Use this option if you use public/private keys. Select 2.0 if you use the distribution password and password policies.

Item	Description
Password Failure Notification User	The user whose password fails to synchronize receives an e-mail notification whenever password updates fail. To send a copy of that e-mail to an additional user, type or browse to and select the DN of that additional user.

4.1.2 Importing by Using Designer for Identity Manager

You can import the basic driver configuration file for the eDirectory driver by using Designer for Identity Manager. This basic file creates and configures the objects and policies needed to make the driver work properly.

The following procedure explains one of several ways to import the sample configuration file:

1. Open a project in Designer.
2. In the modeler, right-click the Driver Set object, then select *Add Connected Application*.
3. From the drop-down list, select *eDirectory.xml*, then click *Run*.
4. Click *Yes*, in the Perform Prompt Validation window.
5. Configure the driver by filling in the fields.

   Specify information specific to your environment. For information on the settings, see the table in Step 2 on page 23.
6. After specifying parameters, click *OK* to import the driver.
7. Customize and test the driver.
8. Deploy the driver into the Identity Vault.

   See "Deploying a Driver to an Identity Vault" in the *Designer for Identity Manager 3: Administration Guide*.

4.2 Configuring Secure Identity Manager Data Transfers

All eDirectory driver communication is secured through SSL. To configure your eDirectory system to handle secure Identity Manager data transfers, run the NDS2NDS wizard in Novell iManager.

- Section 4.2.1, "Understanding eDirectory Driver Security," on page 25
- Section 4.2.2, "Setting Up a KMO," on page 26

4.2.1 Understanding eDirectory Driver Security

The following items can help you understand eDirectory driver security:

- The driver uses SSL sockets to provide authentication and a secure connection. SSL uses digital certificates to allow the parties to an SSL connection to authenticate one another. Identity Manager in turn uses Novell Certificate Server certificates for secure management of sensitive data.
- To use the driver, you must have the Novell Certificate Server running in each tree. We recommend that you use the Certificate Authority from one of the trees containing the driver to

issue the certificates used for SSL. If your tree does not have a Certificate Authority, you need to create one. You can use an external Certificate Authority.

- The Novell implementation of SSL that the driver uses is based on Novell Secure Authentication Services (SAS) for eDirectory and NTLS for eDirectory 8.7.*x*. These must be installed and configured on the server where the driver runs. eDirectory usually does this automatically.
- To configure driver security, it is necessary to create and reference certificates in the eDirectory trees that will be connected using the driver. Certificate objects in eDirectory are called Key Material Objects (KMOs) because they securely contain both the certificate data (including the public key) and the private key associated with the certificate.

  A minimum of two KMOs (one KMO per tree) must be created for use with the Identity Manager Driver for eDirectory. This section explains using a single KMO per tree.

  The NDS2NDS Driver Certificate Wizard sets up the KMOs.
- For more information:
  - For an overview of Novell Certificate Server, see the Novell Certificate Server online documentation (http://www.novell.com/documentation/crtsrv20/index.html).
  - For more information on CAs, and in particular for information about setting up Certificate Authorities in your trees, see Setting Up Novell PKI Services (http://www.novell.com/documentation/lg/ndsse/ndsseenu/data/h6172k4q.html).

4.2.2 Setting Up a KMO

To configure your Identity Vault system to handle secure Identity Manager data transfers:

1. Find out the tree name or IP address of the destination server.
2. Launch iManager and authenticate to your first tree.
3. Click *Identity Manager Utilities* > *NDS2NDS Driver Certificates*.
4. At 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: Type the distinguished name of the eDirectory driver (for example, EDir-Workforce.Employee Provisioning.Services.YourOrgName).
   - The tree name: Specify the IP address for the Workforce Tree.
   - A username for an account with Admin privileges (for example, Admin).
   - The password for the user.
   - The user's context (for example Services.YourOrgName).
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. Specify the requested information for the second tree.

   At the Welcome page, enter the requested information for the first tree.

   Specify or confirm the following information:

   - Driver DN: Type the distinguished name of the eDirectory driver (for example, EDir-Account.DriverSet.YourOrgName).

- The tree name: Type the tree name or IP address for the Account Tree.
- A username for an account with Admin privileges (for example, Admin).
- The password for the user.
- The user's context (for example, London.YourOrgName).

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 KMOs already existed 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 IDs.

4.3 Which Attributes Are Synchronized

The filter for the sample driver configuration synchronizes the following attributes:

accessCardNumber	Initials	preferredDeliveryMethod
ACL	instantMessagingID	preferredName
assistant	internationaliSDNNumber	Private Key
assistantPhone	Internet EMail Address	Public Key
businessCategory	jackNumber	registeredAddress
city	jobCode	roomNumber
CN	L	S
co	Language	SA
company	Mailbox ID	Security Equals
costCenter	Mailbox Location	Security Flags
costCenterDescription	mailstop	See Also
departmentNumber	manager	siteLocation
Description	managerWorkforceID	Surname
destinationIndicator	mobile	Telephone Number
directReports	NSCP:employeeNumber	teletexTerminalIdentifier
EMail Address	otherPhoneNumber	telexNumber
employeeStatus	O	Timezone
employeeType	OU	Title
Equivalent To Me	pager	tollFreePhoneNumber

Facsimile Telephone Number	personalTitle	UID
Full Name	photo	uniqueID
Generational Qualifier	Physical Delivery Office Name	vehicleInformation
Given Name	Postal Address	workforceID
Group Membership	Postal Code	x121Address
Higher Privileges	Postal Office Box	x500UniqueIdentifier

4.4 Password Synchronization

This section contains information that is specific to the Identity Manager Driver for eDirectory, and assumes that you are familiar with the information in "Implementing Password Synchronization" in the *Novell Identity Manager 3.0.1 Administration Guide*.

- The driver shim continues to work as in earlier releases. In Identity Manager 2.0, new policies were added to the sample driver configuration to support Identity Manager Password Synchronization, including synchronizing Universal Password.
- If you decide to enforce password policies in multiple trees, make sure that the Advanced Password Rules in the password policies are compatible in each tree, so that password synchronization can be successful.

  If you enforce incompatible password policies in multiple eDirectory trees, and choose to set a password back if it does not comply (with the option *If password does not comply, enforce Password Policy on the connected system by resetting user's password to the Distribution Password*), you could encounter a loop in which each Identity Vault server tries to change a noncompliant password.

  Information about password policies is in "Managing Passwords by Using Password Policies," in the Password Management Administration Guide (http://www.novell.com/documentation/password_management/index.html).
- If the filter for the driver has the setting *Synchronize* for the Public Key and Private Key attributes, the NDS® password is synchronized between trees, regardless of any other settings you have created.

  If you want to synchronize passwords using Universal Password, make sure you set the filter on both eDirectory drivers to *Ignore* for the Public Key and Private Key attributes for all classes that you want to synchronize Universal Password.
- To add Identity Manager Password Synchronization functionality to an existing driver configuration, see "Upgrading Existing Driver Configurations to Support Password Synchronization" in *Novell Identity Manager 3.0.1 Administration Guide*.

  The new policies for password synchronization are intended to support Universal Password and Distribution Password. If you are planning to synchronize only the NDS Password, these policies should not be added to the driver configuration. NDS Password is synchronized by using Public Key and Private Key attributes instead of these policies.
- The Check Password Status task in iManager does not work for a connected system if the Password Policy has Universal Password enabled and does not have the setting selected for synchronizing Universal Password with NDS Password.

  The Check Password Status task lets you see whether a user's password in Identity Manager is synchronized with the password on connected systems.

If you are using the Identity Manager Driver for eDirectory, and the password policy for a user specifies in the Configuration Options tab that the NDS Password should not be updated when the Universal Password is updated, then the Check Password Status task for that user always shows that the password is not synchronized. The password status is shown as not synchronized, even if the Identity Manager Distribution Password and the Universal Password on the connected system are in fact the same.

This is because the Identity Vault check-password functionality is checking the NDS Password at this time, instead of going through NMAS™ to refer to the Universal Password.

By default, the NDS Password is updated when the Universal Password is updated in the password policy. If you select this option, Check Password Status should be accurate for the connected system.

- To use the driver, you must have the Novell® Certificate Server™ running on each server that hosts the driver. You must also create a Certificate Authority (CA) for SSL encryption to work. We recommend that the certificates used for SSL be issued by the Certificate Authority from one of the trees containing the driver. If your tree does not have a Certificate Authority, create one. You can use an external Certificate Authority.

  For instructions on creating CAs and configuring the Certificate Server, refer to Section 4.2, “Configuring Secure Identity Manager Data Transfers,” on page 25.

Configuring the Driver

5

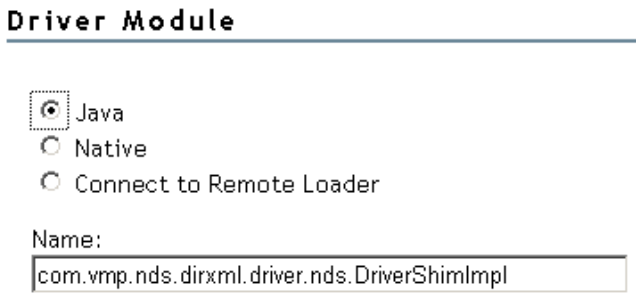
For information about password synchronization, see “Password Synchronization” on page 28.

5.1 Configuring Driver Object Properties

Typically, the driver’s properties are automatically configured when you import the driver configuration file and run the Certificate Wizard.

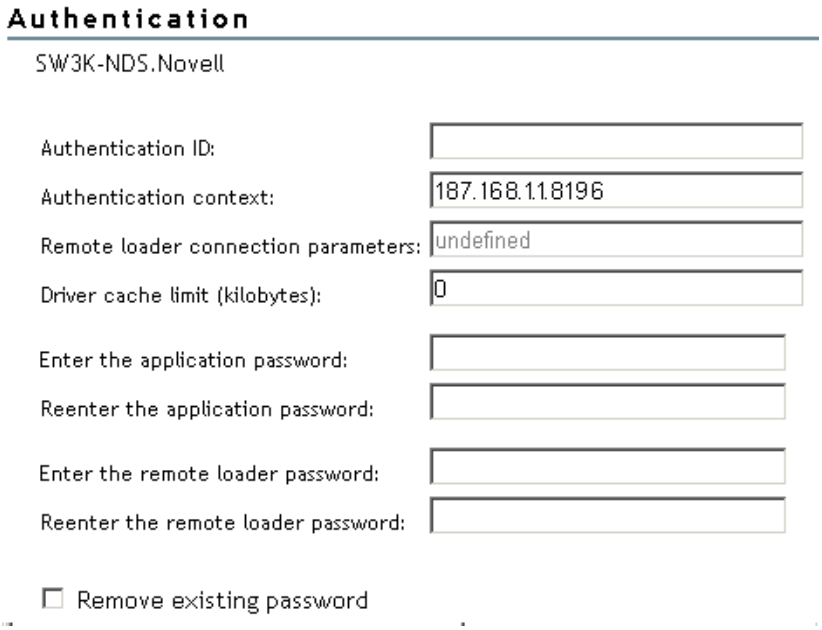
To configure properties manually:

1. In iManager, click *Identity Manager* > *Identity Manager Overview*.
2. Locate the driver set that contains the eDirectory™ driver, then click the driver’s icon.
3. From the *Identity Manager Driver Overview* page, click the eDirectory Driver object, which displays the driver configurations.
4. Locate the *Driver Module* section, then select *Java*.



5. In the Name edit box, type the following eDirectory Driver Java class name:
   `com.novell.nds.dirxml.driver.nds.DriverShimImpl`
6. Set parameters.

5.1.1 Authentication Parameters



Provide information that allows the source server to communicate with the destination server.

Authentication ID

If you want the source server and destination server to exchange secure information (for example, passwords), run the NDS2NDS eDirectory Certificates Wizard. This wizard creates Key Material Objects (KMOs) and places the correct KMO name in the Authentication ID field.

The KMOs are Secure Socket Layer (SSL) certificates:

Authentication Context

In the Authentication Context field, enter the host name or IP address of the destination server as well as the decimal port number (for example, 187.168.1.1:8196).

You can specify a separate port for Subscriber and Publisher channels by specifying a second port number following a second colon. If a second port number is specified, the Publisher channel uses the second port number rather than using the same port number as the Subscriber channel (for example, 255.255.255.255:2000:2001).

If your server has multiple IP addresses, you can specify the IP address you want the Publisher channel to use. This requires specifying the remote IP address, the Subscriber channel port, the local IP address, and the Publisher channel port. For example. 137.65.134.81:2000:137.65.134.83:2000 specifies that the Subscriber channel will communicate with the remote tree on 137.65.134.81, port 2000, and that the Publisher channel will listen on address 137:65.134.83, port 2000.

NOTE: If you see “java.net.ConnectException: Connection Refused,” no port connection is available on the remote side. This error might be caused by one of the following:

- The driver on the remote side is not running.
- The driver is running but is configured to use a different port.

Remote Loader Connection Parameters

The Remote Loader option isn’t needed (and isn’t used) for the Identity Manager Driver for eDirectory.

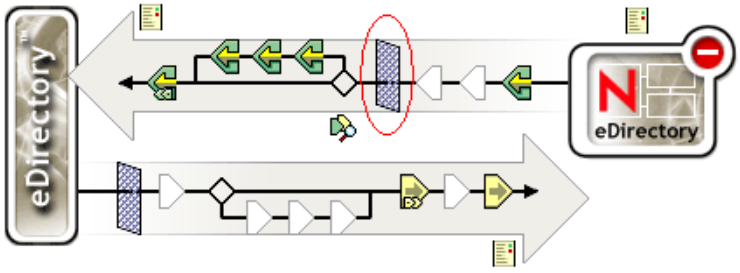
Driver Cache Limit

Don’t modify this field unless Novell Support asks you to do so.

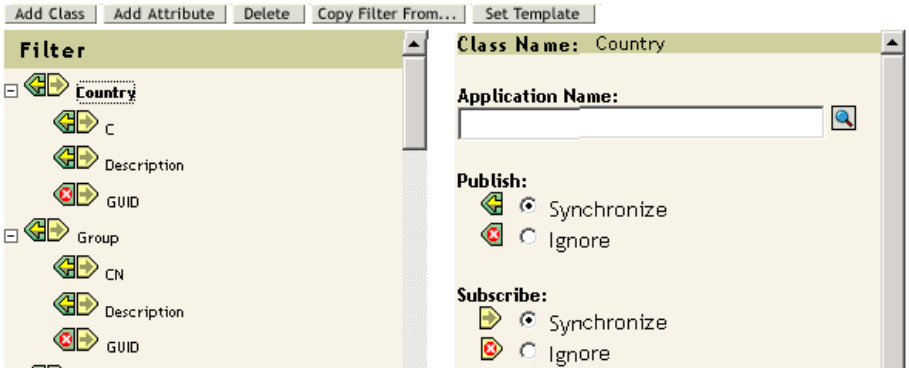
5.2 Configuring the Filter

One filter controls both the Publisher and the Subscriber channels. You should modify the filter to include object classes and attributes you want to be available for Identity Manager processing. To modify the filter:

1. In iManager, click *Identity Manager > Identity Manager Overview*.
2. Locate the driver set containing the eDirectory driver, then click the driver’s icon to display the *Identity Manager Driver Overview* page.
3. Click the filter on the Publisher channel.



4. Customize the driver.



In this example, Country and Group are classes. To add a class, click *Add Class*, then select the class. To delete a class, select it, then click *Delete*.

In this example, CN is an attribute of the Group class. To add an attribute, select the class, click A*dd Attribute*, then select the attribute.

To modify a class or attribute, select it, then select options in the right pane. In this example, the Country attribute is synchronized on the Publisher and Subscriber channels. However, the GUID attribute isn't synchronized on the Publisher channel.

To synchronize the GUID attribute, select it, then click *Synchronize* in the *Publish* section.

The GUID attribute is required for all classes that are set to Synchronize on the Subscriber channel.

In general, except for the GUID attribute, the Subscriber channel filter in one tree should match the Publisher channel filter in the other tree, and vice versa.

5 Click *Apply*, then click *OK*.

5.3 Configuring Rules on the Publisher Channel

The rules on a driver should generally be placed only on the Publisher object, not on the Subscriber object. The Matching and Placement policies cannot operate correctly on the Subscriber channel because the Subscriber channel is acting primarily as a source of events for the Publisher channel of the other tree.

It is sometimes desirable to place an Event Transform or Create Policy on the Subscriber channel in order to prevent sending unnecessary data across the channel. See "Managing Users on Different Servers Using Scope Filtering " in the *Identity Manager 3.0.1 Installation Guide*.

5.4 Using Driver Object Passwords

In addition to the mandatory certificates needed to use SSL, for additional security you should configure the driver so that the Subscriber channel on one tree authenticates to the Publisher channel on the remote tree. The Driver object password in each tree should be set up to match the application password in the other tree.

To set the Identity Manager Driver object password in a tree:

1 In iManager, click *Identity Manager > Identity Manager Overview*.

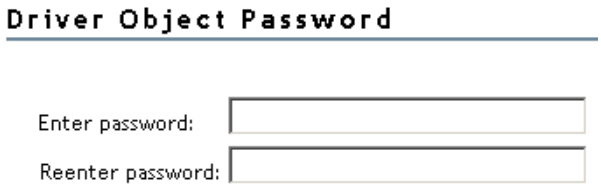
2 Locate the driver set containing the eDirectory driver, then click the driver's icon.

3 From the Identity Manager Driver Overview page, click the eDirectory driver object.

4 Select *Driver Configuration*.

Select from a drop-down list or tab, depending on the iManager version and your environment.

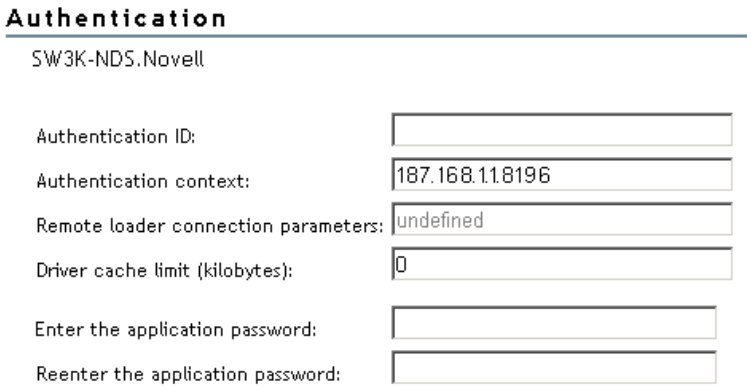
5 Locate the *Driver Object Password* section.



6 Type a Driver object password.

IMPORTANT: After a Driver object password is set, it can't be removed.

7 In the *Authentication* section, type the application password.



8 Click *Apply*, then click *OK*.

5.5 Migrating or Copying Objects

Although iManager doesn't have a Copy function, you can use the *Migrate from eDirectory* option to copy objects from one eDirectory tree to another. The scope of the copying depends on the policies of the driver. For example, depending on policies that apply to the driver, you can copy (sync) all the attributes from one eDirectory tree to another. Such a "copy" requires that you synchronize all the attributes across the trees, put objects in the same location during a migration, and not change any data during the migration.

A time stamp is always associated with a resync operation. A resync operation looks for objects that are already associated (have already been synchronized) but have been changed since the time stamp. It also attempts to look for objects that might have been created since the time stamp. Clicking *Resync* might cause new users to be synchronized.

Instead of using the *Resync* option to copy objects, you can use the *Migrate from eDirectory* option. This option enables you to specify and synchronize a list of objects. For each object in the list, iManager writes data to the directory. Identity Manager notes the changes and starts the synchronization process for listed objects.

1 Make sure that Identity Manager 3 is installed on a server in the source eDirectory tree and on a server in the destination eDirectory tree.

2 Configure an Identity Manager Driver for eDirectory on the server in the source tree.

In the eDirectory driver's Authentication pane, provide the name or IP address and port of the destination server. See Section 5.1, "Configuring Driver Object Properties," on page 31.

Select a migration option: *Flat*, *Mirrored*, or *Department*. To preserve the directory structure (including subcontainers and names) when data is migrated from the source tree to the destination tree, select *Mirrored*.

3 Configure an Identity Manager Driver for eDirectory on the server in the destination tree.

In the Authentication pane, provide the name or IP address and port of the source server.

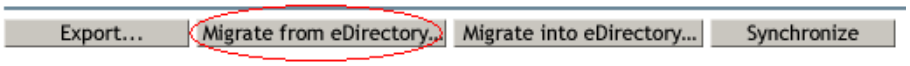
4 Set up SSL between the two trees.

Using the NDS2NDS Wizard, create KMO certificates in both trees. See Section 4.2.2, “Setting Up a KMO,” on page 26.

To launch the NDS2NDS Wizard, in iManager select *Identity Manager Utilities* > *NDS-to-NDS Driver Certificates*.

5 In iManager, select *Identity Manager*, click *Identity Manager Overview*, then click the driver.

6 Select *Migrate from eDirectory*.



With eDirectory-to-eDirectory migrations, migrate from the source tree to the destination tree.

The *Migrate into eDirectory* option doesn’t work with the Identity Manager Driver for eDirectory.

7 Select objects.

For example, select a User object or a Container object. You can search for or browse to the objects. Also, you can add multiple objects.

8 Click *OK* twice.

The client (for example, iManager) writes a value to each object in the list. This change event causes Identity Manager to push the data into your destination tree.

Documentation Updates

A

This section contains new or updated information on the Identity Manager Driver for eDirectory.

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

If you need to know whether a copy of the PDF documentation you are using is the most recent, check the date that the PDF file was published. The date is in the Legal Notices section, which immediately follows the title page.

A.1 May 8, 2006

Table A-1 *Changes Made on May 8, 2006*

Location	Change
Section 2.4, “Installing the Driver Shim,” on page 11	Clarified the following: ◆ This section assumes that eDirectory has already been installed on the server. ◆ This section explains how to add an eDirectory driver to the server.

A.2 August 10, 2006

Updated cross-references to the Identity Manager 3.0.1 documentation set.

A.3 September 12, 2006

Table A-2 *Changes Made on September 12, 2006*

Location	Change
Section 4.1, “Importing the Sample Driver Configuration,” on page 23	Added *Password Sync Version* to the table of parameters.

A.4 February 9, 2007

Table A-3 *Changes Made on February 9, 2007*

Location	Change
Section 5.1, “Configuring Driver Object Properties,” on page 31	Added two paragraphs to the Authentication Context heading, under Authentication Parameters topic. This information was in the DirXML 1.0 release and should have been carried forward.

A.5 June 25, 2007

Table A-4 *Changes Made on June 25, 2007*

Location	Change
Chapter 5, “Configuring the Driver,” on page 31	Updated the links at the beginning of the section, to include “Migrating or Copying Objects,” as recommended in a User Comment.