

# Novell Identity Manager Driver for Exchange 5.5

1.6.2

August 10, 2006

---

IMPLEMENTATION GUIDE

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



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/](http://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 © 2000-2005 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](http://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](http://www.novell.com/documentation).

## **Novell Trademarks**

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

## **Third-Party Materials**

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



# Contents

<b>About This Guide</b>	<b>7</b>
<b>1 Introducing the Identity Manager Driver for Exchange</b>	<b>9</b>
1.1 Overview	9
1.2 Changes in Terminology	9
1.3 Driver Features	10
1.4 Key Terms	10
1.5 Benefits	11
1.6 Required Skills	11
1.7 Adding to the Identity Manager Basics	12
1.7.1 Event Processing Support	12
1.7.2 Policies	12
1.7.3 Associations	13
<b>2 Installing and Configuring the Driver</b>	<b>15</b>
2.1 Prerequisites	15
2.1.1 Software Requirements	15
2.1.2 Hardware Requirements	15
2.2 Upgrading to Identity Manager 3	15
2.3 Installing the Driver Shim for Exchange	15
2.4 Post-Installation Tasks	17
2.4.1 Importing the Driver Configuration File	17
2.4.2 Configuring the Exchange Server	19
2.4.3 Installing a Remote Exchange Driver	21
2.4.4 Configuring the Driver Filter	22
2.4.5 Starting the Driver	23
2.4.6 Migrating and Resynchronizing Data	23
2.4.7 Activating the Driver	24
<b>3 Upgrading</b>	<b>25</b>
3.1 Running the Normalize Exchange Associations Utility	25
3.2 Upgrading the Driver Shim	26
3.3 Upgrading the Driver Configuration	26
<b>4 Customizing the Identity Manager Driver for Exchange</b>	<b>29</b>
4.1 Integrating the Identity Manager Driver for Exchange and the Identity Manager Driver for NT Domain	29
4.2 Managing External Recipients	31
4.3 Synchronizing Proxy-Address and Target-Address Attributes	32
4.4 Using Authoritative Bind	33
4.5 Using a Custom Bind	33
4.6 Specifying the LDAP Port	34

<b>5 Troubleshooting the Driver</b>	<b>37</b>
5.1 Troubleshooting .....	37
5.2 Driver Error Messages .....	37
<b>A Documentation Updates</b>	<b>39</b>
A.1 August 10, 2006 .....	39

# About This Guide

This guide explains how to install and configure the Identity Manager Driver for Microsoft\* Exchange 5.5.

- [Chapter 1, “Introducing the Identity Manager Driver for Exchange,” on page 9](#)
- [Chapter 2, “Installing and Configuring the Driver,” on page 15](#)
- [Chapter 3, “Upgrading,” on page 25](#)
- [Chapter 4, “Customizing the Identity Manager Driver for Exchange,” on page 29](#)
- [Chapter 5, “Troubleshooting the Driver,” on page 37](#)
- [Appendix A, “Documentation Updates,” on page 39](#)

## Audience

This document is for administrators who have expertise in Exchange and Novell® Identity Manager.

## 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](http://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 Exchange* in the Identity Manager Drivers section on the [Novell Documentation Web site \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

## Additional Documentation

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



# Introducing the Identity Manager Driver for Exchange

# 1

- [“Overview” on page 9](#)
- [“Changes in Terminology” on page 9](#)
- [“Driver Features” on page 10](#)
- [“Key Terms” on page 10](#)
- [“Benefits” on page 11](#)
- [“Required Skills” on page 11](#)
- [“Adding to the Identity Manager Basics” on page 12](#)

## 1.1 Overview

The Identity Manager Driver for Exchange is a connector that synchronizes data between an Identity Vault and Microsoft Exchange. This synchronization makes it possible for Exchange accounts to be managed in an Identity Vault. You no longer need to manage a user’s Identity Vault and Exchange accounts separately. The Identity Manager Driver for Exchange increases the efficiency of your network management by allowing you to manage an Identity Vault and Exchange accounts as a single account in a single management tool.

The Identity Manager Driver for Exchange runs on Windows\* NT\*<sup>64</sup>.

The driver supports only the Distribution List, Remote, and Mailbox classes.

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*.

## 1.2 Changes in Terminology

The following terms have changed from earlier releases:

**Table 1-1** *Changes in Terminology*

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

## 1.3 Driver Features

- The AuthoritativeBind parameter lets you use an authoritative LDAP bind instead of an anonymous LDAP bind. See [“Using Authoritative Bind” on page 33](#).
- You can use the Assoc-NT-Account attribute for queries into Exchange.
- Instead of preferredName, the attribute named DirXML-NTAccountName now is used in eDirectory. See [“Integrating the Identity Manager Driver for Exchange and the Identity Manager Driver for NT Domain” on page 29](#).

You can still use the preferredName attribute.

- Role-Based Entitlements features are supported. You can choose this option during import. Using Role-Based Entitlements is a design decision. Before choosing this option, see [“Creating and Using Entitlements” in \*Novell Identity Manager 3.0.1 Administration Guide\*](#).
- You can customize the driver to provide a driver heartbeat. See [“Adding Driver Heartbeat” in \*Novell Identity Manager 3.0.1 Administration Guide\*](#).

## 1.4 Key Terms

**Driver Shim.** A dynamically linked library (Exchange55Shim.dll) loaded directly by Identity Manager or by the Remote Loader. The shim collects the changes to be sent from Exchange to the Identity Vault, communicates changes from the Identity Vault to Exchange, and operates as the link that connects the Identity Vault and Exchange.

**Driver.** A set of policies, filters, and objects that act as the connector between the Identity Vault and the driver shim. The Identity Manager Driver for Exchange is a bidirectional synchronization connector between Microsoft Exchange and an Identity Vault. This connector uses XML to convert Exchange objects to Identity Vault objects and vice versa.

The driver 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 Exchange, 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 Identity Vault management of the driver shim parameters.

**Identity Vault.** A hub, with other 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
- The Subscriber channel

The Identity Manager Driver for Exchange is a bidirectional synchronization connector between Microsoft Exchange and an Identity Vault. This connector uses XML to convert Exchange objects to Identity Vault objects and vice versa.

**Publisher Channel.** Reads information from your Exchange Server and submits that information to the Identity Vault via the Metadirectory engine.

By using the poll parameters, the Publisher channel polls the Exchange server for changes to objects. If the Identity Manager Driver for Exchange detects changes in Exchange, the data between Exchange and the Identity Vault is synchronized. If the change was caused by data sent to Exchange from the Subscriber, no synchronization is necessary.

**Subscriber Channel.** Watches for additions and modifications to Identity Vault objects and creates changes on the Exchange server via the Metadirectory engine.

The Subscriber channel synchronizes changes made in the Identity Vault with data on the Exchange server. If an associated object is changed in the Identity Vault, the Subscriber channel updates the Exchange server with the new information.

## 1.5 Benefits

You can use the driver to automate and maintain business processes in the following ways:

- Automatically create Identity Vault objects from Exchange objects.
- Synchronize bidirectional data between Exchange and an Identity Vault.
- Maintain accurate and consistent Identity Vault IDs.
- Enable integration between Exchange and multiple applications (for example, an Identity Vault, Lotus Notes\*, Netscape\*, SAP\*, and Active Directory\*) by using Identity Manager and an Identity Vault.
- Manage Exchange distribution lists and remote objects.

You can configure the Identity Manager Driver for Exchange to enhance your organization's processes by using custom business logic in the form of policies. Before installing and configuring the driver, you evaluate and define those processes. During installation, you configure the driver's policies to automate these processes wherever possible.

## 1.6 Required Skills

Implementing the driver requires expertise in Exchange and Identity Manager. This document assumes that your expertise in Exchange is equivalent to one of the following:

- An Exchange developer
- An Exchange administrator
- An application designer
- An upgrade administrator
- A database administrator

This document assumes that your expertise in Identity Manager is equivalent to an eDirectory administrator or an Identity Manager administrator.

## 1.7 Adding to the Identity Manager Basics

The following Identity Manager functionality is important to the driver:

- “Event Processing Support” on page 12
- “Policies” on page 12
- “Associations” on page 13

### 1.7.1 Event Processing Support

The driver supports the following events on the Publisher and Subscriber channels.

**Table 1-2** Supported Events

Functionality	Event
Publisher	Add Modify Delete Rename
Subscriber	Add Modify Delete Rename

The driver also supports a defined query capability so that Identity Manager can query the synchronized application or directory.

### 1.7.2 Policies

Policies are used to control the synchronization of the driver with the Identity Vault and the application, database, or directory. Policies help Identity Manager transform an event on a channel input into a set of commands on the channel output.

You can configure policies by using the iManager plug-ins for Identity Manager. The sample driver configuration includes the following set of policies:

**Table 1-3** Policies in the Sample Configuration File

Policy	Description
Placement	Operates on both the Publisher and Subscriber channels
Matching	Operates on both the Publisher and Subscriber channels
Mapping	Configured on the Driver object
Input Transform	Configured on the Driver object
Output Transform	Configured on the Driver object
Create	Operates on the Publisher and Subscriber channels

---

Policy	Description
Event Transform	Operates on the Publisher channel
Command Transform	Operates on the Publisher channel

---

For more information about creating your own policies, see the *Policy Builder and Driver Customization Guide*.

### 1.7.3 Associations

The driver uses the Exchange DN for associations. A unique ID or unique user name is created for records relating to Exchange objects. However, Identity Manager does not need to share these same unique IDs.

The association attribute received from Exchange is unique to the Exchange application, based on each driver for Exchange that you install and enable. If other drivers are installed, they use an association specific to that application. The association attribute is multivalued. Therefore, if Identity Manager is being used to connect multiple applications, all of their associations can be stored on this attribute.

The unique ID association links an object in Exchange to its associated object in the Identity Vault. This association allows the driver to perform subsequent tasks on the appropriate object.

The Association field is stored on the Identity Vault object on the Identity Manager property page.



# Installing and Configuring the Driver

# 2

- “Prerequisites” on page 15
- “Installing the Driver Shim for Exchange” on page 15
- “Post-Installation Tasks” on page 17

## 2.1 Prerequisites

This section lists the software and hardware requirements for running the Identity Manager Driver for Exchange.

### 2.1.1 Software Requirements

- Novell® Identity Manager 2 or later, and its prerequisites
- Windows NT 4 with the latest patches and service packs (SP6a or later)
- Exchange 5.5 with Service Pack 4 or later and the latest patches

---

**NOTE:** If the Exchange Server doesn't have the latest patches, an Entitlement Policy won't correctly assign membership in an Exchange distribution list. Also, proxy addresses are handled improperly because of a defect in Exchange.

---

### 2.1.2 Hardware Requirements

- 128 MB RAM (256 MB or more recommended)

## 2.2 Upgrading to Identity Manager 3

During an Identity Manager installation, you can install the Driver for Exchange 5.5 (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.

## 2.3 Installing the Driver Shim for Exchange

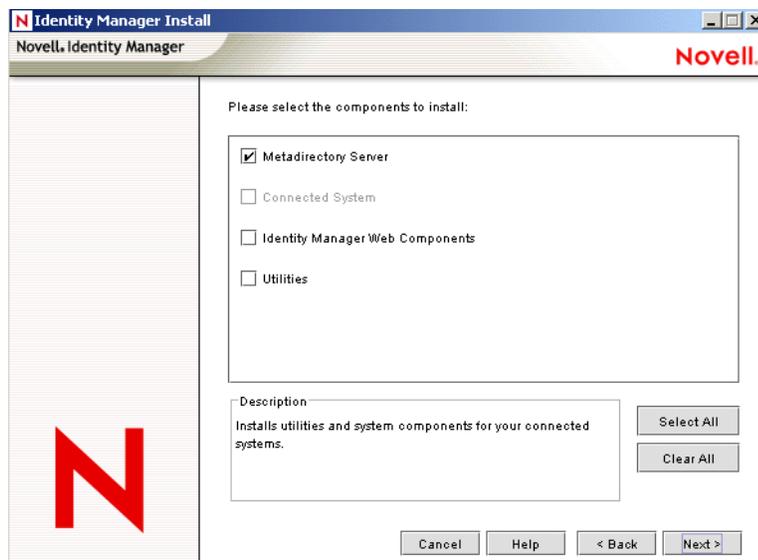
You can install the Driver for Exchange (along with other Identity Manager drivers) at the same time that the Metadirectory engine is installed. See the *Identity Manager 3.0.1 Installation Guide*.

You can also install the driver separately, after the Metadirectory engine is installed. If you don't have a CD, download `Identity_Manager_3_NW_Win.iso` and create one. Downloads are available from [Novell Downloads \(http://download.novell.com/index.jsp\)](http://download.novell.com/index.jsp).

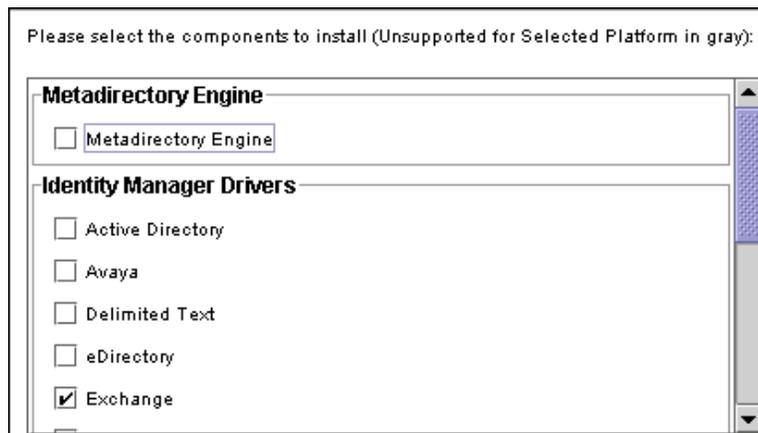
- 1 From the CD or download image, run the installation program.

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 DirXML 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 DirXML Overview dialog box, review the 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 *Exchange*, then click *Next*.



- 7 In the Identity Manager Upgrade Warning dialog box, click *OK*.
- 8 In the Summary dialog box, review selected options, then click *Finish*.

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

After installing the driver shim, create and configure a driver object. Do this by completing [Section 2.4, “Post-Installation Tasks,”](#) on page 17.

## 2.4 Post-Installation Tasks

- “Importing the Driver Configuration File” on page 17
- “Configuring the Exchange Server” on page 19
- “Installing a Remote Exchange Driver” on page 21
- “Configuring the Driver Filter” on page 22
- “Starting the Driver” on page 23
- “Migrating and Resynchronizing Data” on page 23
- “Activating the Driver” on page 24

### 2.4.1 Importing the Driver Configuration File

The sample Exchange 5.5 driver configuration creates and configures the objects needed to make the driver work properly.

For example, consider the following scenario:

You create a driver set and driver object in the lab. After configuring the driver, you save the configuration. To save time and keep the same settings that worked well in the lab, you import the driver’s configuration file from the lab environment into your production environment.

#### Importing by Using iManager

1 In iManager, select *Identity Manager Utilities > Import Drivers*.

2 Select whether to place the configuration file in a new or existing driver set.

Select *In an Existing Driver Set* for the following situations:

- The driver should be logically grouped with the other drivers in the tree.
- The server can handle the additional traffic that would the new driver would generate.
- You want to update or customize an existing driver.

For example, you can point the driver to a different container but keep all the rules that you have set up.

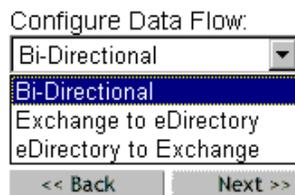
3 In the Import Drivers dialog box, select the Exchange 5\_5 driver, then click *Next*.



4 Scroll to the following parameters and provide required information. Refer to the descriptions provided in the interface.

- *Driver name*
- *Domain name*

- *IP address of the Exchange Server*
- *Authoritative Bind*  
See [Section 4.4, “Using Authoritative Bind,”](#) on page 33.
- *Exchange Server Name*
- *Exchange Site Organization*
- *Exchange Site*
- *Polling Frequency*
- *Authoritative User*
- *User Password*
- *eDir Users Container*
- *eDir Groups Container*
- *Configure Data Flow*



- *Password Failure Notification User*
- *Enable Entitlements*  
Using Role-Based Entitlements is a design decision. Don't select this option unless you have reviewed [“Creating and Using Entitlements”](#) in *Novell Identity Manager 3.0.1 Administration Guide*.

If you select this option, also provide information for *Action - Remove Mailbox Entitlement*.

- *Action - Remove Mailbox Entitlement*
- *Driver is Remote/Local*
- Remote Host Name and Port
- Driver Password
- Remote Password

**5** Define security equivalences.

The tendency is to assign Admin. However, you might want to create a DriversUser (for example) and assign security equivalence to that user.

**6** Identify all objects that represent Administrative Roles and exclude them from replication.

Exclude the security-equivalence object (for example, DriversUser) that you specified in Step 5. If you delete the security-equivalence object, you have removed the rights from the driver. Therefore, the driver can't make changes to the Identity Vault.

**7** (Conditional) If you are re-creating or updating a driver, select *Update Everything about That Driver*, then click *Next*.

**8** In the Summary screen, review options, then click *Finish*.

If you need to make changes, click *Back*.

After importing, configure the Driver Set object and the Driver object for your setup, then start or restart the driver.

### Importing by Using Designer for Identity Manager

You can import the basic driver configuration file for JDBC 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 *Exchange55.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.
- 6 After specifying parameters, click *OK* to import the driver.
- 7 Customize and test the driver.
- 8 Deploy the driver into the Identity Vault.

## 2.4.2 Configuring the Exchange Server

This section contains information on configuring the Exchange server for use with the Identity Manager Driver for Exchange. You should already be familiar with Exchange administration and deployment.

Before you proceed, you must have the following information about your setup:

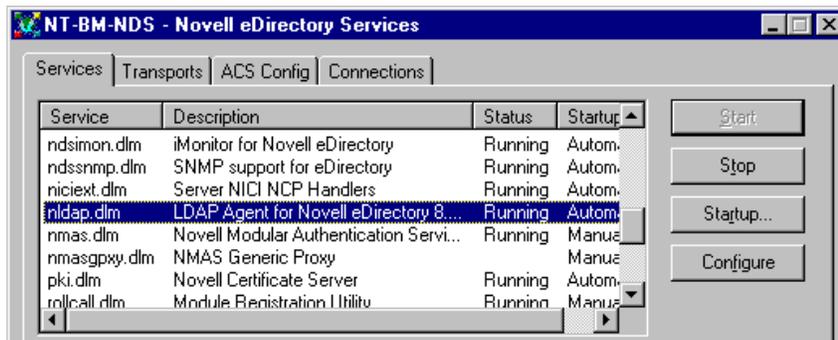
- The name of the Exchange Server that the driver will be synchronizing with.
- The name of the Exchange site you want to administer.
- The IP address or hostname of the Exchange server.
- The name of the Exchange service account and its password.

If the Exchange server is running on the same computer as the Identity Vault, unload the LDAP server or reconfigure it to run on a different port.

To unload LDAP:

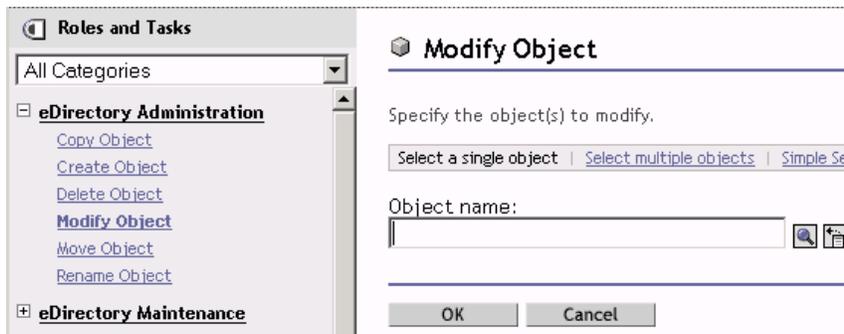
- 1 In the *Control Panel*, double-click *Novell eDirectory*.

- 2 Scroll to and select `ldap.dlm`, then click *Stop*.

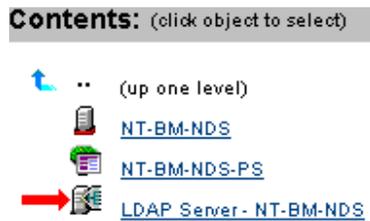


To reconfigure LDAP to run on a different port:

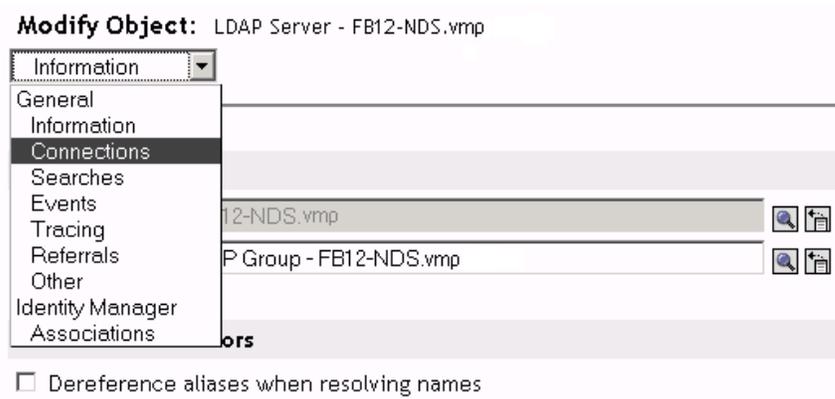
- 1 In Novell iManager, select *eDirectory Administration > Modify Object*.



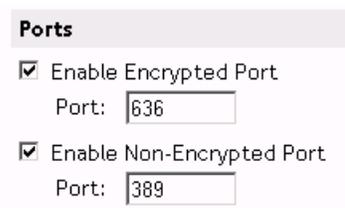
- 2 Navigate to and select the LDAP Server object.



3 From the drop-down list, select *General > Connections*.



4 Scroll to the Ports section.



5 Change *Enable Non-Encrypted Port* to a value other than 389, then click *OK*.

If another LDAP service is already using port 389, change the Exchange server's LDAP port number so that it doesn't conflict with the other service. If you change the Exchange server's port number, also change the LDAP port that the Identity Manager Driver for Exchange looks at. See [Section 4.6, "Specifying the LDAP Port," on page 34](#).

### 2.4.3 Installing a Remote Exchange Driver

The driver doesn't need to run on the same machine as the Exchange Server. However, when running remotely, the driver can run only on an NT server or member server that belongs to the same domain as the Exchange server domain. This restriction is a Microsoft-imposed NT credential restriction.

The NT server where you install the driver needs to have three Microsoft .dll files installed before the driver can run: `libxds.dll`, `exchmem.dll`, and `expsrv.dll`. The files are installed by the Exchange Administrator program. You can install Exchange Administrator from the *Microsoft Exchange Server CD*.

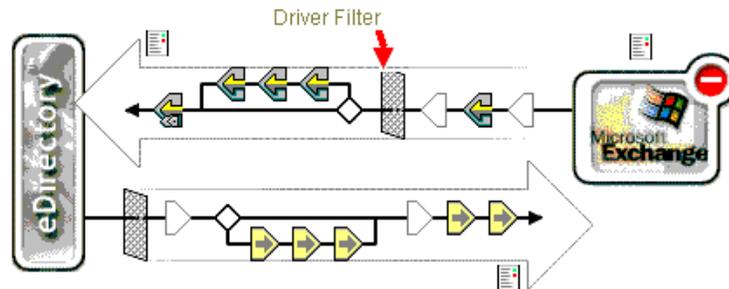
A remote driver doesn't create NT accounts when a new Exchange mailbox is created. This is also because of restrictions imposed by the Microsoft DAPI API that the driver uses.

For instructions on installing the Remote Loader, see "[Setting Up a Connected System](#)" in *Novell Identity Manager 3.0.1 Administration Guide*.

## 2.4.4 Configuring the Driver Filter

Modify the filter on the Publisher and Subscriber channels to include object classes and attributes that you want Identity Manager to process.

- 1 In iManager, click *Identity Manager > Identity Manager Overview*.
- 2 Locate the driver set that contains the Exchange driver, then click the driver's icon to display the Identity Manager Driver Overview page.
- 3 Click the driver filter icon.



- 4 (Optional) Add classes that you want Identity Manager to process.

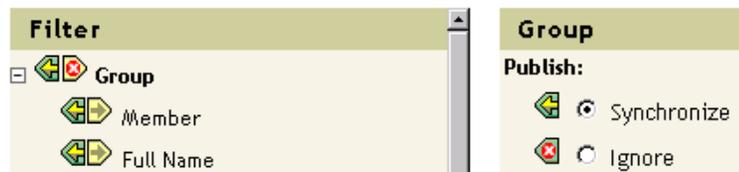
The Exchange driver supports the Distribution List, Remote, and Mailbox classes.

- 5 Enable synchronization.

As the following figure illustrates with red Xs, when you add a class, the Publisher and Subscriber channels aren't enabled.



To enable a channel, click the channel icon, then click *Synchronize*.

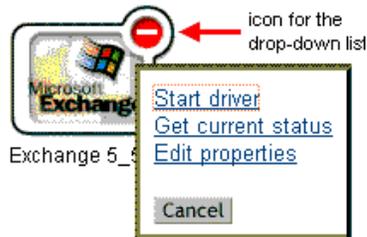


- 6 Save changes by clicking *OK*.

Mail-nickname is the Alias attribute on the General page in the Exchange Administrator. It is the Exchange attribute name that the driver supports but does not map to any existing eDirectory attributes. Based on your organization's needs, you can map this Exchange attribute to existing or new eDirectory attributes (after extending the schema) by modifying the Schema Mapping policy. Make sure that the syntax for any maps you add is valid. You can also handle this in a style sheet.

## 2.4.5 Starting the Driver

- 1 In iManager, click *Identity Manager > Identity Manager Overview*.
- 2 Browse to and select the driver set where the driver exists.
- 3 In the driver that you want to start, click the icon for the drop-down list.



- 4 Select *Start Driver*.

After the driver starts, you can open DSTrace to see driver processing details.

Synchronization takes place on an object-by-object basis as changes are made to individual objects. To have immediate synchronization, initiate synchronization as explained in [“Migrating and Resynchronizing Data” on page 23](#).

## 2.4.6 Migrating and Resynchronizing Data

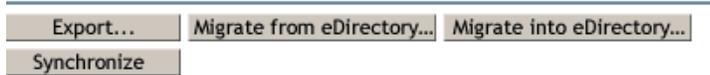
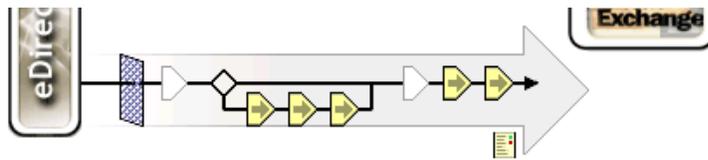
Identity Manager synchronizes data as it changes. If you want to synchronize all data immediately, you can choose from the following options:

- **Migrate Data from eDirectory:** Allows you to select containers or objects you want to migrate from eDirectory to an application. When you migrate an object, the Metadirectory engine applies all of the Matching, Placement, and Create policies, as well as the Subscriber filter, to the object.
- **Migrate Data into eDirectory:** Allows you to define the criteria the Metadirectory engine uses to migrate objects from an application into Novell eDirectory. When you migrate an object, the Metadirectory engine applies all of the Matching, Placement, and Create policies, as well as the Publisher filter, to the object. Objects are migrated into eDirectory by using the order you specify in the Class list.
- **Synchronize:** The Metadirectory engine looks in the Subscriber class filter and processes all objects for those classes. Associated objects are merged. Unassociated objects are processed as Add events.

To use one of the options explained above:

- 1 In iManager, select *Identity Manager > Identity Manager Overview*.
- 2 Locate the driver set containing the Exchange driver, then double-click the driver icon.

3 Click the appropriate migration button.



## 2.4.7 Activating the Driver

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

For information on activation, refer to “[Activating Novell Identity Manager Products](#)” in the *Identity Manager 3.0.1 Installation Guide*.

- “Running the Normalize Exchange Associations Utility” on page 25
- “Upgrading the Driver Shim” on page 26
- “Upgrading the Driver Configuration” on page 26

## 3.1 Running the Normalize Exchange Associations Utility

If you are upgrading from the DirXML<sup>®</sup> Driver 1.0 for Exchange, you need to run the Normalize Exchange Associations utility. This utility searches the eDirectory tree and normalizes the Identity Manager Driver for Exchange associations.

---

**NOTE:** If you are upgrading from the 1.0a patch or later, you don't need to run the Normalize Exchange Associations utility.

---

- 1 Get the `changeAssocKey.zip` file from Novell<sup>®</sup> Support.
- 2 Create a temporary directory on the NT server where the Identity Manager Driver for Exchange is installed.
- 3 Expand `changeAssocKey.zip` into the directory.
- 4 Open the `run.bat` file and edit the file with these parameters:

---

Parameter	Value
Java	Driver letter and path for Java*. For example, enter C:\Novell\consoleone\1.2\jre\bin\java or D:\Novell\NDS\jre\bin\java
LDAP address:port	The IP address and port number of the Identity Vault server. Normally, this is localhost:389.
LDAP Bind ID	The LDAP authentication ID.
LDAP Bind Password	The LDAP authentication password.
Driver Name	The name of the Driver object. For example, ExchangeDriver.
Action	Specify one of these desired actions: <ul style="list-style-type: none"><li>• 1- Lists Identity Vault objects with no association to the driver specified above.</li><li>• 2- Lists Identity Vault objects with an incomplete association to the driver specified above.</li><li>• 3- Lists Identity Vault objects with associations to be normalized.</li><li>• 4- Modifies the associations in the Identity Vault and lists the objects.</li></ul>

---

---

**NOTE:** We recommend that you first set the action to 3 so you can see what associations will change when you set the action to 4. Then, you can set the action to 4 and run the program again. You don't cause any problems by running the program more than once. If you are concerned about the current state of the associations, you can run the utility with the action set to 1 or 2.

---

5 Run the `run.bat` file.

## 3.2 Upgrading the Driver Shim

---

**NOTE:** Running an Identity Manager driver configuration with a DirXML 1.x driver shim is not supported.

---

When you upgrade, the new driver shim replaces the previous driver shim but keeps the previous driver's configuration. The new driver shim can run the DirXML 1.x configuration with no changes.

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.

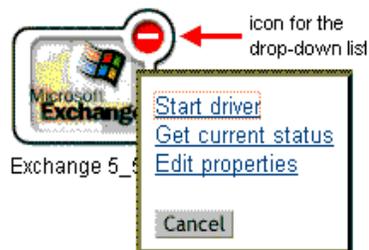
You can do this at the same time that you install the Metadirectory engine, or you can do it after the engine is installed. See [“Installing the Driver Shim for Exchange” on page 15](#).

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 Activate the driver shim with your Identity Manager activation credentials.

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 26](#).

## 3.3 Upgrading the Driver Configuration

You can run a DirXML 1.x driver configuration with a driver shim for this release of Identity Manager and the Metadirectory engine, with no changes to the driver configuration.

However, you might want to edit a DirXML 1.x driver configuration. To do this, do one of the following:

- Use the DirXML 1.x iManager plug-ins.

See “[Managing DirXML 1.1a Drivers in an Identity Manager Environment](#)” in *Novell Identity Manager 3.0.1 Administration Guide*.

- Run the wizard that converts DirXML 1.x configurations to Identity Manager format so that you can use the iManager plug-ins for Identity Manager.

See “[Upgrading a Driver Configuration from DirXML 1.1a to Identity Manager Format](#)” in *Novell Identity Manager 3.0.1 Administration Guide*.

To take advantage of the features of Identity Manager, do the following:

- Review the sample configuration provided.
- For information on new features, see *Novell Identity Manager 3.0.1 Administration Guide*.



# Customizing the Identity Manager Driver for Exchange

# 4

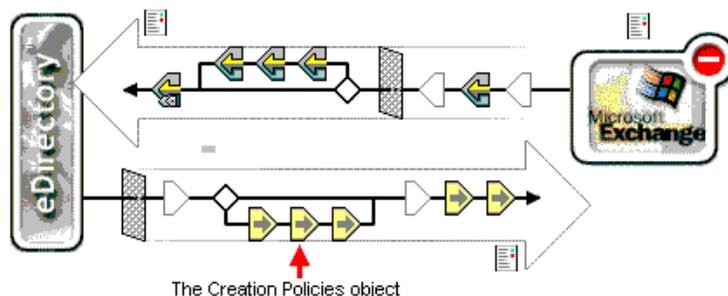
- “Integrating the Identity Manager Driver for Exchange and the Identity Manager Driver for NT Domain” on page 29
- “Managing External Recipients” on page 31
- “Synchronizing Proxy-Address and Target-Address Attributes” on page 32
- “Using Authoritative Bind” on page 33
- “Using a Custom Bind” on page 33
- “Specifying the LDAP Port” on page 34

## 4.1 Integrating the Identity Manager Driver for Exchange and the Identity Manager Driver for NT Domain

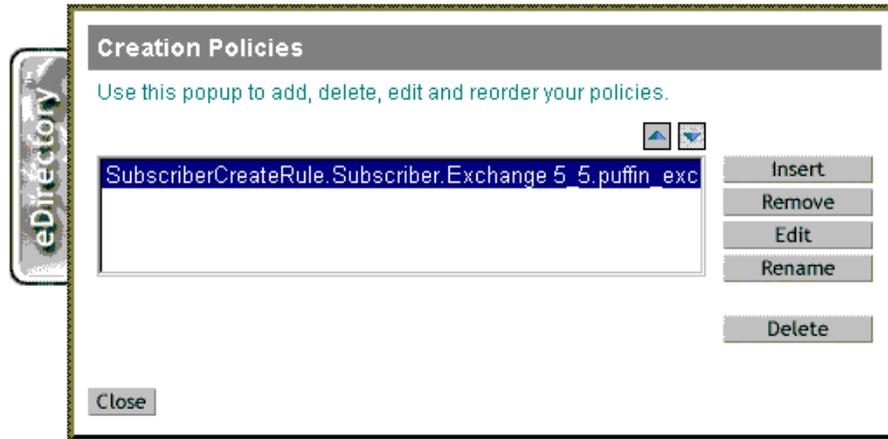
**IMPORTANT:** If you are using the Identity Manager Driver for NT Domain and the Identity Manager Driver for Exchange, edit the default policy or create a new one to resolve an account issue between the two drivers. This policy prevents the Exchange driver from attempting to create an NT Domain account before the NT Domain driver creates the account.

The Identity Manager Driver for NT Domain has a User attribute called DirXML-NTAccountName. This attribute contains the DomainName/UserName value. The Exchange MailBox object needs the value to associate to a domain account. For that association to occur correctly, the value in DirXML-NTAccountName needs to be put in the MailBox attribute Assoc-NT-Account. Keep in mind that attribute names are case sensitive.

- 1 Create a policy so that a new MailBox object isn't created unless the DirXML-NTAccountName attribute is populated.
  - 1a In iManager, select *Identity Manager > Identity Manager Overview*.
  - 1b Select the Creation Policies object on the Subscriber channel.



1c In the Creation Policies dialog box, click *Edit*.



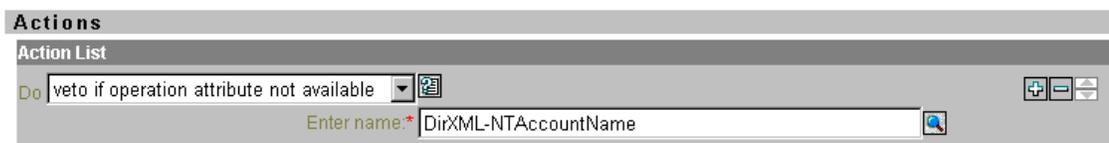
1d Click *User Required Attributes*.



1e In the Actions section, add an action for the DirXML-NTAccountName attribute. Click the + icon, then select *Veto If Operation Attribute Not Available* from the *Do* drop-down list.

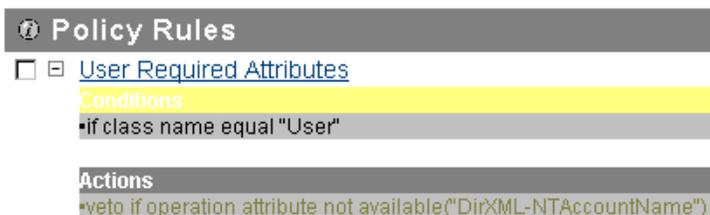


Select *DirXML-NTAccountName* from the *Enter Name* drop-down list.

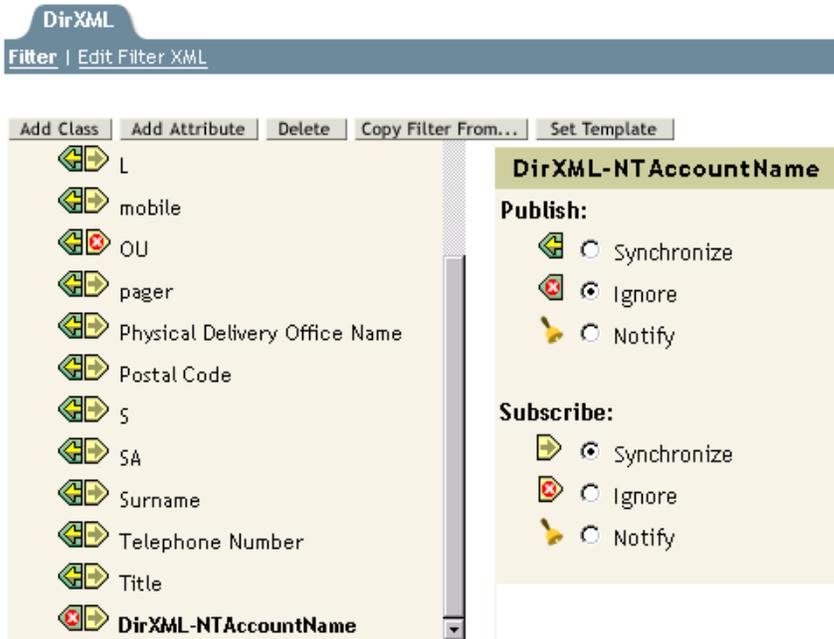


1f Click *OK*.

As the following figure illustrates, the action is placed in the User Required Attributes section.



- 2 Verify that the DirXML-NTAccountName attribute is in the following locations:
  - The Publisher filter on the Identity Manager Driver for NT Domains
  - The Subscriber filter on the Identity Manager Driver for Exchange
- 3 Synchronize the Subscriber channel.



- 4 Restart both drivers.

After you have made these changes to the drivers, the following control flow occurs when you create a user in an Identity Vault:

1. The Identity Manager Driver for NT Domain is handed a create request.
2. The Identity Manager Driver for Exchange Create event is vetoed because of the absence of the DirXML-NTAccountName attribute.
3. The Identity Manager Driver for NT Domain creates the NT account and publishes the name of the NT account just created to the DirXML-NTAccountName attribute.
4. The Identity Manager Driver for Exchange is notified. It creates the mailbox and associates the mailbox with the NT account information stored in the Identity Vault.

---

**NOTE:** The examples used DirXML-NTAccountName as the eDirectory™ attribute to hold the NT account information, but you can choose any attribute that works for you.

---

## 4.2 Managing External Recipients

Microsoft Exchange directories let you create special objects called External Recipients. Think of these objects as address book entries that represent recipients in external messaging systems. You can modify the Schema Mapping policy so that you can map a remote object to a User object or any other desired Identity Vault object. For example:

```

<class-name>
  <nds-name>User</nds-name>
  <app-name>remote</app-name>
</class-name>

```

If you decide to make this change, you should also add the Internet EMail Address attribute as a required attribute to the Create policy as shown in the following example:

```

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

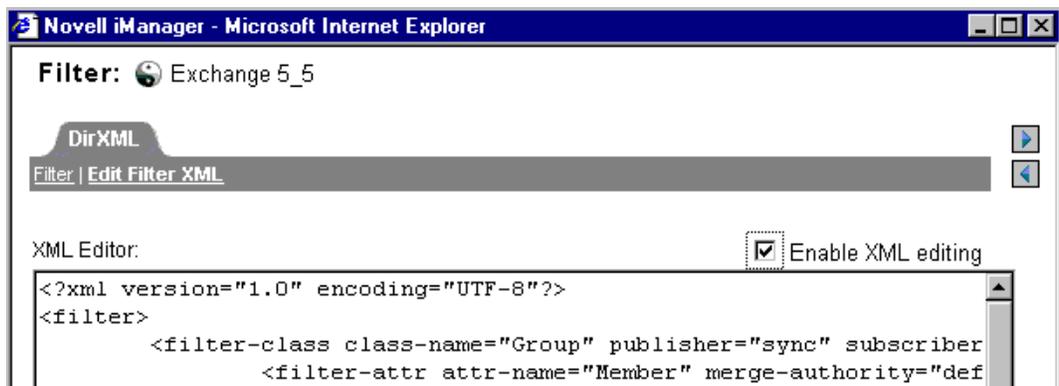
```

An Internet EMail Address attribute is required to create an External Recipient object in the Exchange directory. Failure to add the Internet EMail Address attribute results in an error when you try to create an External Recipient.

## 4.3 Synchronizing Proxy-Address and Target-Address Attributes

To synchronize all the e-mail values of the multivalue Proxy-Address and Target-Address attributes, add the `<proxyFlg/>` tag to the driver parameters.

- 1 In iManager, click *eDirectory Administration > Modify Object*.
- 2 Locate and select the Identity Manager Driver for Exchange object (for example, EXCHANGE 5\_5), then click *OK*.
- 3 Locate the *Driver Parameters* section at the bottom of the Driver Configuration page, then click *Edit XML*.
- 4 Click *Enable XML Editing* so that you can edit the script.



- 5 Add the `<proxyFlg/>` tag.

This tag can go anywhere between the `<driver-options>` tags. The updated parameters could look similar to the following example:

```

<driver-options>
  <x-ldap-server display-name="IP address of Exchange Server (for
LDAP queries) :">167.55.135.28</x-ldap-server>
  <x-remote display-name="Remote Exchange Driver?(1=true;

```

```

0=false):">0</x-remote>
  <x-server display-name="Exchange Server Name:">DHEAD</x-
server>
      <x-site display-name="Exchange Site:">/o=Novell/
ou=DOMAINLIMA</x-site>
      <proxyFlg/>
</driver-options>

```

**6** Deselect *Enable XML Editing*, then return to the *Driver Parameters* section.

**7** Click *OK*.

## 4.4 Using Authoritative Bind

Whenever a query happens with a scope of subordinate or subtree, the driver uses LDAP. In the past, only an anonymous bind was possible. When using an anonymous bind, the driver can't see attributes that are hidden in Exchange.

The new `AuthoritativeBind` parameter lets you use an authoritative LDAP bind instead of an anonymous LDAP bind. This option is one of the prompts when you import the sample driver configuration.

We recommend that you use authoritative bind only in cases where you need to see hidden attributes, such as when you want to do matching based on a hidden attribute.

Keep in mind that when you use authoritative bind, hidden attributes, such as `NT4AccountName`, are seen in the trace. After using authoritative bind for a specific purpose such as migrating users, if you no longer need to use authoritative bind, you could change the driver parameters back to using anonymous bind.

## 4.5 Using a Custom Bind

You might need to bind to LDAP by using a custom bind. For example, to find hidden objects in Exchange, you need to bind as user admin.

To use a custom bind:

**1** In the *Driver Parameters* section, click *Edit XML*.

**Driver Parameters**

---

S3K-NDS.Vmp

**Driver Settings**

Exchange LDAP Server	<input type="text"/>
Create NT Security Account 0=Yes 1=No	<input type="text" value="0"/>
Exchange Server	<input type="text"/>
Exchange Site	<input "="" type="text" value="/o=/ou="/>
Authoritative Bind:	<input type="text" value="Yes"/>

**2** Click *Enable XML Editing*.

3 In the <driver-options> section, add the tags and string that specify a custom bind.

For example, type

```
<hiddenObjectBind>cn=Administrator,dc=DOMAIN,cn=admin</hiddenObjectBind/>
```

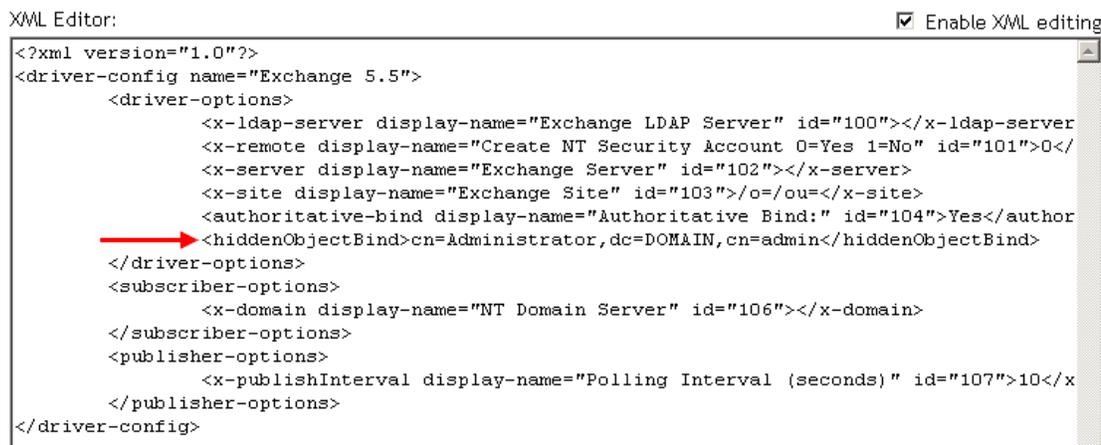
This example uses the following, which you need to customize in your configuration:

String	Description
Administrator	A user with administrative rights
DOMAIN	The name of your domain

The following figure illustrates these tags and string:

**Figure 4-1** Syntax for a custom bind

**Driver:** Exchange 5\_5.hraun\_set.Vmp  
**Server:** S3K-NDS.Vmp



```
XML Editor:  Enable XML editing
<?xml version="1.0"?>
<driver-config name="Exchange 5.5">
  <driver-options>
    <x-ldap-server display-name="Exchange LD&P Server" id="100"></x-ldap-server
    <x-remote display-name="Create NT Security Account 0=Yes 1=No" id="101">0</
    <x-server display-name="Exchange Server" id="102"></x-server>
    <x-site display-name="Exchange Site" id="103">/o=/ou=</x-site>
    <authoritative-bind display-name="Authoritative Bind:" id="104">Yes</author
    <hiddenObjectBind>cn=Administrator,dc=DOMAIN,cn=admin</hiddenObjectBind>
  </driver-options>
  <subscriber-options>
    <x-domain display-name="NT Domain Server" id="106"></x-domain>
  </subscriber-options>
  <publisher-options>
    <x-publishInterval display-name="Polling Interval (seconds)" id="107">10</x
  </publisher-options>
</driver-config>
```

4 Click *OK* twice.

The Exchange driver then uses the string in the tag as the user for the bind.

Also, an additional value to not allow deleted objects is placed in the search filter.

If this custom tag is present, it overrides the authoritative bind tag. If it isn't present, the authoritative bind takes precedence. If neither tag is present, an anonymous bind is used.

## 4.6 Specifying the LDAP Port

If you changed the Exchange Server's port number from the default 389 value, you need to configure the Identity Manager Driver for Exchange, so that it looks at the port that the server users.

- 1 In the Driver Parameters section, click *Edit XML*.
- 2 Click *Enable XML Editing*.

- 3 In the <driver-options> section, add the tags (<ldap-port></ldap-port> and value (for example, 391) that specify the different port number.

**Driver:** Exchange\_5\_5.hraun\_set.Vmp  
**Server:** S3K-NDS.Vmp

XML Editor:  Enable XML editing

```
<?xml version="1.0"?>
<driver-config name="Exchange 5.5">
  <driver-options>
    <x-ldap-server display-name="Exchange LDAP Server" id="100"></x-ldap-server>
    <x-remote display-name="Create NT Security Account 0=Yes 1=No" id="101">0</x-remote>
    <x-server display-name="Exchange Server" id="102"></x-server>
    <x-site display-name="Exchange Site" id="103">/o=/ou=</x-site>
    <authoritative-bind display-name="Authoritative Bind:" id="104">Yes</authoritative-bind>
    <hiddenObjectBind id="105">cn=Administrator,dc=DOMAIN,cn=admin</hiddenObjectBind>
    <ldap-port>391</ldap-port>
  </driver-options>
</driver-config>
```

- 4 Click *OK* twice.



# Troubleshooting the Driver

# 5

This section provides information on the following:

- “[Troubleshooting](#)” on page 37
- “[Driver Error Messages](#)” on page 37

## 5.1 Troubleshooting

- Exchange Directory names used in the Placement policy are case sensitive.
- If Exchange and the Identity Vault are running on the same machine, you must disable the Identity Vault LDAP server or change the port assignment from port 389.
- If you encounter syntax errors in XML, verify the syntax by using Identity Manager and a Web browser.
- The authentication credentials you specify should be for an NT account/domain that has rights to the Exchange Directory.
- CN and Object-Class should not be in the filter.
- If there is an invalid attribute in the filter (for example, one for which Schema Mapping is not defined), the following happens:
  - At each polling loop, the Publisher fails to synchronize the class that contains the invalid attribute, and gives an error indicating an unsupported attribute.
  - The driver is still able to start.
  - The Subscriber channel still functions correctly unless the invalid attribute is referenced. A task that references an invalid attribute gives an error and is not successful.

The sample driver configuration supports the standard attributes in Exchange, so this issue could occur only for custom attributes you have added in Exchange.

- The Identity Manager Driver for Exchange supports the following classes:
  - Distribution List
  - Remote
  - Mailbox

## 5.2 Driver Error Messages

The following is a list of error messages the driver might return:

- `USN Cache Initialized from disk`

This is an informational message printed at the beginning of the driver initialization. The message indicates that the driver’s last state was read from the disk.

- `USN Cache could not be initialized. Most likely reason:  
Insufficient memory.`

The previous driver state was not initialized correctly. This means that another process manipulated the registry or the driver configuration file. This might happen if you accidentally deleted one of the driver configuration files. This results in a loss of event data.

- DAPIStart() failed. Please check the Event Log for details. Returned error code =

This usually suggests that the Exchange Server is down or could not be reached. The NT Application Event Log should contain a more detailed description of the error.

- DAPIStart() encountered non fatal error. Please check the Event Log for details. Returned error code =

This error message is returned when Exchange returned a warning. The returned warning is logged in the NT Application Event Log.

- Call to Import function failed. Likely cause- bad XML or too little memory.
- Subscriber Import attempt failed. Please check the NT Event Log for details. Returned error code =

An attempt to write to the Event log did not succeed.

- Subscriber Import attempt encountered non critical error. Please check the NT Event Log for details. Returned error code =
- A bad XML document was sent to the driver. Critical error in the Subscriber XML document.
- A bad XML document was sent to the driver. The subscriber could not process the input node.
- A bad XML document was sent to the driver. An unsupported operation type was received.
- A bad XML document was sent to the driver. The operation node could not be processed.
- Bad Subscriber filter or Subscriber filter contains an unsupported attribute. Please check the Subscriber filter.

An unsupported attribute was added to the Subscriber filter. Verify the Subscriber filter with the list of supported attributes in the file ATTRIBUTES.TXT (located in the NT\DIRXML\DRIVERS\EXCHANGE\RULES directory).

- Could not log in to Exchange with the specified credentials. Driver will not start.

The authentication credentials supplied were incorrect. The credentials specified should be for an NT account/domain that has rights to the Exchange directory.

- NT Event handles could not be created. The System could be low on memory
- An expected initialization parameter was missing from the parameter list.

One or more of the initialization parameters was missing. Try restarting. If the problem persists, try retyping the initialization parameters.

- Could not allocate memory.
- Failed to initialize the base of the USN cache. Driver will not start.

# Documentation Updates

# A

This section contains information about documentation content changes that have been made in this guide.

The information is grouped according to the date the documentation updates were published.

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

If you need to know whether a copy of the PDF documentation you are using is the most recent, the PDF document contains the date it was published in the Legal Notices section immediately following the title page.

The documentation was updated on the following dates:

## **A.1 August 10, 2006**

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