

Implementation Guide

Novell[®] Identity Manager Driver for GroupWise[®]

3.5.1

September 28, 2007

www.novell.com



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. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](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 © 2000-2007 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 on the [Novell Legal Patents Web page \(http://www.novell.com/company/legal/patents/\)](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 latest online documentation for this and other Novell products, see [the Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

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

Contents

About This Guide	9
1 Introducing the Identity Manager Driver for GroupWise	11
1.1 New Features	11
1.1.1 Driver Features	11
1.1.2 Identity Manager Features	12
1.2 Key Driver Features	12
1.2.1 Supported Platforms	12
1.2.2 Remote Platforms	12
1.2.3 Role-Based Entitlements	13
1.2.4 Password Synchronization Support	13
1.2.5 Objects Synchronized	13
1.3 Methods for Managing GroupWise Accounts	13
1.4 Driver Components	14
1.4.1 GroupWise API	14
1.4.2 Driver Shim	14
1.4.3 Driver Configuration	14
1.5 Publisher Channel Issues	14
1.6 Subscriber Channel Issues	15
2 Planning and Installing the Identity Manager Driver for GroupWise	17
2.1 Meeting the Requirements for the Driver	17
2.2 Planning for the Installation	17
2.2.1 Understanding a Local Installation	18
2.2.2 Understanding a Remote Installation	19
2.3 Configuring Driver Authentication	19
2.3.1 Creating a User Account for the System Containing the Driver for Windows	20
2.3.2 Creating a User Account for the System Containing the GroupWise Domain	22
2.4 Installing the Driver	24
3 Upgrading the Driver	25
3.1 Upgrading from the 2.1 Version of the GroupWise Driver	25
3.2 Upgrading from the 2.2 Version of the GroupWise Driver	26
3.3 Upgrading the GroupWise Database Version in the Driver Configuration	26
3.4 Upgrading the Driver to Use the Identity Manager 3.5 Architecture	27
3.4.1 Upgrading the Driver in Designer	28
3.4.2 Upgrading the Driver in iManager	30
4 Configuring the GroupWise Driver	33
4.1 Importing the Driver Configuration File in Designer	33
4.2 Importing the Driver Configuration in iManager	33
4.3 Configuration Parameters	34
4.4 Viewing Driver Parameters	41
4.5 Modifying Global Configuration Values	41
4.6 Post-Installation Tasks	42

4.6.1	Installation on NetWare	42
4.6.2	Modifying Policies	42
4.6.3	Modifying Global Configuration Values	42
4.6.4	Starting the Driver	42
4.6.5	Verifying That the Driver is Working Properly	43
4.6.6	Migrating eDirectory Users to GroupWise	43
5	Activating the Driver	45
6	Customizing the Driver by Using Policies and Filters	47
6.1	Default Driver Actions	47
6.2	Modifying Default Settings in Policies and the Filter	47
6.2.1	Modifying the Driver Filter	48
6.2.2	Adding Entries to the Schema Mapping Policy	48
6.2.3	Modifying the Create Policy	48
6.2.4	Modifying the Matching Policy	48
6.3	Modifying Policies	48
6.3.1	Specifying the GroupWise Post Office	49
6.3.2	Specifying Distribution Lists	51
6.3.3	Setting Defaults for GroupWise Attributes	55
6.3.4	Configuring the GroupWise UserID	55
6.3.5	Creating Mappings for Additional Attributes	56
6.3.6	Getting a Record Count from a Query	56
6.3.7	Deleting the GroupWise User without Deleting the eDirectory User	57
6.3.8	Creating a GroupWise Nickname	57
6.3.9	Creating a GroupWise Nickname Record	58
6.3.10	Specifying a New Resource Owner on an Owner Delete	59
6.3.11	Specifying a New Resource Owner on an Owner Disable	60
6.3.12	Controlling Creation of GroupWise Accounts	60
6.3.13	Moving Users from One Post Office to Another Post Office	61
6.3.14	Adding Additional Attributes to Be Synchronized	62
6.3.15	Renaming Users	62
6.3.16	Creating a Gateway Alias	63
6.3.17	Querying for a Nickname	64
6.3.18	Querying for a Gateway Alias	66
6.3.19	Querying for Internet EMail Address	67
6.3.20	Synchronizing GroupWise External Users	68
6.3.21	Verifying if an E-Mail Address or Gateway Alias Is Unique	70
6.4	Setting GroupWise Client Options with the Driver	72
6.4.1	Using Policies to Set Client Options	72
6.4.2	Client Options	74
6.4.3	Environment > General	75
6.4.4	Environment > Client Access	78
6.4.5	Environment > Views	79
6.4.6	Environment > File Location > Archive Directory	82
6.4.7	Environment > Cleanup	83
6.4.8	Send > Send Options	85
6.4.9	Send > Mail	89
6.4.10	Send > Appt	92
6.4.11	Send > Task	95
6.4.12	Send > Note	98
6.4.13	Send > Security	101
6.4.14	Send > Disk Space Management	103
6.4.15	Date and Time > Calendar	106
6.4.16	Date and Time > Calendar > Alarm Options	109
6.4.17	Date and Time > Busy Search	111

6.5	Client Options Quick Reference	113
6.5.1	Environment	114
6.5.2	Send	114
6.5.3	Date and Time	116
7	Managing the Driver	117
7.1	Using Anti-Virus Software on a GroupWise System	117
7.2	Disabling the Driver	117
7.3	Partition Issues	117
7.4	Driver Access Rights and Membership	118
7.5	Synchronizing Group Objects	118
7.6	Synchronizing GroupWise Distribution List Objects	118
7.7	Using the GroupWise Snap-Ins to Remove a GroupWise Account	118
7.8	Re-associating a GroupWise Account with an eDirectory User	119
7.9	User Renames	119
7.10	Starting, Stopping, or Restarting the Driver	119
7.10.1	Starting the Driver in Designer	119
7.10.2	Starting the Driver in iManager	120
7.10.3	Stopping the Driver in Designer	120
7.10.4	Stopping the Driver in iManager	120
7.10.5	Restarting the Driver in Designer	120
7.10.6	Restarting the Driver in iManager	120
7.11	Migrating and Resynchronizing Data	120
7.12	Using the DirXML Command Line Utility	121
7.13	Viewing Driver Versioning Information	121
7.13.1	Viewing a Hierarchical Display of Versioning Information	121
7.13.2	Viewing the Versioning Information as a Text File	123
7.13.3	Saving Versioning Information	125
7.14	Reassociating a Driver Set Object with a Server Object	126
7.15	Changing the Driver Configuration	126
7.16	Storing Driver Passwords Securely with Named Passwords	126
7.16.1	Using Designer to Configure Named Passwords	127
7.16.2	Using iManager to Configure Named Passwords	127
7.16.3	Using Named Passwords in Driver Policies	129
7.16.4	Using the DirXML Command Line Utility to Configure Named Passwords	129
7.17	Adding a Driver Heartbeat	133
8	Synchronizing Objects	135
8.1	What Is Synchronization?	135
8.2	When Is Synchronization Done?	135
8.3	How Does the Metadirectory Engine Decide Which Object to Synchronize?	136
8.4	How Does Synchronization Work?	137
8.4.1	Scenario One	137
8.4.2	Scenario Two	139
8.4.3	Scenario Three	140
9	Troubleshooting the Identity Manager Driver for GroupWise	143
9.1	Avoiding Data Corruption	143
9.2	Error Messages	143
9.3	Troubleshooting Driver Processes	150
9.3.1	Viewing Driver Processes	150

10 Backing Up the Driver	157
10.1 Exporting the Driver in Designer	157
10.2 Exporting the Driver in iManager	157
11 Security: Best Practices	159
A Class and Attribute Descriptions	161
B DirXML Command Line Utility	171
B.1 Interactive Mode.....	171
B.2 Command Line Mode.....	180
C Properties of the Driver	185
C.1 Driver Configuration	185
C.1.1 Driver Module	186
C.1.2 Driver Object Password	186
C.1.3 Authentication	187
C.1.4 Startup Option	188
C.1.5 Driver Parameters	189
C.2 Global Configuration Values	190
C.3 Named Passwords	195
C.4 Engine Control Values	196
C.5 Log Level	198
C.6 Driver Image.....	199
C.7 Security Equals	199
C.8 Filter	200
C.9 Edit Filter XML	200
C.10 Misc	201
C.11 Excluded Users	201
C.12 Driver Manifest.....	202
C.13 Driver Inspector	202
C.14 Driver Cache Inspector	203
C.15 Inspector	203
C.16 Server Variables.....	204

About This Guide

This driver provides data integration between users in an Identity Vault and GroupWise®. For example, the driver can automatically create e-mail accounts when an employee is hired. The driver can also disable an e-mail account when a user is no longer active. This configurable solution gives organizations the ability to increase productivity and streamline business processes by integrating GroupWise and an Identity Vault.

The guide contains the following sections:

- ♦ Chapter 1, “Introducing the Identity Manager Driver for GroupWise,” on page 11
- ♦ Chapter 2, “Planning and Installing the Identity Manager Driver for GroupWise,” on page 17
- ♦ Chapter 3, “Upgrading the Driver,” on page 25
- ♦ Chapter 4, “Configuring the GroupWise Driver,” on page 33
- ♦ Chapter 5, “Activating the Driver,” on page 45
- ♦ Chapter 6, “Customizing the Driver by Using Policies and Filters,” on page 47
- ♦ Chapter 7, “Managing the Driver,” on page 117
- ♦ Chapter 8, “Synchronizing Objects,” on page 135
- ♦ Chapter 9, “Troubleshooting the Identity Manager Driver for GroupWise,” on page 143
- ♦ Chapter 10, “Backing Up the Driver,” on page 157
- ♦ Chapter 11, “Security: Best Practices,” on page 159
- ♦ Appendix A, “Class and Attribute Descriptions,” on page 161
- ♦ Appendix B, “DirXML Command Line Utility,” on page 171
- ♦ Appendix C, “Properties of the Driver,” on page 185

Audience

This guide is for Identity Manager and GroupWise administrators who are using the Identity Manager Driver for GroupWise.

Feedback

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

Documentation Updates

For the most recent version of this document, see the [Drivers Documentation Web site \(http://www.novell.com/documentation/idm35drivers/index.html\)](http://www.novell.com/documentation/idm35drivers/index.html)

Additional Documentation

For documentation on using Identity Manager and the other Identity Manager drivers, see the [Identity Manager Documentation Web site \(http://www.novell.com/documentation/idm35\)](http://www.novell.com/documentation/idm35).

Documentation Conventions

The term *driver* refers to all components of the Identity Manager Driver for GroupWise and not to any one particular component.

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 GroupWise

1

The Identity Manager Driver for GroupWise® is designed to synchronize data between the Identity Vault and GroupWise, and to manage GroupWise accounts and account information. When a user or group in the Identity Vault is modified, created, renamed, moved, or deleted, the driver synchronizes the changes with the GroupWise accounts.

Because the Identity Vault is the authoritative data source, any data created, modified, renamed, and deleted in the Identity Vault synchronizes to GroupWise.

- ♦ [Section 1.1, “New Features,” on page 11](#)
- ♦ [Section 1.2, “Key Driver Features,” on page 12](#)
- ♦ [Section 1.3, “Methods for Managing GroupWise Accounts,” on page 13](#)
- ♦ [Section 1.4, “Driver Components,” on page 14](#)
- ♦ [Section 1.5, “Publisher Channel Issues,” on page 14](#)
- ♦ [Section 1.6, “Subscriber Channel Issues,” on page 15](#)

1.1 New Features

The following section contains information about the new driver features, as well as new features provided in Novell Identity Manager.

- ♦ [Section 1.1.1, “Driver Features,” on page 11](#)
- ♦ [Section 1.1.2, “Identity Manager Features,” on page 12](#)

1.1.1 Driver Features

This version of the driver provides the following new functionality:

- ♦ Updated the driver configuration file to allow for configuration of the following options:
 - ♦ GroupWise Distribution List synchronization options
 - ♦ GroupWise External Entity synchronization options
 - ♦ eDirectory™ Organizational Unit to GroupWise External Post Office synchronization
 - ♦ Cleanup Group Memberships option
 - ♦ Limiting the scope of object synchronization. It has been added as a global configuration value.

For more information on configuring the driver, see [Chapter 4, “Configuring the GroupWise Driver,” on page 33](#).

- ♦ Added information on setting GroupWise client options through the driver. For more information, see [Section 6.4, “Setting GroupWise Client Options with the Driver,” on page 72](#).

1.1.2 Identity Manager Features

For more information on the new features of Identity Manager, refer to “[What’s New in Identity Manager 3.5.1?](#)” in the *Identity Manager 3.5.1 Installation Guide*.

1.2 Key Driver Features

The sections below contain information about the key driver features.

- ♦ [Section 1.2.1, “Supported Platforms,” on page 12](#)
- ♦ [Section 1.2.2, “Remote Platforms,” on page 12](#)
- ♦ [Section 1.2.3, “Role-Based Entitlements,” on page 13](#)
- ♦ [Section 1.2.4, “Password Synchronization Support,” on page 13](#)
- ♦ [Section 1.2.5, “Objects Synchronized,” on page 13](#)

1.2.1 Supported Platforms

The GroupWise driver is supported on the following platforms:

- ♦ NetWare® 6.0 and NetWare 6.5 with the latest support packs
- ♦ Windows* 2000 and 2003 with the latest service packs
- ♦ SUSE® Linux Enterprise Server 9 and 10

The GroupWise driver is compatible with the following versions of GroupWise:

- ♦ GroupWise 5.5 with the latest support packs
- ♦ GroupWise 6.0 with the latest support packs
- ♦ GroupWise 6.5 with the latest support packs
- ♦ GroupWise 7.0 with the latest support packs

IMPORTANT: The GroupWise binaries in the older drivers are not compatible with GroupWise 7.0 databases. An Identity Manager 2.x driver with the `idm20xgwir3a.tgz` patch applied, is compatible with GroupWise 7.0 databases.

- ♦ GroupWise 8.0 with the latest support packs

IMPORTANT: The GroupWise binaries in the older drivers are not compatible with GroupWise 8.0 databases. An Identity Manager 3.5.x driver with the `idm360groupwiseir2.tar.gz` patch applied, is compatible with GroupWise 8.0 databases.

1.2.2 Remote Platforms

The GroupWise driver is supported on the following platforms running the Remote Loader:

- ♦ NetWare 6.0 and NetWare 6.5 with the latest support packs
- ♦ Windows 2000 and 2003 with the latest service packs
- ♦ SUSE Linux Enterprise Server 9 and 10

1.2.3 Role-Based Entitlements

The sample driver configuration supports Role-Based Entitlements. If the Role-Based Entitlements are enabled, the driver does the following actions by default:

- ◆ Adds User object accounts
- ◆ Removes User object accounts
- ◆ Adds members of the distribution list
- ◆ Removes members of the distribution list

1.2.4 Password Synchronization Support

The Subscriber channel sets the password. Passwords are not synchronized on the Publisher channel.

NOTE: The best practice is to configure GroupWise to authenticate against the Identity Vault, in which case password synchronization is not required.

1.2.5 Objects Synchronized

The GroupWise driver synchronizes users, groups, distribution lists, external entities, containers, and post offices.

1.3 Methods for Managing GroupWise Accounts

Before the Identity Manager driver for GroupWise was developed, you managed GroupWise accounts in conjunction with eDirectory entirely with the ConsoleOne® GroupWise snap-ins. Now, you can also use the driver to manage certain components of GroupWise accounts. For instance, you can automatically provision new users from eDirectory or your HR system by using Identity Manager.

We recommend that you make account changes in eDirectory. You should use either iManager or ConsoleOne (without the GroupWise snap-ins) to administer users in eDirectory, then let the driver synchronize any changes into GroupWise.

Do not use the ConsoleOne GroupWise snap-ins, iManager tasks associated with GroupWise, or other GroupWise administration tools for anything the driver is configured to do. When you have the driver installed, if you manage GroupWise user accounts with the ConsoleOne GroupWise snap-ins or other tools, it results in redundant synchronization of data because data changes are synchronized by both the snap-ins and the driver. Redundant synchronization of data might result in warnings or errors in the Identity Manager logs. However, these warnings or errors can usually be ignored.

WARNING: If you create eDirectory users with ConsoleOne, be sure to use ConsoleOne with GroupWise 6.5 or above snap-ins installed. If you are using GroupWise 6.0 or older versions, do not use ConsoleOne with the GroupWise snap-ins installed to create eDirectory users. The ConsoleOne snap-ins for the older GroupWise versions operate after the driver and remove some vital data from eDirectory.

You should use the GroupWise ConsoleOne snap-ins to manage these components of GroupWise accounts:

- ◆ GroupWise system-wide parameters, such as nickname expiration date
- ◆ X.400 information
- ◆ Resources
- ◆ Mailbox and library maintenance
- ◆ Client options and preferences
- ◆ Grafting (use caution)
- ◆ Backup and restore

1.4 Driver Components

The driver uses the following components:

- ◆ [Section 1.4.1, “GroupWise API,” on page 14](#)
- ◆ [Section 1.4.2, “Driver Shim,” on page 14](#)
- ◆ [Section 1.4.3, “Driver Configuration,” on page 14](#)

1.4.1 GroupWise API

This API is necessary for the driver to perform the required actions in GroupWise. It is installed together with the driver shim.

1.4.2 Driver Shim

A Java* driver shim is used to communicate between the Metadirectory engine and the GroupWise API. This driver shim is installed at the same time as the GroupWise API.

1.4.3 Driver Configuration

The XML driver configuration file contains all Identity Vault objects necessary for the driver, including the appropriate policies for adding, modifying, and deleting or disabling GroupWise accounts. In addition, the driver configuration file controls the information being sent from the Identity Vault to GroupWise. The driver configuration file should be installed to the computer where your management tool (iManager) resides.

1.5 Publisher Channel Issues

The driver filter specifies the classes and attributes that GroupWise publishes to eDirectory. We do not recommend making changes to the driver filter regarding which attributes are published to eDirectory. If the filter is changed, it can cause objects not to synchronize correctly.

1.6 Subscriber Channel Issues

GroupWise accounts are administered through eDirectory. Driver customizations are usually done in the Subscriber channel or at the driver level. The Subscriber channel receives commands from the Metadirectory engine and executes those commands in GroupWise. The Subscriber channel is used to synchronize eDirectory events with GroupWise. It watches for additions, modifications, renames, moves, and deletes in eDirectory and creates events in GroupWise to reflect those changes.

You can add to the base configuration that comes with the driver. However, do not remove or modify preconfigured attributes from the Subscriber filter or the Mapping policy.

Planning and Installing the Identity Manager Driver for GroupWise

2

If you have an existing driver, proceed to [Chapter 3, “Upgrading the Driver,” on page 25](#). You do not need to follow the instructions in this section.

- ◆ [Section 2.1, “Meeting the Requirements for the Driver,” on page 17](#)
- ◆ [Section 2.2, “Planning for the Installation,” on page 17](#)
- ◆ [Section 2.3, “Configuring Driver Authentication,” on page 19](#)
- ◆ [Section 2.4, “Installing the Driver,” on page 24](#)

2.1 Meeting the Requirements for the Driver

The Identity Manager Driver for GroupWise[®] has the following software requirements:

- Novell[®] Identity Manager 3.5 or above
- Novell Client[™] 4.9 or later for Windows 2000
- GroupWise 7

You can use earlier versions of GroupWise, but some new features might not be supported in earlier releases.

- GroupWise 8 with the latest support packs

Ensure that you have downloaded the latest patch. By default, Groupwise 8 is not supported on Identity Manager 3.5.1.

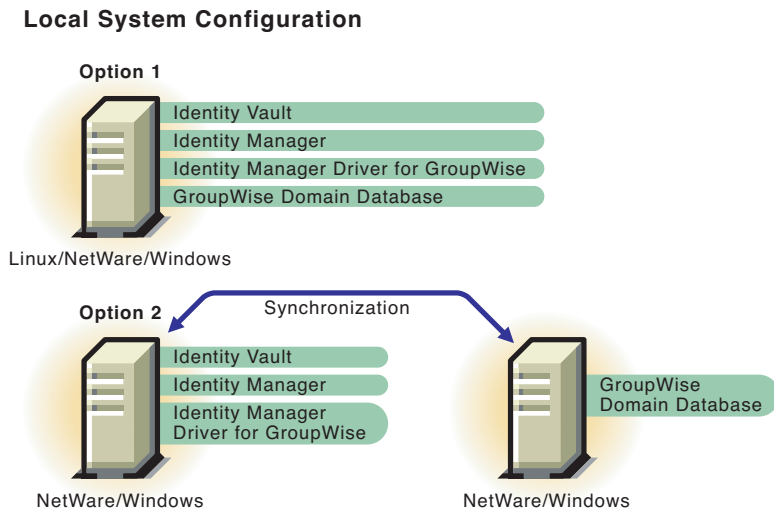
2.2 Planning for the Installation

Before you install and use the driver, you must plan a local or remote installation and define user accounts for GroupWise driver access. The GroupWise driver provisions accounts between the Identity Vault and GroupWise. The driver can connect to a secondary GroupWise domain, but Novell recommends that the GroupWise driver connects to the primary GroupWise domain.

- ◆ [Section 2.2.1, “Understanding a Local Installation,” on page 18](#)
- ◆ [Section 2.2.2, “Understanding a Remote Installation,” on page 19](#)

2.2.1 Understanding a Local Installation

Figure 2-1 Local System Configuration



A local installation installs the driver on the same Windows, Linux*, or NetWare® computer where you installed Identity Manager and eDirectory™. The GroupWise domain database can either be on the same computer or a different computer.

If Identity Manager is installed on one NetWare server and the GroupWise domain database is on another NetWare server, these servers must be installed in the same eDirectory tree.

Table 2-1 Installation Configuration Options

If . . .	Then . . .
The GroupWise driver is running on a NetWare server. . .	The GroupWise server (domain database) must also exist on NetWare. The GroupWise database can be installed on the same NetWare server as Identity Manager or on another NetWare server.
The GroupWise driver is running on a Linux server. . .	The GroupWise domain must be on the same server.

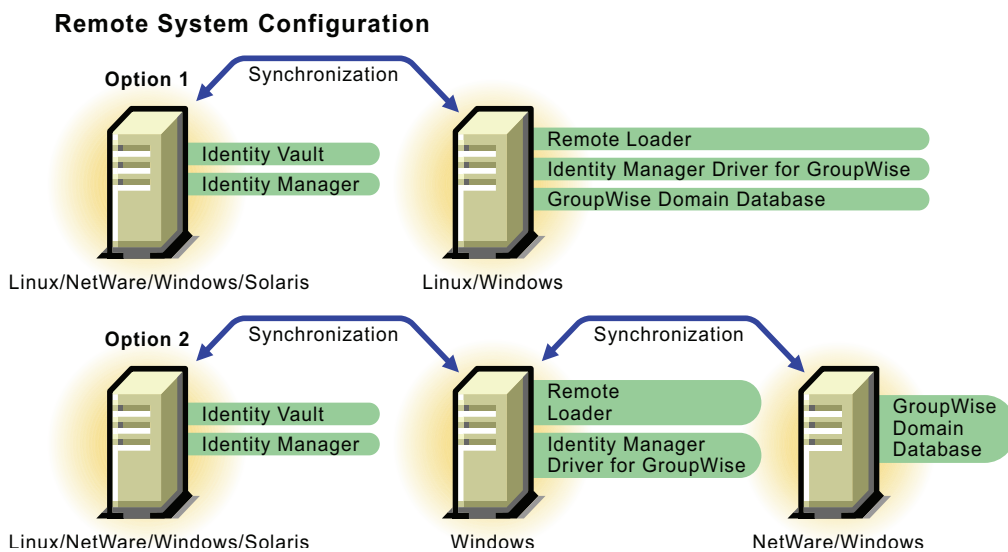
NOTE: NFS or any other type of mounted file system is not supported if the GroupWise driver connects to it. For example, the GroupWise driver running on Linux should not connect to a domain database on another server through a mounted file system; or a domain database on a Linux server should not be accessed by a GroupWise driver running on any other server, regardless of the operating system.

2.2.2 Understanding a Remote Installation

A remote installation installs the driver on a different computer than the one where Identity Manager and eDirectory are installed. Identity Manager and the Identity Vault can run on different platforms than the driver can run on. For example, Option 1 in [Figure 2-2](#) shows that if your Identity Vault and Identity Manager are installed on Solaris*, you would need to install the driver with the Remote Loader on a Linux or Windows system.

GroupWise can be installed on a separate system from where the Metadirectory engine is installed and from where the Remote Loader is installed as long as the Remote Loader runs on Windows as shown in Option 2 for [Figure 2-2 on page 19](#).

Figure 2-2 Remote System Configuration



2.3 Configuring Driver Authentication

In order for the driver to authenticate to the GroupWise domain, the driver must first authenticate to its local operating system, and then authenticate to the system holding the GroupWise domain. (If the driver is on the same computer as the domain database, you do not need to configure authentication.)

As part of configuring authentication, you create the same user name and password on each system, and assign administrative rights to the account.

IMPORTANT: To establish a connection between systems, you must create user accounts with the same username and password for each system.

The following topics help you configure authentication:

- ◆ [Section 2.3.1, “Creating a User Account for the System Containing the Driver for Windows,” on page 20](#)
- ◆ [Section 2.3.2, “Creating a User Account for the System Containing the GroupWise Domain,” on page 22](#)

2.3.1 Creating a User Account for the System Containing the Driver for Windows

As part of configuring authentication, you should create the same username and password on the system containing the driver, and assign administrative rights to the account.

After you have created the user account for the driver system, refer to [“Creating a User Account for the System Containing the GroupWise Domain” on page 22.](#)

- ♦ [“Defining an Account When the Driver Is on Windows 2000” on page 20](#)
- ♦ [“Defining an Account When the Driver Is on a Windows 2000 AD Domain Controller” on page 20](#)
- ♦ [“Defining An Account When the Driver Is on a Windows 2003 Server” on page 21](#)

Defining an Account When the Driver Is on Windows 2000

- 1 From the Start Menu, click *Settings > Control Panel > Administrative Tools > Computer Management*.
- 2 Double-click *Local Users and Groups*.
- 3 Right-click *Users > New User*.
- 4 Specify a username and a case-sensitive password.
The username and password must be the same on both systems.
- 5 Deselect *User must change password at next logon*, then select *Password never expires*.
- 6 Deselect all other boxes.
- 7 Click *Create*, then click *Close*.
- 8 Double-click *Groups*.
- 9 Double-click *Administrators*.
- 10 Click *Add*.
- 11 Browse to and select the user you just created in [Step 4](#), then click *OK*.
- 12 Click *OK* again.
- 13 Close the Computer Management window.
- 14 Double-click *Local Security Policy* in the Administrative Tools window.
- 15 Select *Local Policies*, then double-click *User Rights Assignment*.
- 16 Double-click *Log On As a Service*.
- 17 Select *Add*, browse to and select the user you just created in [Step 4](#), click *Add*, then click *OK*.
- 18 Click *OK* again.
- 19 Close the Local Security Settings window.
- 20 Close the Administrative Tools window.
- 21 Restart the computer.

Defining an Account When the Driver Is on a Windows 2000 AD Domain Controller

- 1 From the Start Menu, click *Settings > Control Panel > Administrative Tools > Active Directory Users and Computers*.

- 2 Expand the domain, then right-click *Users > New > User*.
- 3 Specify the first name, last name, then specify the user logon name.
The user logon name is used in the driver configuration. The user name must be the same on both systems.
- 4 Click *Next*.
- 5 Specify a case-sensitive password.
The password must be the same on both systems.
- 6 Select *Password Never Expires*.
- 7 Click *Next*, then click *Finish*.
- 8 Select *Builtin*, then double-click *Administrators > Members > Add*.
- 9 Browse to and select the full name of the user you entered in **Step 3**, click *Add*, then click *OK*.
- 10 Click *OK*.
- 11 Close the Active Directory Users and Computers window.
- 12 In the Administrative Tools window, select *Domain Controller Security Policy*.
- 13 Expand the *Security Settings*, click *Local Policies*, then double-click *User Rights Assignment*.
- 14 Select *Log on as a service* and select *Define These Policy Settings*. Click *Add*, then click *Browse*.
- 15 Browse to and select the user you created in **Step 3**. Click *Add*, click *OK*, then click *OK* again.
- 16 Click *OK* and close the Domain Controller Security Policy window.
- 17 In the Administrative Tools window, select *Local Security Policy*.
- 18 Double-click *Local Policies*, then click *User Rights Assignment*.
- 19 Select *Log on as a service*, select *Local Policy Settings* for the user created in **Step 3**, then click *OK*.
- 20 Close the Local Security Policy window.
- 21 Restart the computer.

Defining An Account When the Driver Is on a Windows 2003 Server

- 1 From the Start Menu, click *Control Panel > Administrative Tools > Computer Management*.
- 2 Select *Local Users and Groups*.
- 3 Right-click *Users > New User*.
- 4 Specify a User name, Full name, and a case-sensitive password.
The user name and password must be the same on both systems.
- 5 Deselect *User must change password at next logon*.
- 6 Select *Password never expires*, then deselect all other check boxes.
- 7 Click *Create*, then click *Close*.
- 8 Double-click *Groups* under *Local User and Groups*.
- 9 Double-click *Administrators*.
- 10 Click *Add*.

- 11 Type the name of the user you created in [Step 4](#), click *Check Names* to verify the name, then click *OK*.
- 12 Click *OK* again.
- 13 Close the Computer Management window.
- 14 From the Start Menu, click *Control Panel > Administrative Tools > Computer Management > Local Security Policy*.
- 15 Expand *Local Policies*, then select *User Rights Assignment*.
- 16 Double-click *Log on as a service*.
- 17 Select *Add User or Group*, then specify the name of the user you created in [Step 4](#).
- 18 Click *Check Names* to verify the name, then click *OK*.
- 19 Click *OK* again.
- 20 Close the Local Security Settings window.
- 21 Restart the computer.

2.3.2 Creating a User Account for the System Containing the GroupWise Domain

As part of configuring authentication, you should create a username and password on the system containing the GroupWise domain and assign administrative rights to the account.

IMPORTANT: To establish a connection between the driver and the GroupWise domain system, you should create user accounts with the same username and password for each system.

If you have not created the user account for the driver system, refer to [“Creating a User Account for the System Containing the Driver for Windows” on page 20](#). (If the driver runs on NetWare, you do not need to create this user account.)

- ♦ [“Defining an Account When the GroupWise Domain Is on Windows 2000” on page 22](#)
- ♦ [“Defining an Account When the GroupWise Domain Is on a Windows 2003 Server” on page 23](#)
- ♦ [“Defining an Account When the GroupWise Domain Is on NetWare” on page 24](#)

Defining an Account When the GroupWise Domain Is on Windows 2000

- 1 From the Start Menu, click *Settings > Control Panel > Administrative Tools > Computer Management*.
- 2 Select *Local Users and Groups*, then right-click *Users > New User*.
- 3 Specify a User name and the Full name.
The user name must be the same on both systems.
- 4 Specify a case-sensitive password.
- 5 Deselect *User must change password at next logon*.
- 6 Select *Password never expires*, then deselect all other check boxes.
- 7 Click *Create*, then click *Close*.
- 8 Close the Windows Manager window.

- 9 Double-click the *My Computer* icon on the desktop.
- 10 Right-click the drive that contains the GroupWise Domain, then select *Properties > Sharing*.
- 11 Select *New Share*.
- 12 Specify a share name to be used by the driver.
- 13 Restart the computer.
- 14 Double-click the *My Computer* icon on the desktop.
- 15 Right-click the drive that contains the GroupWise Domain, then select *Properties > Sharing*.
- 16 From the drop-down menu, select the new share you created in **Step 12**.
- 17 Select *Permissions > Everyone*, then click *Remove*.
- 18 Select *Add*.
- 19 Browse to and select the user you created in **Step 3**.
- 20 Click *Add*, then click *OK*.
- 21 Select *Full Control* under permissions, then click *OK*.
- 22 Click *OK*.
- 23 Restart the computer.

Defining an Account When the GroupWise Domain Is on a Windows 2003 Server

- 1 From the Start Menu, click *Control Panel > Administrative Tools > Computer Management*.
- 2 Select *Local Users and Groups*.
- 3 Right-click *Users > New User*.
- 4 Specify a User name, Full name, and a case-sensitive password.
The user name and password must be the same on both systems.
- 5 Deselect *User must change password at next logon*.
- 6 Select *Password never expires*, then deselect all other check boxes.
- 7 Click *Create*, then click *Close*.
- 8 Close the Windows Manager window.
- 9 Double-click the *My Computer* icon on the desktop.
- 10 Right-click the drive that contains the GroupWise Domain, then select *Properties > Sharing*.
- 11 Select *New Share*.
- 12 Specify a share name to be used by the driver.
- 13 Click *Permissions*.
- 14 Select the *Everyone* group, then click *Remove*.
- 15 Click *Add*.
- 16 Enter the name of the user created in **Step 4**, then click *Check Names*.
- 17 Click *OK*.
- 18 Select *Full Control* for the user, then click *OK*.
- 19 Click *OK*, then click *OK* again.
- 20 Restart the computer.

Defining an Account When the GroupWise Domain Is on NetWare

If the driver is running on NetWare or Windows and the GroupWise domain is on a remote NetWare server, it's especially important to verify that this user has file system rights to the GroupWise domain directory structure. If access is not granted to this user, changes do not replicate to the rest of the GroupWise system.

- 1 In ConsoleOne[®], create a user in NetWare with the same username and password as the Windows user account. If the driver is not running on Windows, use any user name or password.
- 2 Give the user Read, Write, Create, Erase, Modify, and File Scan access to the GroupWise domain directory and subdirectories for the domain to which the driver will connect. We recommend connecting to the GroupWise primary domain.

2.4 Installing the Driver

You can install the driver locally or by using the Remote Loader service. Make sure you have planned how to install the driver. See [Section 2.2, “Planning for the Installation,” on page 17](#) for more information.

To install the driver locally, you install the driver as part of the Novell Identity Manager 3.5.1 installation program. For installation instructions, refer to the “[Installing Identity Manager](#)” section in the *Identity Manager 3.5.1 Installation Guide*.

To install the driver remotely, use the Remote Loader service. The Remote Loader service is installed and then connects to the server running Identity Manager. For installation instructions see “[Deciding Whether to Use the Remote Loader](#)” in the *Novell Identity Manager 3.5.1 Administration Guide*.

Upgrading the Driver

If you have been using a previous version of the driver, follow these instructions instead of the ones in [Chapter 2, “Planning and Installing the Identity Manager Driver for GroupWise,”](#) on page 17.

When you upgrade to a newer version of Identity Manager, the executable files for the driver shim are upgraded, but not the configuration file for the driver. If you want to take advantage of the many changes in the import file, you have two options:

- ♦ Create a new driver using the new configuration file. If you have customized policies in the old driver, they have to be added to the new driver.
- ♦ Analyze the new configuration file and copy portions that you want to use into the current driver configuration.

The following sections describe some different upgrade procedures to take advantage of newer features. Before following any procedures, create a backup of your current driver. For instructions on how to back up your driver, see [Chapter 10, “Backing Up the Driver,”](#) on page 157.

- ♦ [Section 3.1, “Upgrading from the 2.1 Version of the GroupWise Driver,”](#) on page 25
- ♦ [Section 3.2, “Upgrading from the 2.2 Version of the GroupWise Driver,”](#) on page 26
- ♦ [Section 3.3, “Upgrading the GroupWise Database Version in the Driver Configuration,”](#) on page 26
- ♦ [Section 3.4, “Upgrading the Driver to Use the Identity Manager 3.5 Architecture,”](#) on page 27

3.1 Upgrading from the 2.1 Version of the GroupWise Driver

- 1 In iManager, click *Identity Manager > Identity Manager Overview*.
- 2 Click *Search* to find the Driver Set object, then click *Edit properties* in the upper right corner of the driver you want to upgrade.
- 3 Under Startup Options, select *Manual*, then click *OK*.
- 4 Stop the driver and the Remote Loader service.
- 5 Run the Identity Manager 3.5.1 installation and select the GroupWise driver to install the new files.

See “[Installing Identity Manager](#)” in the *Identity Manager 3.5.1 Installation Guide* for more information.

You install the driver over the existing 2.1 driver files. This step updates all necessary driver files. Depending on where your iManager server resides, you might need to copy the driver configuration to that server, if it is a remote server.

- 6 When the installation completes, reboot the computer where the driver exists, and restart eDirectory or the Remote Loader.
- 7 Delete `GWADJ1.DLL` from any DirXML-related directories. If the file exists in any other directory in the search path, you might encounter problems. Do not delete this file from the ConsoleOne® directory.

- 8 Delete `gwenv1a.DLL` and `xgbas10a.DLL` from the `Novell\NDS` directory after installing the update. Do not remove these files from the `\winnt\system32` directory if they exist there.
- 9 If you are running the driver on NetWare, delete `gwenv1a.nlm` and `xgbas10a.nlm` from `sys:system\GwDriver`.
- 10 Change the Startup Options on the driver to your desired setting. The options are:
 - ♦ *Auto Start*
 - ♦ *Manual*
 - ♦ *Disabled*
- 11 Start the driver by clicking *Start* in the driver overview page in iManager.
- 12 (Optional) In iManager, select the *Migrate > Migrate from Identity Vault* option, on the driver overview page if the driver set or driver name changed during the upgrade.

3.2 Upgrading from the 2.2 Version of the GroupWise Driver

- 1 In iManager, click *Identity Manager > Identity Manager Overview*.
- 2 Click *Search* to find the Driver Set object, then click *Edit properties* in the upper right corner of the driver you want to upgrade.
- 3 Under Startup Options, select *Manual*, then click *OK*.
- 4 Stop the driver and the Remote Loader service.
- 5 Run the Identity Manager 3.5.1 installation and select the GroupWise driver to install the new files.

See “[Installing Identity Manager](#)” in the *Identity Manager 3.5.1 Installation Guide* for more information.

You install the driver over the existing 2.2 driver files. This step updates all necessary driver files. Depending on where your iManager server resides, you might need to copy the driver configuration to that server, if it is a remote server.
- 6 When the installation completes, reboot the computer where the driver exists, and restart eDirectory or the Remote Loader.
- 7 Change the Startup Options on the driver to your desired setting. The options are:
 - ♦ *Auto Start*
 - ♦ *Manual*
 - ♦ *Disabled*
- 8 Start the driver by clicking *Start* in the driver overview page in iManager.
- 9 (Optional) In iManager, select the *Migrate > Migrate from Identity Vault* option, on the driver overview page if the driver set or driver name changed during the upgrade.

3.3 Upgrading the GroupWise Database Version in the Driver Configuration

If you have upgraded the GroupWise database version:

- 1 Verify that the version of the GroupWise database is 7.

- 2 Verify that the version of the GroupWise driver you are running supports the new version of the GroupWise database.
The driver version must be 2.1.3 or above.
- 3 In iManager, click *Identity Manager > Identity Manager Overview*.
- 4 Click *Search* to find the Driver Set object, then click *Edit properties* in the upper right corner of the driver you want to upgrade.
- 5 Select *Global Config Values > Edit XML*, then click *Enable XML editing*.
- 6 Add the following text to the GroupWise Domain Database Version definition display-name section: `<enum-choice display-name="GroupWise 7">700</enum-choice>`.
- 7 Click *OK* to save the changes.
- 8 On the global configuration values page under *GroupWise Domain Database Version*, select the version of the GroupWise database you are running.
- 9 Click *OK* to save the settings.
- 10 Restart the driver for the setting to take effect.

The old definition of the GroupWise database version in XML is

```
<definition display-name="GroupWise Domain Database Version"
name="domainVersion" type="enum">
  <description>Specify the version of GroupWise Domain Database to which this
driver will connect.</description>
  <enum-choice display-name="GroupWise 6.5">650</enum-choice>
  <enum-choice display-name="GroupWise 6.0">600</enum-choice>
  <enum-choice display-name="GroupWise 5.5">550</enum-choice>
  <value>6.5</value>
</definition>
```

The changed version of the GroupWise database version in XML is

```
<definition display-name="GroupWise Domain Database Version"
name="domainVersion" type="enum">
  <description>Specify the version of GroupWise Domain Database to which this
driver will connect.</description>
  <enum-choice display-name="GroupWise 7">700</enum-choice>
  <enum-choice display-name="GroupWise 6.5">650</enum-choice>
  <enum-choice display-name="GroupWise 6.0">600</enum-choice>
  <enum-choice display-name="GroupWise 5.5">550</enum-choice>
  <value>700</value>
</definition>
```

3.4 Upgrading the Driver to Use the Identity Manager 3.5 Architecture

Identity Manager 3.5 contains a new architecture for how policies reference one another. To take advantage of this new architecture, the driver configuration file provided for GroupWise must be upgraded. For more information on the new architecture, see [“Upgrading Identity Manager Policies”](#)

in *Understanding Policies for Identity Manager 3.5.1*. You can upgrade the driver in Designer or iManager. If you are upgrading from Identity Manager 3.5.0 to Identity Manager 3.5.1, the following information does not apply.

- ♦ [Section 3.4.1, “Upgrading the Driver in Designer,” on page 28](#)
- ♦ [Section 3.4.2, “Upgrading the Driver in iManager,” on page 30](#)

3.4.1 Upgrading the Driver in Designer

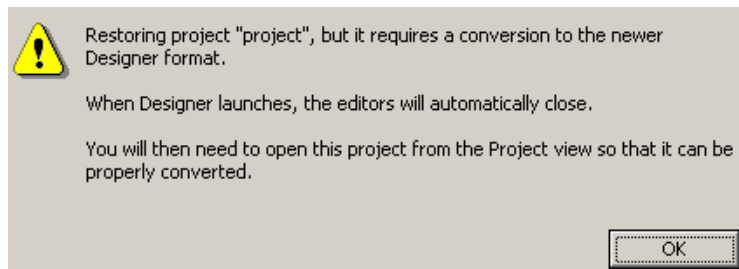
- 1 Make sure you have updated your driver with all the patches for the version you are currently running.

We recommend this step for all drivers, to help minimize upgrade issues.

- 2 Back up the driver.
- 3 See [Chapter 10, “Backing Up the Driver,” on page 157](#) for instruction on how to back up the driver.
- 4 Install Designer version 2.0 or above, then launch Designer.

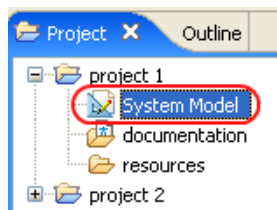
If you had a project open in Designer when you upgraded Designer, proceed to [Step 5](#). If you didn't have a project open in Designer when you upgraded Designer, skip to [Step 6](#).

- 5 If you had a project open when upgrading Designer, the following warning message is displayed. Read the warning message, then click *OK*.

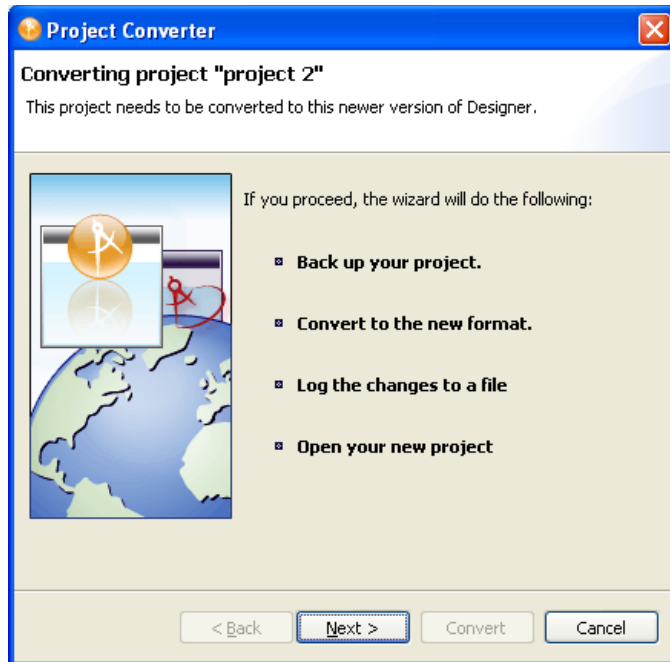


Designer closes the project to preform the upgrade.

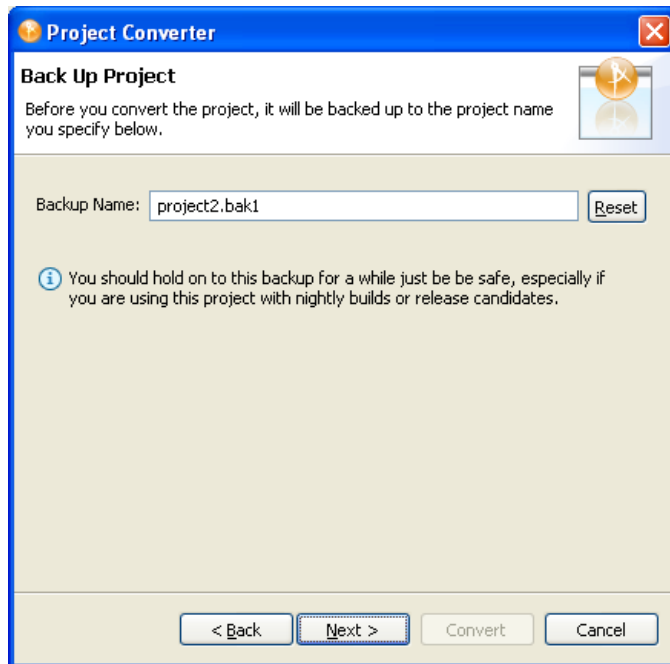
- 6 In the Project view, double-click *System Model* to open and convert the project.



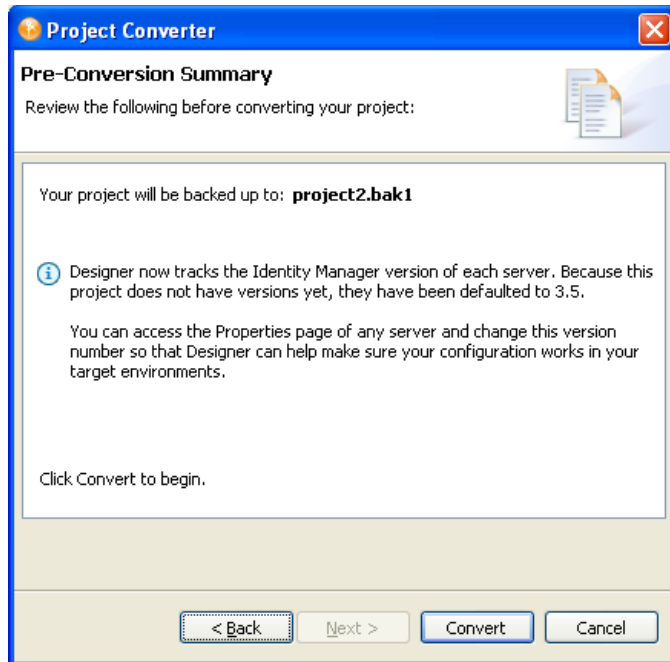
- 7 Read the Project Converter message explaining that the project is backed up, converted to the new format, changes logged to a file, and the new project is opened, then click *Next*.



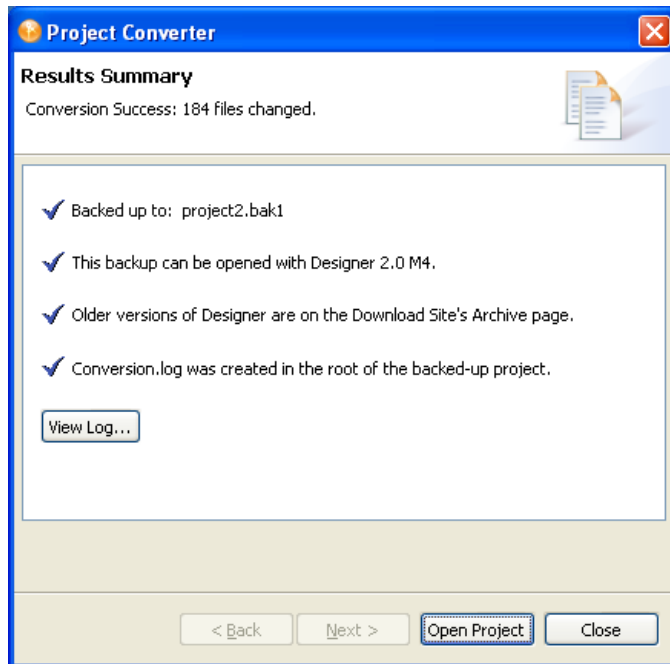
8 Specify the name of the backup project name, then click *Next*.



9 Read the project conversion summary, then click *Convert*.



- 10 Read the project conversion result summary, then click *Open Project*.



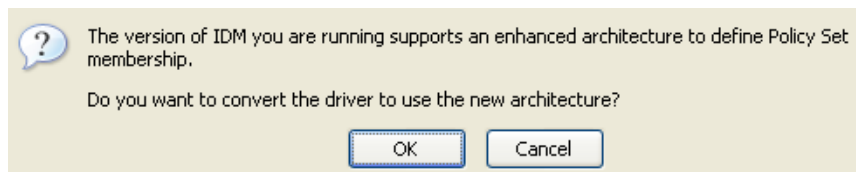
If you want to view the log file that is generated, click *View Log*.

3.4.2 Upgrading the Driver in iManager

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

We recommend this step for all drivers, to help minimize upgrade issues.

- 2 Back up the driver.
- 3 See [Chapter 10, “Backing Up the Driver,”](#) on page 157 for instruction on how to back up the driver.
- 4 Verify that Identity Manager 3.5.1 has been installed and you have the current plug-ins installed, then launch iManager.
- 5 Click *Identity Manager > Identity Manager Overview*.
- 6 Click *Search* to find the Driver Set object, then click the driver you want to upgrade.
- 7 Read the message that is displayed, then click *OK*.



- 8 If there is more than one driver to upgrade, repeat [Step 2](#) through [Step 7](#).

Configuring the GroupWise Driver

4

This section explains how to import the driver configuration for the Identity Manager Driver for GroupWise®. Importing the driver configuration also creates the driver object. After you have imported the configuration, you can use iManager to configure and manage the driver.

- ♦ [Section 4.1, “Importing the Driver Configuration File in Designer,” on page 33](#)
- ♦ [Section 4.2, “Importing the Driver Configuration in iManager,” on page 33](#)
- ♦ [Section 4.3, “Configuration Parameters,” on page 34](#)
- ♦ [Section 4.4, “Viewing Driver Parameters,” on page 41](#)
- ♦ [Section 4.5, “Modifying Global Configuration Values,” on page 41](#)
- ♦ [Section 4.6, “Post-Installation Tasks,” on page 42](#)

4.1 Importing the Driver Configuration File in Designer

Designer allows you to import the basic driver configuration file for GroupWise. This file creates and configures the objects and policies needed to make the driver work properly. The following instructions explain how to create the driver and import the driver’s configuration.

There are many different ways of importing the driver configuration file in Designer. This procedure documents one way.

- 1 Open a project in Designer. In the Modeler, right-click the Driver Set object and select *New > Driver*.
- 2 Browse to and select *GroupWise* from the list, then click *Run*.
- 3 Configure the driver by filling in the fields with information specific to your environment.
For information on the settings, see [Table 4-1 on page 35](#).
- 4 After specifying parameters, click *Finish* to import the driver.
- 5 After the driver is imported, customize and test the driver.
- 6 After the driver is fully tested, deploy the driver into the Identity Vault.
See [“Deploying a Driver to an Identity Vault” in Designer 2.1 for Identity Manager 3.5.1](#).

4.2 Importing the Driver Configuration in iManager

The Create Driver Wizard in iManager helps you import the basic driver configuration file for GroupWise. This file creates and configures the objects and policies needed to make the driver work properly. The following instructions explain how to create the driver and import the driver’s configuration.

- 1 In Novell® iManager, click *Identity Manager Utilities > Import Configurations*.
- 2 Select a driver set, then click *Next*.

If you place this driver in a new driver set, you must specify a driver set name, context, and associated server.

- 3 Select how you want the driver configurations sorted:
 - ◆ All configurations
 - ◆ Identity Manager 3.5 configurations
 - ◆ Identity Manager 3.0 configurations
 - ◆ Configurations not associated with an IDM version
- 4 Select *GroupWise*, and then click *Next*.



- 5 Configure the driver by filling in the fields with information specific to your environment.
For information on the settings, see [Table 4-1 on page 35](#).
- 6 After specifying parameters, click *Next* to import the driver.
When the import is finished, you can define security equivalences and exclude administrative roles from replication.
The driver object must be granted sufficient eDirectory™ rights to any object it reads or writes to. You can do this by granting Security Equivalence to the driver object. The driver must have Read/Write access to users, post offices, resources, groups, and distribution lists, and Create, Read, and Write rights to the post office container. Normally, the driver should be given security equal to Admin.
- 7 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 6](#). 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.
- 8 Review the driver objects in the Summary page, then click *Finish*.

Keep in mind that installing the driver software lets you get the driver up and running, but it does not install the product license. Without the license and activation, the driver will not run after 90 days. For more information, refer to [Chapter 5, “Activating the Driver,” on page 45](#).

4.3 Configuration Parameters

The following table explains the parameters you must provide during initial driver configuration.

There are options in the driver configuration that add policies to the driver to allow additional functionality. If you are not sure you need these options now, but you might want them in the future, it is better to select them now. After the driver is created, these options are enabled or disabled through global configuration values on the driver. Trying to properly add policy sets from the default driver configuration to an existing driver after it is configured is a complex process.

IMPORTANT: Selecting options during the configuration of the driver parameters does not enable the functionality. After the driver is imported, the global configuration values must be modified to enable the functionality of the selection. See [Section 4.5, “Modifying Global Configuration Values,” on page 41](#) for more information.

Some parameters are displayed only if the answer to a previous prompt requires more information to properly configure the policy.

Table 4-1 *Driver Configuration Parameters*

Field	Description
<i>Driver name</i>	The default value is GroupWise. Specify the name you want for the driver.
<i>Enable Entitlements</i>	<p>There are two options, Yes or No.</p> <p>The GroupWise driver uses entitlements to manage user accounts and distribution list membership in GroupWise. Entitlements work in conjunction with external services such as the Identity Manager User Application or Role-Based Entitlements. These external services control provisioning to GroupWise. See “Creating and Using Entitlements” in the <i>Novell Identity Manager 3.5.1 Administration Guide</i>.</p> <hr/> <p>IMPORTANT: After the driver is imported, review Section 4.4, “Viewing Driver Parameters,” on page 41 and Section 4.5, “Modifying Global Configuration Values,” on page 41 for additional configuration options.</p> <hr/>
<i>Default Post Office</i>	<p>The DN for the default GroupWise Post Office for creating Accounts. The post office can be entered in slash or dot notation.</p> <p>Examples:</p> <p>Novell\GroupWise\PO (slash)</p> <p>PO.GroupWise.Novell (dot)</p>
<i>GroupWise Domain Database Version</i>	<p>Select the version of GroupWise you have installed.</p> <p>Options:</p> <ul style="list-style-type: none">◆ <i>GroupWise 7</i>◆ <i>GroupWise 6.5</i>◆ <i>GroupWise 6.0</i>◆ <i>GroupWise 5.5</i>

Field	Description
<i>Driver and Domain servers</i>	<p>Select the server OS where the GroupWise driver is installed and the server OS where the GroupWise domain resides.</p> <p>Depending upon the option that is selected, there are additional fields that are presented. See Table 4-2 on page 38 for information about each option.</p> <p>Options:</p> <ul style="list-style-type: none"> ◆ <i>This driver is on a NetWare server - the GroupWise domain is on the same NetWare server as the driver.</i> ◆ <i>This driver is on a NetWare server - the GroupWise domain is on a different NetWare server from the driver.</i> ◆ <i>This driver is on a Linux server - the GroupWise domain is on the same Linux server as the driver.</i> ◆ <i>This driver is on a Windows server - the GroupWise domain is on the same Windows server as the driver.</i> ◆ <i>This driver is on a Windows server - the GroupWise domain is on a different Windows server from the driver.</i> ◆ <i>This driver is on a Windows server - the GroupWise domain is on a NetWare server.</i>
<i>Default Subscriber Source Location</i>	<p>Specify the eDirectory container in which object changes are detected and synchronize. Synchronization occurs for objects below the specified location. Specify the eDirectory tree if you want the entire tree to be monitored.</p>
<i>Include Policies for Group to GroupWise Distribution List Synchronization?</i>	<p>The GroupWise driver can be configured to synchronize eDirectory Groups to the GroupWise Distribution List objects. Selecting Yes adds a base set of policies to the driver that allows the eDirectory Groups to synchronize to the GroupWise Distribution List objects.</p> <hr/> <p>IMPORTANT: This feature is not enabled by selecting this option. You must edit the GCVs on the driver after it is imported to enable this feature. See Section 4.5, "Modifying Global Configuration Values," on page 41.</p>
<i>Include Policies for GroupWise Distribution List Synchronization?</i>	<p>The GroupWise driver can be configured to synchronize GroupWise Distribution List objects from eDirectory to GroupWise. Selecting Yes adds a base set of policies to the driver that allows the GroupWise Distribution List objects to synchronize.</p> <hr/> <p>IMPORTANT: This feature is not enabled by selecting this option. You must edit the GCVs on the driver after it is imported to enable this feature. See Section 4.5, "Modifying Global Configuration Values," on page 41.</p>

Field	Description
<i>Include Policies for GroupWise External Entity Synchronization?</i>	<p>The GroupWise driver can be configured to synchronize GroupWise External Entity objects from eDirectory to an External GroupWise Post Office. Selecting Yes adds a base set of policies to the driver that allows GroupWise External Entity objects to be synchronize from eDirectory to an External GroupWise Post Office.</p> <hr/> <p>IMPORTANT: This feature is not enabled by selecting this option. You must edit the GCVs on the driver after it is imported to enable this feature. See Section 4.5, "Modifying Global Configuration Values," on page 41.</p>
<i>Include Policies for eDirectory OrgUnit to GroupWise External Post Office Synchronization?</i>	<p>The GroupWise driver can be configured to synchronize eDirectory Organizational Units to GroupWise External Post Offices. Selecting Yes adds a base set of policies to the driver that allows eDirectory Organizational Units to synchronize to GroupWise External Post Offices.</p> <hr/> <p>IMPORTANT: This feature is not enabled by selecting this option. You must edit the GCVs on the driver after it is imported to enable this feature. See Section 4.5, "Modifying Global Configuration Values," on page 41.</p>
<i>Driver is Local/Remote</i>	<p>Configure the driver for use with the Remote Loader service by selecting <i>Remote</i>, or select <i>Local</i> to configure the driver for local use.</p>
<i>Action On GroupWise Account Entitlement Add</i>	<p>Entitlement option only.</p> <p>When a user is created in eDirectory with a GroupWise account entitlement, select the action you want to occur on the associated GroupWise account:</p> <ul style="list-style-type: none"> ◆ <i>Disable the GroupWise Account</i> ◆ <i>Enable the GroupWise Account</i>
<i>Action On GroupWise Account Entitlement Remove</i>	<p>Entitlements option only.</p> <p>When a user's GroupWise account entitlement is removed in eDirectory, specify the action you want the driver to take on an associated GroupWise account:</p> <ul style="list-style-type: none"> ◆ <i>Disable the GroupWise account</i> ◆ <i>Delete the GroupWise account</i> ◆ <i>Expire the GroupWise account</i> ◆ <i>Disable and expire the GroupWise account</i>
<i>Non-GroupWise Domain Name</i>	<p>GroupWise External Entity synchronization policies only.</p> <p>To properly configure the Subscriber Placement policy, specify a default Non-GroupWise Domain defined within the GroupWise system which contains the External Post Office where the GroupWise External Entities can be created and synchronized.</p>

Field	Description
<i>GroupWise External Post Office</i>	GroupWise External Entity synchronization policies only. To properly configure the Subscriber Placement policy, specify a default External Post Office defined within GroupWise which is subordinate to the Non-GroupWise Domain name where the GroupWise External Entities can be created and synchronized.
<i>Non-GroupWise Domain Name</i>	eDirectory Organizational Unit to GroupWise External Post Office synchronization policies only. To properly configure the Subscriber placement policy, specify a Non-GroupWise Domain defined within the GroupWise System where the External Post Offices and users can be created and synchronized.
<i>Remote Host Name and Port</i>	Remote option only. Specify the host name or IP address and port number where the Remote Loader service is installed. The default port is 8090.
<i>Driver password</i>	Remote option only. The driver password is used by the Remote Loader service to authenticate it to the Identity Manager server. It must be the same password that is specified as the Driver Object Password on the Identity Manager Remote Loader.
<i>Remote password</i>	Remote option only. The remote password is used to control access to the Remote Loader instance. It must be the same password that is specified as the Remote Loader password on the Remote Loader service.

Table 4-2 *Optional Fields for Driver and Domain Entry*

Option	Fields	Description
<i>This driver is on a NetWare server - the GroupWise domain is on the same NetWare server as the driver.</i>	<i>Primary Domain Path</i>	The path to the directory containing the GroupWise primary domain database (<code>wppdomain.db</code>). Example: <code>volume:\Novell\GroupWise\Domain</code>
<i>This driver is on a NetWare server - the GroupWise domain is on a different NetWare server from the driver.</i>	<i>Primary Domain Server</i>	The name or address of the NetWare® server containing the GroupWise primary domain database (<code>wppdomain.db</code>). Examples: <code>hostname</code> - the name of the remote NetWare server or <code>###.###.###.###</code> - the IP address of the remote NetWare server

Option	Fields	Description
	<i>Primary Domain Path</i>	<p>The path to the directory containing the GroupWise primary domain database (wpdomain.db).</p> <p>Example:</p> <pre>volume:\Novell\GroupWise\Domain</pre>
	<i>Username</i>	<p>The username this driver uses to authenticate to the remote NetWare server that contains the GroupWise domain database.</p> <p>The user account is on the remote NetWare server must have sufficient privileges to access to the domain directory.</p>
	<i>Password</i>	The password of the user listed in the Username field.
	<i>eDirectory User Context</i>	<p>The context of the user listed in the Username field.</p> <p>Examples:</p> <pre>\TREE\Novell\adminContainer</pre> <p>or</p> <pre>ou=adminContainer.o=Novell</pre>
<i>This driver is on a Linux server - the GroupWise domain is on the same Linux server as the driver.</i>	<i>Primary Domain Path</i>	<p>The path to the directory containing the GroupWise primary domain database (wpdomain.db).</p> <p>Example:</p> <pre>/novell/groupwise/domain</pre>
<i>This driver is on a Windows server - the GroupWise domain is on the same Windows server as the driver.</i>	<i>Primary Domain Path</i>	<p>The path to the directory containing the GroupWise primary domain database (wpdomain.db).</p> <p>Example:</p> <pre>c:\Novell\GroupWise\Domain</pre>

Option	Fields	Description
<i>This driver is on a Windows server - the GroupWise domain is on a different Windows server from the driver.</i>	<i>Primary Domain Server</i>	<p>The name or address of the server containing the GroupWise primary domain database (<code>wpdomain.db</code>).</p> <p>Examples:</p> <p>hostname - the name of the remote Windows server</p> <p>or</p> <p>hostname.com - the DNS name of the remote Windows server</p> <p>or</p> <p>###.###.###.### - the IP address of the remote Windows server</p>
	<i>Primary Domain Path</i>	<p>The path to the directory containing the GroupWise primary domain database (<code>wpdomain.db</code>).</p> <p>Example:</p> <p><code>c\$\Novell\GroupWise\Domain</code></p>
	<i>Username</i>	<p>The user name this driver uses to authenticate to the remote Windows server that contains the GroupWise domain database.</p> <p>It must be the name of a user account on the remote Windows server. The same username and password must also be configured on both Windows servers.</p>
<i>This driver is on a Windows server - the GroupWise domain is on a NetWare server.</i>	<i>Password</i>	<p>The password of the user specified above.</p>
	<i>Primary Domain Server</i>	<p>The name or address of the NetWare server containing the GroupWise primary domain database (<code>wpdomain.db</code>).</p> <p>Examples:</p> <p>hostname - the name of the NetWare server</p> <p>or</p> <p>hostname.com - the DNS name of the NetWare server</p> <p>or</p> <p>###.###.###.### - the IP address of the NetWare server</p>

Option	Fields	Description
	<i>Primary Domain Path</i>	<p>The path to the directory containing the GroupWise primary domain database (wpdomain.db).</p> <p>Example:</p> <p>volume\Novell\GroupWise\Domain</p> <hr/> <p>NOTE: There is no colon after the volume.</p>
	<i>Username</i>	<p>The username this driver uses to authenticate to the remote NetWare server that contains the GroupWise domain database. It must be the name of a user account on the NetWare server that has sufficient privileges to access the domain directory. The same username and password must also be configured on this Windows server.</p>
	<i>Password</i>	<p>The password of the user specified above.</p>
	<i>eDirectory User Context</i>	<p>The eDirectory context of the user name specified above.</p> <p>Browse to and select the context or enter the context as</p> <p>\TREE\Novell\adminContainer or ou=adminContainer.o=Novell</p>

4.4 Viewing Driver Parameters

During the driver import process, you enter the driver configuration values. Use the following procedure to view or modify these values.

- 1 In iManager, click *Identity Manager > Identity Manager Overview*.
- 2 Browse to the driver set that includes the GroupWise driver exists, then click *Search*.
- 3 Click the upper right corner of the GroupWise driver icon, then click *Edit properties*.
- 4 Click the *Driver Configuration* tab, then modify any of the parameters.

See [Section C.1.5, “Driver Parameters,” on page 189](#) for a list of all of the driver parameters.

4.5 Modifying Global Configuration Values

Global configuration values (GCVs) are settings that are similar to driver parameters. Global configuration values are specified for a driver set as well as an individual driver. If a driver does not have a GCV, the driver inherits the value for that GCV from the driver set. GCVs allow you to specify settings for new Identity Manager features such as password synchronization and driver heartbeat, as well as settings that are specific to the GroupWise driver. For more information and a list of all of the GroupWise driver GCVs, refer to [Section C.2, “Global Configuration Values,” on page 190](#).

4.6 Post-Installation Tasks

This section outlines tasks you need to complete after a local or remote installation.

- ♦ [Section 4.6.1, “Installation on NetWare,” on page 42](#)
- ♦ [Section 4.6.2, “Modifying Policies,” on page 42](#)
- ♦ [Section 4.6.3, “Modifying Global Configuration Values,” on page 42](#)
- ♦ [Section 4.6.4, “Starting the Driver,” on page 42](#)
- ♦ [Section 4.6.5, “Verifying That the Driver is Working Properly,” on page 43](#)
- ♦ [Section 4.6.6, “Migrating eDirectory Users to GroupWise,” on page 43](#)

4.6.1 Installation on NetWare

If you installed the driver on the a NetWare server, you need to modify the `autoexec.ncf` file. Open the file and locate the following line:

```
SEARCH ADD SYS:\GRPWISE\AGENTS
```

The `\GRPWISE\AGENTS` directory specifies where the GroupWise agents are installed. Immediately below this line, you should see the following:

```
PROTECT SYS:\GRPWISE\AGENTS\GRPWISE.NCF
```

This SYS line might already exist. If it does, do not add it again, but ensure that `PROTECT` precedes the command. This loads the `grpwise.ncf` file into protected memory. The `grpwise.ncf` needs to run in protected memory.

You should replace `\GRPWISE\AGENTS` with the path to where the GroupWise agents are installed on your server.

NOTE: If the GroupWise agents are installed in `SYS:\SYSTEM`, Novell recommends moving the agents to another directory and modifying the `autoexec.ncf` file accordingly.

4.6.2 Modifying Policies

Before you start the driver and use it to synchronize data between eDirectory and GroupWise, you must modify the driver’s policies and filters for your specific business rules. See [Chapter 6, “Customizing the Driver by Using Policies and Filters,” on page 47](#) for complete information.

4.6.3 Modifying Global Configuration Values

Before starting the driver, you need to review and make necessary changes to the Global Configuration Values for your environment. For more information [Section C.2, “Global Configuration Values,” on page 190](#).

4.6.4 Starting the Driver

In order for the driver to synchronize information, it must be started. To start the driver, see [Section 7.10, “Starting, Stopping, or Restarting the Driver,” on page 119](#).

4.6.5 Verifying That the Driver is Working Properly

After the driver is installed, the driver configuration is imported, and the policies have been customized, you should test the driver to see that it is working properly. (For more information on customizing policies, see [Chapter 6, “Customizing the Driver by Using Policies and Filters,” on page 47.](#))

Use the following steps to verify that the driver is working properly. When properly installed and configured, the driver synchronizes the changes to GroupWise.

- 1 In Novell iManager, click *Identity Manager > Identity Manager Overview*.
- 2 Do one of the following:
 - ♦ Click *Search Entire Tree* to search your entire tree for the Driver set that contains the driver, then click *Search*.
 - ♦ Click *Search in Container*, enter or browse for and select the container that holds the driver, then click *Search*.
- 3 Click the Identity Manager Driver for GroupWise driver status button, then click *Start Driver*.
- 4 Add a new user to eDirectory.

You need to specify only the Name and Surname attributes for this user.
- 5 Open ConsoleOne with the GroupWise snap-ins.
- 6 Verify that a new GroupWise account was created in the correct post office.
- 7 Using Novell iManager, delete the user from eDirectory.

The default driver import file converts eDirectory deletes to GroupWise Disable events. This results in a disabled external user in GroupWise. This can be changed through the global configuration values.
- 8 Using ConsoleOne with the GroupWise snap-ins, verify that the GroupWise account is external and disabled (assuming you are using the default configuration).
- 9 Use ConsoleOne with the GroupWise snap-ins to verify that the changes have been synchronized with GroupWise.

WARNING: If you create eDirectory users with ConsoleOne, be sure to use ConsoleOne with GroupWise 6.5 or above snap-ins installed. If you are using GroupWise 6.0 or older versions, do not use ConsoleOne with the GroupWise snap-ins to create eDirectory users. The ConsoleOne snap-ins for the older GroupWise version operate after the driver and remove some vital data from eDirectory.

4.6.6 Migrating eDirectory Users to GroupWise

Under most circumstances, eDirectory and GroupWise already contain information prior to the installation of Identity Manager. The Migrate function in Novell iManager lets you select the users in eDirectory, then perform a migration to GroupWise. You can use the migration function to establish the initial association between eDirectory and the GroupWise driver. The driver does not work properly unless you do this. You should also complete a migrate operation if the driver or driver set name changes.

The migration option in iManager lets you select individual users to migrate from eDirectory into GroupWise. For more information about the synchronization process, see [Chapter 8, “Synchronizing Objects,” on page 135](#). The Metadirectory engine applies all Matching, Placement, and Creation policies and the filter to the objects that you choose to migrate.

To migrate eDirectory users to GroupWise:

- 1** In Novell iManager, click *Identity Manager > Identity Manager Overview*.
- 2** Browse to and select the driver object to which you will be migrating data.
- 3** Click *Migrate > Migrate from Identity Vault*.
- 4** Click *Add*, then select the container or user objects you want to migrate.
- 5** Click *OK*.

When using this functionality, take into consideration any global configuration setting that controls whether or not GroupWise accounts are created for selected users who don't already have an account.

Activating the Driver

5

Novell® Identity Manager, Integration Modules, and the Provisioning Module must be activated within 90 days of installation, or they shut down. At any time during the 90 days, or afterward, you can choose to activate Identity Manager products.

NOTE: If you are upgrading from previous versions of the driver, you do not need to reactivate the driver.

To activate the driver, see “[Activating Novell Identity Manager Products](#)” in the *Identity Manager 3.5.1 Installation Guide*.

Customizing the Driver by Using Policies and Filters

6

This section explains how to use and modify policies and filters to synchronize data between Novell® eDirectory™ and GroupWise® according to your specific business rules.

The Identity Manager Driver for GroupWise synchronizes data and events from eDirectory through a series of policies. Policies help Identity Manager make decisions as the documents traverse a channel. A policy might determine that a document needs to be transformed in some way before continuing to the destination. For example, a Create policy specifies that a User object must have a value for the CN attribute, so any attempt to create a User object without a CN value is not allowed by that policy.

The policies in this section are examples of the many possible solutions for your company's business rules. The code segments show simple and partial solutions and do not cover all situations and conditions. In addition, the code segments only process the attributes of interest and do not handle other attributes.

- ◆ [Section 6.1, “Default Driver Actions,” on page 47](#)
- ◆ [Section 6.2, “Modifying Default Settings in Policies and the Filter,” on page 47](#)
- ◆ [Section 6.3, “Modifying Policies,” on page 48](#)
- ◆ [Section 6.4, “Setting GroupWise Client Options with the Driver,” on page 72](#)
- ◆ [Section 6.5, “Client Options Quick Reference,” on page 113](#)

6.1 Default Driver Actions

The driver performs several actions by default:

- ◆ The user's eDirectory Common Name (CN) is used as the GroupWise user ID when a GroupWise account is created.
- ◆ The driver configuration uses a single post office. All accounts are created in a single post office.

6.2 Modifying Default Settings in Policies and the Filter

You set defaults for policies and filters when you import the driver configuration. If you want to change the default behavior of the driver, we recommend that you make modifications in this order:

1. Modify the driver filter to include additional attributes to be synchronized. See [“Modifying the Driver Filter” on page 48](#) for more information.
2. Modify the Schema Mapping policy to include all attributes to be synchronized. See [“Adding Entries to the Schema Mapping Policy” on page 48](#) for more information.

3. Modify the Subscriber Create policy. See [“Modifying the Create Policy” on page 48](#) for more information.
4. Modify the Subscriber Placement policy. See [“Modifying Policies” on page 48](#).

6.2.1 Modifying the Driver Filter

The driver filter contains the eDirectory classes and attributes for the Publisher and Subscriber channels. The purpose of the filter is to define how attributes are shared between systems. All attributes in the driver filter are required for processing, so you should not remove attributes from the filter.

You can, however, make additions to the filter. If you add classes or attributes to the filter, you must append the `merge-authority="edir"` string to the added attribute in the Mapping policy.

For example:

```
<filter-attr attr-name="Description" merge-authority="edir"
  publ      sher="ignore" subscriber="sync"/>
```

6.2.2 Adding Entries to the Schema Mapping Policy

The Schema Mapping policy is contained in the driver object and applies to both the Subscriber and Publisher channel. The purpose of the Schema Mapping policy is to map schema names (particularly attribute names and class names) between the eDirectory namespace and the GroupWise namespace. Do not modify or remove existing entries in the Schema Mapping policy. You can, however, add entries to the Schema Mapping policy.

6.2.3 Modifying the Create Policy

You modify the Create policy to implement your specific business rules. The Create policy determines whether or not a GroupWise account is created. A Create policy also can perform other modifications to the Add event, such as providing default values for attributes.

In the driver configuration, the Create policy specifies two required attributes: CN and Surname.

The policy is controlled by a global configuration value (GCV) that sets the initial password to Surname and CN. For more information on GCVs, refer to [Section C.2, “Global Configuration Values,” on page 190](#).

6.2.4 Modifying the Matching Policy

Matching policies define the minimum criteria that two objects must meet to be considered the same. We recommend that you do not change the default Matching policy.

6.3 Modifying Policies

You can modify the existing driver policies to perform additional functionality.

- ◆ [Section 6.3.1, “Specifying the GroupWise Post Office,” on page 49](#)
- ◆ [Section 6.3.2, “Specifying Distribution Lists,” on page 51](#)
- ◆ [Section 6.3.3, “Setting Defaults for GroupWise Attributes,” on page 55](#)

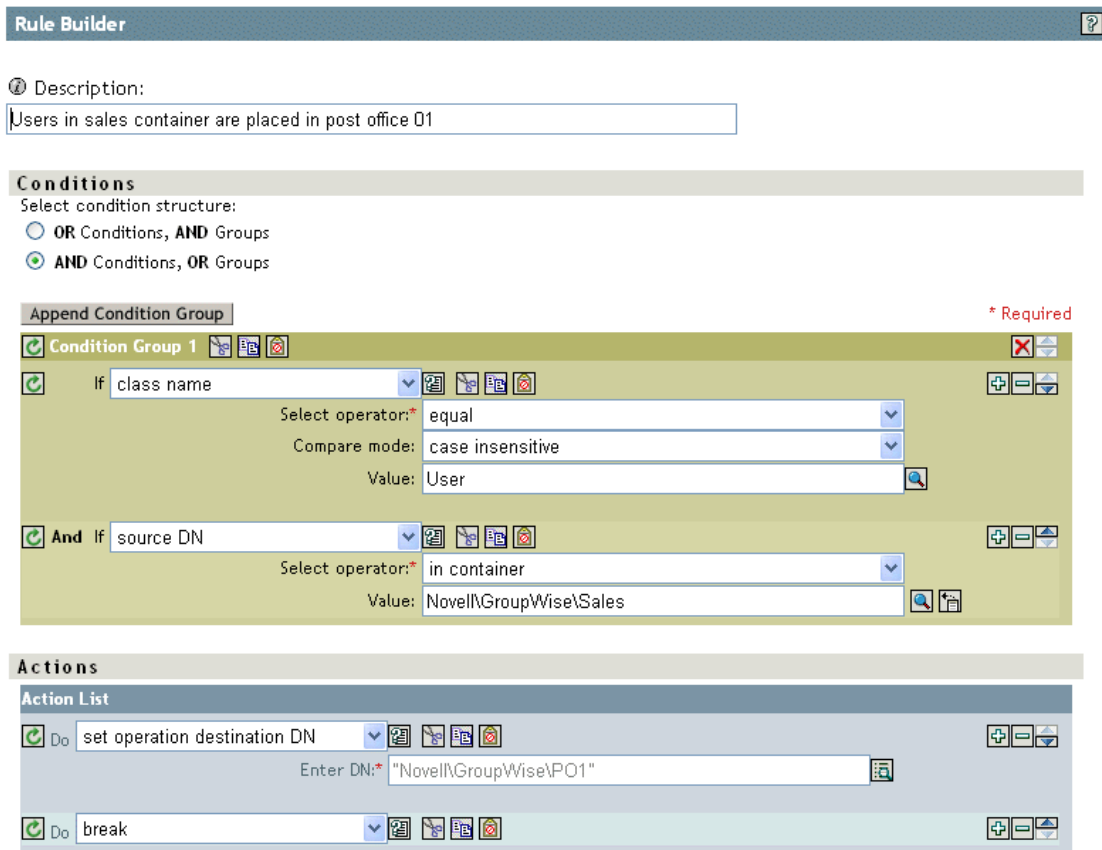
- ◆ Section 6.3.4, “Configuring the GroupWise UserID,” on page 55
- ◆ Section 6.3.5, “Creating Mappings for Additional Attributes,” on page 56
- ◆ Section 6.3.6, “Getting a Record Count from a Query,” on page 56
- ◆ Section 6.3.7, “Deleting the GroupWise User without Deleting the eDirectory User,” on page 57
- ◆ Section 6.3.8, “Creating a GroupWise Nickname,” on page 57
- ◆ Section 6.3.9, “Creating a GroupWise Nickname Record,” on page 58
- ◆ Section 6.3.10, “Specifying a New Resource Owner on an Owner Delete,” on page 59
- ◆ Section 6.3.11, “Specifying a New Resource Owner on an Owner Disable,” on page 60
- ◆ Section 6.3.12, “Controlling Creation of GroupWise Accounts,” on page 60
- ◆ Section 6.3.13, “Moving Users from One Post Office to Another Post Office,” on page 61
- ◆ Section 6.3.14, “Adding Additional Attributes to Be Synchronized,” on page 62
- ◆ Section 6.3.15, “Renaming Users,” on page 62
- ◆ Section 6.3.16, “Creating a Gateway Alias,” on page 63
- ◆ Section 6.3.17, “Querying for a Nickname,” on page 64
- ◆ Section 6.3.18, “Querying for a Gateway Alias,” on page 66
- ◆ Section 6.3.19, “Querying for Internet EMail Address,” on page 67
- ◆ Section 6.3.20, “Synchronizing GroupWise External Users,” on page 68
- ◆ Section 6.3.21, “Verifying if an E-Mail Address or Gateway Alias Is Unique,” on page 70

6.3.1 Specifying the GroupWise Post Office

By default, the GroupWise Subscriber Placement policy puts all new users in the same post office. The Placement policy can also determine the post office based on an attribute value or the eDirectory user container.

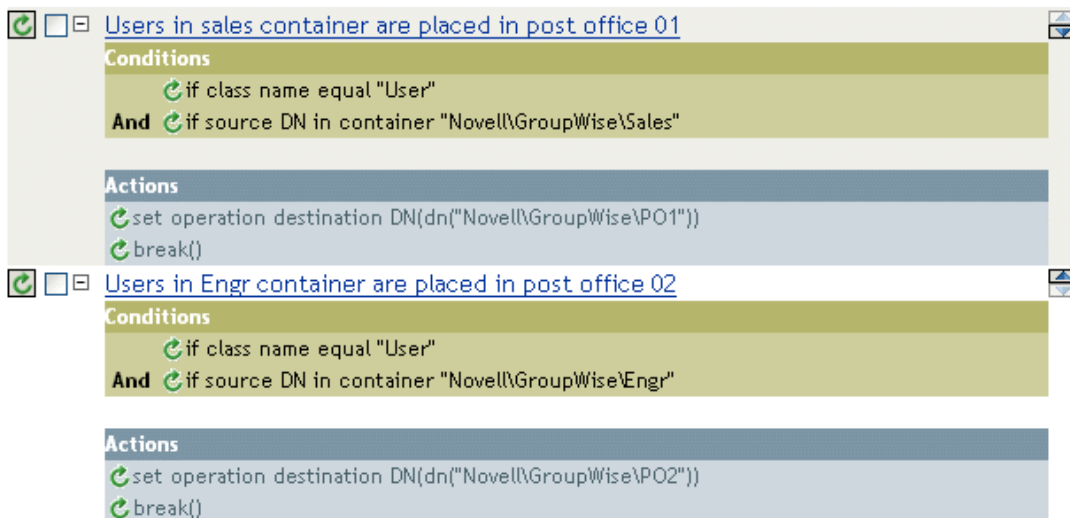
The following example, created in Policy Builder, specifies the post office based on the eDirectory container where the user was created.

Figure 6-1 Placement Policy Specifying a Post Office Based on the eDirectory Container



The following graphic shows the policies needed to place users in the Sales container into PO1 and users in the Engineering container into PO2.

Figure 6-2 Placement Policy for placing Users in Different Containers



6.3.2 Specifying Distribution Lists

Distribution lists are used by organizations to assure that the appropriate individuals are included in various internal communications. Wherever possible, organizations should automatically assign new employees to these distribution lists so that they can immediately participate in the communications that are relevant to them.

Using a Subscriber Create policy when an eDirectory user is created, the GroupWise account can be added to a distribution list based on the eDirectory container. When a user is created in the Sales container, the user is added to the Sales Distribution List. When a user is created in the Engineering container, the user is added to the Engineering Distribution List.

The policies in this section, created by using Policy Builder, show how to configure the following actions:

- ◆ [“Creating a New User as a Member of a Distribution List Based on the User’s eDirectory Container” on page 52](#)
- ◆ [“Adding a User as a Blind Copy or Carbon Copy Participant in a Distribution List” on page 52](#)
- ◆ [“Adding a User to a Distribution List When He or She Becomes a Manager” on page 53](#)
- ◆ [“Removing a User from a Distribution List When the User is No Longer a Manager” on page 54](#)
- ◆ [“Removing a User from All Distribution Lists” on page 54](#)

Using Policy Builder, you can use these examples to create similar policies and Distribution Lists for your business rules and environment.

Creating a New User as a Member of a Distribution List Based on the User's eDirectory Container

Figure 6-3 Create Policy

The screenshot shows the 'Rule Builder' interface with the following sections:

- Description:** A text box containing 'Users in Engr container are placed in the EngrDL distribution list'.
- Conditions:**
 - Selected condition structure: AND Conditions, OR Groups
 - Append Condition Group:** A green box containing two conditions:
 - Condition Group 1:** 'If class name' with operator 'equal', compare mode 'case insensitive', and value 'User'.
 - And If:** 'source DN' with operator 'in container' and value 'Novell\GroupWise\Engr'.
- Actions:**
 - Action List:** A blue box containing two actions:
 - Do:** 'set destination attribute value' with attribute name 'Distribution List DN', class name 'User', mode 'add to current operation', object 'Current object', value type 'dn', and DN value 'Novell\GroupWise\EngrDL'.
 - Do:** 'break'.

Adding a User as a Blind Copy or Carbon Copy Participant in a Distribution List

The user participates in the distribution list as a primary, blind copy, or carbon copy member. The XML attributes of `gw:participation="bc"` and `gw:participation="cc"` are used to set the type of membership a user has in the distribution list. If these attributes are not specified, it defaults to primary.

```
<modify-attr attr-name="Distribution List DN" xmlns:gw="http://www.novell.com/
dirxml/gwdriver" gw:participation="bc">
  <add-value>
    <value type="string">\IDMTREE\Novell\Users\cDL1</value>
    <value type="string">\IDMTREE\Novell\Users\cG1</value>
  </add-value>
</modify-attr>
```

or

```

<add-attr attr-name="Distribution List DN xmlns:gw="http://www.novell.com/
dirxml/gwdriver" gw:participation="bc">
  <value type="string">\IDMTREE\Novell\Users\cDL1</value>
  <value type="string">\IDMTREE\Novell\Users\cG1</value>
</add -attr>

```

To add the user as a carbon copy member, replace the attribute gw:participation="bc" with gw:participation="cc".

Adding a User to a Distribution List When He or She Becomes a Manager

Figure 6-4 Adding a User to a Distribution List

The screenshot shows the 'Rule Builder' window with the following configuration:

- Description:** Add a user to the MgrDL distribution list when made a manager
- Conditions:**
 - Select condition structure: AND Conditions, OR Groups
 - Append Condition Group:**
 - Condition Group 1:**
 - If class name
 - Select operator: equal
 - Compare mode: case insensitive
 - Value: User
 - And If operation attribute
 - Enter name: isManager
 - Select operator: changing to
 - Compare mode: case insensitive
 - Value: true
 - Actions:**
 - Action List:**
 - Do set destination attribute value
 - Enter attribute name: Distribution List DN
 - Enter class name: User
 - Select mode: add to current operation
 - Select object: Current object
 - Enter value type: dn
 - Enter DN: "Novell\GroupWise\MgrDL"

Removing a User from a Distribution List When the User is No Longer a Manager

Figure 6-5 Removing a User from a Distribution List

The screenshot shows the Rule Builder interface with two main sections: a condition and an action.

Condition: A green checkmark icon is followed by the text "And If" and a dropdown menu set to "operation attribute". Below this are four input fields: "Enter name:*" with the value "isManager", "Select operator:*" with the value "changing from", "Compare mode:" with the value "case insensitive", and "Value:" with the value "true".

Actions: A section titled "Action List" contains a single action. It starts with a green checkmark icon and the text "Do" followed by a dropdown menu set to "remove destination attribute value". Below this are five input fields: "Enter attribute name:*" with the value "Distribution List DN", "Enter class name:" with the value "User", "Select mode:" with the value "add to current operation", "Select object:" with the value "Current object", and "Enter value type:" with the value "dn". At the bottom, there is an "Enter DN:*" field with the value "Novell\GroupWise\MgrDL".

Removing a User from All Distribution Lists

Figure 6-6 Removing a User from All Distribution Lists

The screenshot shows the Rule Builder interface with three main sections: a description, a condition, and an action.

Rule Builder: The title bar of the window is "Rule Builder".

Description: A text box contains the description "Remove a user from all distribution lists".

Conditions: A section titled "Conditions" has a "Select condition structure:" label. Two radio buttons are present: "OR Conditions, AND Groups" (unselected) and "AND Conditions, OR Groups" (selected).

Append Condition Group: A section titled "Append Condition Group" has a red asterisk and the word "Required" to its right. It contains a "Condition Group 1" section with a green checkmark icon and a dropdown menu set to "If class name". Below this are three input fields: "Select operator:*" with the value "equal", "Compare mode:" with the value "case insensitive", and "Value:" with the value "User".

Actions: A section titled "Action List" contains a single action. It starts with a green checkmark icon and the text "Do" followed by a dropdown menu set to "clear destination attribute value". Below this are four input fields: "Enter attribute name:*" with the value "Distribution List DN", "Enter class name:" with the value "User", "Select mode:" with the value "add to current operation", and "Select object:" with the value "Current object".

When a user is removed from the distribution list, the driver cleans up the Member attribute from the associated group object.

6.3.3 Setting Defaults for GroupWise Attributes

Other attributes can be set in the GroupWise account by using the Create policy. Some attributes must be set in both eDirectory and GroupWise. When the eDirectory user object contains a corresponding attribute, it must be set. It is important that attribute values are set in both eDirectory and GroupWise. If the attribute is set only in GroupWise, it could be overwritten with the value in eDirectory. You must customize the driver to update values in eDirectory; the driver does not do this by default.

The following example shows setting the Description attribute in eDirectory and GroupWise. The attribute write-back = "true" causes the attribute to also be written in eDirectory.

```
<?xml version="1.0" encoding="UTF-8"?>
<create-rules>
  <create-rule class-name="User" description="GroupWise Account Required
Attributes">
    <!-- Description attribute is given a default value in both
eDirectory and in GroupWise -->
    <required-attr attr-name="Description" write-back="true">
      <value type="String"><![CDATA[eDirectory User synchronized by
GroupWise Driver]]></value>
    </required-attr>
  </create-rule>
</create-rules>
```

6.3.4 Configuring the GroupWise UserID

The CN attribute in eDirectory is used to name the GroupWise account. You must include this in the Create policy as a required attribute. The CN value from eDirectory can be ignored in the Subscriber Create policy and a CN based on other attributes can be generated. An example code segment from a Create policy is shown below. If you make modifications to this policy, the modify events coming from the engine also need to be modified.

When an attribute used to construct the CN is modified, a GroupWise Rename event should be generated via the policies. The UserID must be unique within a post office. If UserID is used to generate Internet EMail Address, it must be unique in the entire GroupWise system. The UserID contains 1 to 256 characters, and cannot contain the () @ . : , { } * " characters. The UserID must be unique within its namespace (UserID shares the same namespace as nicknames, resources, and distribution lists.) Do not use "mapi" (reserved ID) for this value.

An Output Transformation or Event Transformation policy can monitor the attributes used to build the CN. If one of these attributes changes, a Rename event should also be generated. Any attributes used here need to be added to the list of required attributes. In this case, Rename events should still be forwarded to the driver with an empty <newname> element. See ["Renaming Users" on page 62](#) for more information.

```
<rule>
  <!--CN is used to set the GroupWise UserID. Construct a new CN from Given
Name.-->
  <description>Use Given Name for GroupWise Account Name</description>
  <conditions>
    <and>
```

```

    <if-class-name op="equal">User</if-class-name>
  </and>
</conditions>
<actions>
  <!-- 'CN' and 'Given Name' must be present -->
  <do-veto-if-op-attr-not-available name="CN"/>
  <do-veto-if-op-attr-not-available name="Given Name"/>
  <!-- replace current CN value with the 'Given Name' value -->
  <do-reformat-op-attr name="CN">
    <arg-value type="string">
      <token-op-attr name="Given Name"/>
    </arg-value>
  </do-reformat-op-attr>
</actions>
</rule>

```

6.3.5 Creating Mappings for Additional Attributes

You can synchronize any attribute that can be represented as a string in eDirectory with one of twenty GroupWise generic attributes (excluding octet strings and structured attributes). You specify the eDirectory attribute you want to map in the filter. In addition, the eDirectory and GroupWise attribute names must be connected in the Schema Mapping policy.

The Schema Mapping rule code segment below connects the eDirectory attribute Location with the GroupWise attribute 55003.

```

<attr-name class-name="User">
  <nds-name>Location</nds-name>
  <app-name>55003</app-name>
</attr-name>

```

The twenty GroupWise attribute names are 50106 through 50115 and 55002 through 55011. Address book labels can be assigned to these GroupWise attributes through the GroupWise ConsoleOne[®] snap-ins. You should configure the same mappings in GroupWise as you do in the driver mappings.

6.3.6 Getting a Record Count from a Query

The following query, sent to the driver, returns the number of users in dom1.po1.

```

<nds dtdversion="1.1" ndsversion="8.6">
  <input>
    <query event-id="query-groupwise" scope="subtree">
      <search-class class-name="User"/>
      <!-- Referenced Domain Name -->
      <search-attr attr-name="50035">
        <value>dom1</value>
      </search-attr>
      <!-- Referenced Post Office Name -->
      <search-attr attr-name="50062">
        <value>po1</value>
      </search-attr>
    </query>
  </input>
</nds>

```



```

        <!-- return Record Count-->
        <read-attr attr-name="Record Count"/>
    </query>
</input>
</nds>

```

If you remove the post office search attr, it returns the number of users in dom1. If you remove the domain search attr, it returns the number of users in the system. This search can be altered to apply to other search criteria.

6.3.7 Deleting the GroupWise User without Deleting the eDirectory User

After deleting the user in GroupWise, the driver cleans up the GroupWise attributes in eDirectory. The result is the same as deleting the user with the GroupWise snap-ins and only selecting Delete from GroupWise.

You need to change the match criteria to match the needs of your environment.

```

<!-- You need to change the conditions to meet the needs of your system. -->
<policy xmlns:gw="http://www.novell.com/dirxml/gwdriver">
  <rule>
    <description>Delete GroupWise user but keep eDirectory user</description>
    <conditions>
      <and>
        <if-class-name op="equal">User</if-class-name>
        <if-operation op="equal">modify</if-operation>
        <if-op-attr name="OU" op="changing-to">inactive</if-op-attr>
      </and>
    </conditions>
    <actions>
      <do-delete-dest-object/>
      <do-set-xml-attr expression='../delete[@class-name="User"]'
name="gw:original-event">
        <arg-string>
          <token-text xml:space="preserve">modify</token-text>
        </arg-string>
      </do-set-xml-attr>
      <do-veto/>
    </actions>
  </rule>
</policy>

```

6.3.8 Creating a GroupWise Nickname

GroupWise nicknames can be automatically created when an eDirectory User is renamed or when a GroupWise account is moved. This is controlled in iManager on the driver through the Global Configuration Value page. When you set this option to True, nicknames are automatically created when an eDirectory rename occurs or when a GroupWise account is moved. When you set this option to False, nicknames are not created. Nickname creation requires GroupWise 6.5 SP1 or higher agents to be running. You can override this option by adding code to the Output Transformation policy to specify whether a nickname should be created.

```

<policy xmlns:gw="http://www.novell.com/dirxml/gwdriver">
  <rule>
    <description>Create GroupWise Nickname</description>
    <conditions>
      <and>
        <if-operation op="equal">rename</if-operation>
        <if-class-name op="equal">User</if-class-name>
      </and>
    </conditions>
    <actions>
      <do-set-xml-attr expression="." name="gw:create-nickname">
        <arg-string>
          <token-text xml:space="preserve">>true</token-text>
        </arg-string>
      </do-set-xml-attr>
    </actions>
  </rule>
</policy>

```

6.3.9 Creating a GroupWise Nickname Record

The following examples show two ways to create a nickname record. The first specifies the post office in which the nickname is created in the <dest-dn> attribute (this implies the domain). The second example uses <add-attr> nodes to specify the domain and post office.

The nickname can contain 1 to 256 characters, and cannot contain the ()@.,{}*" characters. It must be unique within its namespace (nicknames share the same namespace as users, resources, and distribution lists.)

```

          <add class-name="GroupWise Nickname" dest-
dn="Novell\dirxml\groupwise\xmlPO" event-id="0" >
  <!-- Domain of user this nickname refers to -->
  <add-attr attr-name="50068" >
    <value type="string">xmlDom</value>
  </add-attr>
  <!-- Post Office of user this nickname refers to -->
  <add-attr attr-name="50069" >
    <value type="string">xmlPO</value>
  </add-attr>
  <!-- user this nickname refers to -->
  <add-attr attr-name="50070" >
    <value type="string">Usern1</value>
  </add-attr>

  <!-- name of nickname record -->
  <add-attr attr-name="50073" >
    <value type="string">nn1</value>
  </add-attr>
</add>

```

OR

```

<add class-name="GroupWise Nickname" event-id="0" >
  <!-- Domain of user this nickname refers to -->
  <add-attr attr-name="50068" >
    <value type="string">xmlDom</value>
  </add-attr>

```

```

    <!-- Post Office of user this nickname refers to -->
    <add-attr attr-name="50069" >
      <value type="string">xmlPO</value>
    </add-attr>
    <!-- user this nickname refers to -->
    <add-attr attr-name="50070" >
      <value type="string">Usern1</value>
    </add-attr>

    <!-- Domain of nickname record -->
    <add-attr attr-name="50035" >
      <value type="string">xmlDom</value>
    </add-attr>
  <!-- Post Office of nickname record -->
  <add-attr attr-name="50062" >
    <value type="string">xmlPO</value>
  </add-attr>
  <!-- name of nickname record -->
  <add-attr attr-name="50073" >
    <value type="string">nn1</value>
  </add-attr>
</add>

```

6.3.10 Specifying a New Resource Owner on an Owner Delete

If the owner of a resource (a conference room, for instance) is deleted, the driver automatically assigns that resource to another owner. You must designate a default user for all resource assignments. At the time the resource is assigned, if the driver detects no default user account, it creates the default user account and assigns the resource to that user.

Through a policy, you can specify an override owner. Using the Output Transformation policy, the eDirectory User delete is selected. The special attribute, `gw:resource-owner-dn`, is used to notify the shim of the override resource owner. This special attribute is specified on the `<delete>` element. Resources are always reassigned on a delete. The new owner must already exist in GroupWise and be in the same post office as the user being deleted. If a failure occurs using the override owner, the resources are automatically assigned to the default user specified in the driver options. The XSLT code segment is:

```

<policy xmlns:gw="http://www.novell.com/dirxml/gwdriver">
  <rule>
    <description>Specify Resource Owner DN for User Delete</description>
    <conditions>
      <and>
        <if-operation op="equal">delete</if-operation>
        <if-class-name op="equal">User</if-class-name>
      </and>
    </conditions>
    <actions>
      <do-set-xml-attr expression="." name="gw:resource-ownerdn">
        <arg-string>
          <token-text
xml:space="preserve">\GWDRIVERTREE\novell\users\sales\ResourceOwner</token-
text>

```

```

        </arg-string>
      </do-set-xml-attr>
    </actions>
  </rule>
</policy>

```

6.3.11 Specifying a New Resource Owner on an Owner Disable

If the owner of a resource (a conference room, for instance) is disabled, you can use GCVs to configure the driver to automatically assign that resource to another owner. In this process, you can designate a default user for all resource assignments. At the time a resource is being reassigned, if the driver detects no default user account, it creates a default user account and assigns it as the resource owner only if the Reassign Resource Ownership driver GCV is set to True.

When an eDirectory User Login Disabled attribute is set, the GroupWise resources of the disabled or expired account can be assigned to another GroupWise account. Normally, the new owner is a default user specified in the Default Resource Owner UserID parameter. Through a policy, an override owner can be specified. Using the Output Transformation policy, the eDirectory User login disable is selected. The special attribute, gw:resource-owner-dn, is used to notify the shim of the override resource owner. This special attribute is specified in the <modify-attr> element.

The resources are assigned to the override owner even when the Reassign Resource Ownership GCV is set to False. The new owner must already exist in GroupWise and be in the same post office as the user being disabled. If a failure occurs using the override owner, the resources are automatically assigned to the default user specified in the Driver Options. The policy for disabling is:

```

<policy xmlns:gw="http://www.novell.com/dirxml/gwdriver">
  <rule>
    <description>Specify Resource Owner DN for User Delete</description>
    <conditions>
      <and>
        <if-operation op="equal">modify</if-operation>
        <if-op-attr name="50058" op="changing-to">>true</if-op-attr>
        <if-class-name op="equal">User</if-class-name>
      </and>
    </conditions>
    <actions>
      <do-set-xml-attr expression="." name="gw:resource-ownerdn">
        <arg-string>
          <token-text
xml:space="preserve">\GWDRIVERTREE\novell\users\sales\ResourceOwner</token-
text>
          </arg-string>
        </do-set-xml-attr>
      </actions>
    </rule>
  </policy>

```

6.3.12 Controlling Creation of GroupWise Accounts

There might be situations where an eDirectory user is created and you do not want to create a corresponding GroupWise account. In addition, not all eDirectory users initially have a GroupWise account. You can use the driver to control the creation of GroupWise accounts.

One way to control the creation of an account is to trigger the account creation using an extended attribute such as createGroupWiseAccount.

The eDirectory schema must be extended to include the attribute createGroupWiseAccount. When the createGroupWiseAccount attribute is set to True, the GroupWise account is created. When the createGroupWiseAccount attribute is set to False, the GroupWise account is not created. Changing the value from False to True causes the GroupWise account to be created.

The createGroupWiseAccount attribute must be added to the Create policy as a required attribute and also added to the Subscriber Filter.

```
<rule>
  <description>Require createGroupWiseAccount attribute</description>
  <conditions>
    <and>
      <if-class-name op="equal">User</if-class-name>
    </and>
  </conditions>
  <actions>
    <do-veto-if-op-attr-not-available name="createGroupWiseAccount"/>
  </actions>
</rule>
<rule>
  <description>Check createGroupWiseAccount attribute</description>
  <conditions>
    <and>
      <if-class-name op="equal">User</if-class-name>
      <if-op-attr name="createGroupWiseAccount" op="not-equal">>true</if-op-attr>
    </and>
  </conditions>
  <actions>
    <do-veto/>
  </actions>
</rule>
```

You can also use the global configuration value **“Default Sync Source: eDir Container/Subtree”** on [page 191](#) to select what part of the tree you want to synchronize to GroupWise.

6.3.13 Moving Users from One Post Office to Another Post Office

When a style sheet is not configured to move GroupWise accounts, we recommend that you use the GroupWise 7 snap-ins (or higher) for user moves.

When the Output Transformation style sheet is configured to move GroupWise accounts, we recommend that user moves be made in eDirectory and that the driver assign the object to a new post office in GroupWise. The XSLT code segment for the Output Transformation policy is shown below. The dest-dn attribute on the parent element specifies the new post office.

```
<rule>
  <description>Move User to GW PostOffice</description>
  <conditions>
    <and>
      <if-operation op="equal">move</if-operation>
      <if-class-name op="equal">User</if-class-name>
    </and>
  </conditions>
  <actions>
    <do-veto/>
  </actions>
</rule>
```

```

    </and>
  </conditions>
<actions>
  <do-if>
    <arg-conditions>
      <and>
        <if-xpath op="true">parent/@src-
dn="\GWDRIVERTREE\Novell\Users\Sales"</if-xpath>
      </and>
    </arg-conditions>
    <arg-actions>
      <do-set-xml-attr expression="parent" name="dest-dn">
        <arg-string>
          <token-text
xml:space="preserve">\GWDRIVERTREE\Novell\GroupWise\Post Offices\Sales PO</
token-text>
        </arg-string>
      </do-set-xml-attr>
    </arg-actions>
  </do-if>
  <do-if>
    <arg-conditions>
      <and>
        <if-xpath op="true">parent/@src-
dn="\GWDRIVERTREE\Novell\Users\Engineering"</if-xpath>
      </and>
    </arg-conditions>
    <arg-actions>
      <do-set-xml-attr expression="parent" name="dest-dn">
        <arg-string>
          <token-text
xml:space="preserve">\GWDRIVERTREE\Novell\GroupWise\Post Offices\Engineering
PO</token-text>
        </arg-string>
      </do-set-xml-attr>
    </arg-actions>
  </do-if>
</actions>
</rule>

```

6.3.14 Adding Additional Attributes to Be Synchronized

You can map up to twenty user eDirectory attributes to generic GroupWise attributes and display them in the address book. For these attributes, you use the ranges 50106-50115 and 55002-55011. You must first add these eDirectory attributes to the filter. You must configure these attributes in the GroupWise ConsoleOne snap-ins for these attributes to appear in the GroupWise address book.

6.3.15 Renaming Users

We recommend that you rename users by changing the naming attribute in eDirectory and letting the driver rename the GroupWise account. When CN is the naming attribute (this is the default), no special style sheet coding is required for a rename process. However, the GroupWise MailboxID can be built from attributes other than CN. When one of these attributes is modified, the GroupWise account should also be renamed. The XSLT code segment is shown below. In this example, the eDirectory attribute Given Name is used to name the GroupWise account. When Given Name is modified, a GroupWise rename is generated. In the second template below, `<xsl:template`

match="@class-name='User'"]"> handles the case where the eDirectory User object was renamed. In this case the <rename> command is passed through to the driver. The empty <new-name/> element blocks the driver from renaming the GroupWise account. Even though the GroupWise account is not renamed, the rename event must pass to the driver.

We do not recommend that you use the GroupWise snap-ins to do a rename. However, if the user is renamed using the GroupWise snap-ins, it must be done with GroupWise 6.5 SP1 or higher. If you use an older version of the GroupWise snap-ins, it can cause the driver to generate errors.

Example 1

(placed in the subscriber event transform, or subscriber command transform)

```
<rule>
  <description>Rename User if Given Name is changing</description>
  <conditions>
    <and>
      <if-operation op="equal">modify</if-operation>
      <if-op-attr name="Given Name" op="changing"/>
      <if-class-name op="equal">User</if-class-name>
    </and>
  </conditions>
  <actions>
    <do-rename-dest-object>
      <arg-string>
        <token-op-attr name="Given Name"/>
      </arg-string>
    </do-rename-dest-object>
  </actions>
</rule>
```

Example 2

(placed in the subscriber event transform)

```
<rule>
  <description>Veto Rename User operations</description>
  <conditions>
    <and>
      <if-operation op="equal">rename</if-operation>
      <if-class-name op="equal">User</if-class-name>
    </and>
  </conditions>
  <actions>
    <do-veto/>
  </actions>
</rule>
```

6.3.16 Creating a Gateway Alias

The following XSLT code segment shows how to create a gateway alias in the Output Transformation policy. Your code is responsible for generating the value of attributes 50140 and 50077.

```

<rule>
  <description>Create GW Gateway Alias attribute for new user</description>
  <conditions>
    <and>
      <if-operation op="equal">add</if-operation>
      <if-class-name op="equal">User</if-class-name>
    </and>
  </conditions>
  <actions>
    <do-add-dest-attr-value class-name="User" name="Gateway Alias">
      <arg-value type="structured">
        <arg-component name="50140">
          <token-text xml:space="preserve">SMTP</token-text>
        </arg-component>
        <arg-component name="50077">
          <token-text xml:space="preserve">UserOne@novell.com</token-text>
        </arg-component>
      </arg-value>
    </do-add-dest-attr-value>
  </actions>
</rule>

```

6.3.17 Querying for a Nickname

The following Output Transformation policy shows how to query for GroupWise nicknames. The search-attrs in this style sheet are optional. They are used to scope the search. When you specify a post office name (50069), you must also specify a domain name (50068). More than one nickname can be returned.

For example, User2a is renamed to User2b, then renamed to User2c. There will be two nickname records (User2a and User2b) which both reference User2c. This code sample queries the User of the current event for nicknames. You should use a different match criterion.

```

<rule>
  <description>Query for User's GroupWise Nicknames</description>
  <conditions>
    <and>
      <if-operation op="equal">modify</if-operation>
      <if-class-name op="equal">User</if-class-name>
    </and>
  </conditions>
  <actions>
    <do-set-local-variable name="gw-user-name">
      <arg-node-set>
        <token-query class-name="User" scope="entry">
          <arg-association>
            <token-association/>
          </arg-association>
          <arg-string>
            <token-text xml:space="preserve">50035</token-text>
          </arg-string>
          <arg-string>
            <token-text xml:space="preserve">50062</token-text>
          </arg-string>
          <arg-string>
            <token-text xml:space="preserve">50073</token-text>
          </arg-string>
        </token-query>
      </arg-node-set>
    </do-set-local-variable>
  </actions>
</rule>

```



```

        </token-query>
    </arg-node-set>
</do-set-local-variable>
<do-set-local-variable name="gw-nickname">
    <arg-node-set>
        <token-query class-name="GroupWise Nickname">
            <arg-match-attr name="50068">
                <arg-value>
                    <token-xpath expression="$gw-user-name//attr[@attr-name='50035']/"
value"/>
                </arg-value>
            </arg-match-attr>
            <arg-match-attr name="50069">
                <arg-value>
                    <token-xpath expression="$gw-user-name//attr[@attr-name='50062']/"
value"/>
                </arg-value>
            </arg-match-attr>
            <arg-match-attr name="50070">
                <arg-value>
                    <token-xpath expression="$gw-user-name//attr[@attr-name='50073']/"
value"/>
                </arg-value>
            </arg-match-attr>
            <arg-string>
                <token-text xml:space="preserve">50035</token-text>
            </arg-string>
            <arg-string>
                <token-text xml:space="preserve">50062</token-text>
            </arg-string>
            <arg-string>
                <token-text xml:space="preserve">50073</token-text>
            </arg-string>
        </token-query>
    </arg-node-set>
</do-set-local-variable>
</actions>
</rule>

```

Result

```

<nds dtdversion="1.1" ndsversion="8.6">
    <source>
        <product build="20020409_1220" instance="GroupWise ZDS Driver"
version="1.0a Beta">DirXML Driver for GroupWise</product>
        <contact>Novell, Inc.</contact>
    </source>
    <output>
        <instance class-name="GroupWise Nickname" event-id="0">
            <attr attr-name="50035">
                <value type="string">TaoDom</value>
            </attr>
            <attr attr-name="50062">
                <value type="string">TaoPO</value>
            </attr>
            <attr attr-name="50073">
                <value type="string">User2b</value>
            </attr>
        </instance>
    </output>
</nds>

```

```

</instance>
<instance class-name="GroupWise Nickname" event-id="0">
  <attr attr-name="50035">
    <value type="string">TaoDom</value>
  </attr>
  <attr attr-name="50062">
    <value type="string">TaoPO</value>
  </attr>
  <attr attr-name="50073">
    <value type="string">User2a</value>
  </attr>
</instance>
<status level="success"/>
</output>
</nds>

```

6.3.18 Querying for a Gateway Alias

The following XSLT code segment shows how to query in the Output Transformation policy for a gateway alias.

```

<rule>
  <description>Query for User's GroupWise Gateway Alias</description>
  <conditions>
    <and>
      <if-operation op="equal">modify</if-operation>
      <if-class-name op="equal">User</if-class-name>
    </and>
  </conditions>
  <actions>
    <do-set-local-variable name="gw-alias">
      <arg-node-set>
        <token-query class-name="User" scope="entry">
          <arg-association>
            <token-association/>
          </arg-association>
          <arg-string>
            <token-text xml:space="preserve">Gateway Alias</token-text>
          </arg-string>
        </token-query>
      </arg-node-set>
    </do-set-local-variable>
  </actions>
</rule>

```

Result

```

<nds dtdversion="1.0" ndsversion="8.5">
  <source>
    <product version="1.0 SP1 Beta, 20020307_1205">GroupWise ZDS Driver</product>
    <contact>Novell, Inc.</contact>
  </source>
  <output>
    <instance class-name="User" event-id="0" src-
dn="TaoDom.TaoPO.User1{106}DFD036A0-0776-0000-A246-4100F0001300">
      <association>TaoDom.TaoPO.User1{106}DFD036A0-0776-0000-A246-
4100F0001300<association>

```

```

        <attr attr-name="Gateway Alias">
            <value type="structured">
                <component name="50140">SMTP</component>
                <component name="50077">UserOne@novell.com</component>
            </value>
        </attr>
    </instance>
    <status level="success"/>
</output>
</nds>

```

6.3.19 Querying for Internet EMail Address

The following XSLT code segment shows how to query in the Output Transformation policy for the Internet Email Address generated by GroupWise.

```

<rule>
  <description>Query for User's GroupWise Internet E-mail Address</
description>
  <conditions>
    <and>
      <if-operation op="equal">modify</if-operation>
      <if-class-name op="equal">User</if-class-name>
    </and>
  </conditions>
  <actions>
    <do-set-local-variable name="gw-email-address">
      <arg-node-set>
        <token-query class-name="User" scope="entry">
          <arg-association>
            <token-association/>
          </arg-association>
          <arg-string>
            <token-text xml:space="preserve">Internet EMail Address</token-
text>
          </arg-string>
        </token-query>
      </arg-node-set>
    </do-set-local-variable>
  </actions>
</rule>

```

Results

```

<nds dtdversion="1.1" ndsversion="8.6">
  <source>
    <product build="20020502_1251" instance="GroupWise Driver"
      version="1.0a Beta">DirXML Driver for GroupWise</product>
    <contact>Novell, Inc.</contact>
  </source>
  <output>
    <instance class-name="User" event-id="0"
      src-dn="TaoDom.TaoPO.User2{106}5B8C40F0-0E79-0000-9ADA-
350037009300">
      <association>TaoDom.TaoPO.User2{106}5B8C40F0-0E79-
0000-9ADA-350037009300</association>
      <attr attr-name="Internet EMail Address">
        <value type="string">User2@domain.com</value>

```

```
</attr>
  </instance>
  <status level="success"/>
</output>
</nds>
```

6.3.20 Synchronizing GroupWise External Users

In your business, you might have several different e-mail applications. Although not all employees will have GroupWise e-mail accounts, you want the GroupWise address book to contain all employee information. The driver has the ability to create GroupWise external users, which enables the driver to obtain data from other e-mail systems (via the Identity Vault) and display it in the GroupWise address book. The users in the Identity Vault can be assigned to a GroupWise External Post Office.

If you are using multiple e-mail systems (GroupWise and NetMail[®]/Notes/Exchange) you can create external users and external post offices to add the users in the non-GroupWise systems to the GroupWise address book.

To synchronize data between external e-mail systems and GroupWise, your implementation must meet the following conditions:

- ♦ External users must be assigned to or be created in an external post office. These users do not have a GroupWise mailbox.
- ♦ External post offices must belong to a non-GroupWise domain.

The default driver configuration does allow for this customization. To implement this functionality, you must select the following options during the configuration of the driver:

- ♦ [“Include Policies for GroupWise External Entity Synchronization?” on page 37](#)
- ♦ [“Include Policies for eDirectory OrgUnit to GroupWise External Post Office Synchronization?” on page 37](#)

Creating External Users

There are three ways you can specify placement when creating external users:

- ♦ In the Placement rule, you can specify the DN of an eDirectory object associated with the external post office. For additional information, refer to [“Creating External Post Offices” on page 69](#).
- ♦ Identify the external post office by [“Specifying an External Post Office in an Add Event” on page 69](#).
- ♦ Create a user in an organizational unit associated with the External GroupWise Post Office. For more information, see [“Include Policies for eDirectory OrgUnit to GroupWise External Post Office Synchronization?” on page 37](#).

When creating accounts in eDirectory for a non-GroupWise user, make sure the attribute `gw:classification=“external”` is part of the Add event. The attribute can be used on the User object and on the Post Office object. If you have selected the options of [“Include Policies for GroupWise External Entity Synchronization?” on page 37](#) and [“Include Policies for eDirectory OrgUnit to GroupWise External Post Office Synchronization?” on page 37](#) during the configuration of the driver, the attribute is automatically part of the Add event.

You can modify the Schema Mapping policy or Output Transformation policy so that it modifies the class name of the user based on some criterion, such as the parent container name. The external users were formerly a separate class. The preferred method is to add the attributes instead of adding a new class. These two methods are mutually exclusive.

When a new GroupWise external user is added to GroupWise, the driver creates an association on the User object in the Identity Vault. If the non-GroupWise user's information changes in the Identity Vault, the driver synchronizes those changes to GroupWise. If the association key is altered or deleted, the connection is broken, and the driver does not synchronize any changes made to the User object in the Identity Vault to GroupWise.

Specifying an External Post Office in an Add Event

If you do not use the driver to create an external post office, you need to generate the following information in the XML Add event. You must replace the external post office name and non-GroupWise domain values with names specific to your system.

```
<!-- The external post office name to which the user belongs. -->
  <add-attr attr-name="50062">
    <value type="string"><![CDATA[External post office name]]></
value>
  </add-attr>

<!-- The non-GroupWise domain name to which the external post office belongs.
-->
  <add-attr attr-name="50035">
    <value type="string"><![CDATA[Non-GroupWise domain name]]></value>
  </add-attr>
```

NOTE: If you include the additional XML in the Add event, the value in your Placement policy is overridden.

Creating External Post Offices

There are two ways you can create external post offices:

- ◆ Let the driver create a GroupWise external post office and associate it to an eDirectory object, such as an Organizational Unit (recommended). Select **“Include Policies for eDirectory OrgUnit to GroupWise External Post Office Synchronization?”** on page 37 during the configuration of the driver.
- ◆ Create an external post office through ConsoleOne.

NOTE: Before you can create an external post office, you must create a non-GroupWise domain in ConsoleOne.

There are two ways you can specify placement when creating external post offices:

- ♦ In the Placement policy, you can specify the name of the non-GroupWise domain in which to create the external post office.
- ♦ Identify the non-GroupWise domain by generating XML code to specify the non-GroupWise domain. For additional information, refer to [“Specifying a Non-GroupWise Domain in an Add Event” on page 70](#).

Specifying a Non-GroupWise Domain in an Add Event

You can generate the following information in the XML Add event. You must replace the non-GroupWise domain value with the name specific to your system. If you use the configuration option of [“Include Policies for eDirectory OrgUnit to GroupWise External Post Office Synchronization?” on page 37](#), the driver does this automatically. If you do not use this option, you need to use the following information to manually specify a Non-GroupWise domain in an Add event.

```
<!-- The non-GroupWise domain name to which the external post office belongs.
-->
  <add-attr attr-name="50035">
    <value type="string"><![CDATA[Non-GroupWise domain name]]</value>
  </add-attr>
```

NOTE: If you include the additional XML in the Add event, the value in your Placement policy is overridden.

If you associate the external post office with an Organizational Unit, you must also map the OU attribute to the CN attribute for the Organizational Unit class, and the driver will use that attribute value for the post office name.

NOTE: The Schema Mapping policy has a mapping for the OU attribute on the User class. Do not change the User class mapping.

When creating external users, you should use the DN of the Organizational Unit in the Placement policy. When an external post office is added, you should specify the GroupWise domain to which the external post office belongs:

When you create an external post office with the driver, GroupWise uses the default time zone setting on the non-GroupWise domain. If you want to change the time zone setting for the post office, generate the following XML in the Add event. Insert the appropriate time zone value in place of EST.

```
  <add-attr attr-name="50088" >
    <value type="string">EST</value>
  </add-attr>
```

6.3.21 Verifying if an E-Mail Address or Gateway Alias Is Unique

The GroupWise driver has a special query that allows you to see if a proposed Internet e-mail address or gateway alias is unique. If the address is unique, a success status without an instance node is returned. If the address is not unique, the record owning the conflicting address is returned.

A query example follows, with a hard-coded value *helloworld@mydomain.com*. Make sure to replace each instance of the hard-coded value with your value.

```
<query event-id="query-groupwise" scope="subtree">
  <search-class class-name="User"/>
  <search-attr attr-name="Internet EMail Address">
    <value>helloworld@mydomain.com</value>
  </search-attr>
  <!-- Domain Name of Object -->
  <read-attr attr-name="50035"/>
  <!-- Post Office Name of Object -->
  <read-attr attr-name="50062"/>
  <!-- Object Name of Object -->
  <read-attr attr-name="50073"/>
</query>
```

If there is a gateway alias with this value, you receive the following:

```
<instance class-name="GroupWise GateWay Alias" event-id="0">
  <attr attr-name="50035">
    <value type="string">gwdom</value>
  </attr>
  <attr attr-name="50062">
    <value type="string">gwpo</value>
  </attr>
  <attr attr-name="50073">
    <value type="string">User3</value>
  </attr>
</instance>
```

The value of the `<attr attr-name>` elements give the name of the user to which the gateway belongs.

If an existing user owns the Internet e-mail address, you receive the following:

```
<instance class-name="User" event-id="0" src-dn="gwdom.gwpo.User3">
  <association>gwdom.gwpo.User3{106}7F7B2F70-0434-000-A0DE-DB0019009700</
association>
  <attr attr-name="50035">
    <value type="string">gwdom</value>
  </attr>
  <attr attr-name="50062">
    <value type="string">gwpo</value>
  </attr>
  <attr attr-name="50073">
    <value type="string">User3</value>
  </attr>
</instance>
```

Only one instance is returned, even if there are multiple conflicts.

6.4 Setting GroupWise Client Options with the Driver

The GroupWise driver allows you to use Identity Manager policies to set some of the GroupWise client options on users and external entities. Normally, the client options are set by the administrator through the GroupWise snap-ins in ConsoleOne, and if you want to set these options for objects other than users and external entities, you must use the GroupWise snap-ins.

- ♦ [Section 6.4.1, “Using Policies to Set Client Options,” on page 72](#)
- ♦ [Section 6.4.2, “Client Options,” on page 74](#)

6.4.1 Using Policies to Set Client Options

The Identity Manager policies use XML attributes and fields to set the GroupWise client options. The XML attribute and field names are different from the field names in ConsoleOne. However, you can access the client options in ConsoleOne, to see how the options are related and to decide which ones you want to edit, then use this documentation to find the corresponding XML attribute and field name to edit in the policy.

- ♦ [“Considerations” on page 72](#)
- ♦ [“Example Procedure” on page 73](#)

Considerations

As you edit the policy, keep the following considerations in mind:

- ♦ There are many fields for the client options and they are divided into attributes.
- ♦ The structure for all attributes is the same. The policy specifies the attribute, identifies the correct field, sets the value for the field, and allows you to lock the field.

```
<attr attr-name="">
  <value type="structured">
    <component name="lock-level"></component>
    <component name="value"></component>
    <component name="field"></component>
  </value>
</attr>
```

- ♦ The value and field components must be present. The lock level is optional. If the lock level is specified, it must also have a value specified. The absence of the lock level is the same as setting the lock level to 0.
- ♦ The lock level locks the ability to modify the field. The lock level is normally set through ConsoleOne snap-ins. It can be set at the user, post office, or domain level. If the field is locked at the post office, the field cannot be modified on users or external entities. The following lock levels are available in ConsoleOne:
 - ♦ 0: Not locked. Default
 - ♦ 2: Set on the user, but not locked.
 - ♦ 3: Set on the post office, but not locked.
 - ♦ 4: Set on the domain, but not locked.
 - ♦ 5: Locked on the user.

- ♦ 6: Locked on the post office.
- ♦ 7: Locked on the domain.
- ♦ You should set the lock levels through the GroupWise snap-ins in ConsoleOne. If you decide to use policies to set the lock levels, the GroupWise driver has the following restrictions:
 - ♦ The driver sets lock levels only on users and external entities.
 - ♦ Some fields should not be locked at the user level, but only at the Domain and Post Office levels. The driver cannot set these lock levels, so they must be set through ConsoleOne.
 - ♦ The driver can set the lock level values to either 0 or to 5. It cannot set any other value.
 - ♦ The policies must check to see what the current lock level is set to. If the value is greater than 5, the policies must not change the current lock level.
- ♦ Lock levels can be shared by a group of fields. If you want to lock one field in the group, you must lock all fields. A value must be set (even if it is the default value) for the lock to function.

Example Procedure

There are many different ways of adding the attributes to the policies. The following procedure shows how to add the AdvancedSetting attribute when an Add operation occurs.

- 1 In Designer, double-click the default Create policy in the Subscriber channel of the GroupWise driver.

For more information, see [Accessing the Policy Builder \(http://www.novell.com/documentation/idm35/index.html?page=/documentation/idm35/policy_designer/data/pbaccessing.html#pbaccessing\)](http://www.novell.com/documentation/idm35/index.html?page=/documentation/idm35/policy_designer/data/pbaccessing.html#pbaccessing).

- 2 Right-click the last rule.
- 3 Select *New > Rule > Insert Rule After*.
- 4 Specify a name for the new rule, then click *Next*.
- 5 Select *AND Conditions, OR Groups*, then click *Next*.
- 6 Select *operation* for the condition.
- 7 Select *equal*, then set the mode to *case sensitive*.
- 8 Select the value of *add*, then click *Next*.
- 9 Select *Continue*, then click *Next*.
- 10 Select the action of *add destination attribute value*.

The screenshot shows the 'Action 1' configuration window with the following settings:

- Do:** add destination attribute value
- Specify attribute name:** * AdvancedSettings
- Specify class name:** User
- Select mode:** add to current operation
- Select object:** Current object
- Specify value type:** structured
- Enter components:** * lock-level, value, field

- 11 Specify an attribute value of `AdvancedSettings` in the *attribute name* field.
- 12 Specify a class name of `User` in the *class name* field.
- 13 Select the *add to current operation* mode.
- 14 Select *Current object* to decide where to place the value.
- 15 Specify the value type of *structured*.
- 16 Click the *Edit the components* icon to specify the values of the attribute.
- 17 Specify `lock-level` in the *Name* field, then specify `0` for the value.
- 18 Click the *Append new item* icon.
- 19 Specify `value` in the *Name* field, then specify `0` for the value.
- 20 Click the *Append new item* icon.
- 21 Specify `field` in the *Name* field, then specify `autoSpellCheck` for the value.
- 22 Click *Finish* to save the values.

Argument Components

The argument components are structured argument values.



Name	Values	+	×	✂	📄	📋	↑	↓	?
lock-level	0								
value	0								
field	autoSpellCheck								

- 23 Click *Next*.
- 24 Select *Continue*, then click *Next*.
- 25 Review the summary, then click *Finish*.
- 26 Press `Ctrl+S` to save the new rule.

6.4.2 Client Options

To view the client options in ConsoleOne:

- 1 Select a Domain, Post Office, or User object, then click *Tools > GroupWise Utilities > Client Options*.



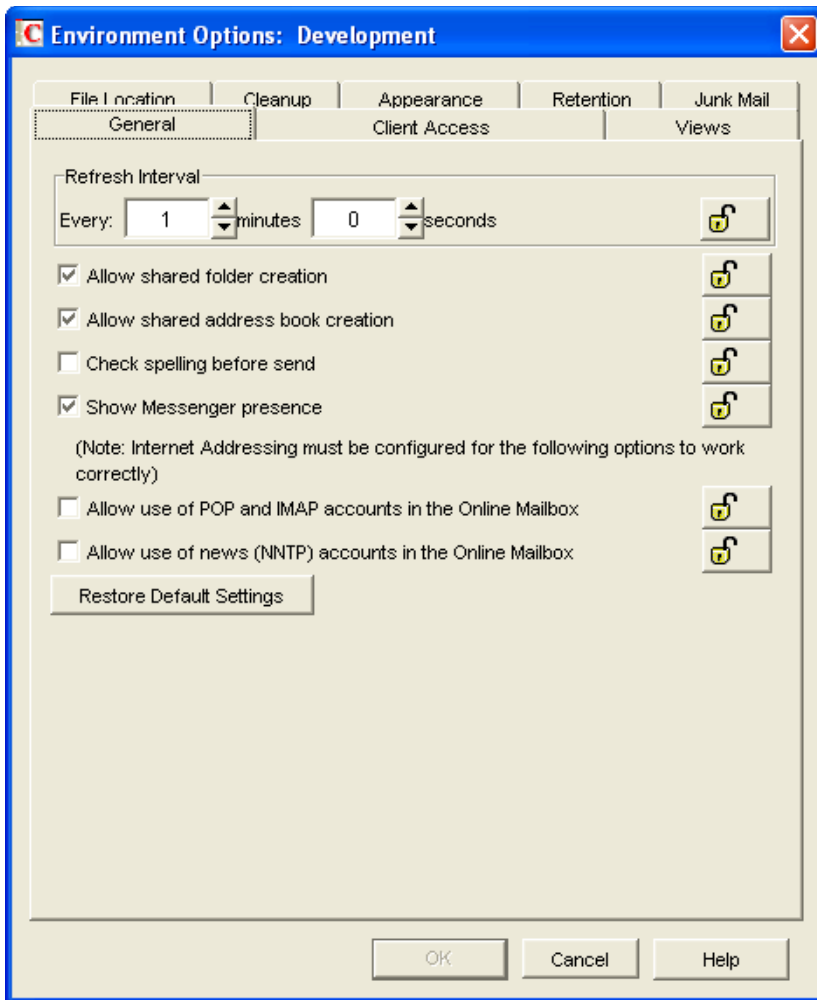
Use the following information to create policies to set the GroupWise client options on user objects.

- ◆ [Section 6.4.3, “Environment > General,” on page 75](#)
- ◆ [Section 6.4.4, “Environment > Client Access,” on page 78](#)
- ◆ [Section 6.4.5, “Environment > Views,” on page 79](#)
- ◆ [Section 6.4.6, “Environment > File Location > Archive Directory,” on page 82](#)
- ◆ [Section 6.4.7, “Environment > Cleanup,” on page 83](#)
- ◆ [Section 6.4.8, “Send > Send Options,” on page 85](#)
- ◆ [Section 6.4.9, “Send > Mail,” on page 89](#)
- ◆ [Section 6.4.10, “Send > Appt,” on page 92](#)
- ◆ [Section 6.4.11, “Send > Task,” on page 95](#)
- ◆ [Section 6.4.12, “Send > Note,” on page 98](#)
- ◆ [Section 6.4.13, “Send > Security,” on page 101](#)
- ◆ [Section 6.4.14, “Send > Disk Space Management,” on page 103](#)
- ◆ [Section 6.4.15, “Date and Time > Calendar,” on page 106](#)
- ◆ [Section 6.4.16, “Date and Time > Calendar > Alarm Options,” on page 109](#)
- ◆ [Section 6.4.17, “Date and Time > Busy Search,” on page 111](#)

6.4.3 Environment > General

The *General* options determine such settings as the refresh interval for new messages, whether users can create shared folders and address books, and which types of accounts can be used while in Online mode. The *General* options are found in ConsoleOne through the GroupWise client options under *Environment > General*.

Figure 6-7 Environment Options Dialog Box with the General Tab Open



There are two attributes that store this information; AdvancedSettings and EnvironmentSettings.

```
<attr attr-name="AdvancedSettings">
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">autoSpellCheck</component>
  </value>
</attr>
```

Check Spelling Before Send

The autoSpellCheck field spell-checks the message text of each item before the item is sent. To enable this option, set the value to 1. To disable this option, set the value to 0. By default, this option is disabled.

```
<attr attr-name="EnvironmentSettings">
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">1</component>
    <component name="field">allowSharedFolders</component>
  </value>
</attr>
```

```

</value>
<value type="structured">
  <component name="lock-level">0</component>
  <component name="value">1</component>
  <component name="field">allowSharedAddressBooks</component>
</value>
<value type="structured">
  <component name="lock-level">0</component>
  <component name="value">0</component>
  <component name="field">allowPOP_IMAPAccounts</component>
</value>
<value type="structured">
  <component name="lock-level">0</component>
  <component name="value">0</component>
  <component name="field">allowNNTPAccounts</component>
</value>
<value type="structured">
  <component name="lock-level">0</component>
  <component name="value">1</component>
  <component name="field">showIMPpresence</component>
</value>
</attr>

```

Allow Shared Folder Creation

The allowSharedFolders field enables users to share folders with other users. To enable this option, set the value to 1. To disable this option, set the value to 0. By default, this option is enabled.

Allow Shared Address Book Creation

The allowSharedAddressBooks field enables users to share address books with other users. To enable this option, set the value to 1. To disable this option, set the value to 0. By default, this option is enabled.

Allow Use of POP and IMAP Accounts in the Online Mailbox

The allowPOP_IMAPAccounts field enables users to access POP and IMAP accounts while using the GroupWise client in Online mode. To enable this option, set the value to 1. To disable this option, set the value to 0. By default, this option is disabled.

If you enable this option, an *Accounts* menu is added to the GroupWise client, allowing users to add POP and IMAP accounts to GroupWise, set account properties, and send and retrieve items from their POP and IMAP accounts. In addition, users are allowed to upload POP and IMAP items from the Remote mailbox to the Online mailbox.

IMPORTANT: If you lock this field, the lock level must be set on a Domain or Post Office, not on users or external entities.

Allow Use of News (NNTP) Accounts in the Online Mailbox

The allowNNTPAccounts field enables users to set up newsgroup (NNTP) accounts while using the GroupWise client in Online mode. To enable this option, set the value to 1. To disable this option, set the value to 0. By default, this option is disabled.

IMPORTANT: If you lock this field, the lock level must be set on a Domain or Post Office, not on users or external entities.

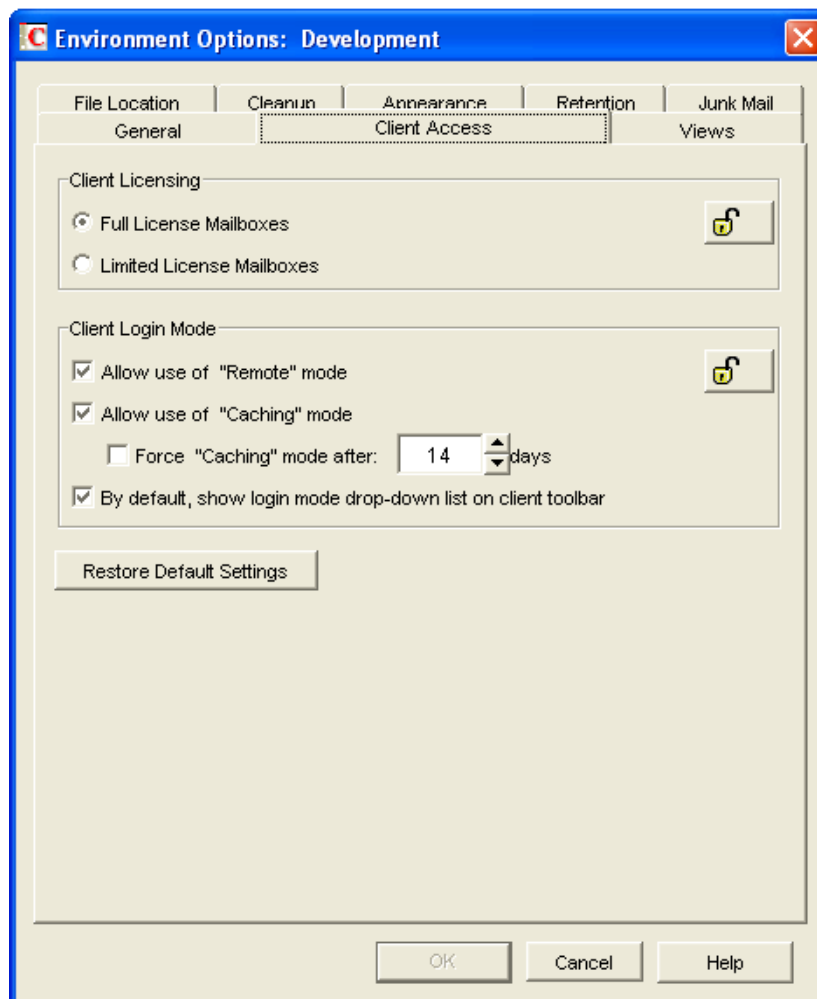
Show Messenger Presence

The showIMPresence field displays the Messenger presence information in the GroupWise Windows client. Messenger presence enables users to easily choose instant messaging as an alternative to e-mail. Messenger presence icons appear in the *From* field of a received message, in the Quick Info for users specified in the To, CC, and BC fields of a new message, and in the Quick Info for users in the Address Book. To enable this option, set the value to 1. To disable this option, set the value to 0. By default, this option is enabled.

6.4.4 Environment > Client Access

The *Client Access* options allow you to apply a license type (full or limited) to users' mailboxes and to enable or disable the Remote and Caching modes in the GroupWise client for Windows. The *Client Access* options are found in ConsoleOne through the GroupWise client options under *Environment > Client Access*.

Figure 6-8 Environment Options Dialog Box with the Client Access Tab Open



The `EnvironmentSettings` attribute stores this information.

```
<attr attr-name="EnvironmentSettings">
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">Full</component>
    <component name="field">clientLicense</component>
  </value>
</attr>
```

Client Licensing

The `clientLicense` field defines whether a: full client mailbox license or a limited client mailbox license is used. To enable full client mailbox licenses, set the value to `Full`. To enable limited client mailbox licenses, set the value to `Limited`.

A full client mailbox license has no mailbox access restrictions; the mailbox can be accessed by any GroupWise client (Windows or WebAccess) as well as any third-party plug-in or POP/IMAP client.

A limited client mailbox license restricts mailbox access to the following:

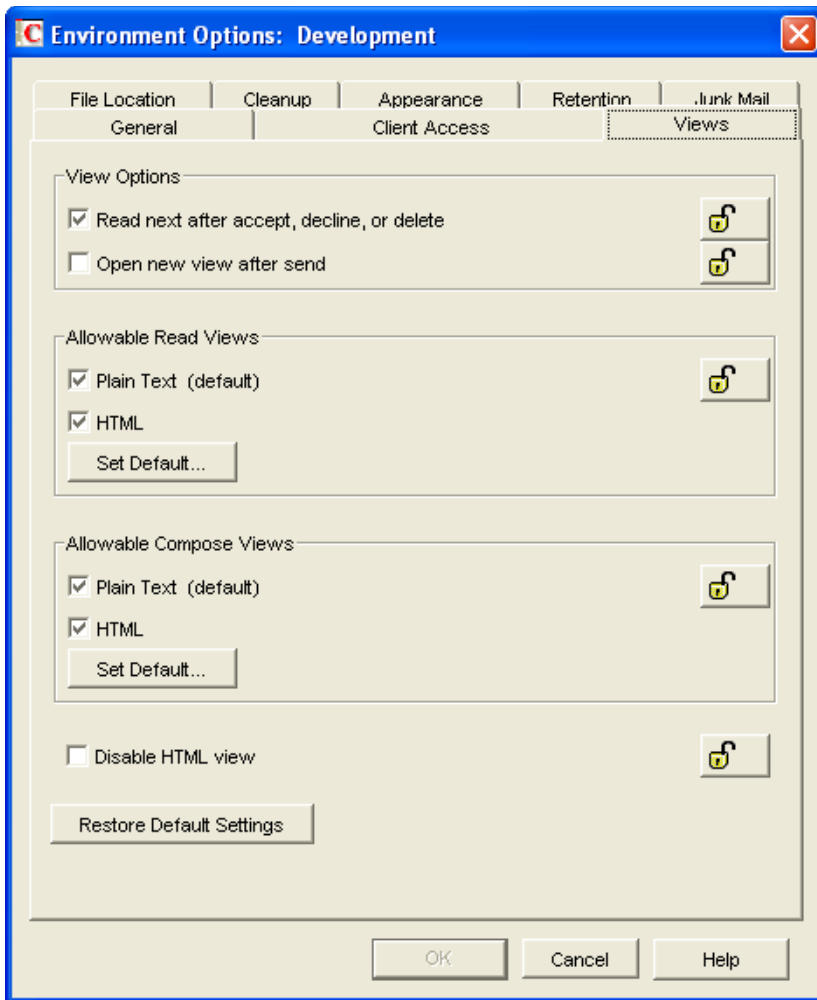
- ◆ The GroupWise WebAccess client (including wireless devices)
- ◆ A GroupWise client (Windows or WebAccess) via the Proxy feature
- ◆ A GroupWise client (Windows or WebAccess) via the Busy Search feature
- ◆ A POP or IMAP client

You can use this option to specify the type of client license that you want applied to users' mailboxes. This enables you to support the type of GroupWise mailbox licenses you purchase. For example, if you only purchased limited client license mailboxes for users on a specific post office, you can mark all mailboxes on that post office as being limited client license mailboxes.

6.4.5 Environment > Views

The *Views* Environment options determine when items open, and whether or not users can read and compose messages in HTML.

Figure 6-9 Environment Options Dialog Box with the Views Tab Open



The EnvironmentSettings attribute stores this information.

```
<attr attr-name="EnvironmentSettings">
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">Text, HTML</component>
    <component name="field">allowableViewRead</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">Text, HTML</component>
    <component name="field">allowableViewCompose</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">HTML</component>
    <component name="field">defaultViewRead</component>
  </value>
  <value type="structured">
```



```
<component name="lock-level">0</component>
<component name="value">HTML</component>
<component name="field">defaultViewCompose</component>
</value>
</attr>
```

Allowable Read Views

The allowableViewRead field determines what read views you allow the clients to use. There are two read views:

- ◆ **Plain Text:** Set the value to `Text` to allow users to read the items in plain text.
- ◆ **HTML:** Set the value to `HTML` to allow users to read the items in HTML.

You can specify both types of read views so users can choose which read view they want to use. The entries are comma-separated. If you want to limit the user's choice of read views, specify only one.

IMPORTANT: If you lock this field, the lock level must be set on a Domain or Post Office, not on users or external entities.

Set Default

The defaultViewRead field allows you to specify which read view is the default read view the client uses. There are two read views available:

- ◆ **Plain Text:** Set the value to `Text` to allow users to read the items in plain text.
- ◆ **HTML:** Set the value to `HTML` to allow users to read the items in HTML.

For this field, you can specify only one value, unlike the allowableViewRead field. The default view must be specified in the defaultViewRead field.

Allowable Compose Views

The allowableViewCompose field allows you to determine what compose views you allow the clients to use. There are two compose views:

- ◆ **Plain Text:** Setting the value to `Text` allows users to compose items in plain text.
- ◆ **HTML:** Setting the value to `HTML` allows users to compose items in HTML.

You can specify both values so users can choose which view they want to use. The entries are comma-separated. If you want to limit the user's choice of compose views, specify only one.

IMPORTANT: If you lock this field, the lock level must be set on a Domain or Post Office, not on users or external entities.

Set Default

The defaultViewCompose field allows you to specify which compose view is the default compose view the client uses. There are two compose views available:

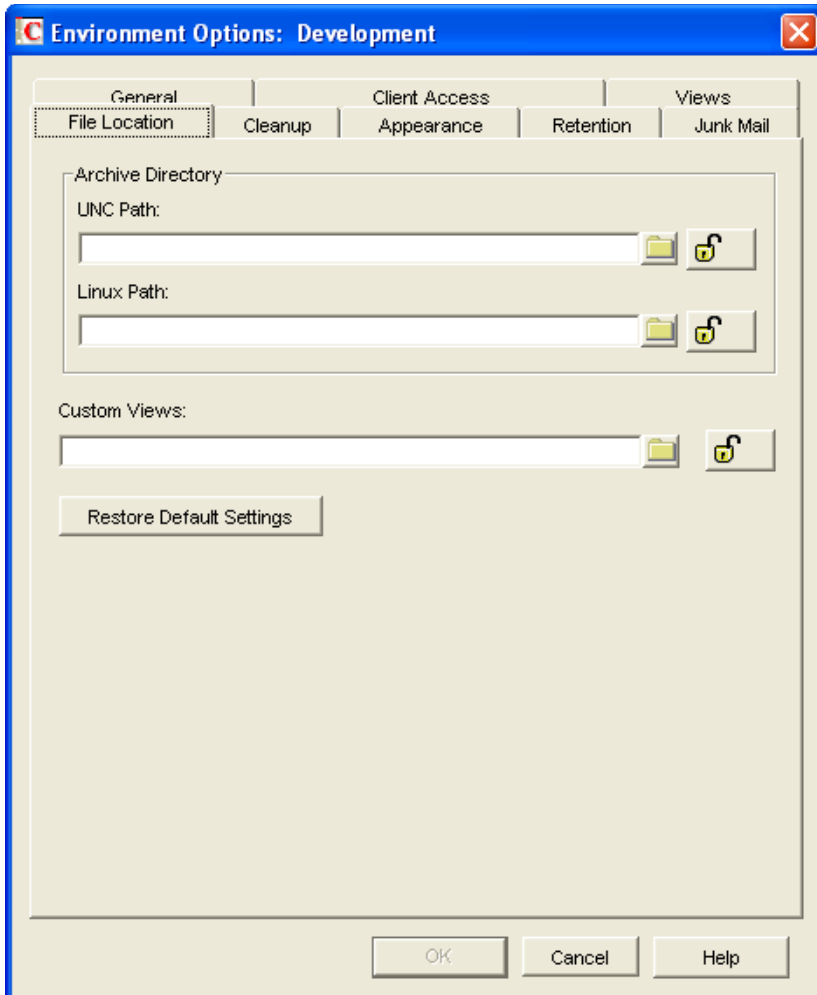
- ◆ **Plain Text:** Setting the value to `Text` allows users to compose items in plain text.
- ◆ **HTML:** Setting the value to `HTML` allows users to compose items in HTML.

For this field, you can specify only one value, unlike the allowableViewCompose field. The default view must be specified in the defaultViewCompose field.

6.4.6 Environment > File Location > Archive Directory

The archive directory settings are found in ConsoleOne through the GroupWise client options under *Environment > File Location > Archive Directory*. *Archive Directory* sets the directory to be used for archiving items.

Figure 6-10 Environment Options Dialog Box with the File Location Tab Open



Each user must have his or her own archive directory. It can be a local directory (for example, `c:\novell\groupwise`) or a personal user directory on a network server. If you set a local drive, make sure the users have the directories created. If you select a network drive, make sure users have the necessary rights to access the directories.

The `LocationsSetting` attribute stores this information.

```

<attr attr-name="LocationsSettings">
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">c:\grpwise</component>
    <component name="field">archiveLocation</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value"></component>
    <component name="field">archiveLocationLinux</component>
  </value>
</attr>

```

Archive Directory UNC Path

The archiveLocation field is the UNC Path or Windows local path of the personal directory where archived messages are stored for Windows clients.

Archive Directory Linux Path

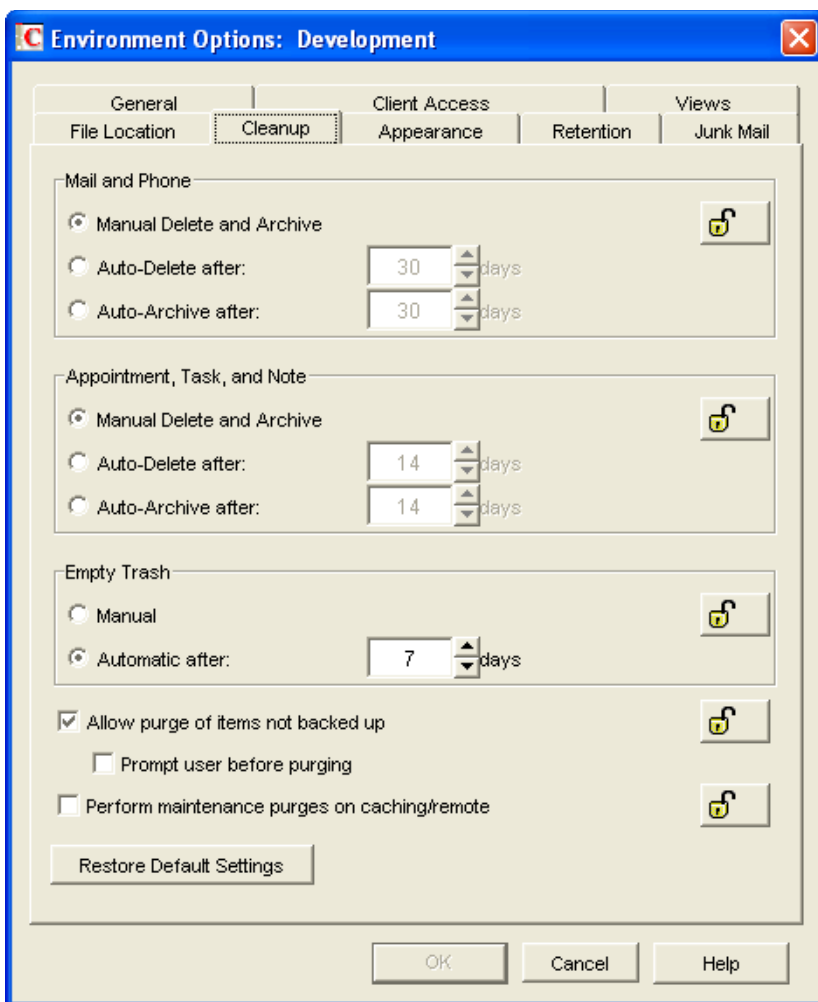
The archiveLocationLinux field is the Linux path of a local or personal directory where archived messages are stored for Linux/Mac clients.

Include the field type for the user workstations. If it's for a Windows workstation, use the *UNC Path* option. If it's for a Linux or Mac workstation, use the *Linux Path* option.

6.4.7 Environment > Cleanup

The *Cleanup* options determine the delete and archive settings for GroupWise items. These options help control the disk space usage for the users, along with the *Disk Space Management* options. The cleanup settings are found in ConsoleOne through the GroupWise client options under *Environment > Cleanup*.

Figure 6-11 Environment Options Dialog Box with the Cleanup Tab Open



The DiscardSettings attribute is used for the *Cleanup* options as well as the *Disk Space Management* options. For more information, see [Section 6.4.14, “Send > Disk Space Management,”](#) on page 103.

```
<attr attr-name="DiscardSettings">
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">ManualDeleteArchive</component>
    <component name="field">mailDelete</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">ManualDeleteArchive</component>
    <component name="field">appointmentDelete</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">AutoPurgeAfterTrashDays</component>
    <component name="field">trashPurge</component>
  </value>
</attr>
```

Mail and Phone

These options are not supported in this release of the driver.

Appointment, Task, and Note

These options are not supported in this release of the driver.

Empty Trash

The `trashPurge` field purges deleted items from the Trash folder. The items can be retrieved from the Trash until it is purged. Items in the Trash still take up disk space. Setting the following values for the `trashPurge` field determines how the Trash folder is emptied:

- ♦ **ManualPurge:** Setting the `ManualPurge` value requires the user to manually empty the Trash.
- ♦ **AutoPurgeAfterTrashDays:** Setting the `AutoPurgeAfterTrashDays` value allows GroupWise to automatically empty items from the trash after they have been in it for the specified number of days.

Days

If you use the `AutoPurgeAfterTrashDays` value in the `trashPurge` field, you must define a `trashDays` field to specify the number of days to wait to purge the items from the Trash. For example:

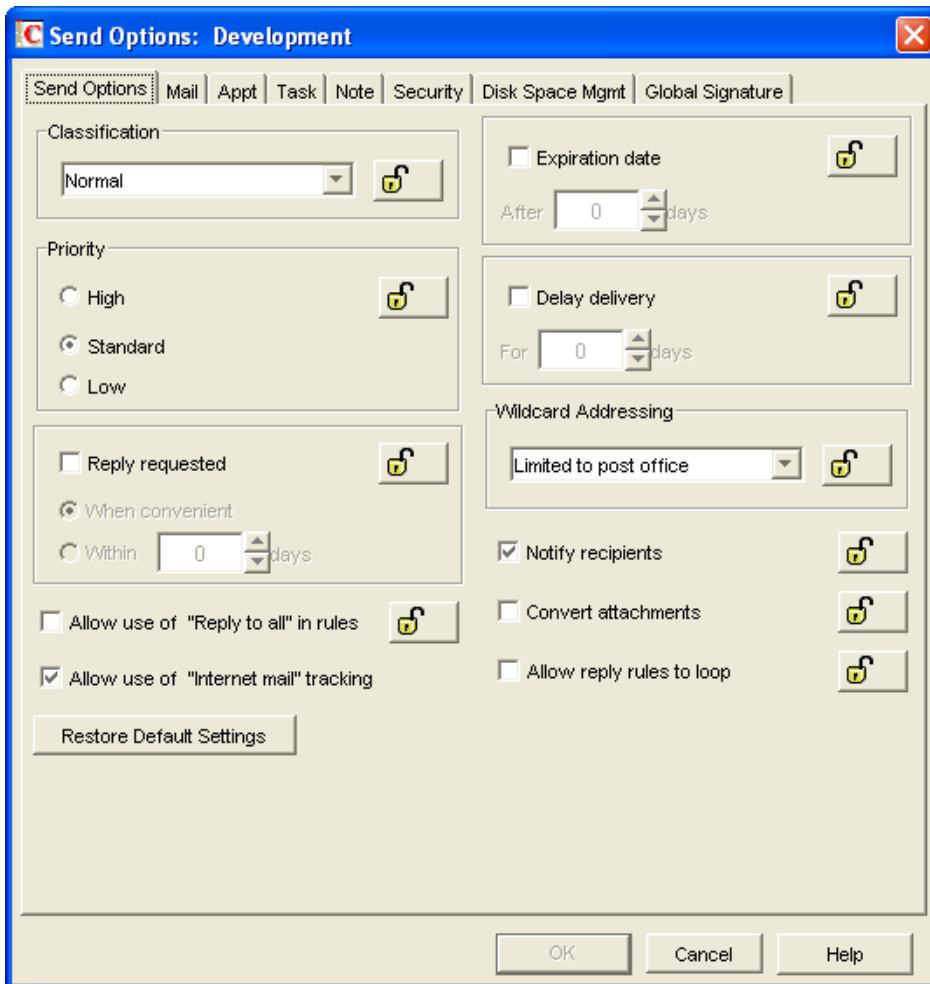
```
<attr attr-name="DiscardSettings">
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">AutoPurgeAfterTrashDays</component>
    <component name="field">trashPurge</component>
  </value>
  <value type="structured">
    <component name="value">7</component>
    <component name="field">trashDays</component>
  </value>
</attr>
```

The valid range for the `trashDays` field is 1-9999. If you set the lock level for the `trashPurge` field, it is inherited by the `trashDays` field.

6.4.8 Send > Send Options

The Send options determine general settings that apply to all GroupWise item types (mail messages, appointments, tasks, and notes). The Send options are accessed in ConsoleOne through the GroupWise client options under *Send > Send Options*.

Figure 6-12 Send Options Dialog Box with the Send Options Tab Open



There are two attributes that store this information: the `AdvancedSettings` attribute and the `MailMessageSettings` attribute. The `MailMessage` Attribute also stores information specific to mail message items. For more information, see [Section 6.4.9, “Send > Mail,” on page 89](#).

```
<attr attr-name="AdvancedSettings">
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">Normal</component>
    <component name="field">sendSecurity</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">-1</component>
    <component name="field">delayDelivery</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">itemConversions</component>
  </value>
  <value type="structured">
```

```

    <component name="lock-level">0</component>
    <component name="value">PostOffice</component>
    <component name="field">asteriskSendRestriction</component>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">allowRuleReplyMoreThanOnce</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">>true</component>
    <component name="field">internetStatusTracking</component>
  </value>
</attr>

```

Classification

The sendSecurity field allows you to set the default value for the security classification label at the top of the message box. The classifications do not provide any encryption or additional security. They are meant to alert the recipient to the relative sensitivity of the item. The values for sendSecurity field are:

- ◆ Proprietary
- ◆ Confidential
- ◆ Secret
- ◆ TopSecret
- ◆ ForYourEyesOnly
- ◆ Normal

Delay Delivery

The delayDelivery field allows you delay to the delivery of messages for the specified number of days. For example, if you specify 3 days, a message is not delivered until 3 days after the day it is sent. Messages are delivered at 12:01 a.m. of the appropriate day. To disable this option set the value to -1. To enable delayed delivery set the value from 0 to 999.

Convert Attachments

The itemConversions field allows you to convert attachments in items sent to non-GroupWise e-mail systems through a GroupWise gateway. To enable this option, set the value to 1. To disable this option, set the value to 0.

Wildcard Addressing

The asteriskSendRestriction field allows you to enable wildcard addressing. Wildcard addressing lets a user send an item to all users in a post office, domain, GroupWise system, or connected GroupWise system by inserting asterisks (*) as wildcards in e-mail addresses. There are five different values to set:

- ♦ **System:** Setting the value to `System` limits wildcard addressing to the user's GroupWise system. This means that a user can send an item to all users in the GroupWise system by entering `*.*.*` in the item's address field. A user can also send an item to all users in another domain by entering `*.domain_name` or to all users in another post office by entering `*.post_office_name`.
- ♦ **PostOffice:** Setting the value to `PostOffice` limits wildcard addressing to the user's post office. This means that a user can send an item to all users on the same post office by entering `*` in the item's address field.
- ♦ **Domain:** Setting the value to `Domain` limits wildcard addressing to the user's domain. This means that a user can send an item to all users in the domain by entering `*.*` in the item's address field. A user can also send an item to all users on another post office in the domain by entering `*.post_office_name` in the item's address field.
- ♦ **NoLimit:** Setting the value to `NoLimit` allows unlimited use of wildcard addressing. This means that a user can send an item to all users in another GroupWise system by entering `*.post_office_name.domain_name` or `*.domain_name` in the item's address field.
- ♦ **NotAllowed:** Setting the value to `NotAllowed` disables wildcard addressing.

Allow Reply Rules to Loop

By default, GroupWise does not allow a rule-generated reply to be replied to by another rule-generated reply. This situation, referred to as looping, can quickly increase message traffic. To allow reply rules to loop, set the value to 1 for the `allowRuleReplyMoreThanOnce` field. To disable this option, set the value to 0.

Allow Use of Internet

The `internetStatusTracking` field allows users' GroupWise clients to automatically embed information in Internet-bound items. The embedded information instructs the receiving system to send back a delivery notification message (if it is supported). To enable the option, set the value to `true`. To disable this option, set the value to `false`. If you set the value to `false`, the lock level is automatically set.

IMPORTANT: The lock level must not be set on this field. This means you should never set the value to `false`.

```
<attr attr-name="MailMessageSettings">
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">Standard</component>
    <component name="field">mailPriority</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">None</component>
    <component name="field">mailReplyRequested</component>
  </value>
</attr>
```



```

</value>
<value type="structured">
  <component name="lock-level">0</component>
  <component name="value">0</component>
  <component name="field">mailExpireDays</component>
</value>
<value type="structured">
  <component name="lock-level">0</component>
  <component name="value">1</component>
  <component name="field">notifyRecipient</component>
</value>
</attr>

```

Priority

The mailPriority field determines the default priority of the item. This, in turn, determines how quickly items are delivered. High priority items are queued ahead of normal or low priority items. There are three values you can specify in the mailPriority field:

- ◆ **High:** The `High` value queues an item ahead of normal and low priority items.
- ◆ **Standard:** The `Standard` value is the default value set for the delivery of an item.
- ◆ **Low:** The `Low` value places an item at the end of the queue.

Reply Requested

The mailReplyRequested field allows items to always include a reply request. By default, this option is disabled. You can specify three values for the mailReplyRequested field:

- ◆ **None:** The `None` value disables this option for all items.
- ◆ **When Convenient:** The `WhenConvenient` value requires a reply, but there is no time limit set.
- ◆ **Within:** The value is the number of days a recipient is given to reply. Specify the number of days in the value of the mailReplyRequested field. The value range is 0-253.

Expiration Date

The mailExpireDays field expires unopened messages after the specified number of days. If the value is set to 0, this option is disabled. If you want to enable this option, specify the number of days to wait before expiring unopened messages. The value range for this field is 1-999. If a message expires, it is deleted.

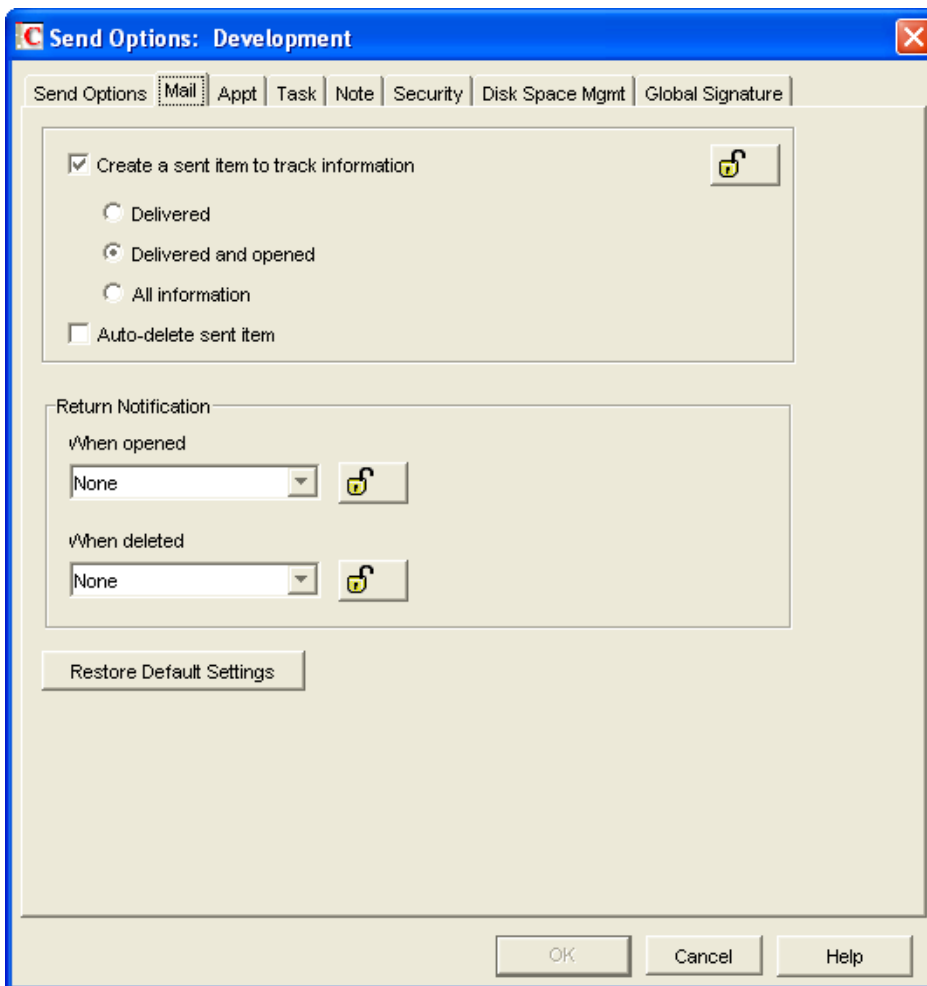
Notify Recipients

The notifyRecipient field notifies recipients when they receive an item, if they are using GroupWise Notify. To enable this option, set the value to 1. To disable this option, set the value to 0.

6.4.9 Send > Mail

The *Mail* options apply to mail messages only. The *Mail* options are found in ConsoleOne through the GroupWise client options under *Send > Mail*. However, enabling certain options in the *Mail* tab enables these same options on the *Appt*, *Task*, and *Note* tabs.

Figure 6-13 Send Options Dialog Box with the Mail Tab Open



There are two attributes that store this information: the `AdvancedSettings` attribute and the `MailMessageSettings` attribute.

```
<attr attr-name="AdvancedSettings">
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">1</component>
    <component name="field">outboxInsert</component>
  </value>
</attr>
```

Create a Sent Item to Track Information

The `outboxInsert` field allows you to insert items in the user's Sent Items folder when a user sends an item. Disable this option if you do not want the items placed there. If items are not placed in the Sent Items folder, users cannot check the delivery status of the item. To enable this option, set the value to 1. To disable this option, set the value to 0.

The lock level for the `outboxInsert` field affects mail, appointment, note, and task items.

Create a Sent Item to Track Information

If you have enabled the `outboxInsert` field, you must use the `MailMessageSettings` attribute to set the status value.

```
<attr attr-name="MailMessageSettings">
  <value type="structured">
    <component name="value">DeliveredAndOpened</component>
    <component name="field">mailStatusInfo</component>
  </value>
</attr>
```

There are three values you can use to track the status of the mail messages:

- ♦ **DeliveredAndOpened:** Setting the value to `DeliveredAndOpened` tracks the delivered and opened status only. The user can open the Properties window of the sent message to view the status.
- ♦ **Full:** Setting the value to `Full` tracks all status information (delivered, opened, deleted). The user can open the Properties window of the message to view the status.
- ♦ **Delivered:** Setting the value to `Delivered` tracks only the delivered status. The user can open the Properties window of the message to view the status.

```
<attr attr-name="MailMessageSettings">
  <value type="structured">
    <component name="value">0</component>
    <component name="field">mailAutoDelete</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">mailReturnOpen</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">mailReturnDelete</component>
  </value>
</attr>
```

Auto-Delete Sent Item

The `mailAutoDelete` field automatically deletes messages from the user's Mailbox after all the recipients have deleted the messages and emptied them from the Trash. To enable this option, set the value to 1. To disable this option, set the value to 0. The `mailAutoDelete` field inherits the lock level setting from the `outboxInsert` field.

Return Notification

In addition to status tracking information, the user can receive notification when a mail message is opened or deleted. Choose from the following notification options:

When Opened

The `mailReturnOpen` field allows users to be notified when a mail message is opened. There are four different notification options:

- ♦ **None:** Set the value to 0 for the user to not receive a notification when the mail message is opened.
- ♦ **Mail Receipt:** Set the value to 1 for the user to receive a mail message stating that the recipient opened the mail message.
- ♦ **Notify:** Set the value to 2 for the user to receive notification through GroupWise Notify when the recipient opens the mail message.
- ♦ **Notify and Mail:** Set the value to 3 for the user to receive notification through GroupWise Notify and a mail message when the recipient opens the mail message.

When Deleted

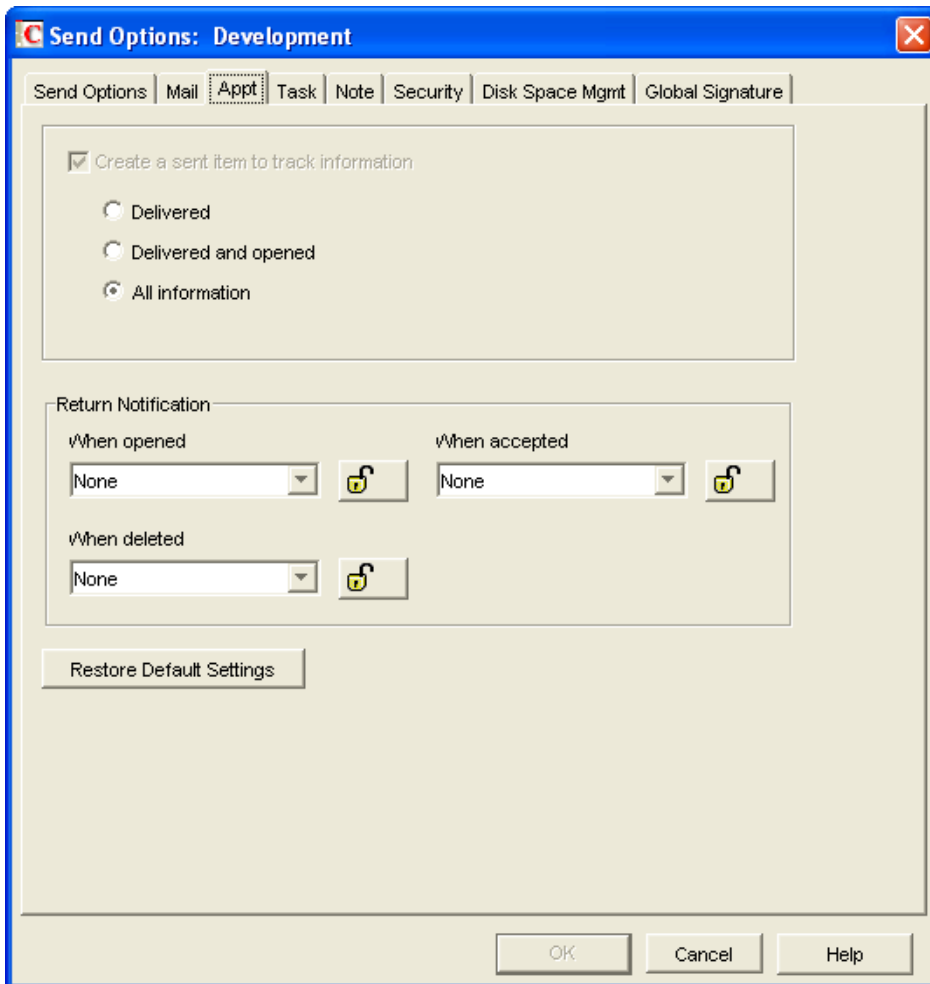
The `mailReturnDelete` field allows users to be notified when a mail message is deleted. There are four different notification options:

- ♦ **None:** Set the value to 0 for the user to not receive a notification when the mail message is deleted.
- ♦ **Mail Receipt:** Set the value to 1 for the user to receive a mail message stating that the recipient deleted the mail message.
- ♦ **Notify:** Set the value to 2 for the user to receive notification through GroupWise Notify when the recipient deletes the mail message.
- ♦ **Notify and Mail:** Set the value to 3 for the user to receive notification through GroupWise Notify and a mail message when the recipient deletes the mail message.

6.4.10 Send > Appt

The *Appt* option applies to appointment messages only. The appointment options are found in ConsoleOne through the GroupWise client options under *Send > Appt*.

Figure 6-14 Send Options Dialog Box with the Appt Tab Open



The AppointmentMessageSettings attribute stores this information.

```
<attr attr-name="AppointmentMessageSettings">
  <value type="structured">
    <component name="value">Full</component>
    <component name="field">appointmentStatusInfo</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">appointmentReturnOpen</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">appointmentReturnAccept</component>
  </value>
  <value type="structured">
```

```

    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">appointmentReturnDelete</component>
  </value>
</attr>

```

Create a Sent Item to Track Information

The `outboxInsert` field allows you to insert items in the user's Sent Items folder when a user sends an item. This option is set through the `AdvancedSettings` attribute. For more information, see [“Send > Mail” on page 89](#).

If you have enabled this option, you must use the `appointmentStatusInfo` field to set the desired status value. The lock level is inherited from the `outboxInsert` field. There are three values you can use to track the status of the appointments:

- ◆ **DeliveredAndOpened:** Setting the value to `DeliveredAndOpened` only tracks the delivered and opened status. The user can open the Properties window of the sent appointment to view the status.
- ◆ **Full:** Setting the value to `Full` tracks all status information (delivered, opened, deleted, emptied). The user can open the Properties window of the appointment to view the status.
- ◆ **Delivered:** Setting the value to `Delivered` tracks only the delivered status. The user can open the Properties window of the appointment to view the status.

Return Notification

In addition to status tracking information, the user can receive notification when an appointment is opened, accepted, or deleted. Choose from the following notification options:

When Opened

The `appointmentReturnOpen` field allows users to be notified when an appointment is opened. There are four different notification options:

- ◆ **None:** Set the value to 0 for the user to not receive a notification when the appointment is opened.
- ◆ **Mail Receipt:** Set the value to 1 for the user to receive a mail message stating that the recipient opened the appointment.
- ◆ **Notify:** Set the value to 2 for the user to receive notification through GroupWise Notify when the recipient opens the appointment.
- ◆ **Notify and Mail:** Set the value to 3 for the user to receive notification through GroupWise Notify and a mail message when the recipient opens the appointment.

When Deleted

The `appointmentReturnDelete` field allows users to be notified when an appointment is deleted. There are four different notification options:

- ◆ **None:** Set the value to 0 for the user to not receive a notification when the appointment is deleted.
- ◆ **Mail Receipt:** Set the value to 1 for the user to receive a mail message stating that the recipient deleted the appointment.

- ♦ **Notify:** Set the value to 2 for the user to receive notification through GroupWise Notify when the recipient deletes the appointment.
- ♦ **Notify and Mail:** Set the value to 3 for the user to receive notification through GroupWise Notify and a mail message when the recipient deletes the appointment.

When Accepted

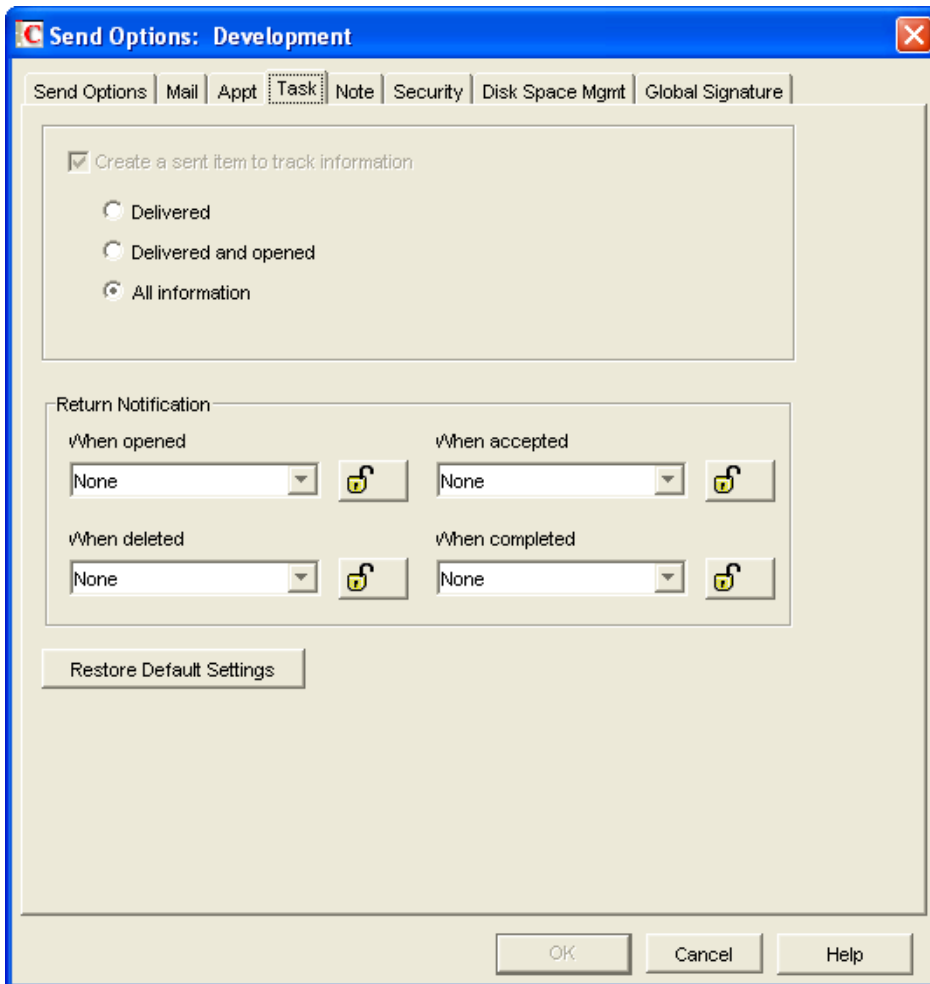
The `appointmentReturnAccept` field allows users to be notified when an appointment is accepted. There are four different notification options:

- ♦ **None:** Set the value to 0 for the user to not receive a notification when the appointment is accepted.
- ♦ **Mail Receipt:** Set the value to 1 for the user to receive a mail message stating that the recipient accepted the appointment.
- ♦ **Notify:** Set the value to 2 for the user to receive notification through GroupWise Notify when the recipient accepts the appointment.
- ♦ **Notify and Mail:** Set the value to 3 for the user to receive notification through GroupWise Notify and a mail message when the recipient accepts the appointment.

6.4.11 Send > Task

The *Task* option applies to task messages only. The *Task* options are found in ConsoleOne through the GroupWise client options under *Send > Task*.

Figure 6-15 Send Options Dialog Box with the Task Tab Open



The TaskMessageSettings attribute stores this information.

```
<attr attr-name="TaskMessageSettings">
  <value type="structured">
    <component name="value">Full</component>
    <component name="field">taskStatusInfo</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">taskReturnOpen</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">taskReturnAccept</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">taskReturnDelete</component>
  </value>
</attr>
```



```

    <value type="structured">
      <component name="lock-level">0</component>
      <component name="value">0</component>
      <component name="field">taskReturnCompleted</component>
    </value>
  </attr>

```

Create a Sent Item to Track Information

The `outboxInsert` field allows you to insert items in the user's Sent Items folder when a user sends an item. This option is set through the `AdvancedSettings` attribute. For more information, see [Section 6.4.9, "Send > Mail," on page 89](#).

If you have enabled this option, you must use the `taskStatusInfo` field to set the desired status value. The lock level is inherited from the `outboxInsert` field. There are three values you can use to track the status of the tasks:

- ◆ **DeliveredAndOpened:** Setting the value to `DeliveredAndOpened` tracks only the delivered and opened status. The user can open the Properties window of the sent task to view the status.
- ◆ **Full:** Setting the value to `Full` tracks all status information (delivered, opened, deleted, emptied). The user can open the Properties window of the task to view the status.
- ◆ **Delivered:** Setting the value to `Delivered` tracks only the delivered status. The user can open the Properties window of the task to view the status.

Return Notification

In addition to status tracking information, the user can receive notification when a task is opened, accepted, completed, or deleted. Choose from the following notification options:

When Opened

The `taskReturnOpen` field allows users to be notified when a task is opened. There are four different notification options:

- ◆ **None:** Set the value to 0 for the user to not receive a notification when the task is opened.
- ◆ **Mail Receipt:** Set the value to 1 for the user to receive a mail message stating that the recipient opened the task.
- ◆ **Notify:** Set the value to 2 for the user to receive notification through GroupWise Notify when the recipient opens the task.
- ◆ **Notify and Mail:** Set the value to 3 for the user to receive notification through GroupWise Notify and a mail message when the recipient opens the task.

When Deleted

The `taskReturnDelete` field allows users to be notified when a task is deleted. There are four different notification options:

- ◆ **None:** Set the value to 0 for the user to not receive a notification when the task is deleted.
- ◆ **Mail Receipt:** Set the value to 1 for the user to receive a mail message stating that the recipient deleted the task.
- ◆ **Notify:** Set the value to 2 for the user to receive notification through GroupWise Notify when the recipient deletes the task.

- ♦ **Notify and Mail:** Set the value to 3 for the user to receive notification through GroupWise Notify and a mail message when the recipient deletes the task.

When Accepted

The `taskReturnAccept` field allows users to be notified when a task is accepted. There are four different notification options:

- ♦ **None:** Set the value to 0 for the user to not receive a notification when the task is accepted.
- ♦ **Mail Receipt:** Set the value to 1 for the user to receive a mail message stating that the recipient accepted the task.
- ♦ **Notify:** Set the value to 2 for the user to receive notification through GroupWise Notify when the recipient accepted the task.
- ♦ **Notify and Mail:** Set the value to 3 for the user to receive notification through GroupWise Notify and a mail message when the recipient accepts the task.

When Completed

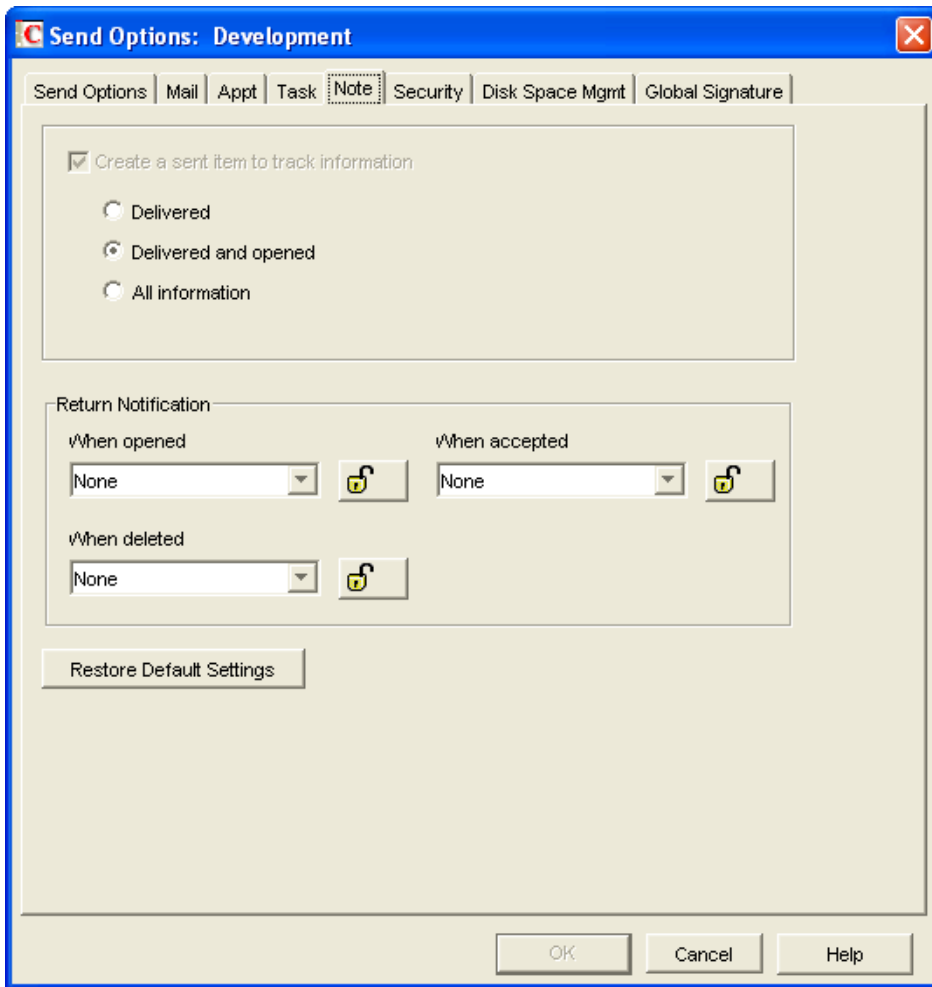
The `taskReturnCompleted` field allows users to be notified when a task is completed. There are four different notification options:

- ♦ **None:** Set the value to 0 for the user to not receive a notification when the task is completed.
- ♦ **Mail Receipt:** Set the value to 1 for the user to receive a mail message stating that the recipient completed the task.
- ♦ **Notify:** Set the value to 2 for the user to receive notification through GroupWise Notify when the recipient completed the task.
- ♦ **Notify and Mail:** Set the value to 3 for the user to receive notification through GroupWise Notify and a mail message when the recipient completes the task.

6.4.12 Send > Note

The *Note* option applies to note messages only. The *Note* options are found in ConsoleOne through the GroupWise client options under *Send > Note*.

Figure 6-16 Send Options Dialog Box with the Note Tab Open



The NoteMessageSettings attribute stores this information.

```
<attr attr-name="NoteMessageSettings">
  <value type="structured">
    <component name="value">DeliveredAndOpened</component>
    <component name="field">noteStatusInfo</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">noteReturnOpen</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">noteReturnDelete</component>
  </value>
  <value type="structured">
```

```
<component name="lock-level">0</component>
<component name="value">0</component>
<component name="field">noteReturnAccept</component>
</value>
</attr>
```

Create a Sent Item to Track Information

The `outboxInsert` field allows you to insert items in the user's Sent Items folder when a user sends an item. This option is set through the `AdvancedSettings` attribute. For more information, see [Section 6.4.9, "Send > Mail," on page 89](#).

If you have enabled this option, you must use the `noteStatusInfo` field to set the desired status value. The lock level is inherited from the `outboxInsert` field. There are three values you can use to track the status of the notes:

- ♦ **DeliveredAndOpened:** Setting the value to `DeliveredAndOpened` only tracks the delivered and opened status. The user can open the Properties window of the sent note to view the status.
- ♦ **Full:** Setting the value to `Full` tracks all status information (delivered, opened, deleted, emptied). The user can open the Properties window of the note to view the status.
- ♦ **Delivered:** Setting the value to `Delivered` tracks only the delivered status. The user can open the Properties window of the note to view the status.

Return Notification

In addition to status tracking information, the user can receive notification when a note is opened, accepted, or deleted. Choose from the following notification options:

When Opened

The `noteReturnOpen` field allows users to be notified when a note is opened. There are four different notification options:

- ♦ **None:** Set the value to 0 for the user to not receive a notification when the note is opened.
- ♦ **Mail Receipt:** Set the value to 1 for the user to receive a mail message stating that the recipient opened the note.
- ♦ **Notify:** Set the value to 2 for the user to receive notification through GroupWise Notify when the recipient opens the note.
- ♦ **Notify and Mail:** Set the value to 3 for the user to receive notification through GroupWise Notify and a mail message when the recipient opens the note.

When Deleted

The `noteReturnDelete` field allows users to be notified when a note is deleted. There are four different notification options:

- ♦ **None:** Set the value to 0 for the user to not receive a notification when the note is deleted.
- ♦ **Mail Receipt:** Set the value to 1 for the user to receive a mail message stating that the recipient deleted the note.
- ♦ **Notify:** Set the value to 2 for the user to receive notification through GroupWise Notify when the recipient deletes the note.

- ♦ **Notify and Mail:** Set the value to 3 for the user to receive notification through GroupWise Notify and a mail message when the recipient deletes the note.

When Accepted

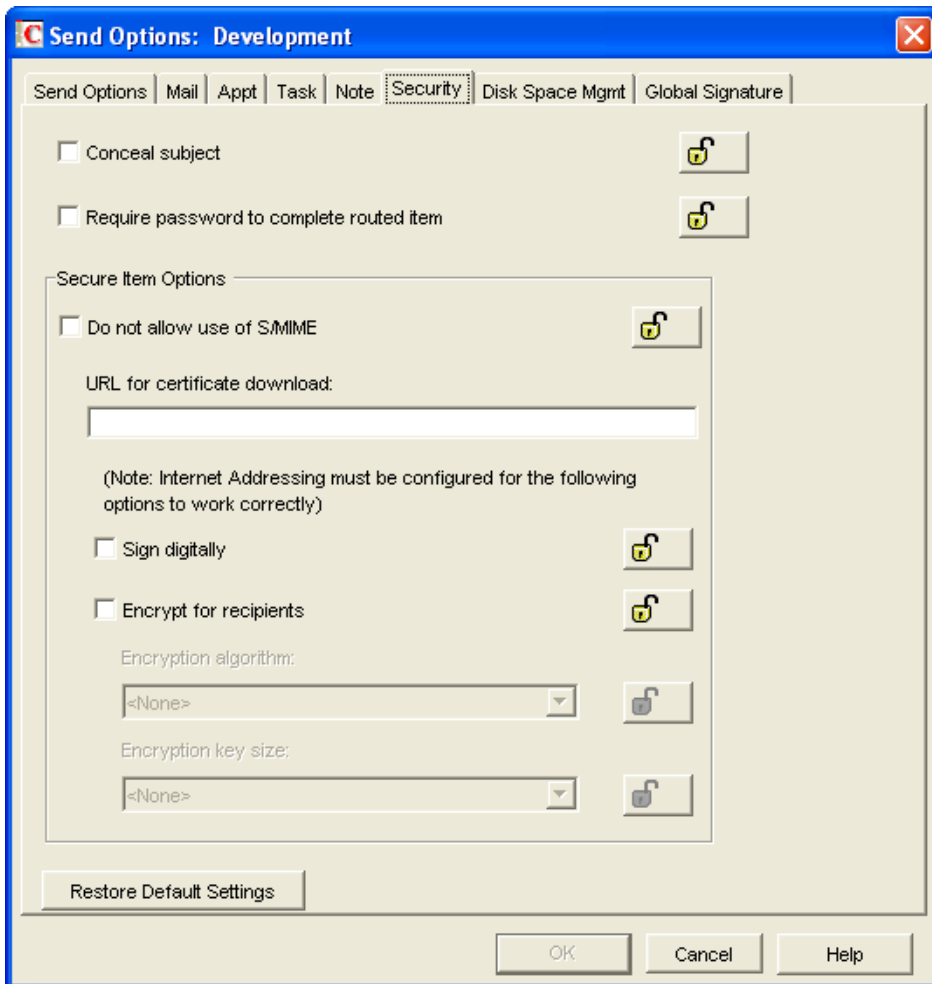
The `noteReturnAccept` field allows users to be notified when a note is accepted. There are four different notification options:

- ♦ **None:** Set the value to 0 for the user to not receive a notification when the note is accepted.
- ♦ **Mail Receipt:** Set the value to 1 for the user to receive a mail message stating that the recipient accepted the note.
- ♦ **Notify:** Set the value to 2 for the user to receive notification through GroupWise Notify when the recipient accepted the note.
- ♦ **Notify and Mail:** Set the value to 3 for the user to receive notification through GroupWise Notify and a mail message when the recipient accepts the note.

6.4.13 Send > Security

The security settings are found in ConsoleOne through the GroupWise client options under *Send > Security*. Security options apply to all GroupWise items types (mail messages, appointments, tasks, and notes).

Figure 6-17 Send Options Dialog Box with the Security Tab Open



```

<attr attr-name="AdvancedSettings">
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">disallowSMIME</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">encryptMessages</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">concealedSubject</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">routePasswordRequired</component>
  </value>
</attr>

```

Conceal Subject

The `concealedSubject` field allows you to conceal the item's subject so the notification that appears on the recipient's screen does not include the subject. The subject of the item is also concealed in the recipient's mailbox and the sender's Sent Items folder. It is visible only when the item is being read. To disable this option, set the value to 0. To enable this option, set the value to 1.

Require Password to Complete Routed Item

The `routePasswordRequired` field allows you to require a user to enter a password before completing a routed item. To disable this option, set the value to 0. To enable this option, set the value to 1.

Secure Item Options

If the users have installed security providers on their workstations, you can set the options you want the users to use.

Do Not Allow Use of S/MIME

Setting the `disallowSMIME` field disables S/MIME functionality. This disables the Encrypt and Digitally Sign buttons (and other related S/MIME functionality) in the GroupWise client. To allow the use of S/MIME, set the value to 0. To disallow the use of S/MIME, set the value to 1.

IMPORTANT: If you lock this field, the lock level must be set on a Domain or Post Office, not on users or external entities.

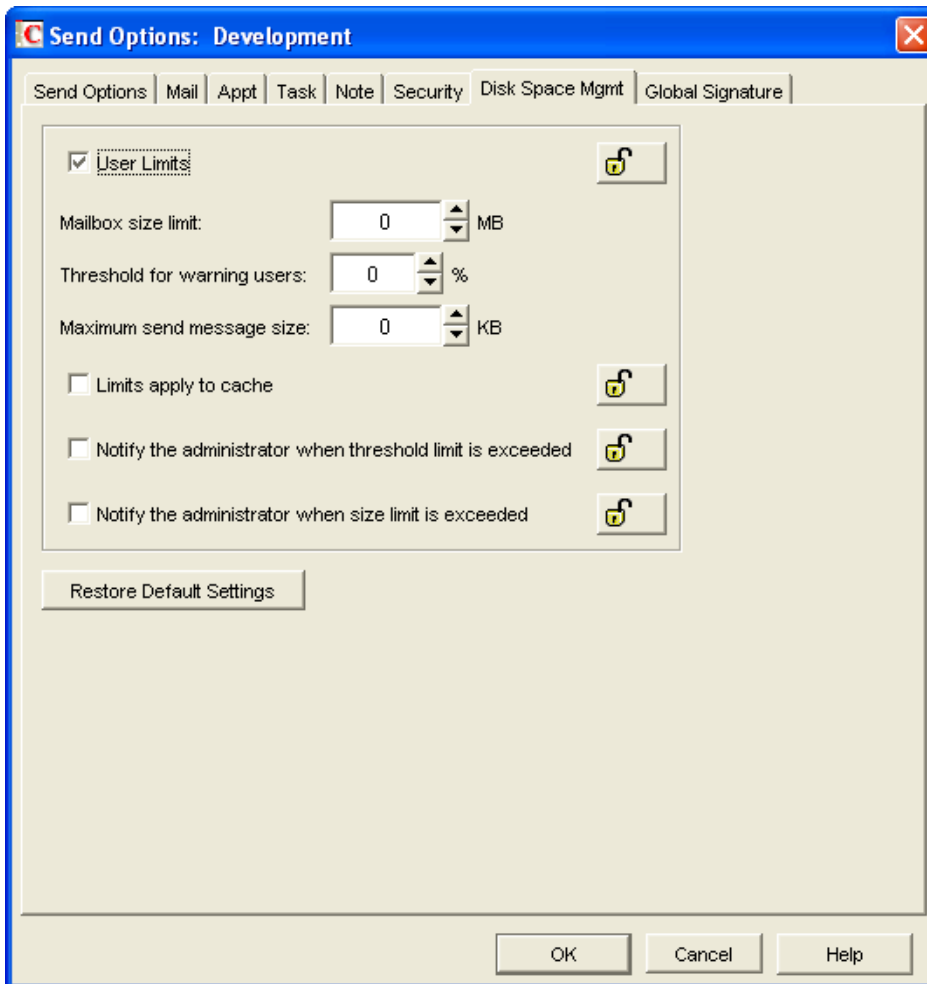
Encrypt for Recipients

The `encryptMessages` field allows you to enable users to encrypt an outgoing item so they can ensure that the intended recipients who have an S/MIME-enabled e-mail product are the only individuals who can read the item. This setting is not a useful security measure unless you lock it as the default. To disable this option, set the value to 0. To enable this option, set the value to 1.

6.4.14 Send > Disk Space Management

The disk space management settings are found in ConsoleOne through the GroupWise client options under *Send > Disk Space Management*. *Disk Space Management* enforces disk space limitations for users on a post office. There are multiple settings for customizing how the disk space is limited for the user.

Figure 6-18 Send Options Dialog Box with the Disk Space Mgmt Tab Open



You can also use the *Cleanup* options to help control the use of disk space by users. The *Disk Space Management* options and the *Cleanup* options use the DiscardSettings attribute. For more information, see [Section 6.4.7, “Environment > Cleanup,” on page 83](#).

```
<attr attr-name="DiscardSettings">
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">userLimitSet</component>
  </value>
  <value type="structured">
    <component name="value">0</component>
    <component name="field">boxSizeLimit</component>
  </value>
  <value type="structured">
    <component name="value">0</component>
    <component name="field">boxThresholdLimit</component>
  </value>
  <value type="structured">
    <component name="value">0</component>
    <component name="field">messageSendLimit</component>
  </value>
</attr>
```



```

</value>
<value type="structured">
  <component name="lock-level">0</component>
  <component name="value">0</component>
  <component name="field">boxLimitAppliesToCache</component>
</value>
<value type="structured">
  <component name="lock-level">0</component>
  <component name="value">0</component>
  <component name="field">enableBoxThresholdNotifickaion</component>
</value>
<value type="structured">
  <component name="lock-level">0</component>
  <component name="value">0</component>
  <component name="field">enableBoxSizeNotifickaion</component>
</value>
</attr>

```

User Limits

The `userLimitSet` field disables or enables the other *Disk Space Management* settings. By default, this option is disabled. To disable this option, set the value to 0. To enable this option, set the value to 1.

If you enable it, you can modify the following options; otherwise, they are ignored. If you set the lock level on the `userLimitSet` field, the lock level is inherited by the `boxSizeLimit`, `boxThresholdLimit`, and `messageSendLimit` fields.

IMPORTANT: If you lock this field, the lock level must be set on a Domain or Post Office, not on users or external entities.

Mailbox Size Limit

The `boxSizeLimit` field controls the maximum logical amount of disk space available to users for storing messages and attachment files. The setting uses logical disk space because attachment storage space is shared by all users on the same post office. Messages in shared folders are counted as disk space only for the owner of the shared folder.

The `boxSizeLimit` field is set in bytes. If the value is set to 0, there is no limit on the box size. If you want to set the limit to 10 MB, enter 10485760. The maximum value is 4 GB (4,294,967,295).

Threshold for Warning Users

The `boxThresholdLimit` field sets a percentage value of the user's mailbox size (specified in the Mailbox Size Limit). When this value is reached, GroupWise triggers a warning to users that the space in their mailboxes is reaching its limit. If users continue to send messages until the limit is met, they are not able to send more until they delete or archive items. The `userLimitSet` field must be set to 1 for this to function.

The `boxThresholdLimit` field is set as a percentage. Set the value to 0 or 100 if you do not want GroupWise to send a warning.

Maximum Send Message Size

The `messageSendLimit` field specifies the maximum size of a message that a user can send. If the user sends an item that exceeds this size, a message notifies the user that the item is too large to send.

The `messageSendLimit` field is set in bytes. If the value is set to 0, there is no limit on the message size. If you want to set the limit to 10 KB, enter 10240. The maximum value is 4 GB (4,294,967,295).

Limits Apply to Cache

The `boxLimitAppliesToCache` field uses the same disk space limits for users' Caching mailboxes on local workstations as you are using for their Online mailboxes in the post office. If you impose this limit on users who have existing Caching mailboxes, their Caching mailboxes might be reduced in size in order to meet the new disk space limit. Such users should be warned in advance so that they can back up their Caching mailboxes before the size reduction takes place. Otherwise, users could lose messages that they want to keep.

The `boxLimitAppliesToCache` field is set to 0 or 1. 0 is No and 1 is Yes.

IMPORTANT: If you lock this field, the lock level must be set on a Domain or Post Office, not on users or external entities.

Notify the Administrator When Threshold Limit is Exceeded

The `enableBoxThresholdNotification` field notifies both the administrator and the user when the user's mailbox exceeds the size established in the Threshold for Warning Users field. The administrator who receives the notification must be defined on the Identification page of the Domain object in ConsoleOne. The administrator cannot be set through the driver.

The `enableBoxThresholdNotification` field is set to 0 or 1. 0 is No and 1 is Yes.

IMPORTANT: If you lock this field, the lock level must be set on a Domain or Post Office, not on users or external entities.

Notify the Administrator When Size Limit is Exceeded

The `enableBoxSizeNotification` field notifies the administrator when the user's mailbox exceeds the size established in the Mailbox Size Limit field. The administrator who receives the notification must be defined on the Identification page of the Domain object in ConsoleOne. The administrator cannot be defined through the driver.

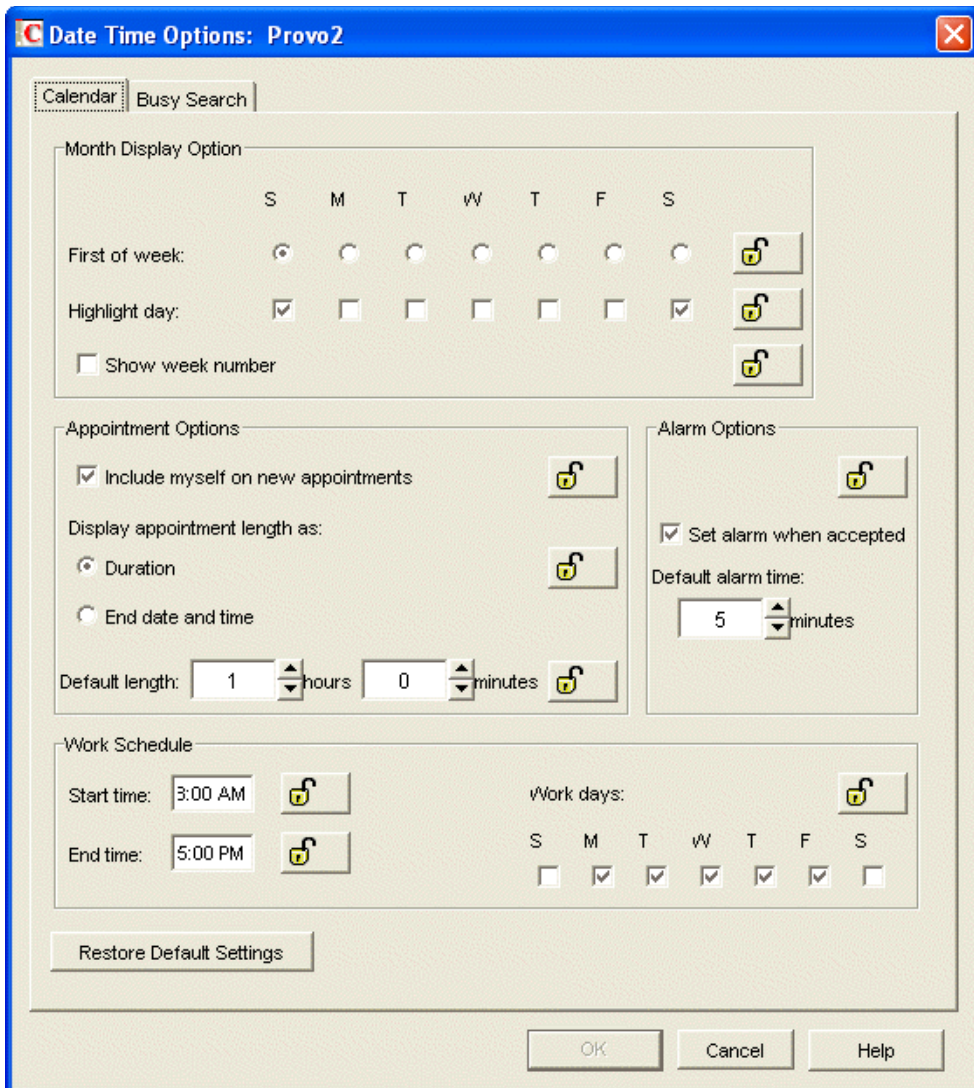
The `enableBoxSizeNotification` field is set to 0 or 1. 0 is No and 1 is Yes.

IMPORTANT: If you lock this field, the lock level must be set on a Domain or Post Office, not on users or external entities.

6.4.15 Date and Time > Calendar

The *Calendar* options determine basic settings for the GroupWise Calendar. The *Calendar* options are found in ConsoleOne through the GroupWise client options under *Date and Time > Calendar*.

Figure 6-19 Date and Time Options with the Calendar Tab Open



The CalendarViewSettings attribute stores this information.

```
<attr attr-name="CalendarViewSettings">
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">Sunday</component>
    <component name="field">firstDay</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">Sunday, Saturday</component>
    <component name="field">hilightDaysOfWeek</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">showWeekNumber</component>
  </value>
</attr>
```

```

<value type="structured">
  <component name="lock-level">0</component>
  <component name="value">1</component>
  <component name="field">appointmentIncludeSelf</component>
</value>
<value type="structured">
  <component name="lock-level">0</component>
  <component name="value">08:00</component>
  <component name="field">startOfWorkday</component>
</value>
<value type="structured">
  <component name="lock-level">0</component>
  <component name="value">17:00</component>
  <component name="field">endOfWorkday</component>
</value>
<value type="structured">
  <component name="lock-level">0</component>
  <component name="value">Monday, Tuesday, Wednesday, Thursday,
Friday</component>
  <component name="field">workdays</component>
</value>
</attr>

```

Month Display Option > First of Week

The firstDay field stores the day of the week that you want to display as the first day on the calendar. Specify the day in the value field. The options are the days of the week, with the first letter of the day capitalized. The value field can store only one day.

Month Display Option > Highlight Day

The highlightDaysOfWeek field stores any days you want highlighted, such as weekends and holidays. Specify the day or days in the value field. It can store more than one day. If you list more than one day, separate the days with a comma. For example: Saturday, Sunday.

Month Display Option > Show Week Number

The showWeekNumber field displays the week number (1 through 52) at the beginning of the calendar week. To disable this option, set the value to 0. To enable this option, set the value to 1.

Appointment Options > Include Myself on New Appointments

The appointmentIncludeSelf field allows the sender to be automatically included in the appointment's To: list. To disable this option, set the value to 0. To enable this option, set the value to 1.

Appointment Options > Default Length

The appointmentDefaultLength field is part of the AppointmentMessageSettings attribute. It sets the default length of the appointments. The value in the example below is for one hour. To set the value for 45 minutes, specify 00:45. The value for the field is HH:MM, where HH is hours and the range is 0-60. MM is minutes and the range is 0-59.

```

<attr attr-name="AppointmentMessageSettings">
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">01:00</component>
    <component name="field">appointmentDefaultLength</component>
  </value>
</attr>

```

Work Schedule > Start Time

The `startOfWorkday` field allows you to specify the time that displays as the daily start time of the user's work day. The value is specified using the 24-hour clock. For example, 8:00. The value for the field is HH:MM, where HH is hours and the range is 0-23. MM is minutes and the range is 0-59.

Work Schedule > End Time

The `endOfWorkday` field allows you to specify the time that displays as the daily end time of the user's work day. The value is specified using the 24-hour clock. For example, 17:00. The value for the field is HH:MM, where HH is hours and the range is 0-23. MM is minutes and the range is 0-59.

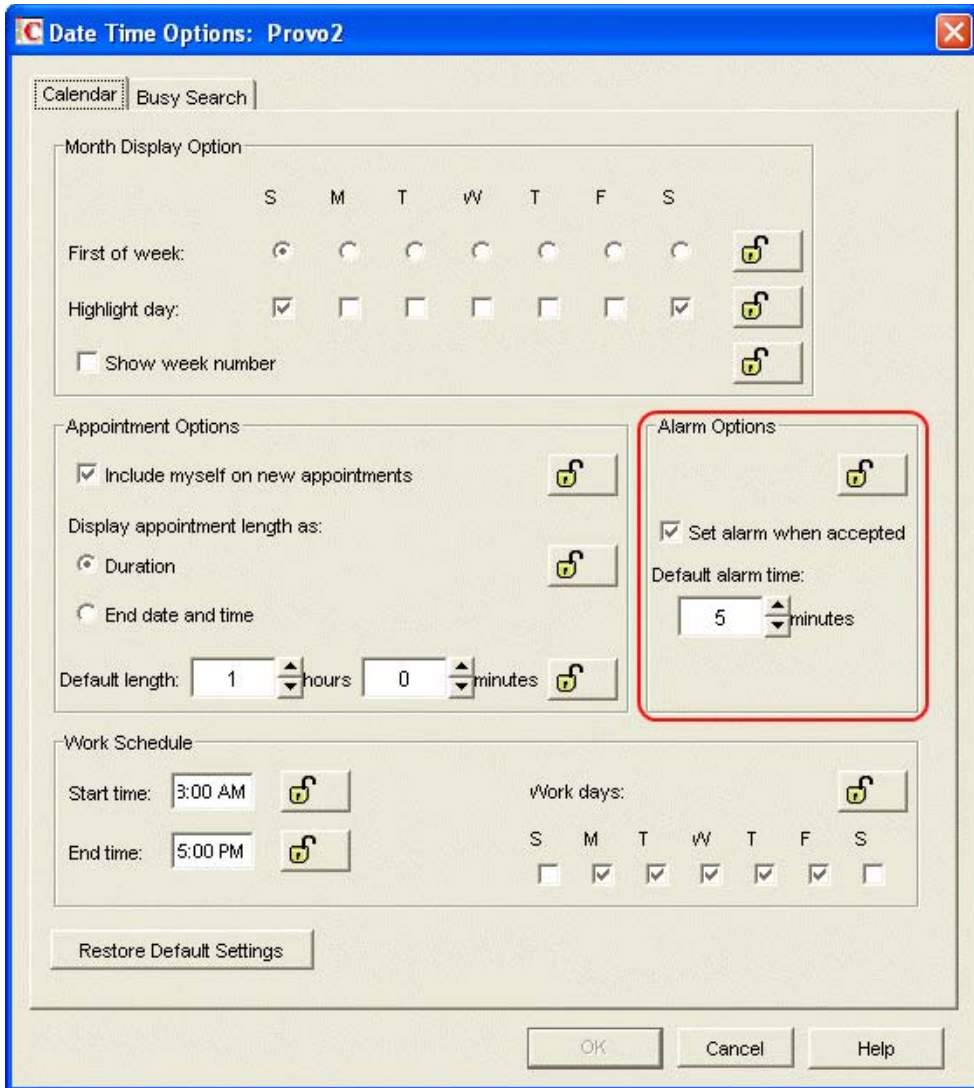
Work Schedule > Work Days

The `workdays` field applies the start time and end time to each work day. Specify the desired work days in the value field. For example, Monday, Tuesday, Wednesday, Thursday, Friday. The value is the days of the week in English, separated by a comma.

6.4.16 Date and Time > Calendar > Alarm Options

The *Alarm Options* allow you to set how a user is notified prior to an appointment time. The options are found in ConsoleOne through the GroupWise client options under *Date and Time > Calendar > Alarm Options*.

Figure 6-20 Date and Time Options with the Alarm Options Highlighted



The AppointmentViewSettings attribute stores the *Alarm Options* information.

```
<attr attr-name="AppointmentViewSettings">
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">1</component>
    <component name="field">appointmentAlarmSet</component>
  </value>
  <value type="structured">
    <component name="value">5</component>
    <component name="field">appointmentAlarmMinutes</component>
  </value>
</attr>
```

Set Alarm When Accepted

The `appointmentAlarmSet` field sets an alarm when the user accepts an appointment. By default, this option is enabled. To enable the option, the value field is set to 1. To disable this options, set the value field to 0.

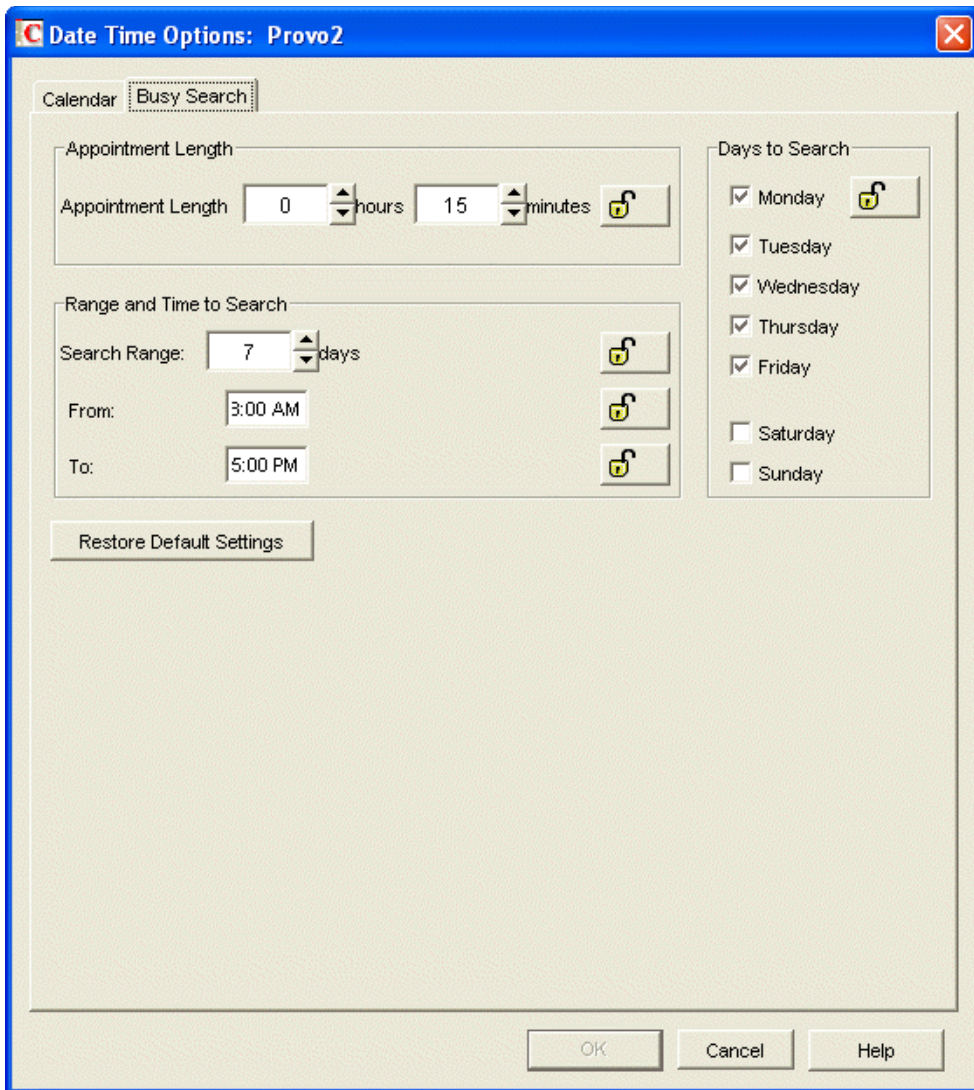
Default Alarm Time

The `appointmentAlarmMinutes` field sets the number of minutes before an appointment to notify the user. The default is 5 minutes. The valid range is 0-999. The `appointmentAlarmMinutes` field inherits the lock level from the `appointmentAlarmSet` field.

6.4.17 Date and Time > Busy Search

The *Busy Search* options determine the amount of free time required for the appointment and the range of dates to search. The *Busy Search* options are found in ConsoleOne through the GroupWise client options under *Date and Time > Busy Search*.

Figure 6-21 Date and Time Options with the Busy Search Tab Open



The BusySettings attribute stores this information.

```
<attr attr-name="BusySettings">
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">08:00</component>
    <component name="field">busyStartTime</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">17:00</component>
    <component name="field">busyEndTime</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">15</component>
    <component name="field">busyInterval</component>
  </value>
</attr>
```



```

    <value type="structured">
      <component name="lock-level">0</component>
      <component name="value">Monday, Tuesday, Wednesday, Thursday, Friday</
component>
      <component name="field">busyDays</component>
    </value>
    <value type="structured">
      <component name="lock-level">0</component>
      <component name="value">7</component>
      <component name="field">busySearchRange</component>
    </value>
  </attr>

```

Range and Time to Search > From

The `busyStartTime` field stores the time when you want to start the busy search. The value is specified by using the 24-hour clock. For example, 8:00. The value for the field is HH:MM, where HH is hours and the range is 0-23. MM is minutes and the range is 0-59.

Range and Time to Search > To

The `busyEndTime` field stores the time when you want to end the busy search. The value is specified by using the 24-hour clock. For example, 17:00. The value for the field is HH:MM, where HH is hours and the range is 0-23. MM is minutes and the range is 0-59.

Range and Time to Each > Search Range

The `busySearchRange` field stores the number of days it searches. The value is set as a number of days. For example, if you want to do a busy search for 7 days, specify 7. The range is 7-99 days.

Appointment Length

The `busyInterval` field sets the default appointment length to search. The value for the field is HH:MM, where HH is hours and the range is 0-8. MM is minutes and the range is 0-55.

This setting is used only when the user does a busy search through the Busy Search option on the Tools menu. Otherwise, the default appointment length defined on the Calendar tab is used (see [Section 6.4.15, "Date and Time > Calendar," on page 106](#)).

Days to Search

The `busyDays` field sets the days to search. You usually specify the work days for your organization. For example, Monday, Tuesday, Wednesday, Thursday, Friday. The value is the days of the week in English, separated by a comma.

6.5 Client Options Quick Reference

The following sections contain a summary of all of the GroupWise Client options that are currently enabled for the driver.

- ◆ [Section 6.5.1, "Environment," on page 114](#)
- ◆ [Section 6.5.2, "Send," on page 114](#)
- ◆ [Section 6.5.3, "Date and Time," on page 116](#)

6.5.1 Environment

The environment options allow you to change how a users interacts with the GroupWise client. These options control views, access, file location, appearance, junk mail settings, retention, and cleanup. [Table 6-1](#) shows the ConsoleOne option a with their corresponding XML field name.

Table 6-1 *GroupWise Client Options: Environment*

ConsoleOne Option	XML Field
<i>General > Check spelling before send</i>	<code>autoSpellCheck</code>
<i>General > Allow shared folder creation</i>	<code>allowSharedFolders</code>
<i>General > Allow shared address book creation</i>	<code>allowSharedAddressBooks</code>
<i>General > Allow use of POP and IMAP accounts in the Online Mailbox</i>	<code>allowPOP_IMAPAccounts</code>
<i>General > Allow use of news (NNTP) accounts in the Online Mailbox</i>	<code>allowNNTPAccounts</code>
<i>General > Show Messenger presence</i>	<code>showIMPresence</code>
<i>Client Access > Client Licensing</i>	<code>clientLicense</code>
<i>Views > Allowable Read Views</i>	<code>allowableViewRead</code>
<i>Views > Allowable Read Views > Set Default</i>	<code>defaultViewRead</code>
<i>Views > Allowable Compose Views</i>	<code>alloableViewCompose</code>
<i>Views > Allowable Compose Views > Set Default</i>	<code>defaultViewCompose</code>
<i>File Location > Archive Directory > UNC Path</i>	<code>archiveLocation</code>
<i>File Location > Archive Directory > Linux Path</i>	<code>archiveLocationLinux</code>
<i>Cleanup > Empty Trash</i>	<code>trashPurge</code>
<i>Cleanup > Empty Trash > days</i>	<code>trashDays</code>

6.5.2 Send

The send options allows you to change how users send mail, appointments, notes, and tasks. [Table 6-2](#) shows the ConsoleOne options with their corresponding XML field names.

Table 6-2 *GroupWise Client Options: Send*

ConsoleOne Option	XML Field
<i>Send Options > Classification</i>	<code>sendSecurity</code>
<i>Send Options > Delay delivery</i>	<code>delayDelivery</code>
<i>Send Options > Convert attachments</i>	<code>itemConversions</code>
<i>Send Options > Wildcard Addressing</i>	<code>asteriskSendRestriction</code>

ConsoleOne Option	XML Field
<i>Send Options > Allow reply rules to loop</i>	allowRuleReplyMoreThanOnce
<i>Send Options > Allow use of Internet mail tracking</i>	internetStatusTracking
<i>Send Options > Priority</i>	mailPriority
<i>Send Options > Reply requested</i>	mailReplyRequested
<i>Send Options > Expiration date</i>	mailExpireDays
<i>Send Options > Notify recipients</i>	notifyRecipient
<i>Mail > Create a sent item to track information</i>	outboxInsert
<i>Mail > Create a sent item to track information > option</i>	mailStatusInfo
<i>Mail > Auto-delete sent item</i>	mailAutoDelete
<i>Mail > Return Notification > When opened</i>	mailReturnOpen
<i>Mail > Return Notification > When deleted</i>	mailReturnDelete
<i>Appt > Create a sent item to track information options</i>	appointmentStatusInfo
<i>Appt > Return Notification > When opened</i>	appointmentReturnOpen
<i>Appt > Return Notification > When deleted</i>	appointmentReturnDelete
<i>Appt > Return Notification > When accepted</i>	appointmentReturnAccept
<i>Task > Create a sent item to track information options</i>	taskStatusInfo
<i>Task > Return Notification > When opened</i>	taskReturnOpen
<i>Task > Return Notification > When accepted</i>	taskReturnAccepted
<i>Task > Return Notification > When deleted</i>	taskReturnDelete
<i>Task > Return Notification > When completed</i>	taskReturnCompleted
<i>Note > Create a sent item to track information options</i>	noteStatusInfo
<i>Note > Return Notification > When opened</i>	noteReturnOpen
<i>Note > Return Notification > When deleted</i>	noteReturnDelete
<i>Note > Return Notification > When accepted</i>	noteReturnAccept
<i>Security > Conceal Subject</i>	concealedSubject
<i>Security > Require password to complete routed item</i>	routePasswordRequired
<i>Security > Secure Item Options > Do not allow use of S/MIME</i>	disallowSMIME
<i>Security > Secure Item Options > Encrypt for recipients</i>	encryptMessages

ConsoleOne Option	XML Field
Disk Space Mgmt > User Limits	userLimitSet
Disk Space Mgmt > Mailbox size limit	boxSizeLimit
Disk Space Mgmt > Threshold for warning users	boxThresholdLimit
Disk Space Mgmt > Maximum send message size	messageSendLimit
Disk Space Mgmt > Limit apply to cache	boxLimitAppliesToCache
Disk Space Mgmt > Notify the administrator when threshold limit is exceeded	enableBoxThresholdNotification
Disk Space Mgmt > Notify the administrator when size limit is exceeded	enableBoxSizeNotification

6.5.3 Date and Time

The Date and Time options allows you to control how the calendar is displayed, and how busy searches are conducted. [Table 6-3](#) shows the ConsoleOne options with their corresponding XML field names.

Table 6-3 GroupWise Client Option: Date and Time

ConsoleOne Option	XML Field
Calendar > Month Display Option > First of week	firstDay
Calendar > Month Display Option > Highlight day	hilightDaysOfWeek
Calendar > Month Display Option > Show week number	showWeekNumber
Calendar > Appointment Options > Include myself on new appointments	appointmentIncludeSelf
Calendar > Appointment Options > Default length	appointmentDefaultLength
Calendar > Work Schedule > Start time	startOfWorkday
Calendar > Work Schedule > End time	endOfWorkday
Calendar > Work Schedule > Work days	workdays
Calendar > Alarm Options > Set alarm when accepted	appointmentAlarmSet
Calendar > Alarm Options > Default alarm time	appointmentAlarmMinutes
Busy Search > Range and Time to Search > From	busyStartTime
Busy Search > Range and Time to Search > To	busyEndTime
Busy Search > Range and Time to Search > Search Range	busySearchRange
Busy Search > Appointment Length	busyInterval
Busy Search > Days to Search	busyDays

Managing the Driver

7

The driver can be managed through Designer, iManager, or the DirXML[®] Command Line utility.

- ♦ Section 7.1, “Using Anti-Virus Software on a GroupWise System,” on page 117
- ♦ Section 7.2, “Disabling the Driver,” on page 117
- ♦ Section 7.3, “Partition Issues,” on page 117
- ♦ Section 7.4, “Driver Access Rights and Membership,” on page 118
- ♦ Section 7.5, “Synchronizing Group Objects,” on page 118
- ♦ Section 7.6, “Synchronizing GroupWise Distribution List Objects,” on page 118
- ♦ Section 7.7, “Using the GroupWise Snap-Ins to Remove a GroupWise Account,” on page 118
- ♦ Section 7.8, “Re-associating a GroupWise Account with an eDirectory User,” on page 119
- ♦ Section 7.9, “User Renames,” on page 119
- ♦ Section 7.10, “Starting, Stopping, or Restarting the Driver,” on page 119
- ♦ Section 7.11, “Migrating and Resynchronizing Data,” on page 120
- ♦ Section 7.12, “Using the DirXML Command Line Utility,” on page 121
- ♦ Section 7.13, “Viewing Driver Versioning Information,” on page 121
- ♦ Section 7.14, “Reassociating a Driver Set Object with a Server Object,” on page 126
- ♦ Section 7.15, “Changing the Driver Configuration,” on page 126
- ♦ Section 7.16, “Storing Driver Passwords Securely with Named Passwords,” on page 126
- ♦ Section 7.17, “Adding a Driver Heartbeat,” on page 133

7.1 Using Anti-Virus Software on a GroupWise System

If you run server-based anti-virus software, you should configure it so that it does not scan the GroupWise directory structures such as domains and post offices. The anti-virus software causes file locking conflicts and can create problems for the GroupWise agents. If you need virus scanning on the GroupWise data, check the [GroupWise Partner Products page \(http://www.novell.com/partnerguides/section/468.html\)](http://www.novell.com/partnerguides/section/468.html).

7.2 Disabling the Driver

It is important not to disable the driver. When a driver is disabled, eDirectory events are not cached.

7.3 Partition Issues

- ♦ The driver can only access eDirectory objects in the partitions on the server where the driver is installed.
- ♦ Users, post offices, resources, and distribution lists must be in the same partition. Or, the partitions containing these objects must all have replicas on the server running the driver.

7.4 Driver Access Rights and Membership

The driver must have Read/Write access to users, post offices, resources, groups, distribution lists, and Create, Read, and Write rights to the post office container in eDirectory™. Normally, the driver should be given security equal to Admin.

If you are creating external post offices, the driver also needs read/write access to the domain.

7.5 Synchronizing Group Objects

If the option to synchronize groups (creating, deleting, renaming, or making membership changes) is enabled, the driver creates a distribution list in GroupWise when the user creates a group in eDirectory and then links the two together. If the group is renamed, the description modified, or users are added or removed to or from the group, the driver synchronizes the changes with the distribution list in GroupWise. This corresponds to similar functionality in the GroupWise snap-ins for ConsoleOne.

The default Placement policy adds the Distribution Lists to the post office specified when the driver is created. If you want the Distributions Lists to be added to a different post office, or various post offices depending on some criteria, you need to change the Placement policy. See [“Specifying Distribution Lists” on page 51](#) for more information.

By default, this occurs for all Groups created in eDirectory. You should add rules to the Create policy to limit what Groups (by containment or attribute value) are processed by the driver.

7.6 Synchronizing GroupWise Distribution List Objects

The driver synchronizes GroupWise distribution list objects. The Filter and the Schema Mapping policy include the GroupWise distribution list objects. The GroupWise distribution list is updated and maintain by the driver just like the Group objects. For more information see, [“Synchronize GroupWise Distribution Lists” on page 192](#) in the [Appendix C, “Properties of the Driver,” on page 185](#).

7.7 Using the GroupWise Snap-Ins to Remove a GroupWise Account

You can delete an eDirectory User and the corresponding GroupWise account with the GroupWise snap-ins. However, the recommended procedure is to remove the user from the authoritative data source and let the driver remove the account from GroupWise. The eDirectory user must have a valid Identity Manager association to the driver for this to work. The driver might log a warning or error if the account is deleted using the GroupWise snap-ins, because the object might have already been removed by the GroupWise snap-ins when the driver tries to delete it.

Use the steps in this section if it is necessary to use the GroupWise snap-ins to remove the GroupWise account.

- 1 Do one of the following:
 - ♦ If an Identity Manager association exists, change the state to Disabled.

When the user has an Identity Manager association to the driver with the state set to Disabled, and an attribute is changed in eDirectory, Identity Manager disregards the Modify request.

- ♦ If an Identity Manager association does not exist, manually create one, set the associated object ID to any value, then set the state to Disabled.

When the user does not have an Identity Manager association and an attribute is changed on the eDirectory user, the GroupWise account is re-created. When a user has an Identity Manager association to the driver with the state set to Disabled, and an attribute is changed in eDirectory, Identity Manager discards the modify request.

- 2 Delete the GroupWise account.
- 3 To re-create the GroupWise account, delete the association.
- 4 Change an eDirectory attribute on the user that the driver watches for modifications or resynchronization.

7.8 Re-associating a GroupWise Account with an eDirectory User

Administrators sometimes delete the value of the GroupWise ID attribute (disassociate it) from an eDirectory user and then re-associate (graft) it. This action resets the relationship between an eDirectory user and a GroupWise account. This action only involves the GroupWise snap-ins and does not involve the driver. Care should be taken when using this procedure. Changes made to the eDirectory user between the time the GroupWise ID is deleted and the user is re-associated are not synchronized to GroupWise. This is not a recommended procedure. Refer to the *GroupWise Administration Guide* (http://www.novell.com/documentation/gw7/pdfdoc/gw7_admin/gw7_admin.pdf) for known issues and precautions.

7.9 User Renames

Using the GroupWise snap-ins to rename users is not recommended. However, if the user is renamed using the GroupWise snap-ins, it must be done with GroupWise 6 Support Pack 1 or higher. Otherwise, the driver could generate errors. Rename the user object in the authoritative data source and let the driver rename the account in GroupWise.

7.10 Starting, Stopping, or Restarting the Driver

- ♦ [Section 7.10.1, “Starting the Driver in Designer,” on page 119](#)
- ♦ [Section 7.10.2, “Starting the Driver in iManager,” on page 120](#)
- ♦ [Section 7.10.3, “Stopping the Driver in Designer,” on page 120](#)
- ♦ [Section 7.10.4, “Stopping the Driver in iManager,” on page 120](#)
- ♦ [Section 7.10.5, “Restarting the Driver in Designer,” on page 120](#)
- ♦ [Section 7.10.6, “Restarting the Driver in iManager,” on page 120](#)

7.10.1 Starting the Driver in Designer

- 1 Open a project in the Modeler, then right-click the driver line.
- 2 Select *Live > Start Driver*.

7.10.2 Starting the Driver in iManager

- 1 In iManager, click *Identity Manager > Identity Manager Overview*.
- 2 Browse to the driver set where the driver exists, then click *Search*.
- 3 Click the upper right corner of the driver icon, then click *Start driver*.

7.10.3 Stopping the Driver in Designer

- 1 Open a project in the Modeler, then right-click the driver line.
- 2 Select *Live > Stop Driver*.

7.10.4 Stopping the Driver in iManager

- 1 In iManager, click *Identity Manager > Identity Manager Overview*.
- 2 Browse to the driver set where the driver exists, then click *Search*.
- 3 Click the upper right corner of the driver icon, then click *Stop driver*.

7.10.5 Restarting the Driver in Designer

- 1 Open a project in the Modeler, then right-click the driver line.
- 2 Select *Live > Restart Driver*.

7.10.6 Restarting the Driver in iManager

- 1 In iManager, click *Identity Manager > Identity Manager Overview*.
- 2 Browse to the driver set where the driver exists, then click *Search*.
- 3 Click the upper right corner of the driver icon, then click *Restart driver*.

7.11 Migrating and Resynchronizing Data

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

- ♦ **Migrate Data from Identity Vault:** Allows you to select containers or objects you want to migrate from the Identity Vault to an application. When you migrate an object, the Identity Manager engine applies all of the Matching, Placement, and Create policies, as well as the Subscriber filter, to the object.
- ♦ **Migrate Data into Identity Vault:** Assumes that the remote application can be queried for entries that match the criteria in the publisher filter.
- ♦ **Synchronize:** The Identity Manager 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, click *Identity Manager > Identity Manager Overview*.
- 2 Browse to and select the driver set where the driver exists, then click *Search*.

- 3 Click the driver icon, then click the *Migrate* tab.
- 4 Click the appropriate migration button.

For more information, see [Chapter 8, “Synchronizing Objects,”](#) on page 135.

7.12 Using the DirXML Command Line Utility

The DirXML Command Line utility provides command line access to manage the driver. This utility is not a replacement for iManager or Designer. The primary use of this utility is to allow you to create platform-specific scripts to manage the driver.

For example, you could create a shell script on Linux to check the status of the driver. See [Appendix B, “DirXML Command Line Utility,”](#) on page 171 for detailed information about the DirXML Command Line utility. For daily tasks, use iManager or Designer.

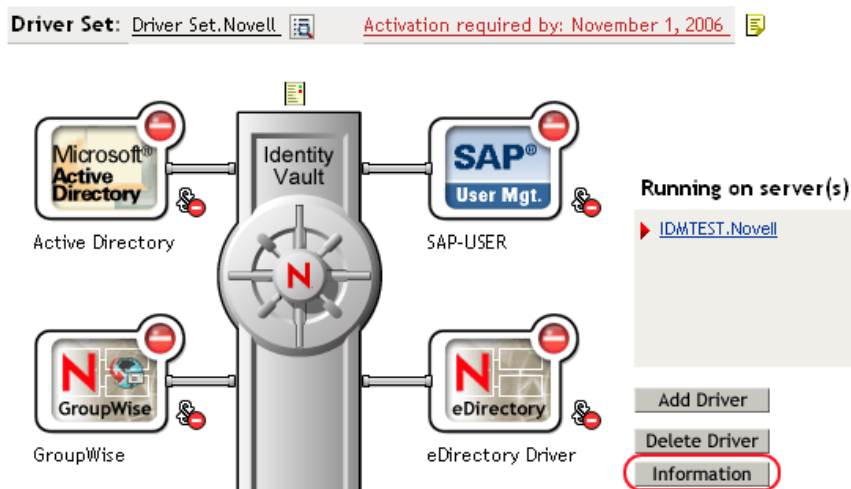
7.13 Viewing Driver Versioning Information

The Versioning Discovery tool only exists in iManager.

- ♦ [Section 7.13.1, “Viewing a Hierarchical Display of Versioning Information,”](#) on page 121
- ♦ [Section 7.13.2, “Viewing the Versioning Information as a Text File,”](#) on page 123
- ♦ [Section 7.13.3, “Saving Versioning Information,”](#) on page 125

7.13.1 Viewing a Hierarchical Display of Versioning Information

- 1 To find your Driver Set object in iManager, click *Identity Manager > Identity Manager Overview*, then click *Search*.
- 2 In the Identity Manager Overview, click *Information*.



You can also select *Identity Manager Utilities > Versions Discovery*, browse to and select the Driver Set object, then click *OK*.

- 3 View a top-level or unexpanded display of versioning information.

Versioning Discovery Tool ?

The Identity Manager Versioning Discovery Tool displays information obtained by scanning your tree for details concerning your Identity Manager configuration.

View

Save As...

Browse Driver Set and Drivers



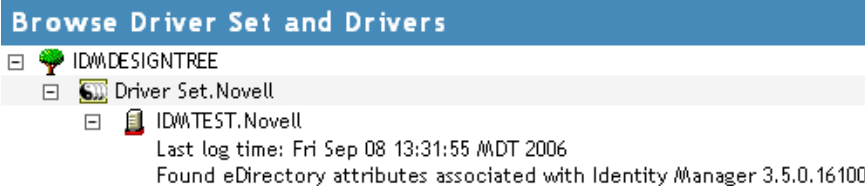
The unexpanded hierarchical view displays the following:

- ◆ The eDirectory™ tree that you are authenticated to
- ◆ The Driver Set object that you selected
- ◆ Servers that are associated with the Driver Set object

If the Driver Set object is associated with two or more servers, you can view Identity Manager information on each server.

- ◆ Drivers

4 View versioning information related to servers by expanding the server icon.



The expanded view of a top-level server icon displays the following:

- ◆ Last log time
- ◆ Version of Identity Manager that is running on the server

5 View versioning information related to drivers by expanding the driver icon.

Browse Driver Set and Drivers

- [-] IDMDESIGNTREE
 - [-] Driver Set.Novell
 - [-] IDWTEST.Novell
 - Last log time: Fri Sep 08 13:31:55 MDT 2006
 - Found eDirectory attributes associated with Identity Manager 3.5.0.16100
 - Active Directory
 - Driver
 - Driver 2
 - eDirectory Driver
 - Driver name: Identity Manager Driver for eDirectory
 - Driver module: com.novell.nds.dirxml.driver.nds.DriverShimImpl
 - [-] IDWTEST.Novell
 - Driver ID: EDIR
 - Driver version: 3.1.100.20061003

The expanded view of a top-level driver icon displays the following:

- ◆ The driver name
- ◆ The driver module (for example, com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver)

The expanded view of a server under a driver icon displays the following:

- ◆ The driver ID
- ◆ The version of the instance of the driver running on that server

7.13.2 Viewing the Versioning Information as a Text File

Identity Manager publishes versioning information to a file. You can view this information in text format. The textual representation is the same information contained in the hierarchical view.

- 1 To find your Driver Set object in iManager, click *Identity Manager > Identity Manager Overview*, then click *Search*.
- 2 In the Identity Manager Overview, click *Information*.

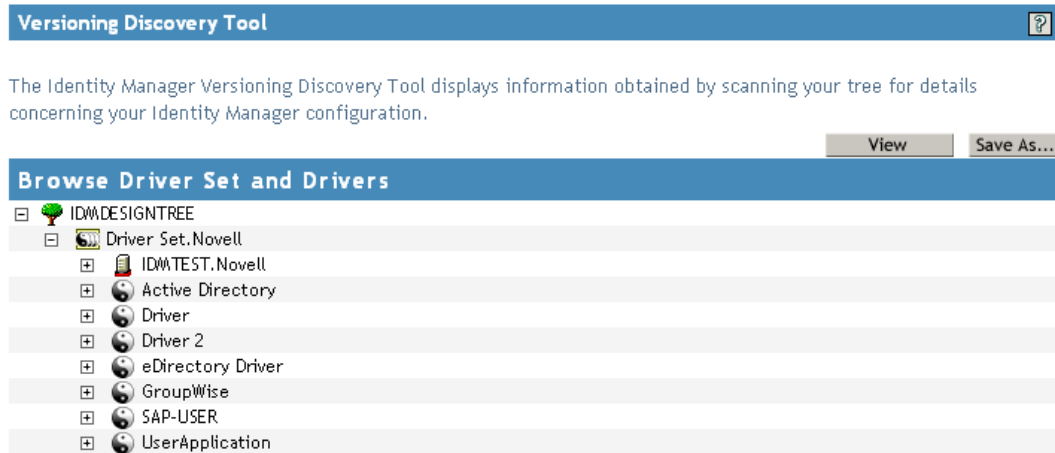
Driver Set: Driver Set.Novell Activation required by: November 1, 2006

Running on server(s):

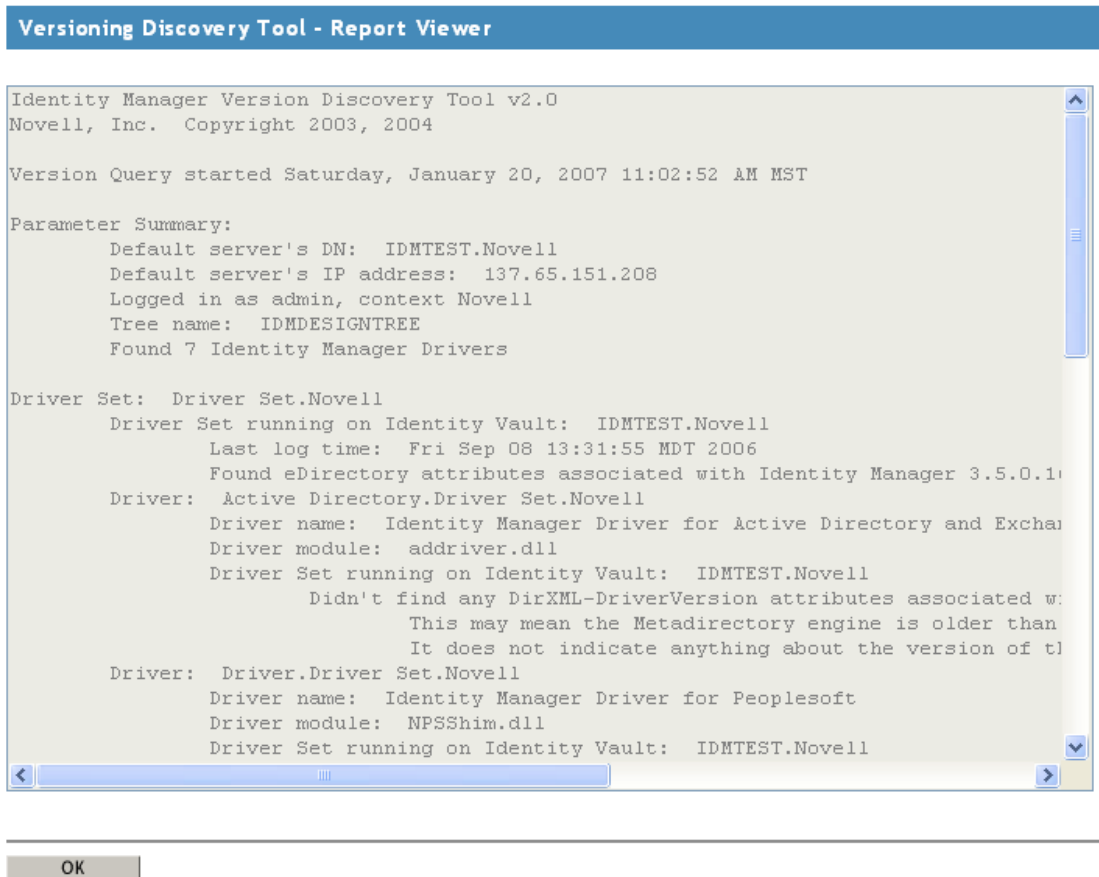
- ▶ [IDWTEST.Novell](#)

You can also select *Identity Manager Utilities > Versioning Discovery*, browse to and select the Driver Set object, then click *Information*.

- 3 In the Versioning Discovery Tool dialog box, click *View*.



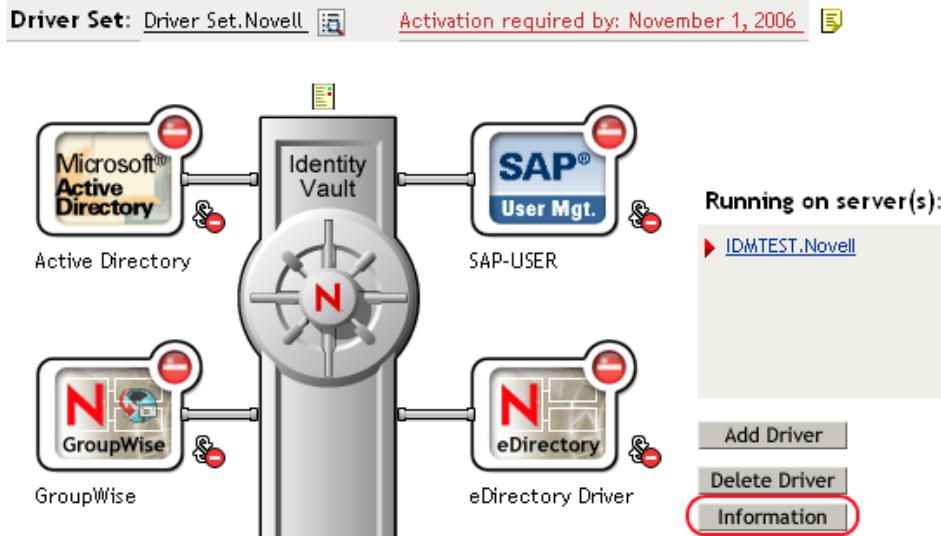
The information is displayed as a text file in the Report Viewer window.



7.13.3 Saving Versioning Information

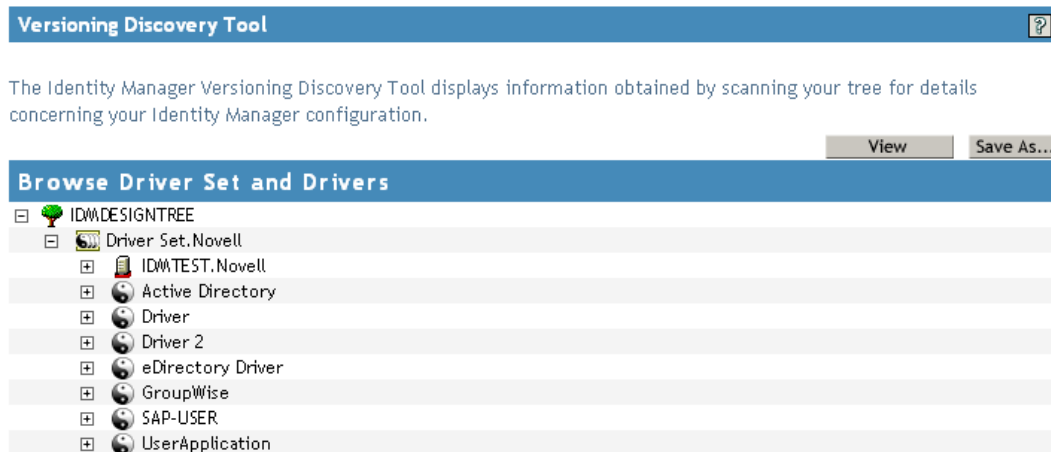
You can save versioning information to a text file on your local or network drive.

- 1 To find the Driver Set object in iManager, click *Identity Manager > Identity Manager Overview*, then click *Search*.
- 2 In the Identity Manager Overview, click *Information*.



You can also select *Identity Manager Utilities > Versioning Discovery*, browse to and select the Driver Set object, then click *Information*.

- 3 In the Versioning Discovery Tool dialog box, click *Save As*.



- 4 In the File Download dialog box, click *Save*.
- 5 Navigate to the desired directory, type a filename, then click *Save*.
Identity Manager saves the data to a text file.

7.14 Reassociating a Driver Set Object with a Server Object

The driver set object should always be associated with a server object. If the driver set is not associated with a server object, none of the drivers in the driver set can start.

If the link between the driver set object and the server object becomes invalid, you see one of the following conditions:

- ♦ When upgrading eDirectory your Identity Manager server, you get the error UniqueSPIException error -783.
- ♦ No server is listed next to the driver set in the Identity Manager Overview window.
- ♦ A server is listed next to the driver set in the Identity Manager Overview window, but the name is garbled text.

To resolve this issue, disassociate the driver set object and the server object, then reassociate them.

- 1 In iManager click *Identity Manager > Identity Manager Overview*, then click *Search* to find the driver set object that the driver should be associated with.
- 2 Click the *Remove server* icon, then click *OK*.
- 3 Click the *Add server* icon, then browse to and select the server object.
- 4 Click *OK*.

7.15 Changing the Driver Configuration

If you need to change the driver configuration, Identity Manager allows you to make the change through iManager or Designer.

To change the driver configuration in iManager:

- 1 Click *Identity Manager > Identity Manager Overview*, then click *Search* to search for the driver set that is associated with the driver.
- 2 Browse to the driver, then click the upper right corner of the driver icon.
- 3 Click *Edit Properties*.

To change the driver configuration in Designer:

- 1 Open a project in the Modeler, then right-click the driver line and select *Properties*.

For a listing of all of the configuration fields, see [Appendix C, “Properties of the Driver,” on page 185](#).

7.16 Storing Driver Passwords Securely with Named Passwords

Identity Manager allows you to store multiple passwords securely for a particular driver. This functionality is referred to as Named Passwords. Each different password is accessed by a key, or name.

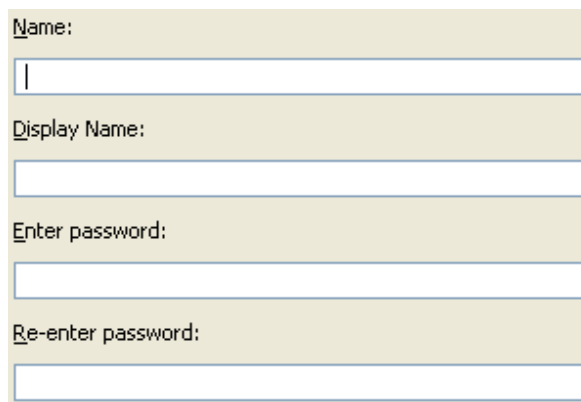
You can also use the Named Passwords feature to store other pieces of information securely, such as a user name.

To use a Named Password in a driver policy, you refer to it by the name of the password, instead of using the actual password, and the Metadirectory engine sends the password to the driver. The method described in this section for storing and retrieving Named Passwords can be used with any driver without making changes to the driver shim.

- ♦ [Section 7.16.1, “Using Designer to Configure Named Passwords,” on page 127](#)
- ♦ [Section 7.16.2, “Using iManager to Configure Named Passwords,” on page 127](#)
- ♦ [Section 7.16.3, “Using Named Passwords in Driver Policies,” on page 129](#)
- ♦ [Section 7.16.4, “Using the DirXML Command Line Utility to Configure Named Passwords,” on page 129](#)

7.16.1 Using Designer to Configure Named Passwords

- 1 Right-click the driver object, then select *Properties*.
- 2 Select *Named Password*, then click *New*.



- 3 Specify the *Name* of the Named Password.
- 4 Specify the *Display name* of the Named Password.
- 5 Specify the Named Password, then re-enter the password.
- 6 Click *OK* twice.

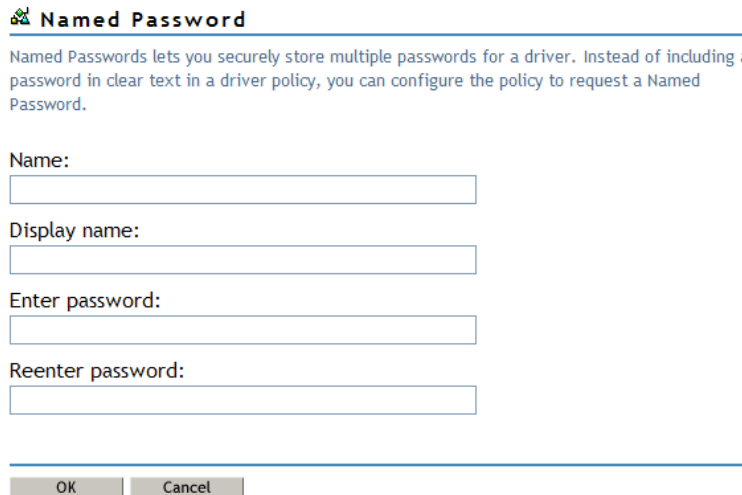
7.16.2 Using iManager to Configure Named Passwords

- 1 Click *Identity Manager > Identity Manager Overview*, then click *Search* to search for the driver set that is associated with the driver.
- 2 In the Identity Manager Overview, click the upper right corner of the driver icon, then click *Edit properties*.
- 3 On the Modify Object page on the Identity Manager tab, click *Named Passwords*.

The Named Passwords page appears, listing the current Named Passwords for this driver. If you have not set up any Named Passwords, the list is empty.



- 4 To add a Named Password, click *Add*, complete the fields, then click *OK*.



- 5 Specify a name, display name and a password, then click *OK* twice.
You can use this feature to store other kinds of information securely, such as a username.
- 6 Click *OK* to restart the driver and have the changes take effect.
- 7 To remove a Named Password, select the password name, then click *Remove*.
The password is removed without prompting you to confirm the action.

7.16.3 Using Named Passwords in Driver Policies

- ♦ “Using the Policy Builder” on page 129
- ♦ “Using XSLT” on page 129

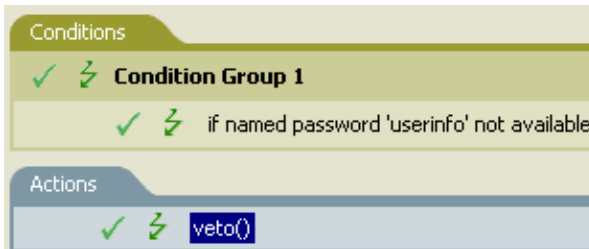
Using the Policy Builder

Policy Builder allows you to make a call to a Named Password. Create a new rule and select Named Password as the condition, then set an action depending upon if the Named Password is available or not available.

- 1 In Designer, launch Policy Builder, right-click, then click *New > Rule*.
- 2 Specify the name of the rule, then click *Next*.
- 3 Select the condition structure, then click *Next*.
- 4 Select *named password* for the *Condition*.
- 5 Browse to and select the Named Password that is stored on the driver.
In this example, it is *userinfo*.
- 6 Select whether the Operator is available or not available.
- 7 Select an action for the *Do* field.
In this example, the action is *veto*.

The example indicates that if the userinfo Named Password is not available, then the event is vetoed.

Figure 7-1 A Policy Using Named Passwords



Using XSLT

The following example shows how a Named Password can be referenced in a driver policy on the Subscriber channel in XSLT:

```
<xsl:value-of  
select="query:getNamedPassword($srcQueryProcessor, 'mynamedpassword')"  
xmlns:query="http://www.novell.com/java/  
com.novell.nds.dirxml.driver.XdsQueryProcessor/">
```

7.16.4 Using the DirXML Command Line Utility to Configure Named Passwords

- ♦ “Creating a Named Password in the DirXML Command Line Utility” on page 130
- ♦ “Using the DirXML Command Line Utility to Remove a Named Password” on page 131

Creating a Named Password in the DirXML Command Line Utility

- 1 Run the DirXML Command Line utility.

For information, see [Appendix B, “DirXML Command Line Utility,”](#) on page 171.

- 2 Enter your username and password.

The following list of options appears.

DirXML commands

```
1: Start driver
2: Stop driver
3: Driver operations...
4: Driver set operations...
5: Log events operations...
6: Get DirXML version

7: Job operations...
99: Quit
```

Enter choice:

- 3 Enter 3 for driver operations.

A numbered list of drivers appears.

- 4 Enter the number for the driver you want to add a Named Password to.

The following list of options appears.

Select a driver operation for:

driver_name

```
1: Start driver
2: Stop driver
3: Get driver state
4: Get driver start option
5: Set driver start option
6: Resync driver
7: Migrate from application into DirXML
8: Submit XDS command document to driver
9: Submit XDS event document to driver

10: Queue event for driver
11: Check object password
12: Initialize new driver object
13: Passwords operations
14: Cache operations
99: Exit
```

Enter choice:

- 5 Enter 13 for password operations.

The following list of options appears.

Select a password operation

```
1: Set shim password
2: Reset shim password

3: Set Remote Loader password
4: Clear Remote Loader password
5: Set named password
6: Clear named password(s)
7: List named passwords
```

```
8: Get passwords state
99: Exit
```

Enter choice:

- 6 Enter 5 to set a new Named Password.

The following prompt appears:

```
Enter password name:
```

- 7 Enter the name by which you want to refer to the Named Password.

- 8 Enter the actual password that you want to secure at the following prompt:

```
Enter password:
```

The characters you type for the password are not displayed.

- 9 Confirm the password by entering it again at the following prompt:

```
Confirm password:
```

- 10 After you enter and confirm the password, you are returned to the password operations menu.

- 11 After completing this procedure, you can use the 99 option twice to exit the menu and quit the DirXML Command Line Utility.

Using the DirXML Command Line Utility to Remove a Named Password

This option is useful if you no longer need Named Passwords that you previously created.

- 1 Run the DirXML Command Line utility.

For information, see [Appendix B, “DirXML Command Line Utility,” on page 171](#).

- 2 Enter your username and password.

The following list of options appears.

```
DirXML commands
```

```
1: Start driver
2: Stop driver
3: Driver operations...
4: Driver set operations...
5: Log events operations...
6: Get DirXML version
```

```
7: Job operations
99: Quit
```

Enter choice:

- 3 Enter 3 for driver operations.

A numbered list of drivers appears.

- 4 Enter the number for the driver you want to remove Named Passwords from.

The following list of options appears.

```
Select a driver operation for:
driver_name
```

1: Start driver
2: Stop driver
3: Get driver state
4: Get driver start option
5: Set driver start option
6: Resync driver
7: Migrate from application into DirXML
8: Submit XDS command document to driver
9: Submit XDS event document to driver
10: Queue event for driver
11: Check object password
12: Initialize new driver object
13: Passwords operations
14: Cache operations
99: Exit

Enter choice:

5 Enter 13 for password operations.

The following list of options appears.

Select a password operation

1: Set shim password
2: Reset shim password
3: Set Remote Loader password
4: Clear Remote Loader password
5: Set named password
6: Clear named password(s)
7: List named passwords
8: Get passwords state
99: Exit

Enter choice:

6 (Optional) Enter 7 to see the list of existing Named Passwords.

The list of existing Named Passwords is displayed.

This step can help you make sure you are removing the correct password.

7 Enter 6 to remove one or more Named Passwords.

8 Enter No to remove a single Named Password at the following prompt:

Do you want to clear all named passwords? (yes/no):

9 Enter the name of the Named Password you want to remove at the following prompt:

Enter password name:

After you enter the name of the Named Password you want to remove, you are returned to the password operations menu:

Select a password operation

1: Set shim password
2: Reset shim password
3: Set Remote Loader password
4: Clear Remote Loader password
5: Set named password
6: Clear named password(s)
7: List named passwords

```
8: Get passwords state
99: Exit

Enter choice:
```

- 10 (Optional) Enter 7 to see the list of existing Named Passwords.

This step lets you verify that you have removed the correct password.

- 11 After completing this procedure, you can use the 99 option twice to exit the menu and quit the DirXML Command Line utility.

7.17 Adding a Driver Heartbeat

The driver heartbeat is a feature of the Identity Manager drivers that ship with Identity Manager 2 and later. Its use is optional. The driver heartbeat is configured by using a driver parameter with a time interval specified. If a heartbeat parameter exists and has an interval value other than 0, the driver sends a heartbeat document to the Metadirectory engine if there is no communication on the Publisher channel for the specified interval of time.

The intent of the driver heartbeat is to give you a trigger to allow you to initiate an action at regular intervals, if the driver does not communicate on the Publisher channel as often as you want the action to occur. To take advantage of the heartbeat, you must customize your driver configuration or other tools. The Metadirectory engine accepts the heartbeat document but does not take any action because of it.

For most drivers, a driver parameter for heartbeat is not used in the sample configurations, but you can add it.

A custom driver that is not provided with Identity Manager can also provide a heartbeat document, if the driver developer has written the driver to support it.

To configure the heartbeat:

- 1 In iManager, click *Identity Manager > Identity Manager Overview*.
- 2 Browse to and select your driver set object, then click *Search*.
- 3 In the Identity Manager Overview, click the upper right corner of the driver icon, then click *Edit properties*.
- 4 On the *Identity Manager* tab, click *Driver Configuration*, scroll to *Driver Parameters*, then look for Heart Beat or a similar display name.

If a driver parameter already exists for heartbeat, you can change the interval and save the changes, and configuration is then complete.

The value of the interval cannot be less than 1. A value of 0 means the feature is turned off.

The unit of time is usually minutes; however, some drivers might choose to implement it differently, such as using seconds.

- 5 If a driver parameter does not exist for heartbeat, click *Edit XML*.
- 6 Add a driver parameter entry like the following example, as a child of <publisher-options>.

```
<pub-heartbeat-interval display-name="Heart Beat">10</pub-heartbeat-interval>
```

If the driver does not produce a heartbeat document after being restarted, check the placement of the driver parameter in the XML.

- 7 Save the changes, and make sure the driver is stopped and restarted.

After you have added the driver parameter, you can edit the time interval by using the graphical view. Another option is to create a reference to a global configuration value (GCV) for the time interval. Like other global configuration values, the driver heartbeat can be set at the driver set level instead of on each individual driver object. If a driver does not have a particular global configuration value, and the driver set object does have it, the driver inherits the value from the driver set object.

Synchronizing Objects

8

This section explains driver and object synchronization in DirXML[®] 1.1a, Identity Manager 2.0, and Identity Manager 3.x. Driver synchronization was not available for DirXML 1.0 and DirXML 1.1.

After the driver is created, instead of waiting for objects to be modified or created, the data between the two connected systems can be sent through the synchronization process.

- ♦ [Section 8.1, “What Is Synchronization?” on page 135](#)
- ♦ [Section 8.2, “When Is Synchronization Done?” on page 135](#)
- ♦ [Section 8.3, “How Does the Metadirectory Engine Decide Which Object to Synchronize?” on page 136](#)
- ♦ [Section 8.4, “How Does Synchronization Work?” on page 137](#)

8.1 What Is Synchronization?

The actions commonly referred to as “synchronization” in Identity Manager refer to several different but related actions:

- ♦ Synchronization (or merging) of attribute values of an object in the Identity Vault with the corresponding attribute values of an associated object in a connected system.
- ♦ Migration of all Identity Vault objects and classes that are included in the filter on the Subscriber channel.
- ♦ Generation of the list of objects to submit to the driver’s Subscriber channel for synchronization or migration in response to a user request (a manual synchronization).
- ♦ Generation of the list of objects to submit to the driver’s Subscriber channel for synchronization or migration in response to enabling a formerly disabled driver, or in response to a cache error.

8.2 When Is Synchronization Done?

The Metadirectory engine performs object synchronization or merging in the following circumstances:

- ♦ A `<sync>` event element is submitted on the Subscriber or Publisher channel.
- ♦ A `<sync>` event element is submitted on the Subscriber channel in the following circumstances:
 - ♦ The state of the object’s association value is set to “manual” or “migrate.” (This causes an eDirectory[™] event, which in turn causes the Identity Manager caching system to queue an object synchronization command in the affected driver’s cache.)
 - ♦ An object synchronization command is read from the driver’s cache.

- ◆ A <sync> event element is submitted on the Publisher channel in the following circumstances:
 - ◆ A driver submits a <sync> event element. No known driver currently does this.
 - ◆ The Metadirectory engine submits a <sync> event element for each object found as the result of a migrate-into-NDS query. These <sync> events are submitted using the Subscriber thread, but are processed using the Publisher channel filter and policies.
- ◆ An <add> event (real or synthetic) is submitted on a channel and the channel Matching policy finds a matching object in the target system.
- ◆ An <add> event with an association is submitted on the Subscriber channel. This normally occurs only in exceptional cases, such as the bulk load of objects into eDirectory with DirXML-Associations attribute values.
- ◆ An <add> event is submitted on the Publisher channel and an object is found in eDirectory that already has the association value reported with the <add> event.

The Metadirectory engine generates synchronization requests for zero or more objects in the following cases:

- ◆ The user issues a manual driver synchronization request. This corresponds to the *Resync* button in the Driver Set property page in ConsoleOne[®], or to the *Synchronize* button on the iManager Identity Manager Driver Overview page.
- ◆ The Metadirectory engine encounters an error with the driver's cache and cannot recover from the cache error. The driver's cache is deleted and the engine generates object synchronization commands as detailed in [Section 8.3, "How Does the Metadirectory Engine Decide Which Object to Synchronize?," on page 136.](#)

8.3 How Does the Metadirectory Engine Decide Which Object to Synchronize?

The Metadirectory engine processes both manually initiated and automatically initiated synchronization requests in the same manner. The only difference in the processing of manually initiated versus automatically initiated driver synchronization requests is the starting filter time used to filter objects being considered for synchronization.

The starting filter time is used to filter objects that have modification or creation times that are older than the starting time specified in the synchronization request.

For automatically initiated driver synchronization, the starting filter time is obtained from the time stamps of cached eDirectory events. In particular, the starting filter time is the earliest time for the cached events that haven't yet been successfully processed by the driver's Subscriber channel.

For manually initiated driver synchronization, the default starting filter time is the earliest time in the eDirectory database. In Identity Manager 2 and Identity Manager 3, an explicit starting filter time can also be set. In DirXML 1.1a there is no facility to set the starting filter time value for synchronization when manually initiating driver synchronization.

The Metadirectory engine creates a list of objects to be synchronized on the Subscriber channel in the following manner:

1. It finds all objects that:
 - ◆ Have an entry modification time stamp greater than or equal to the starting filter time

- and
 - ♦ Exist in the filter on the Subscriber channel.
- 2. It finds all objects that have an entry creation time stamp greater than or equal to the starting filter time.
- 3. It adds a `synchronize object` command to the driver cache for each unique object found that has an entry modification time stamp greater than or equal to the starting filter time and all objects and classes that are in the Subscriber filter channel in the driver being synchronized.

8.4 How Does Synchronization Work?

After the Metadirectory engine determines that an object is to be synchronized, the following processes occur:

1. Each system (the Identity Vault and the connected system) is queried for all attribute values in the appropriate filters.
 - ♦ eDirectory is queried for all values in the Subscriber filter, and for values that are marked for synchronization in Identity Manager 2.x and Identity Manager 3.x.
 - ♦ The connected system is queried for all values in the Publisher filter, and for values that are marked for synchronization in Identity Manager 2.x and Identity Manager 3.x.
2. The returned attribute values are compared and modification lists are prepared for the Identity Vault and the connected system according to [Table 8-1 on page 138](#), [Table 8-2 on page 139](#), and [Table 8-3 on page 141](#).

In the tables the following pseudo-equations are used:

- ♦ “Left = Right” indicates that the left side receives all values from the right side.
- ♦ “Left = Right[1]” indicates that the left side receives one value from the right side. If there is more than one value, it is indeterminate.
- ♦ “Left += Right” indicates that the left side adds the right side values to the left side’s existing values.
- ♦ “Left = Left + Right” indicates that the left side receives the union of the values of the left and right sides.

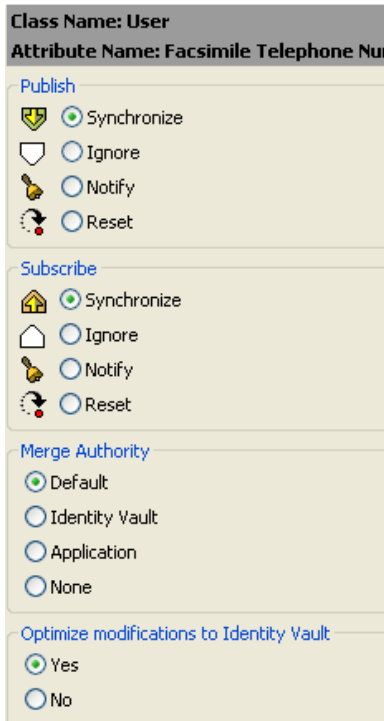
There are three different combinations of selected items in the filter, and each one creates a different output.

- ♦ [Section 8.4.1, “Scenario One,” on page 137](#)
- ♦ [Section 8.4.2, “Scenario Two,” on page 139](#)
- ♦ [Section 8.4.3, “Scenario Three,” on page 140](#)

8.4.1 Scenario One

The attribute is set to *Synchronize* on the Publisher and Subscriber channels, and the merge authority is set to *Default*.

Figure 8-1 Scenario One



The following table contains the values that the Metadirectory engine synchronizes when the attribute is sent through a filter that is set to the configuration for Scenario One. The table shows different outputs depending upon whether the attribute comes from the Identity Vault or the Application, if the attribute is single-valued or multi-valued, and if the attribute is empty or non-empty.

Table 8-1 Output of Scenario One

	Identity Vault single-valued empty	Identity Vault single-valued non-empty	Identity Vault multi-valued empty	Identity Vault multi-valued non-empty
Application single-valued empty	No change	App = Identity Vault	No change	App = Identity Vault[1]
Application single-valued non-empty	Identity Vault = App	App = Identity Vault	Identity Vault = App	Identity Vault + = App
Application multi-valued empty	No change	App = Identity Vault	No change	App = Identity Vault
Application multi-valued non-empty	Identity Vault = App[1]	App + = Identity Vault	Identity Vault = App	App = App + Identity Vault Identity Vault = App + Identity Vault

8.4.2 Scenario Two

The attribute is set to *Synchronize* only on the Subscriber channel, or it is set to *Synchronize* on both the Subscriber and Publisher channels. The merge authority is set to *Identity Vault*.

Figure 8-2 Scenario Two

Class Name: User

Attribute Name: Description

Publish

Synchronize

Ignore

Notify

Reset

Subscribe

Synchronize

Ignore

Notify

Reset

Merge Authority

Default

Identity Vault

Application

None

Optimize modifications to Identity Vault

Yes

No

The following table contains the values that the Metadirectory engine synchronizes when the attribute is sent through a filter that is set to the configuration for Scenario Two. The table shows different outputs depending upon whether the attribute comes from the Identity Vault or the Application, if the attribute is single-valued or multi-valued, and if the attribute is empty or non-empty.

Table 8-2 Output of Scenario Two

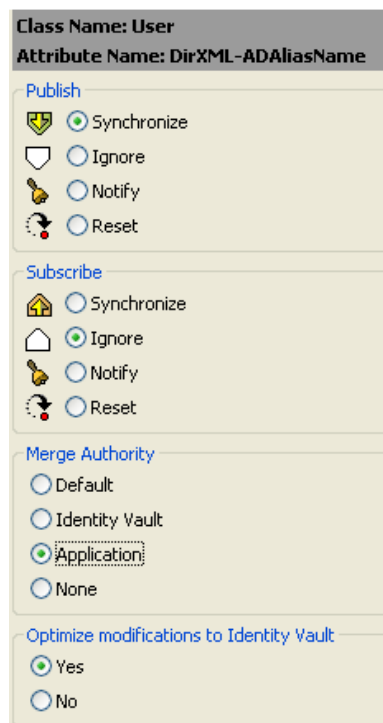
	Identity Vault single-valued empty	Identity Vault single-valued non-empty	Identity Vault multi-valued empty	Identity Vault multi-valued non-empty
Application single-valued empty	No change	App = Identity Vault	No change	App = Identity Vault[1]
Application single-valued empty	App = empty	App = Identity Vault	Identity Vault = App	App = Identity Vault[1]
Application multi-valued empty	No change	App = Identity Vault	No change	App = Identity Vault

	Identity Vault single-valued empty	Identity Vault single-valued non-empty	Identity Vault multi-valued empty	Identity Vault multi-valued non-empty
Application multi-valued non-empty	App = empty	App = Identity Vault	App = empty	App = Identity Vault

8.4.3 Scenario Three

The attribute is set to *Synchronize* on the Publisher channel or the merge authority is set to *Application*.

Figure 8-3 Scenario Three



The following table contains the values that the Metadirectory engine synchronizes when the attribute is sent through a filter that is set to the configuration for Scenario Three. The table shows different outputs depending upon whether the attribute comes from the Identity Vault or the Application, if the attribute is single-valued or multi-valued, and if the attribute is empty or non-empty.

Table 8-3 *Output of Scenario Three*

	Identity Vault single-valued empty	Identity Vault single-valued non-empty	Identity Vault multi-valued empty	Identity Vault multi-valued non-empty
Application single-valued empty	No change	Identity Vault = empty	No change	Identity Vault = empty
Application single-valued non-empty	Identity Vault = App	Identity Vault = App	Identity Vault = App	Identity Vault = App
Application multi-valued empty	No change	Identity Vault = empty	No change	Identity Vault = empty
Application multi-valued non- empty	Identity Vault = App[1]	Identity Vault = App[1]	Identity Vault = App	Identity Vault = App

Troubleshooting the Identity Manager Driver for GroupWise

9

This section explains how to troubleshoot the Identity Manager Driver for GroupWise®.

- ♦ [Section 9.1, “Avoiding Data Corruption,” on page 143](#)
- ♦ [Section 9.2, “Error Messages,” on page 143](#)
- ♦ [Section 9.3, “Troubleshooting Driver Processes,” on page 150](#)

9.1 Avoiding Data Corruption

If you are running the GroupWise driver on a Windows server and the domain database is on a NetWare® server, you can have data corruption if the Novell Client™ is not configured properly. The default setting for the Novell Client can cause problems for the GroupWise driver.

To change the Novell Client settings:

- 1 Right-click the red N in the taskbar, then click *Novell Client Properties*.
- 2 Click the *Advanced Settings* tab, then scroll to verify that *File Caching* is *Off* and that *File Commit* is *On*.
- 3 Click *OK*.

9.2 Error Messages

For each event or operation received from the engine, the driver returns an XML document containing a status report in DSTrace. See [Section 9.3, “Troubleshooting Driver Processes,” on page 150](#) for instructions on how to capture this information. If the operation or event is not successful, the status report also contains a text message describing the error condition.

Table 9-1 *Status Levels*

Status Level	Description
Success	Operation or event was successful.
Warning	Operation or event was partially successful.
Error	Operation or event failed.
Fatal	A fatal error occurred. The driver shuts down.
Retry	Application server was unavailable. Send this event or operation later.

Driver initialization error

Source: The status log or DSTrace screen.

Explanation: On driver initialization, no parameters were provided.

Action: Edit the driver parameters and add valid parameters. See [Section C.1.5, “Driver Parameters,” on page 189](#) for more information.

Level: Fatal

Failure initializing GroupWise

Source: The status log or DSTrace screen.

Explanation: During initialization, the driver cannot communicate with GroupWise.

Possible Cause: A driver parameter is not configured correctly.

Action: Verify that the driver parameters are configured correctly. See [Section C.1.5, “Driver Parameters,” on page 189](#) for more information.

Level: Fatal

Error getting driver DN from src-dn attribute

Source: The status log or DSTrace screen.

Explanation: The src-dn attribute value in `<init-params>` did not have a value or the value was not recognized by the driver.

Action: Verify that the driver parameters are configured correctly. See [Section C.1.5, “Driver Parameters,” on page 189](#) for more information.

Level: Fatal

Invalid GroupWise Primary Domain Path initialization parameter

Source: The status log or DSTrace screen.

Explanation: An invalid format was used to specify the domain path.

Possible Cause: A driver parameter is not configured correctly.

Action: Verify that the driver parameters are configured correctly. See [Section C.1.5, “Driver Parameters,” on page 189](#) for more information.

Level: Fatal

Invalid Admin User ID

Source: The status log or DSTrace screen.

Explanation: The value of this parameter cannot be “mapi,” which is a reserved ID.

Possible Cause: A driver parameter is not configured correctly.

Action: Verify that the driver parameters are configured correctly. See [Section C.1.5, “Driver Parameters,” on page 189](#) for more information.

Level: Fatal

Missing domain path initialization parameter

Source: The status log or DSTrace screen.

Explanation: The GroupWise primary domain path has not been specified in the Driver Parameters page in iManager.

Possible Cause: A driver parameter is not configured correctly.

Action: Verify that the driver parameters are configured correctly. See [Section C.1.5, “Driver Parameters,” on page 189](#) for more information.

Level: Fatal

Missing Admin User ID initialization parameter

Source: The status log or DSTrace screen.

Explanation: The Admin User ID has not been specified in the Driver Parameters page in iManager.

Possible Cause: A driver parameter is not configured correctly.

Action: Verify that the driver parameters are configured correctly. See [Section C.1.5, “Driver Parameters,” on page 189](#) for more information.

Level: Fatal

Invalid character in Admin User ID

Source: The status log or DSTrace screen.

Explanation: An invalid character is used in the Admin User ID in the Driver Parameters page in iManager.

Possible Cause: The User ID contains 1 to 256 characters, and cannot contain the ()@.:,{}* characters. The UserID must be unique within its namespace (UserID shares the same namespace as nicknames, resources, and distribution lists.) Do not use “mapi” (reserved IDs) for this value.

Action: Verify that the driver parameters are configured correctly. See [Section C.1.5, “Driver Parameters,” on page 189](#) for more information.

Level: Fatal

JNDI Naming exception

Source: The status log or DSTrace screen.

Explanation: A name exception occurred.

Possible Cause: A driver parameter is not configured correctly.

Action: Verify that the driver parameters are configured correctly. See [Section C.1.5, “Driver Parameters,” on page 189](#) for more information.

Level: Fatal

Class not found exception

Source: The status log or DSTrace screen.

Explanation: The driver cannot find the requested class.

Possible Cause: The eDirectory™ schema might not be extended properly.

Action: Verify the GroupWise schema is extended properly and that the GroupWise driver was installed correctly. See [Section 2.4, “Installing the Driver,” on page 24](#) for more information.

Level: Fatal

Unsatisfied link error (can't load .dll)

Source: The status log or DSTrace screen.

Explanation: The driver cannot find the proper files.

Possible Cause: The driver might not be installed correctly.

Action: Reinstall the driver. See [Section 2.4, "Installing the Driver," on page 24](#) for more information.

Level: Fatal

Unable to determine initial context

Source: The status log or DSTrace screen.

Explanation: The driver cannot determine the initial context.

Possible Cause: A driver parameter is not configured correctly.

Action: Verify that the driver parameters are configured correctly. See [Section C.1.5, "Driver Parameters," on page 189](#) for more information.

Level: Fatal

Domain path incorrect

Source: The status log or DSTrace screen.

Explanation: The GroupWise domain path is incorrect.

Possible Cause: A driver parameter is not configured correctly.

Action: Verify that the domain path is specified in the correct form. See [Section C.1.5, "Driver Parameters," on page 189](#) for more information.

Level: Fatal

Unable to make connection with remote server

Source: The status log or DSTrace screen.

Explanation: The Identity Manager engine cannot connect to the Remote Loader server

Possible Cause: Missing or invalid authentication information.

Possible Cause: Incorrect setup of authentication accounts.

Action: Verify that the Remote Loader is configured correctly. See ["Deciding Whether to Use the Remote Loader"](#) in the *Novell Identity Manager 3.5.1 Administration Guide* for more information.

Level: Fatal

GroupWise error

Source: The status log or DSTrace screen.

Explanation: There are multiple causes for this error.

Possible Cause: Invalid post office specified. Either the post office does not exist or the driver does not have eDirectory access rights (read/write).

Possible Cause: The parent of an external post office must be an external domain.

Possible Cause: Invalid post office or domain specified.

Possible Cause: Query Scope Entry: No base object identified.

Possible Cause: Requested Query operation is not supported.

Possible Cause: Unsupported Class. The driver received an event for an object other than a Novell® eDirectory User object.

Possible Cause: No username specified. The CN attribute was not specified.

Possible Cause: java.lang.NullPointerException. The XML document is not correctly formed. It might be syntactically correct, but it doesn't make sense.

Action: Specify a valid post office, or verify that the driver has the correct eDirectory access rights. See [Section 7.4, "Driver Access Rights and Membership," on page 118](#) for more information.

Level: Error

Unsupported operation

Source: The status log or DSTrace screen.

Explanation: The driver does not understand the XML event.

Possible Cause: The XML document is not correctly formed. It might be syntactically correct, but it doesn't make sense.

Action: Review and fix the XML document.

Level: Error

Event failed. The Identity Manager association for this driver has been removed

Source: The status log or DSTrace screen.

Explanation: The driver received an event for an object without an expected GroupWise ID.

Possible Cause: This is probably caused when the GroupWise account is deleted through the GroupWise snap-ins. The driver has removed the association to the driver in eDirectory for this object.

Level: Error

Move pending

Source: The status log or DSTrace screen.

Explanation: When GroupWise is in the process of moving an account from one post office to another, other operations cannot be performed on the account.

Level: Retry

Prior modification pending

Source: The status log or DSTrace screen.

Explanation: You attempted to move a user to another post office, but previous modifications have not been processed.

Action: Allow the previous modifications to process before attempting to move the user.

Level: Retry

Name already exists in GroupWise

Source: The status log or DSTrace screen.

Explanation: This can occur on an account create, rename, or post office move event.

Action: Verify that the account has an unique name.

Level: Error

Event is for a different system.

Source: The status log or DSTrace screen.

Explanation: The received event is not for this GroupWise system and is ignored by the driver. There can be multiple GroupWise systems in a single eDirectory tree. An instance of the driver supports only a single GroupWise system.

Action: Add a rule to allow only items for this GroupWise system. See [Section 6.3, “Modifying Policies,” on page 48](#) for more information.

Level: Warning (for event)

Error publishing to eDirectory

Source: The status log or DSTrace screen.

Explanation: GroupWise tried to update attributes in eDirectory for an object. The error message is from Identity Manager or eDirectory.

Possible Cause: You might have a GroupWise object without a corresponding object in eDirectory. If the corresponding object does exist in eDirectory, the attribute values in eDirectory might not be correct.

Level: Error

No commands to execute

Source: The status log or DSTrace screen.

Explanation: An input document without any commands was received.

Possible Cause: This is probably a style sheet error, where the style sheet didn't pass any commands through.

Level: Error

Query posted to publisher failed

Source: The source of the message.

Explanation: This error is generated for the following conditions:

- ◆ The driver received a query for an object other than user.
- ◆ The object to be queried does not exist or cannot be read.

Level: Error

Waiting for publisher to start

Source: The status log or DSTrace screen.

Explanation: The Subscriber channel does not process events until the Publisher channel is initialized and running. The Subscriber channel can initialize before the Publisher channel. Normally, both channels initialize within a short time.

Level: Retry

Invalid reference to GroupWise

Source: The status log or DSTrace screen.

Explanation: This error occurred because there is an invalid reference to GroupWise. This is not a problem if it occurred on a Modify event that is generated by eDirectory in response to a Move event.

Possible Cause: This could also occur if required data is missing, incorrect, invalid, or refers to the wrong type of object. In these cases, the error message includes specific information.

Level: Warning

Password synchronization was not processed

Source: The status message or DSTrace screen.

Explanation: The post office security is set to LDAP Authentication. You cannot set the GroupWise password, which would be ignored.

Level: Success

Rename or Move

Source: The status log or DSTrace screen.

Explanation: Rename or Move error: The operation might not be supported with this GroupWise domain version.

Possible Cause: An error probably occurred processing a move or rename. Part of the event might have been processed. Most likely, this operation is not supported in the GroupWise domain version. You should upgrade the GroupWise system.

Level: Warning

eDirectory Error

Source: The status log or DSTrace screen.

Explanation: This attempt to read from or write to eDirectory failed. See the error message and prior results from eDirectory for more details.

Level: Retry or Error

9.3 Troubleshooting Driver Processes

Viewing driver processes is necessary to analyze unexpected behavior. To view the driver processing events, use DSTrace. You should only use it during testing and troubleshooting the driver. Running DSTrace while the drivers are in production increases the utilization on the Identity Manager server and can cause events to process very slowly.

9.3.1 Viewing Driver Processes

In order to see the driver processes in DSTrace, values are added to the driver set and the driver objects. You can do this in Designer and iManager.

- ♦ “Adding Trace Levels in Designer” on page 150
- ♦ “Adding Trace Levels in iManager” on page 152
- ♦ “Capturing Driver Processes to a File” on page 153

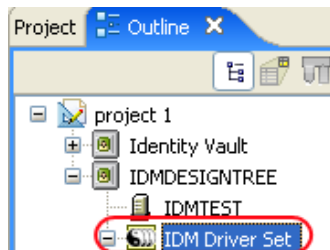
Adding Trace Levels in Designer

You can add trace levels to the driver set object or to each driver object.

- ♦ “Driver Set” on page 150
- ♦ “Driver” on page 151

Driver Set

- 1 In an open project in Designer, select the driver set object in the *Outline* view.



- 2 Right-click and select *Properties*, then click *5. Trace*.
- 3 Set the parameters for tracing, then click *OK*.

Parameter	Description
Driver trace level	<p>As the driver object trace level increases, the amount of information displayed in DSTrace increases.</p> <p>Trace level 1 shows errors, but not the cause of the errors. If you want to see password synchronization information, set the trace level to 5.</p>
XSL trace level	DSTrace displays XSL events. Set this trace level only when troubleshooting XSL style sheets. If you do not want to see XSL information, set the level to zero.
Java debug port	Allows developers to attach a Java* debugger.
Java trace file	<p>When a value is set in this field, all Java information for the driver set object is written to a file. The value for this field is the path for that file.</p> <p>As long as the file is specified, Java information is written to this file. If you do not need to debug Java, leave this field blank.</p>
Trace file size limit	<p>Allows you to set a limit for the Java trace file. If you set the file size to <i>Unlimited</i>, the file grows in size until there is no disk space left.</p> <hr/> <p>NOTE: The trace file is created in multiple files. Identity Manager automatically divides the maximum file size by ten and creates ten separate files. The combined size of these files equals the maximum trace file size.</p> <hr/>

If you set the trace level on the driver set object, all drivers appear in the DSTrace logs.

Driver

- 1 In an open project in Designer, select the driver object in the *Outline* view.
- 2 Right-click and select *Properties*, then click *Trace*.
- 3 Set the parameters for tracing, then click *OK*.

Parameter	Description
Trace level	<p>As the driver object trace level increases, the amount of information displayed in DSTrace increases.</p> <p>Trace level 1 shows errors, but not the cause of the errors. If you want to see password synchronization information, set the trace level to 5.</p> <p>if you select <i>Use setting from Driver Set</i>, the value is taken from the driver set object.</p>
Trace file	<p>Specify a filename and location for where the Identity Manager information is written for the selected driver.</p> <p>if you select <i>Use setting from Driver Set</i>, the value is taken from the driver set object.</p>
Trace file size limit	<p>Allows you to set a limit for the Java trace file. If you set the file size to <i>Unlimited</i>, the file grows in size until there is no disk space left.</p> <p>If you select <i>Use setting from Driver Set</i>, the value is taken from the driver set object.</p> <hr/> <p>NOTE: The trace file is created in multiple files. Identity Manager automatically divides the maximum file size by ten and creates ten separate files. The combined size of these files equals the maximum trace file size.</p> <hr/>
Trace name	<p>The driver trace messages are prepended with the value entered instead of the driver name. Use this option if the driver name is very long.</p>

If you set the parameters only on the driver object, only information for that driver appears in the DSTrace log.

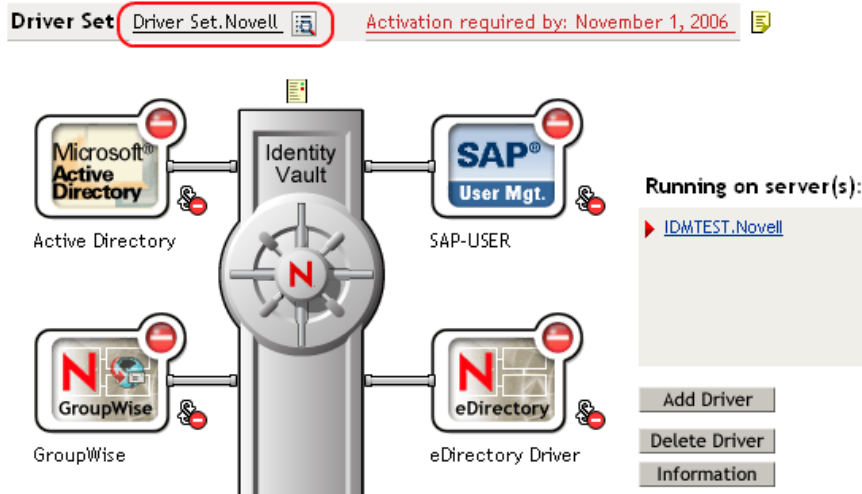
Adding Trace Levels in iManager

You can add trace levels to the driver set object or to each driver object.

- ♦ [“Driver Set” on page 152](#)
- ♦ [“Driver” on page 153](#)

Driver Set

- 1 In iManager, select *Identity Manager > Identity Manager Overview*.
- 2 Browse to the driver set object, then click *Search*.
- 3 Click the driver set name.



- 4 Select the *Misc* tab for the driver set object.
- 5 Set the parameters for tracing, then click *OK*.
See “Misc” on page 201 for the parameters.

Driver

- 1 In iManager, select *Identity Manager > Identity Manager Overview*.
- 2 Browse to the driver set object where the driver object resides, then click *Search*.
- 3 Click the upper right corner of the driver object, then click *Edit properties*.
- 4 Select the *Misc* tab for the driver object.
- 5 Set the parameters for tracing, then click *OK*.
See “Misc” on page 201 for the parameters.

The option *Use setting from Driver Set* does not exist in iManager.

Capturing Driver Processes to a File

You can save driver processes to a file by using the parameter on the driver object or by using DSTrace. The parameter on the driver object is the *Trace file* parameter, under the *MISC* tab.

The driver processes that are captured through DSTrace are the processes that occur on the Identity Manager engine. If you use the Remote Loader, you need to capture a trace on the Remote Loader at the same time as you are capturing the trace on the Identity Manager engine.

The following methods help you capture and save Identity Manager processes through DSTrace on different platforms.

- ♦ “NetWare” on page 154
- ♦ “Windows” on page 154
- ♦ “UNIX” on page 154
- ♦ “iMonitor” on page 155
- ♦ “Remote Loader” on page 156

NetWare

Use `dstrace.nlm` to display trace messages on the system console or trace messages to a file (`sys:\system\dstrace.log`). Use `dstrace.nlm` to display the trace messages to a screen labeled DSTrace Console.

- 1 Enter `dstrace.nlm` at the server console to load `dstrace.nlm` into memory.
- 2 Enter `dstrace screen on` at the server console to allow trace messages to appear on the DSTrace Console screen.
- 3 Enter `dstrace file on` at the server console to capture trace messages sent to the DSTrace Console to the `dstrace.log` file.
- 4 (Optional) Enter `dstrace -all` at the server console to make it easier to read the trace log.
- 5 Enter `dstrace +dxml dstrace +dvrs` at the server console to display Identity Manager events.
- 6 Enter `dstrace +tags dstrace +time` at the server console to display message tags and time stamps.
- 7 Toggle to the DSTrace Console screen and watch for the event to pass.
- 8 Toggle back to the server console.
- 9 Enter `dstrace file off` at the server console.
This stops capturing trace messages to the log file. It also stops logging information into the file.
- 10 Open the `dstrace.log` in a text editor and search for the event or the object you modified.

Windows

- 1 Open the *Control Panel* > *NDS Services* > `dstrace.dlm`, then click *Start* to display the NDS Server Trace utility window.
- 2 Click *Edit* > *Options*, then click *Clear All* to clear all of the default flags.
- 3 Select *DirXML* and *DirXML Drivers*.
- 4 Click *OK*.
- 5 Click *File* > *New*.
- 6 Specify the filename and location where you want the DSTrace information saved, then click *Open*.
- 7 Wait for the event to occur.
- 8 Click *File* > *Close*.
This stops the information from being written to the log file.
- 9 Open the file in a text editor and search for the event or the object you modified.

UNIX

- 1 Enter `ndstrace` to start the `ndstrace` utility.
- 2 Enter `set ndstrace=nodebug` to turn off all trace flags currently set.
- 3 Enter `set ndstrace on` to display trace messages to the console.
- 4 Enter `set ndstrace file on` to capture trace messages to the `ndstrace.log` file in the directory where eDirectory is installed. By default it is `/var/nds`.

- 5 Enter `set ndstrace=+dxml` to display the Identity Manager events.
- 6 Enter `set ndstrace=+dvrs` to display the Identity Manager driver events.
- 7 Wait for the event to occur.
- 8 Enter `set ndstrace file off` to stop logging information to the file.
- 9 Enter `exit` to quite the `ndstrace` utility.
- 10 Open the file in a text editor. Search for the event or the object that was modified.

iMonitor

iMonitor allows you to get DSTrace information from a Web browser. It does not matter where Identity Manager is running. The following files run iMonitor:

- ♦ `ndsimon.nlm` runs on NetWare®.
- ♦ `ndsimon.dlm` runs on Windows.
- ♦ `ndsimonitor` runs on UNIX.

- 1 Access iMonitor from `http://server_ip:XXXX/nds`.

Wheres *XXXX* has these values, depending on the platform:

For eDirectory 8.7.x:

- ♦ NetWare®: 8008 or 8009
- ♦ *Nix: 8028 or 8030
- ♦ Windows: 8008 or 8010
- ♦ OES1: 8028 or 8030

For eDirectory 8.8.x:

- ♦ NetWare: 8008 or 8009
- ♦ *Nix: 8028 or 8030
- ♦ Windows: 8028 or 8030

- 2 Specify a username and password with administrative rights, then click *Login*.
- 3 Select *Trace Configuration* on the left side.
- 4 Click *Clear All*.
- 5 Select *DirXML* and *DirXML Drivers*.
- 6 Click *Trace On*.
- 7 Select *Trace History* on the left side.
- 8 Click the document with the *Modification Time* of *Current* to see a live trace.
- 9 Change the *Refresh Interval* if you want to see information more often.
- 10 Select *Trace Configuration* on the left side, then click *Trace Off* to turn the tracing off.
- 11 Select *Trace History* to view the trace history.

The files are distinguished by their time stamp.

If you need a copy of the HTML file, the default location is:

- ♦ NetWare: `sys:\system\ndsimon\dstrace*.htm`

- ♦ Windows: `Drive_letter:\novell\nds\ndsimon\dstrace*.htm`
- ♦ UNIX: `/var/nds/dstrace/*.htm`

Remote Loader

You can capture the events that occur on the machine by running the Remote Loader service.

- 1 Launch the Remote Loader Console by clicking the icon.
- 2 Select the driver instance, then click *Edit*.
- 3 Set the *Trace Level* to 3 or above.
- 4 Specify a location and file for the trace file.
- 5 Specify the amount of disk space that the file is allowed.
- 6 Click *OK*, twice to save the changes.

You can also enable tracing from the command line by using the switches in [Table 9-1](#). For more information, see “[Configuring the Remote Loader](#)” in the *Novell Identity Manager 3.5.1 Administration Guide*.

Table 9-2 *Command Line Tracing Switches*

Option	Short Name	Parameter	Description
-trace	-t	integer	Specifies the trace level. This is only used when hosting an application shim. Trace levels correspond to those used on the Identity Manager server. Example: <code>-trace 3</code> or <code>-t3</code>
-tracefile	-tf	filename	Specifies a file to write trace messages to. Trace messages are written to the file if the trace level is greater than zero. Trace messages are written to the file even if the trace window is not open. Example: <code>-tracefile c:\temp\trace.txt</code> or <code>-tf c:\temp\trace.txt</code>
-tracefilemax	-tfm	size	Specifies the approximate maximum size that trace file data can occupy on disk. If you specify this option, there is a trace file with the name specified using the tracefile option and up to 9 additional “roll-over” files. The roll-over files are named using the base of the main trace filename plus “_n”, where n is 1 through 9. The size parameter is the number of bytes. Specify the size by using the suffixes K, M, or G for kilobytes, megabytes, or gigabytes. If the trace file data is larger than the specified maximum when the Remote Loader is started, the trace file data remains larger than the specified maximum until roll-over is completed through all 10 files. Example: <code>-tracefilemax 1000M</code> or <code>-tfm 1000M</code>

Backing Up the Driver

10

You can use Designer or iManager to create an XML file of the driver. The file contains all of the information entered into the driver during configuration. If the driver becomes corrupted, the exported file can be imported to restore the configuration information.

IMPORTANT: If the driver has been deleted, all of the associations on the objects are purged. When the XML file is imported again, new associations are created through the migration process.

Not all server-specific information stored on the driver is contained in the XML file. Make sure this information is documented through the Doc Gen process in Designer. See “[Documenting Projects](#)” in the *Designer 2.1 for Identity Manager 3.5.1*.

- ♦ [Section 10.1, “Exporting the Driver in Designer,” on page 157](#)
- ♦ [Section 10.2, “Exporting the Driver in iManager,” on page 157](#)

10.1 Exporting the Driver in Designer

- 1 Open a project in Designer, then right-click the driver object.
- 2 Select *Export to Configuration File*.
- 3 Specify a unique name for the configuration file, browse to location where it should be saved, then click *Save*.
- 4 Click *OK* in the Export Configuration Results window.

10.2 Exporting the Driver in iManager

- 1 In iManager, select *Identity Manager > Identity Manager Overview*.
- 2 Browse to and select the driver set object, then click *Search*.
- 3 Click the driver icon.
- 4 Select *Export* in the Identity Manager Driver Overview window.
- 5 Browse to and select the driver object you want to export, then click *Next*.
- 6 Select *Export all policies, linked to the configuration or not* or select *Only export policies that are linked to the configuration*, depending upon the information you want to have stored in the XML file.
- 7 Click *Next*.
- 8 Click *Save As*, then click *Save*.
- 9 Browse and select a location to save the XML file, then click *Save*.
- 10 Click *Finish*.

Security: Best Practices

11

For more information on how to secure the driver and the information it is synchronizing, see “[Security: Best Practices](#)” in the *Novell Identity Manager 3.5.1 Administration Guide*.

Class and Attribute Descriptions

A

The table in this section lists each Novell® eDirectory™ class and attribute used by the Identity Manager Driver for GroupWise®. The Secondary Effects column in the table contains information about how the attribute is used, special handling, conversions, and relationships of the attributes to other attributes.

eDirectory Class or Attribute	GroupWise Attribute	Description	Secondary Effects
NDS User			
	50319	Preferred Internet eMail ID	<p>Example: JohnDoe</p> <p>“mapi” is not allowed because it is reserved.</p> <p>This ID must be unique in the entire GroupWise system. It contains 1 to 256 characters, and cannot contain the () @ . : , { } * ” characters. The ID must be unique within its namespace (UserID, nicknames, resources, and distribution lists share the same namespace.)</p>
	50045	Internet domain name	Example: MyDomain.com
	59028	LDAP authentication ID in typeful format	Example: cn=admin, o=novell
	50013	Preferred Internet address format (numeric value)	<p>0 - Full (Name.PostOffice.Domain@IDomain.com)</p> <p>1 - Host and User ID (Name.PostOffice@IDomain.com)</p> <p>2 - User ID (Name@IDomain.com)</p> <p>3 - Lastname.firstname</p> <p>4 - Firstname.lastname</p> <p>5 - No setting (reserved)</p> <p>6 - First initial and last name</p>
	50320	Disallowed Internet address formats (bit settings)	<p>0 - None</p> <p>1 - Full (never set this bit)</p> <p>2 - Host</p> <p>4 - User ID</p> <p>8 - Lastname.Firstname</p> <p>16 - Firstname.Lastname</p> <p>32 - First initial and last name</p> <p>You should not set bit one in this attribute value. It is an illegal operation to disallow the Full format.</p> <p>You can “or” values together. For instance, to allow only full name you would use a value of 62 (0x3E).</p>
	50157	Exclusive use of Internet domain name	<p>0 = Off (requires setting an Internet domain name: 50045)</p> <p>1 = On (only recognizes the domain name set in the Internet domain name: 50045)</p>

eDirectory Class or Attribute	GroupWise Attribute	Description	Secondary Effects
GroupWise External Entity			
	50319	Preferred Internet eMail ID	<p>Example: JohnDoe</p> <p>“mapi” is not allowed because it is reserved.</p> <p>This ID must be unique in the entire GroupWise system. It contains 1 to 256 characters, and cannot contain the () @ . : , { } * ” characters. The ID must be unique within its namespace (UserID, nicknames, resources, and distribution lists share the same namespace.)</p>
	50045	Internet domain name	Example: MyDomain.com
	59028	LDAP authentication ID in typeful format	Example: cn=admin, o=novell
	50013	Preferred Internet address format (numeric value)	<p>0 - Full (Name.PostOffice.Domain@IDomain.com)</p> <p>1 - Host and User ID (Name.PostOffice@IDomain.com)</p> <p>2 - User ID (Name@IDomain.com)</p> <p>3 - Lastname.firstname</p> <p>4 - Firstname.lastname</p> <p>5 - No setting (reserved)</p> <p>6 - First initial and last name</p>
	50320	Disallowed Internet address formats (bit settings)	<p>0 - None</p> <p>1 - Full (never set this bit)</p> <p>2 - Host</p> <p>4 - User ID</p> <p>8 - Lastname.Firstname</p> <p>16 - Firstname.Lastname</p> <p>32 - First initial and last name</p> <p>You should not set bit one in this attribute value. It is an illegal operation to disallow the Full format.</p> <p>You can “or” values together. For instance, to allow only full name you would use a value of 62 (0x3E).</p>
	50157	Exclusive use of Internet domain name	<p>0 = Off (requires setting an Internet domain name: 50045)</p> <p>1 = On (only recognizes the domain name set in the Internet domain name: 50045)</p>
CN	None	Common Name of a User object	When a GroupWise account is created or renamed, this value is used to name the GroupWise account and to set NGW: Object ID. For all other operations, this value is ignored.
Given Name	50091	User’s first name	Synchronizes from eDirectory to GroupWise on Create and Modify events. See the note at the end of this table for additional information.

eDirectory Class or Attribute	GroupWise Attribute	Description	Secondary Effects
Surname	50093	User's last name	Synchronizes from eDirectory to GroupWise on Create and Modify events. This attribute is only used on the Publisher channel when creating a default user for resource reassignment. See the note at the end of this table for additional information.
Title	50096	User's title	Synchronizes from eDirectory to GroupWise on Create and Modify events. See the note at the end of this table for additional information.
OU	50089	User's department	Synchronizes from eDirectory to GroupWise on Create and Modify events. See the note at the end of this table for additional information.
Telephone Number	50095	User's telephone number	Synchronizes from eDirectory to GroupWise on Create and Modify events. See the note at the end of this table for additional information.
Facsimile Telephone Number	50145	User's facsimile telephone number	Only synchronizes the telephone number portion from eDirectory to GroupWise on Create and Modify events. See the note at the end of this table for additional information.
Description	50032	Provides additional information	Synchronizes from eDirectory to GroupWise on Create and Modify events. See the note at the end of this table for additional information.
company	55022 50310 for GW 6.5 or later	User's company	Synchronizes from eDirectory to GroupWise on Create and Modify events. See the note at the end of this table for additional information.
Initials	55019 50322 for GW 6.5 or later	Middle initials, up to 8 characters	Synchronizes from eDirectory to GroupWise on Create and Modify events. See the note at the end of this table for additional information.
Generational Qualifier	55020 50323 for GW 6.5 or later	Jr., III, and so forth, up to 8 characters	Synchronizes from eDirectory to GroupWise on Create and Modify events. See the note at the end of this table for additional information.
personalTitle	55021 50324 for GW 6.5 or later	Dr., Mr., Ms., and so forth, up to 8 characters	Synchronizes from eDirectory to GroupWise on Create and Modify events. See the note at the end of this table for additional information.

eDirectory Class or Attribute	GroupWise Attribute	Description	Secondary Effects
NGW: Object ID	50073	GW mailbox name. The name must be unique within a post office. The name contains 1 to 256 characters, and cannot contain the ()@.:",{}* characters.	<p>This attribute takes its value from the CN attribute. The shim writes it via the Publisher channel to eDirectory. It is set when an account is created and modified, and when an account is renamed. Modifying this value might cause the following attributes to be modified:</p> <ul style="list-style-type: none"> ◆ Email Address ◆ Internet Email Address ◆ NGW: GroupWise ID ◆ Identity Manager association key <p>This attribute should not be modified except as the result of a rename.</p>
NGW: Account ID	50116	Optional field for accounting. It can contain a cost account used for posting charges to this user.	When an account is created, the shim queries GroupWise for this value and writes it via the Publisher channel to eDirectory. Normally the driver does not set this value. However, this attribute can be set through the Create rule or Create style sheet. See the note at the end of this table for additional information.
NGW: Gateway Access	59001		When an account is created, the shim queries GroupWise for this value and writes it via the Publisher channel to eDirectory. Normally the driver does not set this value. However, this attribute can be set through the Create rule or style sheet. See the note at the end of this table for additional information.
NGW: Mailbox Expiration Time	50138		When an account is created, the shim queries GroupWise for this value and writes it via the Publisher channel to eDirectory. This attribute can be set through the Create rule or style sheet. For example, the default Output Transformation style sheet uses the eDirectory login expiration time to set this value.
Login Disabled	50058	A Boolean value that indicates whether eDirectory login (authentication) is allowed.	Synchronizes from eDirectory to GroupWise on Create and Modify events. The shim converts true to 1 and false to 0. Setting the GroupWise 50058 attributes to 1 disables the GroupWise account. See the note at the end of this table for additional information.
Login Expiration Time	None	Date and time when authentication rights expire.	This eDirectory attribute has no corresponding GroupWise attribute. The value of this attribute is used to set the eDirectory attribute NGW: Mailbox Expiration Time and the GW attribute 50138, which are connected through the Schema Mapping rule.

eDirectory Class or Attribute	GroupWise Attribute	Description	Secondary Effects
NGW: File ID	50038	Three characters used to name system files for the user. The value must be unique within a post office. This value is set by GroupWise.	This attribute is set in GroupWise when an account is created. The shim queries GroupWise for this value and writes it via the Publisher channel to eDirectory. A Move event could cause this attribute to change. This attribute should not be modified in any style sheet.
NGW: GroupWise ID	None	Uniquely identifies an object in GroupWise. This value is used for the Identity Manager association.	<p>When an account is created or modified, the shim queries GroupWise for this value and writes it via the Publisher channel to eDirectory. A GroupWise Move or a Rename event causes this attribute to change. On any Modify event, the shim reads this value through the GroupWise API and, if it has changed, writes it to eDirectory through the Publisher channel. The shim also changes the Identity Manager association value.</p> <p>This attribute only comes through the Subscriber channel when the GroupWise snap-ins change this value. The shim then changes the Identity Manager association key.</p> <p>This value, not the association key, is used to read the GroupWise object. If the association key does not match this attribute value, the association key is updated. This is because the GroupWise snap-ins can change this attribute and the GroupWise snap-ins do not update the association key.</p> <p>On all events, except delete, the shim queries eDirectory for this value. If the value does not exist, the event is discarded.</p> <p>If the shim cannot read the GroupWise object using this value, an error is returned to Identity Manager. This is a rare occurrence.</p>
NGW: Visibility	50076	Visibility is used to specify the databases into which an object should be replicated. Controls whether objects appear in the address book.	This attribute is set in GroupWise by GroupWise when an account is created. The shim queries GroupWise for this value and writes it via the Publisher channel to eDirectory. Normally, the driver does not set this value. However, this attribute can be set through the Create rule or style sheet. To set it, add code to the Create rule. Use 2 for global visibility, or 4 for no visibility. See the note at the end of this table for additional information.
Email Address	None		This attribute is generated by GroupWise on Create, Rename, or Move events. The shim queries GroupWise for this value and writes it via the Publisher channel to eDirectory.

eDirectory Class or Attribute	GroupWise Attribute	Description	Secondary Effects
Internet Email Address	None		This attribute is generated by GroupWise on a Create or Rename event, or when any attributes used to generate Internet Email Address are modified. The shim queries GroupWise for this value and writes it via the Publisher channel to eDirectory.
NGW: Post Office	None	DN of the Post Office object.	The driver writes this on Create and Move events.
Any User attribute whose value can be represented as a string.	50106 to 50115, 55002 to 55011	Up to 20 eDirectory user attributes can be mapped to generic GroupWise attributes and displayed in the address book.	The eDirectory attribute names must be added to the filter. The eDirectory and GroupWise attribute names must be added to the Schema Mapping rule. NOTE: For these attributes to appear in the address book, GroupWise must be configured through ConsoleOne®. See the note at the end of this table for additional information.
GroupWise Post Office Member	None		On a user create, the shim writes the eDirectory DN of the user to this attribute using the Publisher channel. On a post office move, the shim deletes the user DN from the old post office and writes the user DN to the new post office.
GroupWise Resource NGW: Owner	50081	The user (NGW: Object ID) that owns the resource. An owner is identified by its Object Name.	The shim writes this value to GroupWise and to eDirectory via the Publisher channel. The value is provided by a style sheet or driver option. See the note at the end of this table for additional information.
GroupWise Distribution List Member	None		On eDirectory user Create or Modify events, a set of Distribution Lists can be specified. The user can be added as a Member, BC, or CC. The shim fills in this attribute through the Publisher channel. On a modify event, a user can be removed from a specified Distribution List (member, BC or CC) or from all distribution lists (member, BC or CC). The shim removes the user from the appropriate distribution list.
NGW: Blind Copy Member	None		Use the gw:participation="bc" attribute to have the driver set this information. For more information, see "Adding a User as a Blind Copy or Carbon Copy Participant in a Distribution List" on page 52.

eDirectory Class or Attribute	GroupWise Attribute	Description	Secondary Effects
NGW: Carbon Copy Member	None		Use the gw:participation="cc" attribute to have the driver set this information. For more information, see "Adding a User as a Blind Copy or Carbon Copy Participant in a Distribution List" on page 52.

IMPORTANT: When the Visibility GroupWise attribute is explicitly changed by a style sheet, the corresponding eDirectory attribute must also be updated by the style sheet. Otherwise, the eDirectory User and the GroupWise account are not properly synchronized.

For this attribute, eDirectory is considered the authoritative data source. When the attributes are not synchronized, it is possible that the old value in eDirectory could be used to incorrectly update the correct value in the GroupWise account. Updating the corresponding attribute in eDirectory can prevent this. In the example XSLT code segment below, when an eDirectory User is disabled, the GroupWise account is disabled and the visibility attribute is set to 4. This prevents the account from appearing in the address book. The visibility attribute (50076) is set in GroupWise, together with the disable. The visibility attribute (NGW: Visibility) is set in eDirectory using the channel write-back Identity Manager functionality.

XSLT

```
<!-- User Disable, Remove Address Book Visibility
When a GroupWise Account is Disabled
remove the account from the address book visibility.
Keep eDirectory and GroupWise object synchronized by
updating the attributes in both systems.
-->
<xsl:template match="modify-attr[@attr-name='50058']">
  <!-- When Login Disabled is true -->
  <xsl:if test="add-value//value[.='true']">
    <!-- Update the visibility attribute in GroupWise -->
    <!-- Copy the <modify> through to update GroupWise -->
    <xsl:copy>
      <!-- copy everything through -->
      <xsl:apply-templates select="@*|node()"/>
    </xsl:copy>
    <!-- Set the GroupWise visibility attribute (50076) to "4"
so the account does not show in the address book -->
    <modify-attr attr-name="50076">
      <remove-all-values/>
      <add-value>
        <value type="int">4</value>
      </add-value>
    </modify-attr>
    <!-- Update the visibility attribute in eDirectory -->
    <!-- Send a command to modify "NGW: Visibility" in the eDirectory
User object -->
    <xsl:variable name="command">
      <modify class-name="User">
        <!-- dest-dn and dest-entry-id identify the User
object in eDirectory -->
        <xsl:attribute name="dest-dn">
          <xsl:value-of select="../@src-dn"/>
        </xsl:attribute>
      </modify>
    </xsl:variable>
  </xsl:if>
</xsl:template>
```

```

        </xsl:attribute>
        <xsl:attribute name="dest-entry-id">
            <xsl:value-of select="../@src-entry-id"/>
        </xsl:attribute>
        <!-- Set NGW: Visibility (50076) in eDirectory to
"4" -->
            <modify-attr attr-name="NGW: Visibility">
                <remove-all-values/>
                <add-value>
                    <value type="int">4</value>
                </add-value>
            </modify-attr>
        </modify>
    </xsl:variable>
    <xsl:variable name="result"
select="cmd:execute($srcCommandProcessor, $command)"/>
    </xsl:if>
</xsl:template>

```

DirXML Script

For use in an Output Transformation policy.

```

<rule>
  <description>Adjust GW Visibility when 'Login Disabled' (50058) is changing
to TRUE</description>
  <conditions>
    <and>
      <if-op-attr mode="case" name="50058" op="changing-to">>true</if-op-attr>
      <if-class-name op="equal">User</if-class-name>
    </and>
  </conditions>
  <actions>
    <!-- Set the GroupWise visibility attribute (50076) to "4" so the account
does not show in the GW address book -->
    <do-set-dest-attr-value class-name="User" name="50076">
      <arg-value type="string">
        <token-text xml:space="preserve">4</token-text>
      </arg-value>
    </do-set-dest-attr-value>
    <!-- Update the visibility attribute in eDirectory -->
    <!-- Send a command to modify "NGW: Visibility" in the eDirectory User
object -->
    <do-set-src-attr-value class-name="User" name="NGW: Visibility">
      <arg-value type="string">
        <token-text xml:space="preserve">4</token-text>
      </arg-value>
    </do-set-src-attr-value>
  </actions>
</rule>
<rule>
  <description>Adjust GW Visibility when 'Login Disabled' (50058) is changing
to FALSE</description>
  <conditions>
    <and>
      <if-op-attr mode="case" name="50058" op="changing-to">>false</if-op-attr>
      <if-class-name op="equal">User</if-class-name>
    </and>

```



```

</conditions>
<actions>
  <!-- Set the GroupWise visibility attribute (50076) to "2" so the account
shows in the GW address book -->
  <do-set-dest-attr-value class-name="User" name="50076">
    <arg-value type="string">
      <!-- Post Office -->
      <!-- <token-text xml:space="preserve">1</token-text> -->
      <!-- System -->
      <token-text xml:space="preserve">2</token-text>
      <!-- Domain -->
      <!-- <token-text xml:space="preserve">3</token-text> -->
      <!-- None -->
      <!-- <token-text xml:space="preserve">4</token-text> -->
    </arg-value>
  </do-set-dest-attr-value>
  <!-- Update the visibility attribute in eDirectory -->
  <!-- Send a command to modify "NGW: Visibility" in the eDirectory User
object -->
  <do-set-src-attr-value class-name="User" name="NGW: Visibility">
    <arg-value type="string">
      <!-- Post Office -->
      <!-- <token-text xml:space="preserve">1</token-text> -->
      <!-- System -->
      <token-text xml:space="preserve">2</token-text>
      <!-- Domain -->
      <!-- <token-text xml:space="preserve">3</token-text> -->
      <!-- None -->
      <!-- <token-text xml:space="preserve">4</token-text> -->
    </arg-value>
  </do-set-src-attr-value>
</actions>
</rule>

```


DirXML Command Line Utility

B

The DirXML[®] Command Line utility allows you to use a command line interface to manage the driver. You can create scripts to manage the driver with the commands.

The utility and scripts are installed on all platforms during the Identity Manager installation. The utility is installed to the following locations:

- ♦ Windows: `\Novell\Nds\dxcmd.bat`
- ♦ NetWare[®]: `sys:\system\dxcmd.ncf`
- ♦ UNIX: `/usr/bin/dxcmd`

There are two different methods for using the DirXML Command Line utility:

- ♦ [Section B.1, “Interactive Mode,” on page 171](#)
- ♦ [Section B.2, “Command Line Mode,” on page 180](#)

B.1 Interactive Mode

The interactive mode provides a text interface to control and use the DirXML Command Line utility.

- 1 At the console, enter `dxcmd`.
- 2 Enter the name of a user with sufficient rights to the Identity Manager objects, such as `admin.novell`.
- 3 Enter the user’s password.

```
DirXML commands
1: Start driver
2: Stop driver
3: Driver operations...
4: Driver set operations...
5: Log events operations...
6: Get DirXML version
7: Job operations...
99: Quit
Enter choice:
```

- 4 Enter the number of the command you want to perform.
[Table B-1 on page 172](#) contains the list of options and what functionality is available.
- 5 Enter 99 to quit the utility.

NOTE: If you are running eDirectory™ 8.8 on UNIX or Linux, you must specify the `-host` and `-port` parameters. For example, `dxcmd -host 10.0.0.1 -port 524`. If the parameters are not specified, a `jclient` error occurs:

```
novell.jclient.JCException: connect (to address) 111 UNKNOWN ERROR
```

By default, eDirectory 8.8 is not listening to localhost. The DirXML Command Line utility needs to resolve the server IP address or hostname and the port to be able to authenticate.

Table B-1 *Interactive Mode Options*

Option	Description
1: <i>Start Driver</i>	Starts the driver. If there is more than one driver, each driver is listed with a number. Enter the number of the driver to start the driver.
2: <i>Stop Driver</i>	Stops the driver. If there is more than one driver, each driver is listed with a number. Enter the number of the driver to stop the driver.
3: <i>Driver operations</i>	Lists the operations available for the driver. If there is more than one driver, each driver is listed with a number. Enter the number of the driver to see the operations available. See Table B-2 on page 173 for a list of operations.
4: <i>Driver set operations</i>	Lists the operations available for the driver set. <ul style="list-style-type: none">◆ 1: Associate driver set with server◆ 2: Disassociate driver set from server◆ 99: Exit
5: <i>Log events operations</i>	Lists the operations available for logging events through Novell® Audit. See Table B-5 on page 177 for a description of these options.
6: <i>Get DirXML version</i>	Lists the version of the Identity Manager installed.
7: <i>Job operations</i>	Manages jobs created for Identity Manager.
99: <i>Quit</i>	Exits the DirXML Command Line utility

Figure B-1 *Driver Options*

```
Select a driver operation for:
Active Directory.Driver Set.Novell.IDMDESIGNTREE.

1: Start driver
2: Stop driver
3: Get driver state
4: Get driver start option
5: Set driver start option
6: Resync driver
7: Migrate from application into DirXML
8: Submit XDS command document to driver
9: Submit XDS event document to driver
10: Queue event for driver
11: Check object password
12: Initialize new driver object
13: Passwords operations
14: Cache operations
99: Exit

Enter choice:
```

Table B-2 *Driver Options*

Options	Description
1: <i>Start driver</i>	Starts the driver.
2: <i>Stop driver</i>	Stops the driver.
3: <i>Get driver state</i>	Lists the state of the driver. <ul style="list-style-type: none">◆ 0 - Driver is stopped◆ 1 - Driver is starting◆ 2 - Driver is running◆ 3 - Driver is stopping
4: <i>Get driver start option</i>	Lists the current driver start option. <ul style="list-style-type: none">◆ 1 - Disabled◆ 2 - Manual◆ 3 - Auto
5: <i>Set driver start option</i>	Changes the start option of the driver. <ul style="list-style-type: none">◆ 1 - Disabled◆ 2 - Manual◆ 3 - Auto◆ 99 - Exit
6: <i>Resync driver</i>	<p>Forces a resynchronization of the driver. It prompts for a time delay: <i>Do you want to specify a minimum time for resync? (yes/no)</i>.</p> <p>If you enter Yes, specify the date and time you want the resynchronization to occur: <i>Enter a date/time (format 9/27/05 3:27 PM)</i>.</p> <p>If you enter No, the resynchronization occurs immediately.</p>
7: <i>Migrate from application into DirXML</i>	<p>Processes an XML document that contains a query command: <i>Enter filename of XDS query document:</i></p> <p>Create the XML document that contains a query command by using the Novell nds.dtd (http://developer.novell.com/ndk/doc/dirxml/dirxmlbk/ref/ndsstdtd/query.html).</p> <p>Examples:</p> <p>NetWare: <code>sys:\files\query.xml</code></p> <p>Windows: <code>c:\files\query.xml</code></p> <p>Linux: <code>/files/query.xml</code></p>

Options	Description
8: <i>Submit XDS command document to driver</i>	<p>Processes an XDS command document:</p> <p><i>Enter filename of XDS command document:</i></p> <p>Examples:</p> <p>NetWare: <code>sys:\files\user.xml</code></p> <p>Windows: <code>c:\files\user.xml</code></p> <p>Linux: <code>/files/user.xml</code></p> <p><i>Enter name of file for response:</i></p> <p>Examples:</p> <p>NetWare: <code>sys:\files\user.log</code></p> <p>Windows: <code>c:\files\user.log</code></p> <p>Linux: <code>/files/user.log</code></p>
9: <i>Submit XDS event document to driver</i>	<p>Processes an XDS event document:</p> <p><i>Enter filename of XDS event document:</i></p> <p>Examples:</p> <p>NetWare: <code>sys:\files\add.xml</code></p> <p>Windows: <code>c:\files\add.xml</code></p> <p>Linux: <code>/files/add.xml</code></p>
10: <i>Queue event for driver</i>	<p>Adds an event to the driver queue:</p> <p><i>Enter filename of XDS event document:</i></p> <p>Examples:</p> <p>NetWare: <code>sys:\files\add.xml</code></p> <p>Windows: <code>c:\files\add.xml</code></p> <p>Linux: <code>/files/add.xml</code></p>
11: <i>Check object password</i>	<p>Validates that an object's password in the connected system is associated with a driver. It matches the object's eDirectory password (Distribution Password, used with Universal Password).</p> <p><i>Enter user name:</i></p>
12: <i>Initialize new driver object</i>	<p>Performs an internal initialization of data on a new Driver object. This is only for testing purposes.</p>
13: <i>Password operations</i>	<p>There are nine Password options. See Table B-3 on page 175 for a description of these options.</p>
14: <i>Cache operations</i>	<p>There are five Cache operations. See Table B-4 on page 176 for a description of these options.</p>

Options	Description
99: <i>Exit</i>	Exits the driver options.

Figure B-2 Password Operations

```

Select a password operation

1: Set shim password
2: Clear shim password
3: Set Remote Loader password
4: Clear Remote Loader password
5: Set named password
6: Clear named password(s)
7: List named passwords
8: Get passwords state
99: Exit

Enter choice:

```

Table B-3 Password Operations

Operation	Description
1: <i>Set shim password</i>	Sets the application password. This is the password of the user account you are using to authenticate into the connected system with.
2: <i>Clear shim password</i>	Clears the application password.
3: <i>Set Remote Loader password</i>	The Remote Loader password is used to control access to the Remote Loader instance. Enter the Remote Loader password, then confirm the password by typing it again.
4: <i>Clear Remote Loader password</i>	Clears the Remote Loader password so no Remote Loader password is set on the Driver object.
5: <i>Set named password</i>	Allows you to store a password or other pieces of security information on the driver. See Section 7.16, "Storing Driver Passwords Securely with Named Passwords," on page 126 for more information. There are four prompts to fill in: <ul style="list-style-type: none"> ◆ <i>Enter password name:</i> ◆ <i>Enter password description:</i> ◆ <i>Enter password:</i> ◆ <i>Confirm password:</i>

Operation	Description
6: <i>Clear named passwords</i>	<p>Clears a specified Named Password or all Named Passwords that are stored on the driver object.</p> <p><i>Do you want to clear all named passwords? (yes/no).</i></p> <p>If you enter Yes, all Named Passwords are cleared. If you enter No, you are prompted to specify the password name that you want to clear.</p>
7: <i>List named passwords</i>	Lists all Named Passwords that are stored on the driver object. It lists the password name and the password description.
8: <i>Get password state</i>	<p>Lists if a password is set for:</p> <ul style="list-style-type: none"> ◆ Driver Object password ◆ Application password ◆ Remote loader password <p>The dxcmd utility allows you to set the Application password and the Remote Loader password. You cannot set the Driver Object password with this utility. It shows if the password has been set or not.</p>
99: <i>Exit</i>	Exits the current menu and takes you back to the Driver options.

Figure B-3 *Cache Operations*

```

Enter choice: 14

Select a cache operation

1: Get driver cache limit
2: Set driver cache limit
3: View cached transactions
4: Delete cached transactions
99: Exit

Enter choice:

```

Table B-4 *Cache Operations*

Operation	Description
1: <i>Get driver cache limit</i>	Displays the current cache limit that is set for the driver.
2: <i>Set driver cache limit</i>	Sets the driver cache limit in kilobytes. A value of 0 is unlimited.

Operation	Description
3: <i>View cached transactions</i>	<p>A text file is created with the events that are stored in cache. You can select the number of transactions to view.</p> <ul style="list-style-type: none"> ◆ <i>Enter option token (default=0):</i> ◆ <i>Enter maximum transactions records to return (default=1):</i> ◆ <i>Enter name of file for response:</i>
4: <i>Delete cached transactions</i>	<p>Deletes the transactions stored in cache.</p> <ul style="list-style-type: none"> ◆ <i>Enter position token (default=0):</i> ◆ <i>Enter event-id value of first transaction record to delete (optional):</i> ◆ <i>Enter number of transaction records to delete (default=1):</i>
99: <i>Exit</i>	Exits the current menu and takes you back to the Driver options.

Figure B-4 Log Event Operations

```
Select a log events operation
1: Set driver set log events
2: Reset driver set log events
3: Set driver log events
4: Reset driver log events
99: Exit
Enter choice:
```

Table B-5 Log Events Operations

Operation	Description
1: <i>Set driver set log events</i>	<p>Allows you to log driver set events through Novell Audit. There are 49 items you can select to log. See Table B-6 on page 178 for a list of these options.</p> <p>Type the number of the item you want to log. After the items are selected, enter 99 to accept the selections.</p>
2: <i>Reset driver set log events</i>	Resets all of the log event options.
3: <i>Set driver log events</i>	<p>Allows you to log driver events through Novell Audit. There are 49 items to select to log. See Table B-6 on page 178 for a list of these options.</p> <p>Type the number of the item you want to log. After the items are selected, enter 99 to accept the selections.</p>

Operation	Description
4: <i>Reset driver log events</i>	Resets all of the log event options.
99: <i>Exit</i>	Exits the log events operations menu.

Table B-6 *Driver Set and Driver Log Events*

Options

- 1: Status success
 - 2: Status retry
 - 3: Status warning
 - 4: Status error
 - 5: Status fatal
 - 6: Status other
 - 7: Query elements
 - 8: Add elements
 - 9: Remove elements
 - 10: Modify elements
 - 11: Rename elements
 - 12: Move elements
 - 13: Add-association elements
 - 14: Remove-association elements
 - 15: Query-schema elements
 - 16: Check-password elements
 - 17: Check-object-password elements
 - 18: Modify-password elements
 - 19: Sync elements
 - 20: Pre-transformed XDS document from shim
 - 21: Post input transformation XDS document
 - 22: Post output transformation XDS document
 - 23: Post event transformation XDS document
 - 24: Post placement transformation XDS document
 - 25: Post create transformation XDS document
 - 26: Post mapping transformation <inbound> XDS document
 - 27: Post mapping transformation <outbound> XDS document
-

Options

- 28: Post matching transformation XDS document
 - 29: Post command transformation XDS document
 - 30: Post-filtered XDS document <Publisher>
 - 31: User agent XDS command document
 - 32: Driver resync request
 - 33: Driver migrate from application
 - 34: Driver start
 - 35: Driver stop
 - 36: Password sync
 - 37: Password request
 - 38: Engine error
 - 39: Engine warning
 - 40: Add attribute
 - 41: Clear attribute
 - 42: Add value
 - 43: Remove value
 - 44: Merge entire
 - 45: Get named password
 - 46: Reset Attributes
 - 47: Add Value - Add Entry
 - 48: Set SSO Credential
 - 49: Clear SSO Credential
 - 50: Set SSO Passphrase
 - 51: User defined IDs
 - 99: Accept checked items
-

Table B-7 Enter Table Title Here

Options	Description
1: <i>Get available job definitions</i>	Allows you to select an existing job. <i>Enter the job number:</i> <i>Do you want to filter the job definitions by containment? Enter Yes or No</i> <i>Enter name of the file for response:</i> Examples: NetWare: <code>sys:\files\user.log</code> Windows: <code>c:\files\user.log</code> Linux: <code>/files/user.log</code>
2: <i>Operations on specific job object</i>	Allows you to perform operations for a specific job.

B.2 Command Line Mode

The command line mode allows you to use script or batch files. [Table B-8 on page 180](#) lists the different options that are available.

To use the command line options, decide which items you want to use and string them together.

Example: `dxcmd -user admin.headquarters -host 10.0.0.1 -password n0vell -start test.driverset.headquarters`

This example command starts the driver.

Table B-8 Command Line Options

Option	Description
Configuration	
<code>-user <user name></code>	Specify the name of a user with administrative rights to the drivers you want to test.
<code>-host <name or IP address></code>	Specify the IP address of the server where the driver is installed.
<code>-password <user password></code>	Specify the password of the user specified above.
<code>-port <port number></code>	Specify a port number, if the default port is not used.
<code>-q <quiet mode></code>	Displays very little information when a command is executed.
<code>-v <verbose mode></code>	Displays detailed information when a command is executed.

Option	Description
-s <stdout>	Writes the results of the <code>dxcmd</code> command to <code>stdout</code> .
-? <show this message>	Displays the help menu.
-help <show this message>	Displays the help menu.
Actions	
-start <driver dn>	Starts the driver.
-stop <driver dn>	Stops the driver.
-getstate <driver dn>	Shows the state of the driver as running or stopped.
-getstartoption <driver dn>	Shows the startup option of the driver.
-setstartoption <driver dn> <disabled manual auto> <resync noresync>	Sets how the driver starts if the server is rebooted. Sets whether the objects are to be resynchronized when the driver restarts.
-getcachelimit <driver dn>	Lists the cache limit set for the driver.
-setcachelimit <driver dn> <0 or positive integer>	Sets the cache limit for the driver.
-migrateapp <driver dn> <filename>	Processes an XML document that contains a query command. Create the XML document that contains a query command by using the Novell <code>nds.dtd</code> (http://www.novell.com/documentation/idm35/index.html?page=/documentation/idm35/policy_dtd/data/dtdndsoverview.html#dtdndsoverview).
-setshimpassword <driver dn> <password>	Sets the application password. This is the password of the user account you are using to authenticate into the connected system with.
-clearshimpassword <driver dn> <password>	Clears the application password.
-setremoteloaderpassword <driver dn> <password>	Sets the Remote Loader password. The Remote Loader password is used to control access to the Remote Loader instance.
<clearremoteloaderpassword <driver dn>	Clears the Remote Loader password.

Option	Description
-sendcommand <driver dn> <input filename> <output filename>	<p>Processes an XDS command document.</p> <p>Specify the XDS command document as the input file.</p> <p>Examples:</p> <p>NetWare: sys:\files\user.xml</p> <p>Windows: c:\files\user.xml</p> <p>Linux: /files/user.log</p> <p>Specify the output filename to see the results.</p> <p>Examples:</p> <p>NetWare: sys:\files\user.log</p> <p>Windows: c:\files\user.log</p> <p>Linux: /files/user.log</p>
-sendevent <driver dn> <input filename>	<p>Submits a document to the driver's Subscriber channel, bypassing the driver cache. The document is processed ahead of anything that might be in the cache at the time of the submission. It also means that the submission fails if the driver is not running.</p>
-queueevent <driver dn> <input filename>	<p>Submits a document to the driver's Subscriber channel by queuing the document in the driver cache. The document gets processed after anything that might be in the cache at the time of the submission. The submission won't fail if the driver isn't running.</p>
-setlogevents <dn> <integer ...>	<p>Sets Novell Audit log events on the driver. The integer is the option of the item to log. See Table B-6 on page 178 for the list of the integers to enter.</p>
-clearlogevents <dn>	<p>Clears all Novell Audit log events that are set on the driver.</p>
-setdriverset <driver set dn>	<p>Associates a driver set with the server.</p>
-cleardriverset	<p>Clears the driver set association from the server.</p>
-getversion	<p>Shows the version of Identity Manager that is installed.</p>
-initdriver object <dn>	<p>Performs an internal initialization of data on a new Driver object. This is only for testing purposes.</p>
-setnamedpassword <driver dn> <name> <password> [description]	<p>Sets Named Passwords on the driver object. You specify the name, the password, and the description of the Named Password.</p>
-clearnamedpassword <driver dn> <name>	<p>Clears a specified Named Password.</p>
-startjob <job dn>	<p>Starts the specified job.</p>

Option	Description
-abortjob <job dn>	Aborts the specified job.
-getjobrunningstate <job dn>	Returns the specified job's running state.
-getjobenabledstate <job dn>	Returns the specified job's enabled state.
-getjobnextruntime <job dn>	Returns the specified job's next run time.
-updatejob <job dn>	Updates the specified job.
-clearallnamedpasswords <driver dn>	Clears all Named Passwords set on a specific driver.

If a command line is executed successfully, it returns a zero. If the command line returns anything other than zero, it is an error. For example 0 means success, and -641 means invalid operation. -641 is an eDirectory error code. [Table B-9 on page 183](#) contains other values for specific command line options.

Table B-9 *Command Line Option Values*


Command Line Option	Values
-getstate	0- stopped 1- starting 2- running 3- shutting down 11- get schema Anything else that is returned is an error.
-getstartoption	0- disabled 1- manual 2- auto Anything else that is returned is an error.
-getcachelimit	0- unlimited Anything else that is returned is an error.
-getjobrunningstate	0- stopped 1- running Anything else that is returned is an error.
-getjobenabledstate	0- disabled 1- enabled 2- configuration error Anything else that is returned is an error.

Command Line Option	Values
-getjobnextruntime	Return is the next scheduled time for the job in eDirectory time format (number of seconds since 00:00:00 Jan 1, 1970 UTC).

Properties of the Driver

C

There are many different fields and values for the driver. Sometimes the information is displayed differently in iManager than in Designer. This section is a reference for all of the fields on the driver as displayed in iManager and Designer.

The information is presented from the viewpoint of iManager. If a field is different in Designer, it is marked with an  icon.

- ◆ [Section C.1, “Driver Configuration,” on page 185](#)
- ◆ [Section C.2, “Global Configuration Values,” on page 190](#)
- ◆ [Section C.3, “Named Passwords,” on page 195](#)
- ◆ [Section C.4, “Engine Control Values,” on page 196](#)
- ◆ [Section C.5, “Log Level,” on page 198](#)
- ◆ [Section C.6, “Driver Image,” on page 199](#)
- ◆ [Section C.7, “Security Equals,” on page 199](#)
- ◆ [Section C.8, “Filter,” on page 200](#)
- ◆ [Section C.9, “Edit Filter XML,” on page 200](#)
- ◆ [Section C.10, “Misc,” on page 201](#)
- ◆ [Section C.11, “Excluded Users,” on page 201](#)
- ◆ [Section C.12, “Driver Manifest,” on page 202](#)
- ◆ [Section C.13, “Driver Inspector,” on page 202](#)
- ◆ [Section C.14, “Driver Cache Inspector,” on page 203](#)
- ◆ [Section C.15, “Inspector,” on page 203](#)
- ◆ [Section C.16, “Server Variables,” on page 204](#)

C.1 Driver Configuration

In iManager:

- 1 Click *Identity Manager > Identity Manager Overview*, then click *Search* to search for the driver set that is associated with the driver.
- 2 Browse to the driver, then click the upper right corner of the driver icon.
- 3 Click *Edit Properties > Driver Configuration*.

In Designer:

- 1 Open a project in the Modeler, then right-click the driver line and click *Properties > Driver Configuration*.

There are different sections under *Driver Configuration*. In this document, each section is listed in a table. The table contains a description of the fields, and the default value or an example of the value that should be specified in the field.

C.1.1 Driver Module

The driver module changes the driver from running locally to running remotely or the reverse.



In iManager:

- 1 Click *Identity Manager > Identity Manager Overview*, then click *Search* to search for the driver set that is associated with the driver.
- 2 Browse to the driver, then click the upper right corner of the driver icon.
- 3 Click *Edit Properties > Driver Configuration > Driver Module*.
See [Table C-1](#) for a list of the driver module options.

In Designer:

- 1 Open a project in the Modeler, then right-click the driver line and select *Properties > Driver Configuration*.
- 2 Select the *Driver Module* tab.
See [Table C-1](#) for a list of the driver module options.

Table C-1 *Driver Modules*

Option	Description
<i>Java</i>	Used to specify the name of the Java class that is instantiated for the shim component of the driver. This class can be located in the <code>classes</code> directory as a class file, or in the <code>lib</code> directory as a <code>.jar</code> file. If this option is selected, the driver is running locally.
<i>Native</i>	Used to specify the name of the <code>.dll</code> file that is instantiated for the application shim component of the driver. If this option is selected, the driver is running locally.
<i>Connect to Remote Loader</i>	Used when the driver is connecting remotely to the connected system.
 Remote Loader Client Configuration for Documentation	 Includes the Remote Loader client configuration information in the driver documentation that is generated by Designer.

C.1.2 Driver Object Password

In iManager:

- 1 Click *Identity Manager > Identity Manager Overview*, then click *Search* to search for the driver set that is associated with the driver.
- 2 Browse to the driver, then click the upper right corner of the driver icon.
- 3 Click *Edit Properties > Driver Configuration > Driver Object Password > Set Password*.
See [Table C-2](#) for more information.

In Designer:

- 1 Open a project in the Modeler, then right-click the driver line and click *Properties > Driver Configuration*.
- 2 Click *Driver Module > Connect to Remote Loader > Driver Object Password > Set Password*.
See [Table C-2](#) for more information.

Table C-2 *Driver Object Password*

Option	Description
<i>Driver Object Password</i>	Use this option to set a password for the driver object. If you are using the Remote Loader, you must enter a password on this page or the remote driver does not run. This password is used by the Remote Loader to authenticate itself to the remote driver shim.

C.1.3 Authentication

The authentication section stores the information required to authenticate to the connected system.



In iManager:









- 1 Click *Identity Manager > Identity Manager Overview*, then click *Search* to search for the driver set that is associated with the driver.
- 2 Browse to the driver, then click the upper right corner of the driver icon.
- 3 Click *Edit Properties > Driver Configuration > Authentication*.
See [Table C-3](#) for a list of the authentication parameters.

In Designer:

- 1 Open a project in the Modeler, then right-click the driver line and select *Properties > Driver Configuration*.
- 2 Click *Authentication*.
See [Table C-3](#) for a list of the authentication parameters.

Table C-3 *Authentication Parameters*

Option	Description
<i>Authentication ID</i> or  <i>User ID</i>	Specify a user application ID. This ID is used to pass Identity Vault subscription information to the application. Example: Administrator
<i>Authentication Context</i> or  <i>Connection Information</i>	Specify the IP address or name of the server the application shim should communicate with.

Option	Description
<i>Remote Loader Connection Parameters</i> or  <i>Host name</i>  <i>Port</i>  <i>KMO</i>  <i>Other parameters</i>	Used only if the driver is connecting to the application through the Remote Loader. The parameter to enter is <code>hostname=xxx.xxx.xxx.xxx port=xxxx</code> <code>kmo=certificatename</code> , when the host name is the IP address of the application server running the Remote Loader server and the port is the port the Remote Loader is listening on. The default port for the Remote Loader is 8090. The <code>kmo</code> entry is optional. It is only used when there is an SSL connection between the Remote Loader and the Metadirectory engine. Example: <code>hostname=10.0.0.1 port=8090</code> <code>kmo=IDMCertificate</code>
<i>Driver Cache Limit (kilobytes)</i> or  <i>Cache limit (KB)</i>	Specify the maximum event cache file size (in KB). If it is set to zero, the file size is unlimited.  Click <i>Unlimited</i> to set the file size to unlimited in Designer.
<i>Application Password</i> or  <i>Set Password</i>	Specify the password for the user object listed in the <i>Authentication ID</i> field.
<i>Remote Loader Password</i> or  <i>Set Password</i>	Used only if the driver is connecting to the application through the Remote Loader. The password is used to control access to the Remote Loader instance. It must be the same password specified during the configuration of the Remote Loader on the connected system.

C.1.4 Startup Option

The Startup Option allows you to set the driver state when the Identity Manager server is started.


In iManager:

- 1 Click *Identity Manager > Identity Manager Overview*, then click *Search* to search for the driver set that is associated with the driver.
- 2 Browse to the driver, then click the upper right corner of the driver icon.
- 3 Click *Edit Properties > Driver Configuration > Startup Option*.
See [Table C-4](#) for a list of the startup options.

In Designer:

- 1 Open a project in the Modeler, then right-click the driver line and select *Properties > Driver Configuration*.
- 2 Click *Startup Option*.
See [Table C-4](#) for a list of the startup options.

Table C-4 *Startup Options*

Option	Description
<i>Auto start</i>	The driver starts every time the Identity Manager server is started.
<i>Manual</i>	The driver does not start when the Identity Manager server is started. The driver must be started through Designer or iManager.
<i>Disabled</i>	The driver has a cache file that stores all of the events. When the driver is set to Disabled, this file is deleted and no new events are stored in the file until the driver state is changed to Manual or Auto Start.
 <i>Do not automatically synchronize the driver</i>	This option only applies if the driver is deployed and was previously disabled. If this is not selected, the driver re-synchronizes the next time it is started.

C.1.5 Driver Parameters

In iManager:

- 1 Click *Identity Manager > Identity Manager Overview*, then click *Search* to search for the driver set that is associated with the driver.
- 2 Browse to the driver, then click the upper right corner of the driver icon.
- 3 Click *Edit Properties > Driver Configuration > Driver Parameters*.
See [Table C-5 on page 189](#) for a list of the driver parameters.

In Designer:

- 1 Open a project in the Modeler, then right-click the driver line and select *Properties > Driver Configuration*.
- 2 Click *Driver Parameters*.
See [Table C-5 on page 189](#) for a list of the driver parameters.

Table C-5 *GroupWise Driver Parameters*

Parameter	Description
Driver Settings	
<i>Domain Server</i>	Specify the name or IP address of the server containing the GroupWise domain database (<code>wpdomain.db</code>). Using the primary domain database is recommended. Leave this field blank when the GroupWise domain database is on the same physical server as this driver. You can use the hostname, DNS name or IP address of the server.

Parameter	Description
<i>Domain Path</i>	<p>Enter the path to the directory containing the GroupWise domain database (<code>wpdomain.db</code>). Using the primary domain database is recommended. The domain path format is different depending upon where the domain is running:</p> <ul style="list-style-type: none"> ◆ Driver running locally on NetWare: <code>volume:\Novell\GroupWise\Domain</code> ◆ Driver running remotely on Windows and the GroupWise domain is on a NetWare server: <code>volume\Novell\GroupWise\Domain</code> ◆ Driver running locally or remotely on Windows: <code>c\$\Novell\GroupWise\Domain</code> ◆ Driver running on Linux: <code>\Novell\GroupWise\Domain</code>
<i>Enforce Admin Lockout Setting</i>	<p>Enforces the Minimum Snap-in Release Version and the Minimum Snap-in Release Date set in the Admin Lockout Settings tab of System Preferences in ConsoleOne. If the domain to which the driver connects has overridden these settings, they are used. This means the GroupWise driver must be running with GroupWise support files equal to or later than these settings. Select <i>True</i> to enable this lockout setting, or select <i>False</i> to disable this lockout setting.</p>
<i>Create Nicknames</i>	<p>Select <i>True</i> if you want the driver to create GroupWise Nicknames when GroupWise accounts are renamed or moved to another post office.</p>
<i>Reassign Resource Ownership</i>	<p>Select <i>True</i> if you want the driver to reassign ownership of resources when the GroupWise accounts are disabled or expired.</p>
<i>Default Resource Owner User ID</i>	<p>Specify the default user who becomes the new owner of resources that are reassigned.</p>
<i>GroupWise Domain Database version</i>	<p>Specify the version of the GroupWise Domain database version the driver connects to. The options are:</p> <ul style="list-style-type: none"> ◆ <i>GroupWise 7</i> ◆ <i>GroupWise 6.5</i> ◆ <i>GroupWise 6.0</i> ◆ <i>GroupWise 5.5</i>
<i>Cleanup Group Membership</i>	<p>Cleans up eDirectory Group memberships when removing a user from all GroupWise Distribution Lists. Select <i>True</i> or <i>False</i>.</p>
Publisher Settings	
<i>Publisher Heartbeat Interval</i>	<p>Specifies the Publisher channel heartbeat interval in minutes. Specify 0 to disable the heartbeat.</p>

C.2 Global Configuration Values

Global configuration values (GCVs) allow you to specify settings for the Identity Manager features such as password synchronization and driver heartbeat, as well as settings that are specific to the function of an individual driver configuration. Some GCVs are provided with the drivers, but you can also add your own.

Global configuration values can be specified for a driver set as well as an individual driver. If a driver does not have a GCV value, the driver inherits the value for that GCV from the driver set.

In iManager:

- 1 Click *Identity Manager > Identity Manager Overview*, then click *Search* to search for the driver set that is associated with the driver.
- 2 Browse to the driver, then click the upper right corner of the driver icon.
- 3 Click *Edit Properties > Global Config Values*.

See [Table C-6 on page 191](#) for a list of the global configuration values.

In Designer:

- 1 Open a project in the Modeler, then right-click the driver line, then select *Properties > Global Config Values*.

See [Table C-6 on page 191](#) for a list of the global configuration values.

Table C-6 *Global Configuration Values > Driver Configuration*

GCV Name	Description
<i>GroupWise Domain Database Version</i>	The version of the GroupWise domain database to which this driver should connect. <ul style="list-style-type: none"> ◆ <i>GroupWise 7</i> ◆ <i>GroupWise 6.5</i> ◆ <i>GroupWise 6.0</i> ◆ <i>GroupWise 5.5</i>
<i>Default Sync Source: eDir Container/Subtree</i>	Specify the eDirectory container in which object changes are detected and synchronized. Synchronization occurs for objects subordinate to the specified source location. Object events occurring outside of the specified subtree are vetoed by the driver. Specify the entire eDirectory tree [root] with a backslash if you want all containers within the tree to be monitored for synchronization.
<i>Default Sync Destination: GroupWise PostOffice</i>	Specify the GroupWise Post Office in which newly added eDirectory objects are created. Use the browse button to select the GroupWise Post Office or specify the GroupWise Post Office name as an eDirectory Distinguished Name (DN) in slash format. For example: <code>GW\GWSystem\PO1</code> .
<i>Enforce Admin Lockout Setting</i>	Enforces the Minimum Snap-in Release Version and Minimum Snap-in Release Date set in the <i>Admin Lockout Settings</i> tab of System Preferences in ConsoleOne. If the domain to which the driver connects has overridden these settings, they are used. This means the GroupWise driver must be running with GroupWise support files equal to or later than these settings. Normally, it is set to <i>True</i> . You might need to set it to <i>False</i> , if the GroupWise support pack is installed and ConsoleOne is configured to lock out previous versions. <i>True</i> enforces this lockout setting. <i>False</i> disables this lockout setting.
<i>Synchronize Groups</i>	Allows the driver to synchronize eDirectory groups to GroupWise distribution lists. <i>True</i> enables the synchronization. <i>False</i> disables the synchronization.

GCV Name	Description
<i>Cleanup Group Membership</i>	Available, only if <i>Synchronize Groups</i> is set to <i>True</i> . Removes the user from the Group Membership attribute when the user is removed from the GroupWise Distribution lists.
<i>Synchronize GroupWise Distribution Lists</i>	Allows the driver to synchronize eDirectory GroupWise Distribution List objects with distribution lists in GroupWise. <i>True</i> enables the synchronization. <i>False</i> disables the synchronization.
<i>Synchronize GroupWise External Entity Objects</i>	Allows the driver to synchronize eDirectory GroupWise External Entity objects with external users in GroupWise. <i>True</i> enables the synchronization. <i>False</i> disables the synchronization.
<i>Sync GroupWise External Entities to this Domain</i>	Available only if <i>Synchronize GroupWise Distribution Lists</i> is set to <i>True</i> . Specify a Non-GroupWise Domain name that exists within the GroupWise system. This Domain must host at least one external post office, defined in <i>Sync GroupWise External Entities to this External Post Office</i> .
<i>Sync GroupWise External Entities to this External Post Office</i>	Available only if <i>Synchronize GroupWise Distribution Lists</i> is set to <i>True</i> . Specify an External Post Office name that exists within the GroupWise system. This Post Office must be subordinate to the GroupWise domain defined in <i>Sync GroupWise External Entities to this Domain</i> .
<i>Synchronize eDir OrgUnit to GroupWise External Post Office</i>	Allows the driver to synchronize eDirectory Organizational Units to GroupWise External Post Offices. <i>True</i> enables the synchronization. <i>False</i> disables the synchronization.
<i>Create External Post Offices in the Non-GroupWise Domain</i>	Available only if <i>Synchronize eDir OrgUnit to GroupWise External Post Office</i> is set to <i>True</i> . Specify a Non-GroupWise Domain name that exists within the GroupWise system. This Domain hosts the external post offices created by the GroupWise driver when synchronizing eDirectory Organizational Units to GroupWise Post Offices.
<i>Create Nicknames</i>	Allows the driver to create GroupWise nicknames when GroupWise accounts are renamed or moved to another post office. <i>True</i> creates nicknames when the accounts are renamed or moved. <i>False</i> does not create nicknames when the accounts are renamed or moved.
NOTE: This option should not be used with GroupWise 6.5.0 or earlier.	
<i>Reassign Resource Ownership</i>	The driver reassigns ownership of resources when GroupWise accounts are disabled or expired. <i>True</i> assigns the resources to the default User ID you specify in the next parameter. This setting does not apply when a GroupWise account is deleted because the resources must be reassigned. <i>False</i> is the default.
<i>Default Resource Owner User ID</i>	Specify the prefix of the default user to become the new owner of resources that are reassigned. The default is IS_admin. You must specify this name even when the <i>Reassign Resource Ownership</i> option is <i>False</i> . When a GroupWise account is deleted, its resources are assigned to this account. If the default User ID does not have a GroupWise account in the post office of the deleted account, an account is created.
IMPORTANT: The driver does not start if a default user prefix is not specified.	

GCV Name	Description
<i>Create Accounts During Migration</i>	<p>Allows the driver to create new GroupWise accounts for users without a current account during a migration from eDirectory. <i>True</i> allows the accounts to be created. <i>False</i> does not create the accounts.</p> <p>Migration causes Identity Manager to examine every object specified. When an object does not have a driver association, the Create policy is applied. If the object meets the Create rule criteria, the object is passed to the driver as an Add event. When you specify <i>True</i>, the driver creates a GroupWise account. When <i>False</i> is specified, the Add event is ignored and the driver issues a warning that this option is set to <i>False</i>. The default value is <i>False</i>.</p> <p>Migration sets the driver association on all users with GroupWise accounts. See Section 4.6.6, "Migrating eDirectory Users to GroupWise," on page 43 for more information.</p>
<i>Action on eDirectory User Delete</i>	<p>Specify the action you want the driver to take on an associated GroupWise account when a user is deleted in eDirectory:</p> <ul style="list-style-type: none"> ◆ <i>Delete the GroupWise Account</i> ◆ <i>Disable the GroupWise Account</i> ◆ <i>Expire the GroupWise Account</i> ◆ <i>Disable and Expire the GroupWise Account</i>
<i>Action on eDirectory User Expire/Unexpire</i>	<p>Specify the action you want the driver to take on an associated GroupWise account when its user login in eDirectory is expired or unexpired:</p> <ul style="list-style-type: none"> ◆ <i>Expire/Unexpire the GroupWise Account</i> ◆ <i>Disable/Enable the GroupWise Account</i> ◆ <i>Disable/Enable and Expire/Unexpire the GroupWise Account</i>
<i>Action on eDirectory User Disable/Enable</i>	<p>Specify the action you want the driver to take on an associated GroupWise account when its user login in eDirectory is disabled or enabled:</p> <ul style="list-style-type: none"> ◆ <i>Expire/Unexpire the GroupWise Account</i> ◆ <i>Disable/Enable the GroupWise Account</i> ◆ <i>Disable/Enable and Expire/Unexpire the GroupWise Account</i>
<i>Remove GW Account from All Distribution Lists on Expire</i>	<p>Set this option to <i>True</i>, if you want the driver to remove the GroupWise account from all distribution lists when the next event is processed, otherwise select <i>False</i>.</p>
<i>Remove GW Account from All Distribution Lists on Disable</i>	<p>Set this option to <i>True</i> if you want the driver to remove the GroupWise account from all distribution lists when the next event is processed, otherwise select <i>False</i>.</p>
<i>Action on eDirectory GroupWise External Entity Delete</i>	<p>When a GroupWise External Entity is deleted in eDirectory, specify the action you want the driver to take on the associated GroupWise account. The options are:</p> <ul style="list-style-type: none"> ◆ <i>Delete the GroupWise Account</i> ◆ <i>Disable the GroupWise Account</i> ◆ <i>Expire the GroupWise Account</i> ◆ <i>Disable and Expire the GroupWise Account</i>

GCV Name	Description
<i>Action on eDirectory GroupWise External Entity Expire/Unexpire</i>	When a GroupWise External Entity login in eDirectory is expired/unexpired, specify the action you want the driver to take on the associated GroupWise account: <ul style="list-style-type: none"> ◆ <i>Expire/Unexpire the GroupWise Account</i> ◆ <i>Disable/Enable the GroupWise Account</i> ◆ <i>Disable/Enable and Expire/Unexpire the GroupWise Account</i>
<i>Action on eDirectory GroupWise External Entity Disable/Enable</i>	When a GroupWise External Entity login in eDirectory is disabled/enabled, specify the action you want the driver to take on the associated GroupWise account: <ul style="list-style-type: none"> ◆ <i>Expire/Unexpire the GroupWise Account</i> ◆ <i>Disable/Enable the GroupWise Account</i> ◆ <i>Disable/Enable and Expire/Unexpire the GroupWise Account</i>
<i>Remove GroupWise External Entity from all Distribution lists on expire</i>	Select <i>True</i> if you want the driver to remove the GroupWise External Entity from all Distribution Lists when the GroupWise account is expired; otherwise, select <i>False</i> .
<i>Remove GroupWise External Entity from all Distribution Lists on disable</i>	Select <i>True</i> if you want the driver to remove the GroupWise External Entity from all Distribution Lists when the GroupWise account is disabled; otherwise, select <i>False</i> .
<i>Publisher Heartbeat Interval</i>	Specify the Publisher channel heartbeat interval in minutes. Enter 0 to disable the heartbeat.

If entitlements are enabled in the driver, there are additional GCVs, shown in [Table C-7 on page 194](#).

Table C-7 *Global Configuration Values > Entitlements*

GCV Name	Description
<i>Action On GroupWise Account Entitlement Add</i>	Entitlement option only. When a user is created in eDirectory with a GroupWise account entitlement, select the action you want to occur on the associated GroupWise account: <ul style="list-style-type: none"> ◆ <i>Disable the GroupWise Account</i> ◆ <i>Enable the GroupWise Account</i>
<i>Action On GroupWise Account Entitlement Remove</i>	Entitlement option only. When a user's GroupWise account entitlement is removed in eDirectory, specify the action you want the driver to take on an associated GroupWise account: <ul style="list-style-type: none"> ◆ <i>Disable the GroupWise account</i> ◆ <i>Delete the GroupWise account</i> ◆ <i>Expire the GroupWise account</i> ◆ <i>Disable and expire the GroupWise account</i>

The following GCVs are password synchronization options:

IMPORTANT: Password synchronization settings are GCVs, but it's best to edit them in the graphical interface provided on the Server Variables page for the driver, instead of the GCV page. The Server Variables page that shows Password Synchronization settings is accessible as a tab like other driver parameters, or by clicking *Password Management > Password Synchronization*, searching for the driver, and clicking the driver name. The page contains online help for each password synchronization setting.

Table C-8 *Global Configuration Values > Password Synchronization*

Option	Description
<i>Set the initial/default GroupWise password on account creation</i>	<p>If <i>True</i>, the GroupWise initial/default password is set when an account is created. The initial password value is specified in the Create Policy. If <i>False</i>, the initial password is not set.</p> <p>GroupWise has two passwords, the initial password and the regular password. The initial password is stored in clear text and can be seen by an admin. The regular password is encrypted and cannot be viewed. When it is set, the regular password is used by GroupWise instead of the initial password. When a GroupWise user changes his or her password, it is stored as the regular password. For security, the initial password is never set to a password sent from eDirectory.</p>
<i>Synchronize the eDirectory password to the GroupWise regular password</i>	<p>If <i>True</i>, allows passwords to flow from eDirectory to GroupWise. If <i>False</i>, the regular password is not set.</p> <p>GroupWise has two passwords, the initial password and regular password. The initial password is stored in clear text and can be seen by an admin. The regular password is encrypted and cannot be viewed. When it is set, the regular password is used by GroupWise instead of the initial/default password. When a GroupWise user changes his or her password, it is stored as the regular password. For security, the initial password is never set to a password sent from eDirectory.</p>

C.3 Named Passwords

Identity Manager allows you to store multiple passwords securely for a particular driver. This functionality is referred to as Named Passwords. Each different password is accessed by a key, or name.

You can also use the Named Passwords feature to store other pieces of information securely, such as a user name. To configured Named Passwords, see [Section 7.16, “Storing Driver Passwords Securely with Named Passwords,” on page 126](#).

In iManager:

- 1 Click *Identity Manager > Identity Manager Overview*, then click *Search* to search for the driver set that is associated with the driver.
- 2 Browse to the driver, then click the upper right corner of the driver icon.
- 3 Click *Edit Properties > Named Passwords*.

In Designer:

- 1 Open a project in the Modeler, then right-click the driver line and select *Properties > Named Passwords*.

C.4 Engine Control Values

The engine control values are a means through which certain default behaviors of the Metadirectory engine can be changed. The values can only be accessed if a server is associated with the Driver Set object.

In iManager:

- 1 Click *Identity Manager > Identity Manager Overview*, then click *Search* to search for the driver set that is associated with the driver.
- 2 Browse to the driver, then click the upper right corner of the driver icon.
- 3 Click *Edit Properties > Engine Control Values*.
See [Table C-9](#) for a list of the engine control values.

In Designer:

- 1 In the Modeler, right-click the driver line.
- 2 Select *Properties > Engine Control Values*.
- 3 Click the tooltip icon to the right of the *Engine Controls For Server* field. If a server is associated with the Identity Vault, and if you are authenticated, the engine control values display in the larger pane.
See [Table C-9](#) for a list of the engine control values.

Table C-9 *Engine Control Values*

Option	Description
<i>Subscriber channel retry interval in seconds</i>	The Subscriber channel retry interval controls how frequently the Metadirectory engine retries the processing of a cached transaction after the application shim's Subscriber object returns a retry status.
<i>Qualified form for DN-syntax attribute values</i>	The qualified specification for DN-syntax attribute values controls whether values for DN-syntax attribute values are presented in unqualified slash form or qualified slash form. A True setting means the values are presented in qualified form.
<i>Qualified form from rename events</i>	The qualified form for rename events controls whether the new-name portion of rename events coming from the Identity Vault are presented to the Subscriber channel with type qualifiers. For example, CN=. A True setting means the names are presented in qualified form.

Option	Description
<i>Maximum eDirectory replication wait time in seconds</i>	<p>The maximum eDirectory™ replication wait time controls the maximum time that the Metadirectory engine waits for a particular change to replicate between the local replica and a remote replica. This only affects operations where the Metadirectory engine is required to contact a remote eDirectory server in the same tree to perform an operation and might need to wait until some change has replicated to or from the remote server before the operation can be completed (for example, object moves when the Identity Manager server does not hold the master replica of the moved object; file system rights operations for Users created from a template.)</p>
<i>Use non-compliant backwards-compatible mode for XSLT</i>	<p>This control sets the XSLT processor used by the Metadirectory engine to a backward-compatible mode. The backward-compatible mode causes the XSLT processor to use one or more behaviors that are not XPath 1.0 and XSLT 1.0 standards-compliant. This is done in the interest of backward-compatibility with existing DirXML® style sheets that depend on the non-standard behaviors.</p> <p>For example, the behavior of the XPath “!=” operator when one operand is a node set and the other operand is other than a node set is incorrect in DirXML releases up to and including Identity Manager 2.0. This behavior has been corrected; however, the corrected behavior is disabled by default through this control in favor of backward-compatibility with existing DirXML style sheets.</p>
<i>Maximum application objects to migrate at once</i>	<p>This control is used to limit the number of application objects that the Metadirectory engine requests from an application during a single query that is performed as part of a Migrate Objects from Application operation.</p> <p>If java.lang.OutOfMemoryError errors are encountered during a Migrate from Application operation, this number should be set lower than the default. The default is 50.</p> <hr/> <p>NOTE: This control does not limit the number of application objects that can be migrated; it merely limits the batch size.</p>
<i>Set creatorsName on objects created in Identity Vault</i>	<p>This control is used by the Identity Manager engine to determine if the creatorsName attribute should be set to the DN of this driver on all objects created in the Identity Vault by this driver.</p> <p>Setting the creatorsName attribute allows for easily identifying objects created by this driver, but also carries a performance penalty. If not set, the creatorsName attribute defaults to the DN of the NCP™ Server object that is hosting the driver.</p>
<i>Write pending associations</i>	<p>This control determines whether the Identity Manager engine writes a pending association on an object during Subscriber channel processing.</p> <p>Writing a pending association confers little or no benefit but does incur a performance penalty. Nevertheless, the option exists to turn it on for backward compatibility.</p>

Option	Description
<i>Use password event values</i>	<p>This control determines the source of the value reported for the nspmDistributionPassword attribute for Subscriber channel Add and Modify events.</p> <p>Setting the control to False means that the current value of the nspmDistributionPassword is obtained and reported as the value of the attribute event. This means that only the current password value is available. This is the default behavior.</p> <p>Setting the control to True means that the value recorded with the eDirectory event is decrypted and is reported as the value of the attribute event. This means that both the old password value (if it exists) and the replacement password value at the time of the event are available. This is useful for synchronizing passwords to certain applications that require the old password to enable setting a new password.</p>
<i>Enable password synchronization status reporting</i>	<p>This control determines whether the Identity Manager engine reports the status of Subscriber channel password change events.</p> <p>Reporting the status of Subscriber channel password change events allows applications such as the Identity Manager User Application to monitor the synchronization progress of a password change that should be synchronized to the connected application.</p>

C.5 Log Level

Every driver set and driver has a log level field where you can define the level of errors that should be tracked. The level you indicate here determines which messages are available to the logs. By default, the log level is set to track error messages (this also includes fatal messages). Change the log level if you want to track additional message types.

Novell® recommends that you use Novell Audit instead of setting the log levels. See “[Integrating Identity Manager with Novell Audit](#)” in the *Identity Manager 3.5.1 Logging and Reporting*.

In iManager:

- 1 Click *Identity Manager > Identity Manager Overview*, then click *Search* to search for the driver set that is associated with the driver.
- 2 Browse to the driver, then click the upper right corner of the driver icon.
- 3 Click *Edit Properties > Log Level*.


See [Table C-10](#) for a list of the driver log levels.

In Designer:

- 1 Open a project in the Modeler, then right-click the driver line and select *Properties > Driver Log Level*.

See [Table C-10](#) for a list of the driver log levels.

Table C-10 *Driver Log Levels*

Option	Description
<i>Use log settings from the DriverSet</i>	If this is selected, the driver logs events as the options are set on the Driver Set object.
<i>Log errors</i>	Logs just errors
<i>Log errors and warnings</i>	Logs errors and warnings
<i>Log specific events</i>	Logs the events that are selected. Click the  icon to see a list of the events.
<i>Only update the last log time</i>	Updates the last log time.
<i>Logging off</i>	Turns logging off for the driver.
<i>Turn off logging to DriverSet, Subscriber and Publisher logs</i>	If selected, turns all logging off for this driver on the Driver Set object, Subscriber channel, and the Publisher channel.
<i>Maximum number of entries in the log (50-500)</i>	Number of entries in the log. The default value is 50.

C.6 Driver Image

Allows you to change the image associated with the driver. You can browse and select a different image from the default image.

The image associated with a driver is used by the Identity Manager Overview plug-in when showing the graphical representation of your Identity Manager configuration. Although storing an image is optional, it makes the overview display more intuitive.

NOTE: The driver image is maintained when a driver configuration is exported.

In iManager:

- 1 Click *Identity Manager > Identity Manager Overview*, then click *Search* to search for the driver set that is associated with the driver.
- 2 Browse to the driver, then click the upper right corner of the driver icon.
- 3 Click *Edit Properties > Driver Image*.

In Designer:

- 1 Open a project in the Modeler, then right-click the driver line and select *Properties > iManager Icon*.

C.7 Security Equals

Use the Security page to view or change the list of objects that the driver is explicitly security equivalent to. This object effectively has all rights of the listed objects.

If you add or delete an object in the list, the system automatically adds or deletes this object in that object's "Security Equal to Me" property. You don't need to add the [Public] trustee or the parent containers of this object to the list, because this object is already implicitly security equivalent to them.

In iManager:

- 1 Click *Identity Manager > Identity Manager Overview*, then click *Search* to search for the driver set that is associated with the driver.
- 2 Browse to the driver, then click the upper right corner of the driver icon.
- 3 Click *Edit Properties > Security Equals*.

Designer does not list the users the driver is security equivalent to.

C.8 Filter

Launches the Filter editor. You can edit the filter from this tab.

In iManager:

- 1 Click *Identity Manager > Identity Manager Overview*, then click *Search* to search for the driver set that is associated with the driver.
- 2 Browse to the driver, then click the upper right corner of the driver icon.
- 3 Click *Edit Properties > Filter*.

The Filter editor is accessed through the outline view in Designer.

- 1 In an open project, click the *Outline* tab.
- 2 Select the driver you want to manage the filter for, then click the plus sign to the left.
- 3 Double-click the *Filter* icon to launch the Filter Editor.

C.9 Edit Filter XML

Allows you to edit the filter directly in XML instead of using the Filter Editor.

In iManager:

- 1 Click *Identity Manager > Identity Manager Overview*, then click *Search* to search for the driver set that is associated with the driver.
- 2 Browse to the driver, then click the upper right corner of the driver icon.
- 3 Click *Edit Properties > Filter*.

You can edit the Filter in XML through the Filter Editor in Designer.

- 1 In an open project, click the *Outline* tab.
- 2 Select the driver you want to manage the filter for, then click the plus sign to the left.
- 3 Double-click the *Filter* icon to launch the Filter Editor, then click *XML Source* at the bottom of the Filter Editor.

C.10 Misc

Allows you to add a trace level to your driver. With the trace level set, DSTrace displays the Identity Manager events as the Metadirectory engine processes the events. The trace level only affects the driver it is set for. Use the trace level for troubleshooting issues with the driver when the driver is deployed. DSTrace displays the output of the specified trace level.


In iManager:

- 1 Click *Identity Manager > Identity Manager Overview*, then click *Search* to search for the driver set that is associated with the driver.
- 2 Browse to the driver, then click the upper right corner of the driver icon.
- 3 Click *Edit Properties > Misc*.
See [Table C-11](#) for a list of the driver trace options.

In Designer:

- 1 Open a project in the Modeler, then right-click the driver line and select *Properties > Trace*.
See [Table C-11](#) for a list of the driver trace options.

Table C-11 *Driver Trace Options*

Option	Description
<i>Trace level</i>	Increases the amount of information displayed in DSTrace. Trace level 1 shows errors, but not the cause of the errors. If you want to see password synchronization information, set the trace level to 5.
<i>Trace file</i>	When a value is set in this field, all Java information for the driver is written to the file. The value for this field is the path for that file. As long as the file is specified, Java information is written to this file. If you do not need to debug Java, leave this field blank.
<i>Trace file size limit</i>	Allows you to set a limit for the Java trace file. If you set the file size to Unlimited, the file grows in size until there is no disk space left. NOTE: The trace file is created in multiple files. Identity Manager automatically divides the maximum file size by ten and creates ten separate files. The combined size of these files equals the maximum trace file size.
<i>Trace name</i>	Driver trace messages are prepended with the value entered in this field.
 <i>Use setting from Driver Set</i>	This option is only available in Designer. It allows the driver to use the same setting that is set on the Driver Set object.

C.11 Excluded Users

Use this page to create a list of users or resources that are not replicated to the application. Novell recommends that you add all objects that represent an administrative role to this list (for example, the Admin object).

In iManager:

- 1 Click *Identity Manager > Identity Manager Overview*, then click *Search* to search for the driver set that is associated with the driver.
- 2 Browse to the driver, then click the upper right corner of the driver icon.
- 3 Click *Edit Properties > Excluded Users*.

Designer does not list the excluded users.

C.12 Driver Manifest

The driver manifest is like a resumé for the driver. It states what the driver supports, and includes a few configuration settings. The driver manifest is created by default when the Driver object is imported. A network administrator usually does not need to edit the driver manifest.

In iManager:

- 1 Click *Identity Manager > Identity Manager Overview*, then click *Search* to search for the driver set that is associated with the driver.
- 2 Browse to the driver, then click the upper right corner of the driver icon.
- 3 Click *Edit Properties > Driver Manifest*.

In Designer:

- 1 Open a project in the Modeler, then right-click the driver line and select *Properties > Driver Manifest*.

C.13 Driver Inspector

The Driver Inspector page displays information about all of the objects associated with the driver.

- ♦ **Driver:** A link to run the *Driver Overview* on the driver that is being inspected.
- ♦ **Driver Set:** A link to run the *Driver Set Overview* of the driver set that holds the driver.
- ♦ **Delete:** Deletes the associations of the selected objects.
- ♦ **Refresh:** Select this option to re-read all of the objects associated with the driver and refresh the displayed information.
- ♦ **Actions:** Allows you to perform actions on the objects associated with the driver. Click *Actions* to expand the menu, which includes:
 - ♦ **Show All Associations:** Displays all objects associated with the driver.
 - ♦ **Filter for Disabled Associations:** Displays all objects associated with the driver that have a Disabled state.
 - ♦ **Filter for Manual Associations:** Displays all objects associated with the driver that have a Manual state.
 - ♦ **Filter for Migrate Associations:** Displays all objects associated with the driver that have a Migrate state.
 - ♦ **Filter for Pending Associations:** Displays all objects associated with the driver that have a Pending state.

- ♦ **Filter for Processed Associations:** Displays all objects associated with the driver that have a Processed state.
- ♦ **Filter for Undefined Associations:** Displays all objects associated with the driver that have an Undefined state.
- ♦ **Association Summary:** Displays the state of all objects associated with the driver.
- ♦ **Object DN:** Displays the DN of the associated objects.
- ♦ **State:** Displays the association state of the object.
- ♦ **Object ID:** Displays the value of the association.

C.14 Driver Cache Inspector

The Driver Cache Inspector page uses a table format to display information about the cache file that stores events while the driver is stopped.

- ♦ **Driver:** A link to run the *Driver Overview* on the driver that is associated with this cache file.
- ♦ **Driver Set:** A link to run the *Driver Set Overview* on the driver set that holds the driver.
- ♦ **Driver's cache on:** Lists the server object that contains this instance of the cache file.
- ♦ **Start/Stop Driver icons:** Displays the current state of the driver and allows you to start or stop the driver.
- ♦ **Edit icon:** Allows you to edit the properties of the currently selected Server object.
- ♦ **Delete:** Deletes the selected items from the cache file.
- ♦ **Refresh:** Select this option to re-read the cache file and refresh the displayed information.
- ♦ **Show:** Limits the number of items to be displayed. The options are:
 - ♦ 25 per page
 - ♦ 50 per page
 - ♦ 100 per page
 - ♦ Other: Allows you to specify a desired number.
- ♦ **Actions:** Allows you to perform actions on the entries in the cache file. Click *Actions* to expand the menu, which includes:
 - ♦ **Expand All:** Expands all of the entries displayed in the cache file.
 - ♦ **Collapse All:** Collapses all of the entries displayed in the cache file.
 - ♦ **Go To:** Allows you to access a specified entry in the cache file. Specify the entry number, then click *OK*.
 - ♦ **Cache Summary:** Summarizes all of the events stored in the cache file.

C.15 Inspector

The Inspector displays information about the connected system without directly accessing the system. Designer does not have this option.

C.16 Server Variables

This page lets you enable and disable password synchronization and the associated options for the selected driver.

When setting up password synchronization, consider both the settings on this page for an individual driver and the Universal Password Configuration options in your password policies.

This page lets you control which password Identity Manager updates directly, either the Universal Password for an Identity Vault, or the Distribution Password used for password synchronization by Identity Manager.

However, Novell Modular Authentication Service (NMAS™) controls whether the various passwords inside the Identity Vault are synchronized with each other. Password Policies are enforced by NMAS, and they include settings for synchronizing Universal Password, NDS® Password, Distribution Password, and Simple Password.

To change these settings in iManager:

- 1 In iManager, select *Passwords > Password Policies*.
- 2 Select a password policy, then click *Edit*.
- 3 Select *Universal Password*.

This option is available from a drop-down list or a tab, depending on your version of iManager and your browser.

- 4 Select *Configuration Options*, make changes, then click *OK*.

NOTE: Enabling or disabling options on this page corresponds to values of True or False for certain global configuration values (GCVs) used for password synchronization in the driver parameters. Novell recommends that you edit them here in the graphical interface, instead of on the GCVs page. This interface helps ensure that you don't set conflicting values for the password synchronization GCVs.

Option	Description
<i>Identity Manager accepts password (Publisher Channel)</i>	<p>If this option is enabled, Identity Manager allows passwords to flow from the connected system driver into the Identity Vault data store.</p> <p>Disabling this option means that no <code><password></code> elements are allowed to flow to Identity Manager. They are stripped out of the XML by a password synchronization policy on the Publisher channel.</p> <p>If this option is enabled, and the option below it for Distribution Password is disabled, a <code><password></code> value coming from the connected system is written directly to the Universal Password in the Identity Vault if it is enabled for the user. If the user's password policy does not enable Universal Password, the password is written to the NDS Password.</p>

Option	Description
<i>Use Distribution Password for password synchronization</i>	<p>To use this setting, you must have a version of eDirectory that supports Universal Password, regardless of whether you have enabled Universal Password in your password policies.</p> <p>If this option is enabled, a password value coming from the connected system is written to the Distribution Password. The Distribution Password is reversible, which means that it can be retrieved from the Identity Vault data store for password synchronization. It is used by Identity Manager for bidirectional password synchronization with connected systems. For Identity Manager to distribute passwords to connected systems, this option must be enabled.</p> <p>NMAS and Password policies control whether the Distribution Password is synchronized with other passwords in the Identity Vault. By default, the Distribution Password is the same as the Universal Password in the Identity Vault.</p> <p>If the password in the Identity Vault is to be independent of password synchronization, so that Identity Manager is a conduit only for synchronizing passwords among connected systems, change this default setting. In the Universal Password Configuration Options in a Password policy, disable <i>Synchronize Universal Password with Distribution Password</i>. This use of Identity Manager password synchronization is also referred to as “tunneling.”</p>
<i>Accept password only if it complies with user's Password Policy</i>	<p>To use this setting, users must have a Password policy assigned that has Universal Password enabled, and Advanced Password Rules enabled and configured.</p> <p>If this option is chosen, Identity Manager does not write a password from this connected system to the Distribution Password in the Identity Manager data store or publish it to connected systems unless the password complies with the user's Password policy.</p> <p>By using the notification option that is also on this page, you can inform users when a password is not set because it is not compliant.</p>

Option	Description
<i>If password does not comply, ignore Password Policy on the connected system by resetting user's password to the Distribution Password</i>	<p>This option lets you enforce Password policies on the connected system by replacing a password that does not comply. If you select this option, and a user's password on the connected system does not comply with the user's Password policy, Identity Manager resets the password on the connected system by using the Distribution Password from the Identity Vault data store.</p> <p>Keep in mind that if you do not select this option, user passwords can become out-of-sync on connected systems.</p> <p>By using the notification option that is also on this page, you can inform users when a password is not set or reset. Notification is especially helpful for this option. If the user changes to a password that is allowed by the connected system but rejected by Identity Manager because of the Password policy, the user won't know that the password has been reset until the user receives a notification or tries to log in to the connected system with the old password.</p> <hr/> <p>NOTE: Consider the connected system's password policies when deciding whether to use this option. Some connected systems might not allow the reset because they don't allow you to repeat passwords.</p>
<i>Always accept password; ignore Password Policies</i>	<p>If you select this option, Identity Manager does not enforce the user's Password policy for this connected system. Identity Manager writes the password from this connected system to the Distribution Password in the Identity Vault data store, and distributes it to other connected systems, even if the password does not comply with the user's Password policy.</p>
<i>Application accepts passwords (Subscriber Channel)</i>	<p>If you select this option, the driver sends passwords from the Identity Vault data store to this connected system. This also means that if a user changes the password on a different connected system that is publishing passwords to the Distribution Password in the Identity Vault data store, the password is changed on this connected system.</p> <p>By default, the Distribution Password is the same as the Universal Password in the Identity Vault, so changes to the Universal Password made in the Identity Vault are also sent to the connected system.</p> <p>If you want the password in the Identity Vault to be independent of password synchronization, so that Identity Manager is a conduit only for synchronizing passwords among connected systems, you can change this default setting. In the Universal Password Configuration Options in a password policy, disable <i>Synchronize Universal Password with Distribution Password</i>. This use of password synchronization is also referred to as "tunneling."</p>
<i>Notify the user of password synchronization failure via-email</i>	<p>If you select this option, e-mail is sent to the user if a password is not synchronized, set, or reset. The e-mail that is sent to the user is based on an e-mail template. This template is provided by the password synchronization application. However, for the template to work, you must customize it and specify an e-mail server to send the notification messages.</p> <hr/> <p>NOTE: To set up e-mail notification, select <i>Passwords > Edit EMail Templates</i>.</p>