



NetIQ® Identity Manager

Driver for GroupWise Implementation Guide

October 2014

Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2014 NetIQ Corporation. All Rights Reserved.

For information about NetIQ trademarks, see <https://www.netiq.com/company/legal/>.

Contents

About this Book and the Library	7
About NetIQ Corporation	9
1 Understanding the GroupWise Driver	11
1.1 Supported GroupWise Versions	11
1.2 GroupWise Driver Concepts	11
1.2.1 Methods for Managing GroupWise Accounts	11
1.2.2 Driver Components	12
1.2.3 Publisher Channel	12
1.2.4 Subscriber Channel	13
1.2.5 Object Access	13
1.3 Support for Standard Driver Features	13
1.3.1 Local Platforms	13
1.3.2 Remote Platforms	14
1.3.3 Entitlements	14
1.3.4 Password Synchronization	14
1.3.5 Objects Synchronized	14
2 Installing the Driver Files	15
2.1 Where to Install the GroupWise Driver	15
2.1.1 Local Installation	15
2.1.2 Remote Installation	16
2.2 Installing the Driver Files	17
2.2.1 Local Installation	17
2.2.2 Remote Installation	17
2.3 Installing the Novell Client	18
3 Creating a New Driver Object	19
3.1 Creating Accounts for Authentication	19
3.2 Creating the Driver Object in Designer	20
3.2.1 Importing the Current Driver Packages	20
3.2.2 Installing the Driver Packages	21
3.2.3 Configuring the Driver Object	23
3.2.4 Deploying the Driver	24
3.2.5 Starting the Driver	25
3.2.6 Testing the Driver	25
3.3 Associating Identity Vault Users and GroupWise Users	26
3.4 Activating the Driver	26
4 Upgrading an Existing Driver	27
4.1 Supported Upgrade Paths	27
4.2 What's New in Version 4.5	27
4.3 Upgrade Procedure	27

5	Customizing the Driver by Using Policies and Filters	29
5.1	Default Driver Actions	29
5.2	Modifying Default Settings in Policies and the Filter	29
5.2.1	Modifying the Driver Filter	30
5.2.2	Adding Entries to the Schema Mapping Policy	30
5.2.3	Modifying the Create Policy	30
5.2.4	Modifying the Matching Policy	30
5.3	Modifying Policies	30
5.3.1	Specifying the GroupWise Post Office	31
5.3.2	Specifying Distribution Lists	33
5.3.3	Setting Defaults for GroupWise Attributes	37
5.3.4	Configuring the GroupWise UserID	38
5.3.5	Creating Mappings for Additional Attributes	39
5.3.6	Getting a Record Count from a Query	39
5.3.7	Deleting the GroupWise User without Deleting the Identity Vault User	39
5.3.8	Creating a GroupWise Nickname	40
5.3.9	Creating a GroupWise Nickname Record	40
5.3.10	Specifying a New Resource Owner on an Owner Delete	41
5.3.11	Specifying a New Resource Owner on an Owner Disable	42
5.3.12	Controlling Creation of GroupWise Accounts	43
5.3.13	Moving Users from One Post Office to Another Post Office	44
5.3.14	Adding Additional Attributes to Be Synchronized	44
5.3.15	Renaming Users	45
5.3.16	Creating a Gateway Alias	45
5.3.17	Querying for a Nickname	46
5.3.18	Querying for a Gateway Alias	48
5.3.19	Querying for Internet EMail Address	48
5.3.20	Synchronizing GroupWise External Users	49
5.3.21	Verifying if an E-Mail Address or Gateway Alias Is Unique	52
5.4	Setting GroupWise Client Options with the Driver	53
5.4.1	Using Policies to Set Client Options	53
5.4.2	Client Options	55
5.4.3	Environment > General	56
5.4.4	Environment > Client Access	59
5.4.5	Environment > Views	61
5.4.6	Environment > File Location > Archive Directory	63
5.4.7	Environment > Cleanup	65
5.4.8	Send > Send Options	67
5.4.9	Send > Mail	71
5.4.10	Send > Appt.	74
5.4.11	Send > Task	77
5.4.12	Send > Note	79
5.4.13	Send > Security	82
5.4.14	Send > Disk Space Management	84
5.4.15	Date and Time > Calendar	87
5.4.16	Date and Time > Calendar > Alarm Options	89
5.4.17	Date and Time > Busy Search	91
5.5	Client Options Quick Reference	94
5.5.1	Environment	94
5.5.2	Send	95
5.5.3	Date and Time	96
6	Managing the Driver	99
6.1	Using Anti-Virus Software on a GroupWise System	99
6.2	Synchronizing Group Objects	99
6.3	Synchronizing GroupWise Distribution List Objects	100
6.4	Using the GroupWise Snap-Ins to Remove a GroupWise Account	100

6.5	Re-associating a GroupWise Account with an Identity Vault User	100
6.6	Renaming Users	101
6.7	Common Management Tasks	101
7	Troubleshooting the Driver	103
7.1	Avoiding Data Corruption	103
7.2	Troubleshooting Driver Processes	103
7.3	Error Messages	103
A	Driver Properties	111
A.1	Driver Configuration	111
A.1.1	Driver Module	112
A.1.2	Driver Object Password	112
A.1.3	Authentication	112
A.1.4	Startup Option	113
A.1.5	Driver Parameters	113
A.1.6	ECMAScript	114
A.1.7	Global Configurations	114
A.2	Global Configuration Values	114
A.2.1	Driver Configuration	115
A.2.2	Entitlements	117
A.2.3	Account Tracking	119
A.2.4	Password Synchronization	119
A.2.5	Managed System Information	120
B	Class and Attribute Descriptions	121
C	Trace Levels	131

About this Book and the Library

The *Identity Manager Driver for GroupWise Implementation Guide* explains how to install, configure, and manage the Identity Manager Driver for GroupWise.

Intended Audience

This book provides information for Identity Manager and GroupWise administrators who are using the Identity Manager Driver for GroupWise.

Other Information in the Library

The library provides the following information resources:

Identity Manager Setup Guide

Provides overview of Identity Manager and its components. This book also provides detailed planning and installation information for Identity Manager.

Designer Administration Guide

Provides information about designing, testing, documenting, and deploying Identity Manager solutions in a highly productive environment.

User Application: Administration Guide

Describes how to administer the Identity Manager User Application.

User Application: User Guide

Describes the user interface of the Identity Manager User Application and how you can use the features it offers, including identity self-service, the Work Dashboard, role and resource management, and compliance management.

User Application: Design Guide

Describes how to use the Designer to create User Application components, including how to work with the Provisioning view, the directory abstraction layer editor, the provisioning request definition editor, the provisioning team editor, and the role catalog.

Identity Reporting Module Guide

Describes the Identity Reporting Module for Identity Manager and how you can use the features it offers, including the Reporting Module user interface and custom report definitions, as well as providing installation instructions.

Analyzer Administration Guide

Describes how to administer Analyzer for Identity Manager.

Identity Manager Common Driver Administration Guide

Provides information about administration tasks that are common to all Identity Manager drivers.

Identity Manager Driver Guides

Provides implementation information about Identity Manager drivers.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- ◆ Identity & Access Governance
- ◆ Access Management
- ◆ Security Management
- ◆ Systems & Application Management
- ◆ Workload Management
- ◆ Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

1 Understanding the GroupWise Driver

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, “Supported GroupWise Versions,” on page 11](#)
- ♦ [Section 1.2, “GroupWise Driver Concepts,” on page 11](#)
- ♦ [Section 1.3, “Support for Standard Driver Features,” on page 13](#)

1.1 Supported GroupWise Versions

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

- ♦ GroupWise 8.0 with the latest support packs
- ♦ GroupWise 2012 with the latest support packs

1.2 GroupWise Driver Concepts

The following sections explain concepts you should understand before implementing the GroupWise driver:

- ♦ [Section 1.2.1, “Methods for Managing GroupWise Accounts,” on page 11](#)
- ♦ [Section 1.2.2, “Driver Components,” on page 12](#)
- ♦ [Section 1.2.3, “Publisher Channel,” on page 12](#)
- ♦ [Section 1.2.4, “Subscriber Channel,” on page 13](#)
- ♦ [Section 1.2.5, “Object Access,” on page 13](#)

1.2.1 Methods for Managing GroupWise Accounts

GroupWise accounts are managed through the GroupWise snap-ins for ConsoleOne. The GroupWise driver replaces certain management tasks you perform through the snap-ins. For example, you can use the driver to automatically provision GroupWise accounts to new eDirectory users.

We recommend that you use either iManager or ConsoleOne (without the GroupWise snap-ins) to administer users in eDirectory, then let the driver synchronize any changes into GroupWise. In particular, you should not use the GroupWise snap-ins for ConsoleOne, 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 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.

Not all GroupWise account information can be managed through the driver. You should use the GroupWise snap-ins for ConsoleOne 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

1.2.2 Driver Components

The driver uses the following components:

- ♦ [“GroupWise API” on page 12](#)
- ♦ [“Driver Shim” on page 12](#)
- ♦ [“Driver Packages” on page 12](#)

GroupWise API

This API is necessary for the driver to perform the required actions in GroupWise. It is installed at the same time as the driver shim.

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.

Driver Packages

The driver packages contain all Identity Vault objects necessary for the driver, including the appropriate policies for adding, modifying, and deleting or disabling GroupWise accounts. In addition, the default policies control the information being sent from the Identity Vault to GroupWise.

1.2.3 Publisher Channel

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 to not synchronize correctly.

1.2.4 Subscriber Channel

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.

1.2.5 Object Access

To ensure that the driver has access to the correct objects, be aware of the following:

- ♦ The driver can only access Identity Vault objects located in the partitions on the server associated with the driver set.
- ♦ 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 associated with the driver set.
- ♦ The driver can only synchronize to a GroupWise system that is installed in the same eDirectory tree where the Metadirectory server is installed.

1.3 Support for Standard Driver Features

The following sections provide information about how the GroupWise driver supports these standard driver features:

- ♦ [Section 1.3.1, “Local Platforms,” on page 13](#)
- ♦ [Section 1.3.2, “Remote Platforms,” on page 14](#)
- ♦ [Section 1.3.3, “Entitlements,” on page 14](#)
- ♦ [Section 1.3.4, “Password Synchronization,” on page 14](#)
- ♦ [Section 1.3.5, “Objects Synchronized,” on page 14](#)

1.3.1 Local Platforms

A local installation is an installation of the driver on the Metadirectory server. The GroupWise driver can be installed on the following operating systems supported for the Metadirectory server:

- ♦ Windows Server 2003 SP2 32-bit
- ♦ Windows Server 2008 32-bit
- ♦ SUSE Linux Enterprise Server 10 SP2 or later (32-bit and 64-bit)
- ♦ Open Enterprise Server 2 SP1 or later (32-bit)

IMPORTANT: NetIQ ships only 32-bit GroupWise driver. To install the driver on a 64-bit platform, you need to have a 32-bit Metadirectory on a 64-bit platform.

1.3.2 Remote Platforms

The GroupWise driver can use the Remote Loader service to run on a server other than the Metadirectory server. For example, you might not want to install the Metadirectory server (Metadirectory engine and Identity Vault) on the same server as GroupWise. In this case, you install the Remote Loader and driver on the GroupWise server and the Remote Loader enables the driver to communicate with the Metadirectory server.

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

- ♦ Windows Server 2003 SP2 32-bit
- ♦ Windows Server 2008 32-bit
- ♦ SUSE Linux Enterprise Server 10 SP2 or later (32 and 64-bit)
- ♦ Open Enterprise Server 2 SP1 or later (32-bit)

NOTE: NetIQ ships only 32-bit GroupWise driver. To install the driver on a 64-bit platform, you need to have a 32-bit Remote Loader on a 64-bit platform.

1.3.3 Entitlements

The sample driver configuration supports entitlements. When 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

1.3.4 Password Synchronization

The Subscriber channel sets the password. Passwords are not synchronized on the Publisher channel. This means that passwords are synchronized from the Identity Vault to GroupWise, but not from GroupWise to the Identity Vault.

It is a good practice is to configure GroupWise to authenticate against the Identity Vault, in which case password synchronization is not required.

1.3.5 Objects Synchronized

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

2 Installing the Driver Files

There are several installation scenarios you can use to best meet the needs of your environment. The following sections explain the scenarios and provide instructions for installing the files based upon the scenario you've chosen.

- ♦ [Section 2.1, "Where to Install the GroupWise Driver,"](#) on page 15
- ♦ [Section 2.2, "Installing the Driver Files,"](#) on page 17
- ♦ [Section 2.3, "Installing the Novell Client,"](#) on page 18

2.1 Where to Install the GroupWise Driver

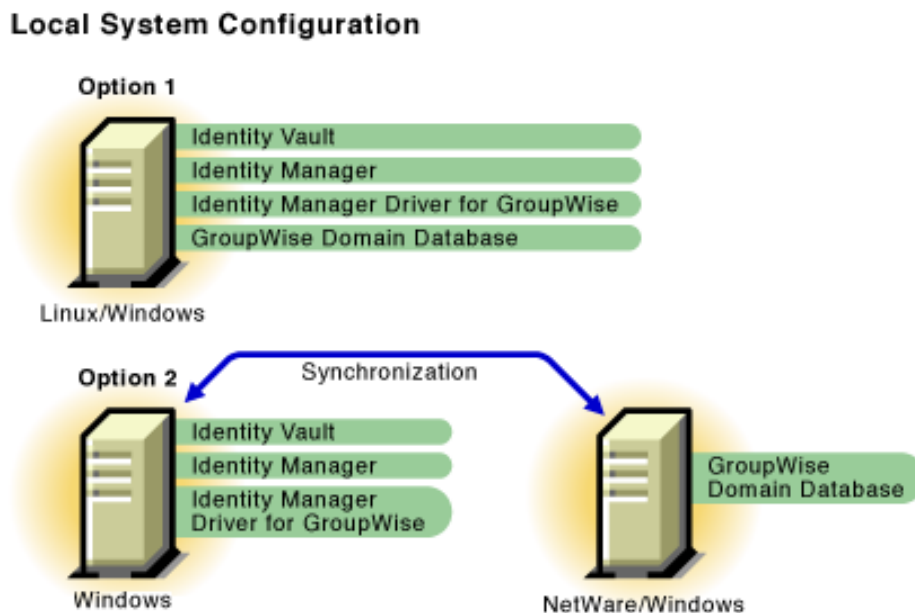
You must decide whether to install the GroupWise driver locally or remotely.

- ♦ [Section 2.1.1, "Local Installation,"](#) on page 15
- ♦ [Section 2.1.2, "Remote Installation,"](#) on page 16

2.1.1 Local Installation

In a local installation, the GroupWise driver is on the same server as the Metadirectory engine and Identity Vault. The GroupWise domain database can be on the same Windows/Linux server (Option 1), or it can be on a different Windows/NetWare server (Option 2).

Figure 2-1 Local System Configuration



In a Linux environment, the GroupWise driver must be on the same server as the GroupWise domain database, which means that Option 1 is the only viable local installation option.

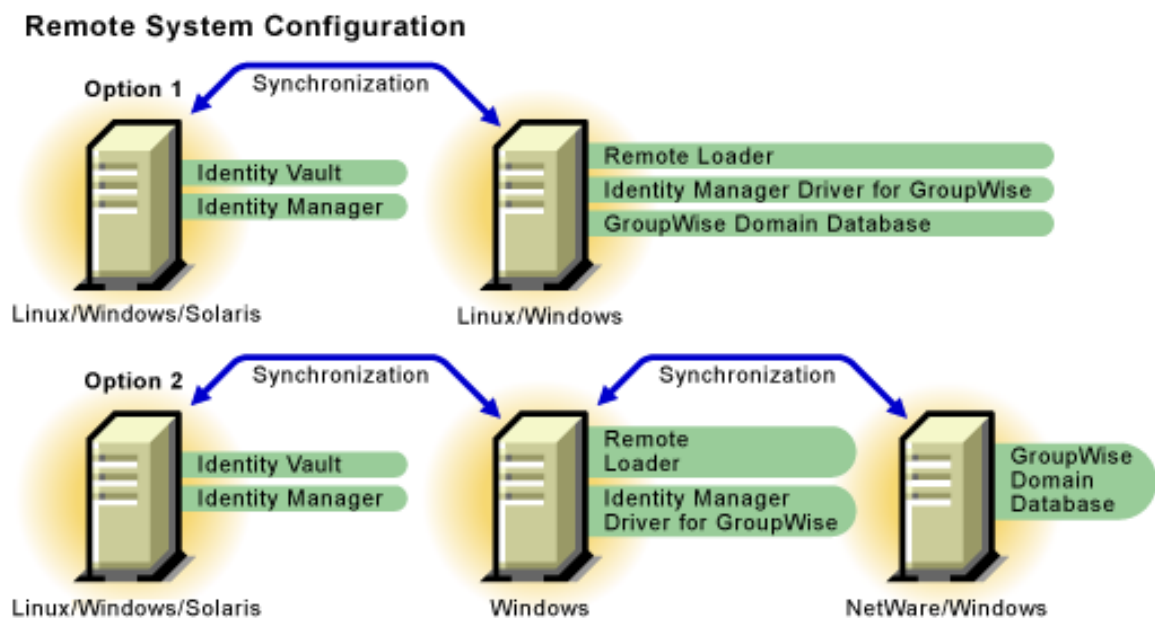
Having the driver connect to a GroupWise domain database on NFS, or any other type of mounted file system, is not supported. For example, the GroupWise driver running on Linux cannot connect to a domain database on another server through a mounted file system, and the GroupWise driver running on any server cannot connect to a domain database on a remote Linux server.

IMPORTANT: When the driver is installed on a Windows server and the GroupWise domain database resides on a remote Windows/NetWare server (Option 2 in [Figure 2-1](#)), you must install the Novell Client 4.9 or later or the Novell Client 2.0 or later on the driver's server.

2.1.2 Remote Installation

In a remote installation, the GroupWise driver is on a different server than the Metadirectory engine and Identity Vault. This can be a Windows/Linux server with the GroupWise domain database (Option 1) or a completely separate Windows server (Option 2). In both options, the driver uses the Remote Loader, installed on the same server as the driver, to communicate with the Metadirectory engine and the GroupWise domain database.

Figure 2-2 Remote System Configuration



A remote installation is the only option if:

- ◆ Your Metadirectory engine and Identity Vault are located on a Solaris server. The GroupWise driver does not run on a Solaris server. Therefore, you must run it on a Linux/Windows server through the Remote Loader.
- ◆ Your Metadirectory engine and Identity Vault are located on one Linux server and your GroupWise domain database is located on another Linux server.

IMPORTANT: When the driver is installed on a Windows server and the GroupWise domain database resides on a remote Windows/NetWare server (Option 2 in [Figure 2-1](#)), you must install the Novell Client 4.9 or later or the Novell Client 2.0 or later on the driver's server.

2.2 Installing the Driver Files

The following sections correspond to the scenarios in [Section 2.1, “Where to Install the GroupWise Driver,” on page 15](#). Complete the steps for the scenario you’ve chosen:

- ♦ [Section 2.2.1, “Local Installation,” on page 17](#)
- ♦ [Section 2.2.2, “Remote Installation,” on page 17](#)

2.2.1 Local Installation

Complete the following steps for a [local installation](#). In this scenario, the Metadirectory engine, Identity Vault, and GroupWise driver are on the same server. The GroupWise database is on the same server or a separate server.

- 1 Install the Metadirectory server (Metadirectory engine and drivers) on the same Linux/Windows server as the GroupWise domain database. This is Option 1 in [Figure 2-1, “Local System Configuration,” on page 15](#).

or

Install the Metadirectory server (Metadirectory engine and drivers) on a Windows server that can access the Windows/NetWare server where the GroupWise domain database resides. This is Option 2 in [Figure 2-1, “Local System Configuration,” on page 15](#).

For instructions, see “[Preparing to Install the Engine, Drivers, and Plug-ins](#)” in the *NetIQ Identity Manager Setup Guide*.

IMPORTANT: On the Windows server, if the driver is configured to connect to Groupwise 2012, ensure that Visual C++ 2008 Runtime Libraries are installed or the Groupwise 2012 client is installed on the driver machine. To download Visual C++ 2008, go to [Microsoft Downloads Web site \(http://www.microsoft.com/en-us/download/details.aspx?id=29\)](http://www.microsoft.com/en-us/download/details.aspx?id=29)

2.2.2 Remote Installation

Complete the following steps for a [remote installation](#). In this scenario, the GroupWise driver is on a different server than the Metadirectory engine and Identity Vault.

- 1 If you have not already done so, install a Metadirectory server. For instructions, see “[Preparing to Install the Engine, Drivers, and Plug-ins](#)” in the *NetIQ Identity Manager Setup Guide*.
- 2 Install the Remote Loader (and GroupWise driver) on the Windows/Linux server where the GroupWise domain database resides. This is Option 1 in [Figure 2-2, “Remote System Configuration,” on page 16](#).

or

Install the Remote Loader (and GroupWise driver) on a Windows server that can access the Windows/NetWare server where the GroupWise domain database resides. This is Option 2 in [Figure 2-2, “Remote System Configuration,” on page 16](#).

For instructions, see “[Preparing to Install the Engine, Drivers, and Plug-ins](#)” in the *NetIQ Identity Manager Setup Guide*.

2.3 Installing the Novell Client

The Novell Client enables access to GroupWise domain database that runs on a remote server. To do this, you need to install the Novell client on a server where the GroupWise driver is installed. The client enables the driver to access the GroupWise domain database on a remote server.

This scenario occurs when you implement Option 2 in [Figure 2-1, “Local System Configuration,”](#) on [page 15](#) or Option 2 in [Figure 2-2, “Remote System Configuration,”](#) on [page 16](#).

WARNING: Improper installation or removal of Novell Client on 64-bit UNIX and Windows systems sometimes damages the existing NCI security keys and their data, such as passwords and policies. To avoid this problem, install the Novell Client before installing eDirectory 8.8. SP5, which upgrades the NCI version to 2.7.7. To install the Novell Client after installing eDirectory or to uninstall the Novell Client, contact Novell/NetIQ customer support.

- 1 Download the Novell Client 4.9 or later from the [Novell Downloads \(http://download.novell.com\)](http://download.novell.com) site.
- 2 To install the client on the driver’s server, execute the file and follow on-screen the instructions.

3 Creating a New Driver Object

After the GroupWise driver files are installed on the server where you want to run the driver (see [Chapter 2, “Installing the Driver Files,” on page 15](#)), you can create the driver in the Identity Vault. You do so by installing the driver packages and then modifying the driver configuration to suit your environment. The following sections provide instructions:

- ♦ [Section 3.1, “Creating Accounts for Authentication,” on page 19](#)
- ♦ [Section 3.2, “Creating the Driver Object in Designer,” on page 20](#)
- ♦ [Section 3.3, “Associating Identity Vault Users and GroupWise Users,” on page 26](#)
- ♦ [Section 3.4, “Activating the Driver,” on page 26](#)

3.1 Creating Accounts for Authentication

If the GroupWise driver is on the same server as the GroupWise domain database, skip this section. No authentication accounts are required.

When the GroupWise driver is installed on a Windows server and the GroupWise domain database resides on a remote Windows/NetWare server, you need to create accounts on both servers to enable the driver to authenticate to the domain database server and access the database. This is the only remote database scenario (Windows server with the driver and remote Windows/NetWare server with the database) that is supported. For more information, see [Section 2.1, “Where to Install the GroupWise Driver,” on page 15](#).

When you create the user account for the Windows server that is running the driver:

- ♦ Add the user account to the Administrators group.
- ♦ Deselect any options that force the account password to be changed or that cause it to expire.
- ♦ In Administrative Tools, access *Local Security Policy > Local Policies > User Rights Assignment* and add the account to the *Log On as a Service* policy.

When you create the user account for the Windows/NetWare server where the GroupWise domain database resides:

- ♦ Use the same username and password you used for the account on the driver’s server.
- ♦ For a Windows server, create a new share for the drive where the GroupWise domain database resides. Remove the *Everyone* group from the share’s *Permissions* list. Add the driver’s user account to the *Permissions* list and give it *Full Control*.
- ♦ For a NetWare server, use iManager or ConsoleOne to give the user account Read, Write, Create, Erase, Modify, and File Scan access to the GroupWise domain directory and subdirectories.

3.2 Creating the Driver Object in Designer

To create the GroupWise driver object, install the driver packages and then modify the configuration to suit your environment. After you've created and configured the driver, you need to deploy it to the Identity Vault and start it.

- ♦ [Section 3.2.1, "Importing the Current Driver Packages," on page 20](#)
- ♦ [Section 3.2.2, "Installing the Driver Packages," on page 21](#)
- ♦ [Section 3.2.3, "Configuring the Driver Object," on page 23](#)
- ♦ [Section 3.2.4, "Deploying the Driver," on page 24](#)
- ♦ [Section 3.2.5, "Starting the Driver," on page 25](#)
- ♦ [Section 3.2.6, "Testing the Driver," on page 25](#)

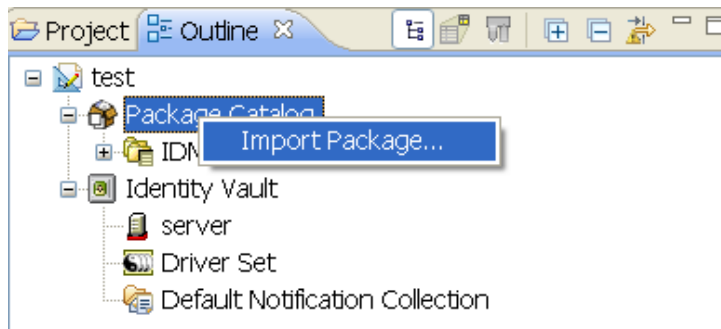
NOTE: You should not create driver objects by using the new Identity Manager 4.0 and later configuration files through iManager. This method of creating driver objects is no longer supported. To create drivers, you now need to use the new package management features provided in Designer.

3.2.1 Importing the Current Driver Packages

The driver packages contain the items required to create a driver, such as policies, entitlements, filters, and Schema Mapping policies. These packages are only available in Designer. You can upgrade any package that is installed if there is a newer version of the package available. It is recommended to have the latest packages in the Package Catalog before creating a new driver object.

To verify that you have the most recent version of the driver packages imported into the Package Catalog:

- 1 Open Designer.
- 2 In the toolbar, click *Help > Check for Package Updates*.
- 3 Click *OK* to update the packages
or
Click *OK* if the packages are up-to-date.
- 4 In the Outline view, right-click the Package Catalog.
- 5 Click *Import Package*.



- 6 Select any GroupWise driver packages
or

Click *Select All* to import all of the packages displayed.

By default, only the base packages are displayed. Deselect *Show Base Packages Only* to display all packages.

- 7 Click *OK* to import the selected packages, then click *OK* in the successfully imported packages message.
- 8 After the current packages are imported, continue with [Section 3.2.2, "Installing the Driver Packages,"](#) on page 21.

3.2.2 Installing the Driver Packages

After you have imported the current driver packages into the Package Catalog, you can install the driver packages to create a new driver.

- 1 In Designer, open your project.
- 2 In the Modeler, right-click the driver set where you want to create the driver, then click *New > Driver*.
- 3 Select *GroupWise Base*, then click *Next*.
- 4 Select the optional features to install for the GroupWise driver. All options are selected by default. The options are:
 - Entitlements:** These packages contain the policies and entitlements required to enable the driver for account creation and management with entitlements.
 - Password Synchronization:** These packages contain the policies required to enable password synchronization. Leave this option selected if you want to synchronize passwords to GroupWise.
 - Data Collection:** These packages contain the policies that enable the driver to collect data for reports. If you are using the Identity Reporting Module, verify that this option is selected. For more information, see the [NetIQ Identity Reporting Module Guide](#).
 - Account Tracking:** These packages contain the policies that enable account tracking information for reports. If you are using the Identity Reporting Module, verify that this option is selected. For more information, see the [NetIQ Identity Reporting Module Guide](#).
- 5 After selecting the optional packages, click *Next*.
- 6 (Conditional) If there are package dependencies for the packages you selected to install, you must install these dependencies to install the selected packages. Click *OK* to install the Common Settings package, if you have not installed any other packages into the selected driver set.
- 7 (Conditional) Click *OK* to install the Password Synchronization Notification package dependency.
- 8 (Conditional) Fill in the following fields on the Common Settings page:

The Common Settings page is displayed only if the Common Settings package is installed as a dependency.

 - User Container:** Select the Identity Vault container where the users are added if they don't already exist in the Identity Vault. This value becomes the default value for all drivers in the driver set.

If you want a unique location for this driver, set the value for all drivers on this page. After the driver is created, change the value on the driver's Global Configuration Values page.

- Group Container:** Select the Identity Vault container the groups are added if they don't already exist in the Identity Vault. This value becomes the default value for all drivers in the driver set.

If you want a unique location for this driver, set the value for all drivers on this page. After the driver is created, change the value on the driver's Global Configuration Values page.
- 9 Click *Next*.

- 10 (Conditional) Fill in the following fields on the Common Settings page:

The Common Settings page is displayed only if the Common Settings package is installed as a dependency.

User Container: Select the Identity Vault container where the users are added if they don't already exist in the Identity Vault. This value becomes the default value for all drivers in the driver set.

If you want a unique location for this driver, set the value for all drivers on this page. After the driver is created, change the value on the driver's Global Configuration Values page.

Group Container: Select the Identity Vault container the groups are added if they don't already exist in the Identity Vault. This value becomes the default value for all drivers in the driver set.

If you want a unique location for this driver, set the value for all drivers on this page. After the driver is created, change the value on the driver's Global Configuration Values page.

- 11 On the Install GroupWise Base page, specify the name of the driver, then click *Next*:

- 12 On the Install GroupWise Base page, fill in the following field, then click *Next*:

Domain Server: Specify the name or IP address of the server that contains the GroupWise domain database (`wdomain.db`) the driver connects to.

You should use the primary domain database. Leave this field blank when the GroupWise domain database is on the same physical server as this driver. The format options are the hostname of the remote server, the DNS name of the remote server, or the IP address of the remote server.

- 13 On the Install GroupWise Base page, fill in the following field, then click *Next*:

Default Sync Destination: GroupWise Post Office: Specify the GroupWise post office in which newly added Identity Vault objects are created. Use the browse button to select the GroupWise post office, or specify the GroupWise post office name as a distinguished name (DN) in slash format. For example: `GW\GWSystem\PO1`.

- 14 Fill in the following fields for Remote Loader information:

Connect To Remote Loader: Select *Yes* or *No* to determine if the driver will use the Remote Loader. For more information, see the [Activating Identity Manager](#) in the *NetIQ Identity Manager Setup Guide*.

If you select *No*, skip to [Step 15](#). If you select *Yes*, use the following information to complete the configuration of the Remote Loader, then click *Next*:

Host Name: Specify the IP address or DNS name of the server where the Remote Loader is installed and running.

Port: Specify the port number for this driver. Each driver connects to the Remote Loader on a separate port. The default value is 8090.

Remote Loader Password: Specify a password to control access to the Remote Loader. It must be the same password that is specified as the Remote Loader password on the Remote Loader.

Driver Password: Specify a password for the driver to authenticate to the Metadirectory server. It must be the same password that is specified as the Driver Object Password on the Remote Loader.

- 15 (Conditional) Fill in the following field on the Account Tracking Information page, then click *Next*:

This page is displayed only if you selected to install the Data Collection and Account Tracking groups of packages.

Realm: Specify the name of the realm, security domain, or namespace in which the account name is unique.

- 16 (Conditional) Fill in the following fields on the Managed System Information page, then click *Next*:

This page is displayed only if you selected to install the Data Collection and Account Tracking groups of packages.

Name: Specify a descriptive name for this GroupWise system. The name is displayed in the reports.

Description: Specify a brief description of the this GroupWise system. The description is displayed in the reports.

Location: Specify the physical location of this GroupWise system. The location is displayed in the reports.

Vendor: Select *NetIQ, Inc.* as the vendor of this system. The vendor information is displayed in the reports.

Version: Specify the version of this GroupWise system. The version is displayed in the reports.

- 17 (Conditional) Fill in the following fields on the Managed System Information page, then click *Next*:

This page is displayed only if you selected to install the Data Collection and Account Tracking groups of packages.

Business Owner: Select a user object in the Identity Vault that is the business owner of this GroupWise system. This can only be a user object, not a role, group, or container.

Application Owner: Select a user object in the Identity Vault that is the application owner for this GroupWise system. This can only be a user object, not a role, group, or container.

- 18 (Conditional) Fill in the following fields on the Managed System Information page, then click *Next*:

This page is displayed only if you selected to install the Data Collection and Account Tracking groups of packages.

Classification: Specify the classification for this GroupWise system in your environment. For example, *Mission-Critical*. If you select *Other*, you must specify a custom classification for the GroupWise system. This information is displayed in the reports.

Environment: Specify the type of environment the GroupWise system provides. For example, *Development*, *Test*, or *Production*. If you select *Other*, you must specify a custom classification for the GroupWise system. This information is displayed in the reports.

Authentication IP Address: Specify the IP address used to authenticate to the GroupWise system.

Authentication Port: Specify the port used to authenticate to the GroupWise system.

Authentication ID: Specify the user ID used to authenticate to the GroupWise system.

- 19 Review the summary of tasks that will be completed to create the driver, then click *Finish*.

- 20 After the driver packages are installed, you can modify the configuration settings by continuing with the next section, continue to [Section 3.2.3, "Configuring the Driver Object,"](#) on page 23.

3.2.3 Configuring the Driver Object

After installing the driver packages, you can configure the driver to suit your environment. Complete the following tasks to configure the driver:

- ♦ **Configure the driver parameters:** There are many settings that can help you customize and optimize the driver. The settings are divided into categories such as Driver Configuration, Engine Control Values, and Global Configuration Values (GCVs). Although it is important for you to


understand all of the settings, your first priority should be to review the [Driver Parameters](#) located on the Driver Configuration page. The Driver Parameters let you configure the LDAP directory type, publication method, and other parameters associated with the Publisher channel.

- ♦ **Customize the driver policies and filter:** The driver policies and filter control data flow between the Identity Vault and GroupWise. You should ensure that the policies and filters reflect your business needs. For instructions, see [Chapter 5, “Customizing the Driver by Using Policies and Filters,”](#) on page 29.

After completing the configuration tasks, continue with the next section, [Deploying the Driver](#).

3.2.4 Deploying the Driver

After a driver object is created in Designer, it must be deployed into the Identity Vault.

- 1 In Designer, open your project.
- 2 In the Modeler, right-click the driver icon  or the driver line, then select *Live > Deploy*.
- 3 If you are authenticated to the Identity Vault, skip to [Step 5](#); otherwise, specify the following information:

Host: Specify the IP address or DNS name of the server hosting the Identity Vault.

Username: Specify the DN of the user object used to authenticate to the Identity Vault.

Password: Specify the user's password.

- 4 Click *OK*.
- 5 Read through the deployment summary, then click *Deploy*.
- 6 Read the successful message, then click *OK*.
- 7 Click *Define Security Equivalence* to assign rights to the driver.

The driver requires rights to objects within the Identity Vault. 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 the Identity Vault. If you are creating external post offices, the driver also needs read/write access to the domain.

The Admin user object is most often used to supply these rights. However, you might want to create a DriversUser (for example) and assign security equivalence to that user.

7a Click *Add*, then browse to and select the object with the correct rights.

7b Click *OK* twice.

For more information about defining a Security Equivalent User in objects for drivers in the Identity Vault, see “Establishing a Security Equivalent User” in the [Identity Manager 4.0.2 Security Guide](#).

- 8 Click *Exclude Administrative Roles* to exclude users that should not be synchronized.

You should exclude any administrative User objects (for example, Admin and DriversUser) from synchronization.

8a Click *Add*, then browse to and select the user object you want to exclude.

8b Click *OK*.

8c Repeat [Step 8a](#) and [Step 8b](#) for each object you want to exclude.

8d Click *OK*.


- 9 Click *OK*.

- 10 Continue with the next section, [Section 3.2.5, “Starting the Driver,”](#) on page 25.

3.2.5 Starting the Driver

When a driver is created, it is stopped by default. To make the driver work, you must start the driver and cause events to occur. Identity Manager is an event-driven system, so after the driver is started, it won't do anything until an event occurs.

To start the driver:

- 1 In Designer, open your project.
- 2 In the Modeler, right-click the driver icon  or the driver line, then select *Live > Start Driver*.
- 3 Continue with the next section, [Testing the Driver](#).

3.2.6 Testing the Driver

After you start the driver, you should test it to ensure that it is working properly. 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 Make sure the driver is started. See [Section 3.2.5, "Starting the Driver," on page 25](#).
- 2 Add a new user to the Identity Vault.
You need to specify only the Name and Surname attributes for this user.
- 3 Open ConsoleOne with the GroupWise snap-ins.
- 4 Verify that a new GroupWise account was created in the correct post office.
- 5 Using NetIQ iManager, delete the user from the Identity Vault.


The default driver import file converts Identity Vault deletes to GroupWise Disable events. This results in a disabled external user in GroupWise. This can be changed through the global configuration values.

- 6 Using ConsoleOne with the GroupWise snap-ins, verify that the GroupWise account is external and disabled (assuming you are using the default configuration).
Use ConsoleOne with the GroupWise snap-ins to verify that the changes have been synchronized with GroupWise.

3.3 Associating Identity Vault Users and GroupWise Users

The first time an event occurs on an Identity Vault user that triggers the GroupWise driver (based on the driver filter), the GroupWise driver uses its Matching policy to associate the Identity Vault user with the appropriate user in the GroupWise domain database.

If desired, you can pre-associate Identity Vault and GroupWise users. This is done through the migration tool in iManager. The migration tool initiates a synchronization of the selected users to GroupWise, causing the Metadirectory engine to apply the driver's Matching, Placement, and Creation policies and filter to the users.

- 1 In iManager, click  to display the Identity Manager Administration page.
- 2 Open the driver set that contains the GroupWise driver:
 - 2a In the *Administration* list, click *Identity Manager Overview*.
 - 2b If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.
 - 2c Click the driver set to open the Driver Set Overview page.
- 3 Click the GroupWise driver icon to display the Driver Overview page.
- 4 Click *Migrate > Migrate from Identity Vault*.
- 5 Click *Add*, then select the container or user objects you want associated.
- 6 Click *OK*.

When you use 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.

3.4 Activating the Driver

If you created the driver in a driver set where you have already activated the Metadirectory engine and service drivers, the driver inherits the activation. If you created the driver in a driver set that has not been activated, you must activate the driver within 90 days. Otherwise, the driver stops working.

For information on activation, refer to "[Activating Identity Manager](#)" in the *NetIQ Identity Manager Setup Guide*.

4 Upgrading an Existing Driver

The following sections provide information to help you upgrade an existing driver to version 4.5:

- ♦ [Section 4.1, “Supported Upgrade Paths,” on page 27](#)
- ♦ [Section 4.2, “What’s New in Version 4.5,” on page 27](#)
- ♦ [Section 4.3, “Upgrade Procedure,” on page 27](#)

4.1 Supported Upgrade Paths

You can upgrade from any 3.x version of the GroupWise driver. Upgrading a pre-3.x version of the driver directly to version 4.5 is not supported.

4.2 What’s New in Version 4.5

Version 4.5 of the GroupWise driver does not include any new features.

4.3 Upgrade Procedure

The process for upgrading the GroupWise driver is the same as for other Identity Manager drivers. For detailed instructions, see [“Upgrading the Identity Manager Drivers”](#) in the *NetIQ Identity Manager Setup Guide*.

5 Customizing the Driver by Using Policies and Filters

This section explains how to use and modify policies and filters to synchronize data between the Identity Vault and GroupWise according to your specific business rules.

The GroupWise driver synchronizes data and events from the Identity Vault 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 5.1, “Default Driver Actions,” on page 29](#)
- ◆ [Section 5.2, “Modifying Default Settings in Policies and the Filter,” on page 29](#)
- ◆ [Section 5.3, “Modifying Policies,” on page 30](#)
- ◆ [Section 5.4, “Setting GroupWise Client Options with the Driver,” on page 53](#)
- ◆ [Section 5.5, “Client Options Quick Reference,” on page 94](#)

5.1 Default Driver Actions

The driver performs several actions by default:

- ◆ The user's Identity Vault 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.

5.2 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 30](#) 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 30](#) for more information.
3. Modify the Subscriber Create policy. See [“Modifying the Create Policy” on page 30](#) for more information.
4. Modify the Subscriber Placement policy. See [“Modifying Policies” on page 30](#).

5.2.1 Modifying the Driver Filter

The driver filter contains the Identity Vault 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" publisher="ignore"
subscriber="sync"/>
```

5.2.2 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 Identity Vault 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.

5.2.3 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 A.2, "Global Configuration Values," on page 114](#).

5.2.4 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.

5.3 Modifying Policies

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

- ◆ [Section 5.3.1, "Specifying the GroupWise Post Office," on page 31](#)
- ◆ [Section 5.3.2, "Specifying Distribution Lists," on page 33](#)
- ◆ [Section 5.3.3, "Setting Defaults for GroupWise Attributes," on page 37](#)
- ◆ [Section 5.3.4, "Configuring the GroupWise UserID," on page 38](#)
- ◆ [Section 5.3.5, "Creating Mappings for Additional Attributes," on page 39](#)
- ◆ [Section 5.3.6, "Getting a Record Count from a Query," on page 39](#)
- ◆ [Section 5.3.7, "Deleting the GroupWise User without Deleting the Identity Vault User," on page 39](#)

- ◆ Section 5.3.8, “Creating a GroupWise Nickname,” on page 40
- ◆ Section 5.3.9, “Creating a GroupWise Nickname Record,” on page 40
- ◆ Section 5.3.10, “Specifying a New Resource Owner on an Owner Delete,” on page 41
- ◆ Section 5.3.11, “Specifying a New Resource Owner on an Owner Disable,” on page 42
- ◆ Section 5.3.12, “Controlling Creation of GroupWise Accounts,” on page 43
- ◆ Section 5.3.13, “Moving Users from One Post Office to Another Post Office,” on page 44
- ◆ Section 5.3.14, “Adding Additional Attributes to Be Synchronized,” on page 44
- ◆ Section 5.3.15, “Renaming Users,” on page 45
- ◆ Section 5.3.16, “Creating a Gateway Alias,” on page 45
- ◆ Section 5.3.17, “Querying for a Nickname,” on page 46
- ◆ Section 5.3.18, “Querying for a Gateway Alias,” on page 48
- ◆ Section 5.3.19, “Querying for Internet EMail Address,” on page 48
- ◆ Section 5.3.20, “Synchronizing GroupWise External Users,” on page 49
- ◆ Section 5.3.21, “Verifying if an E-Mail Address or Gateway Alias Is Unique,” on page 52

5.3.1 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 Identity Vault user container.

[Figure 5-1](#) shows a policy created in Policy Builder that specifies the post office based on the Identity Vault container where the user was created.

Figure 5-1 Placement Policy Specifying a Post Office Based on the Identity Vault Container

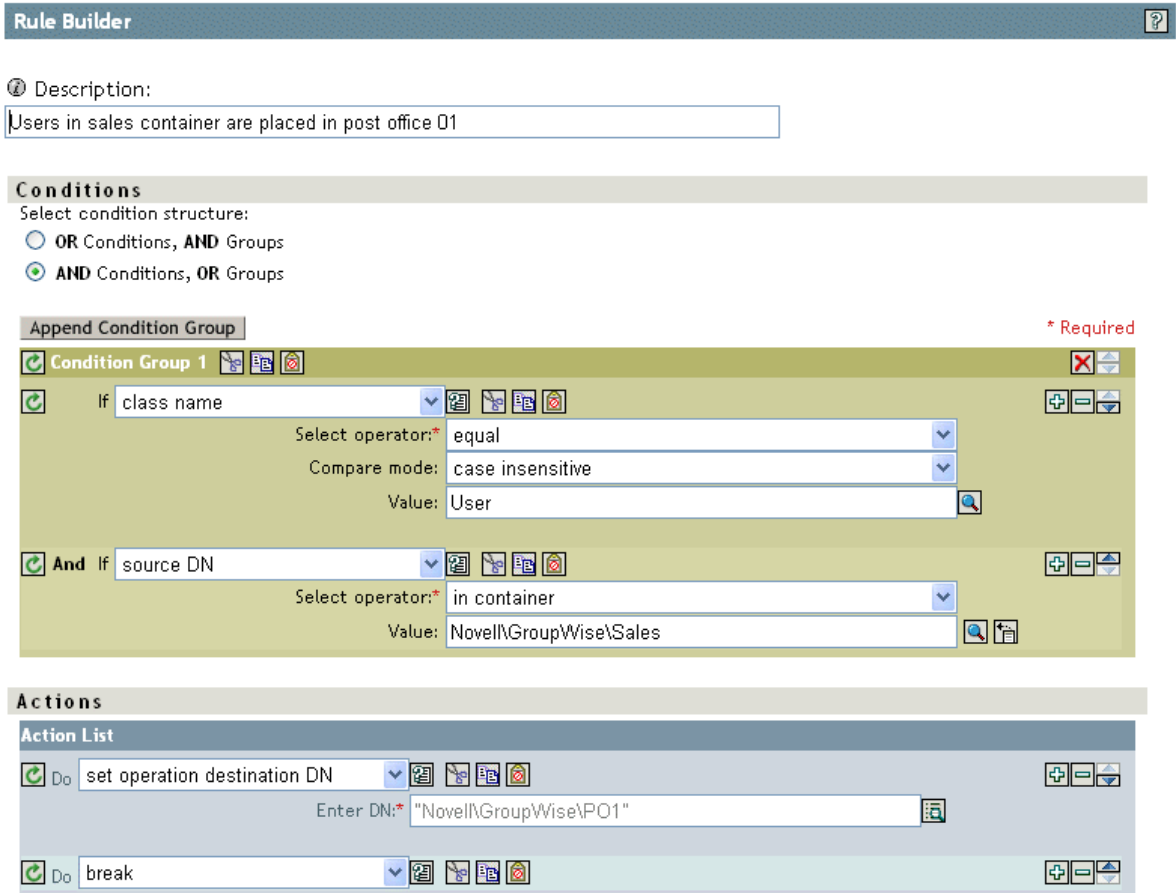
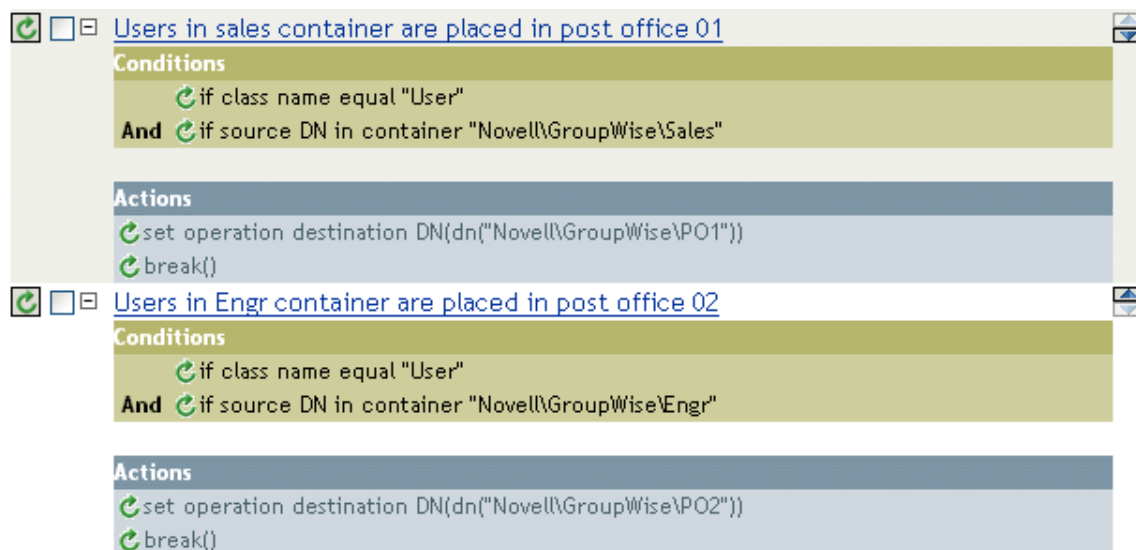


Figure 5-2 shows the policies needed to place users in the Sales container into PO1 and users in the Engineering container into PO2.

Figure 5-2 Placement Policy for Placing Users in Different Containers



5.3.2 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 Identity Vault user is created, the GroupWise account can be added to a distribution list based on the Identity Vault 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.

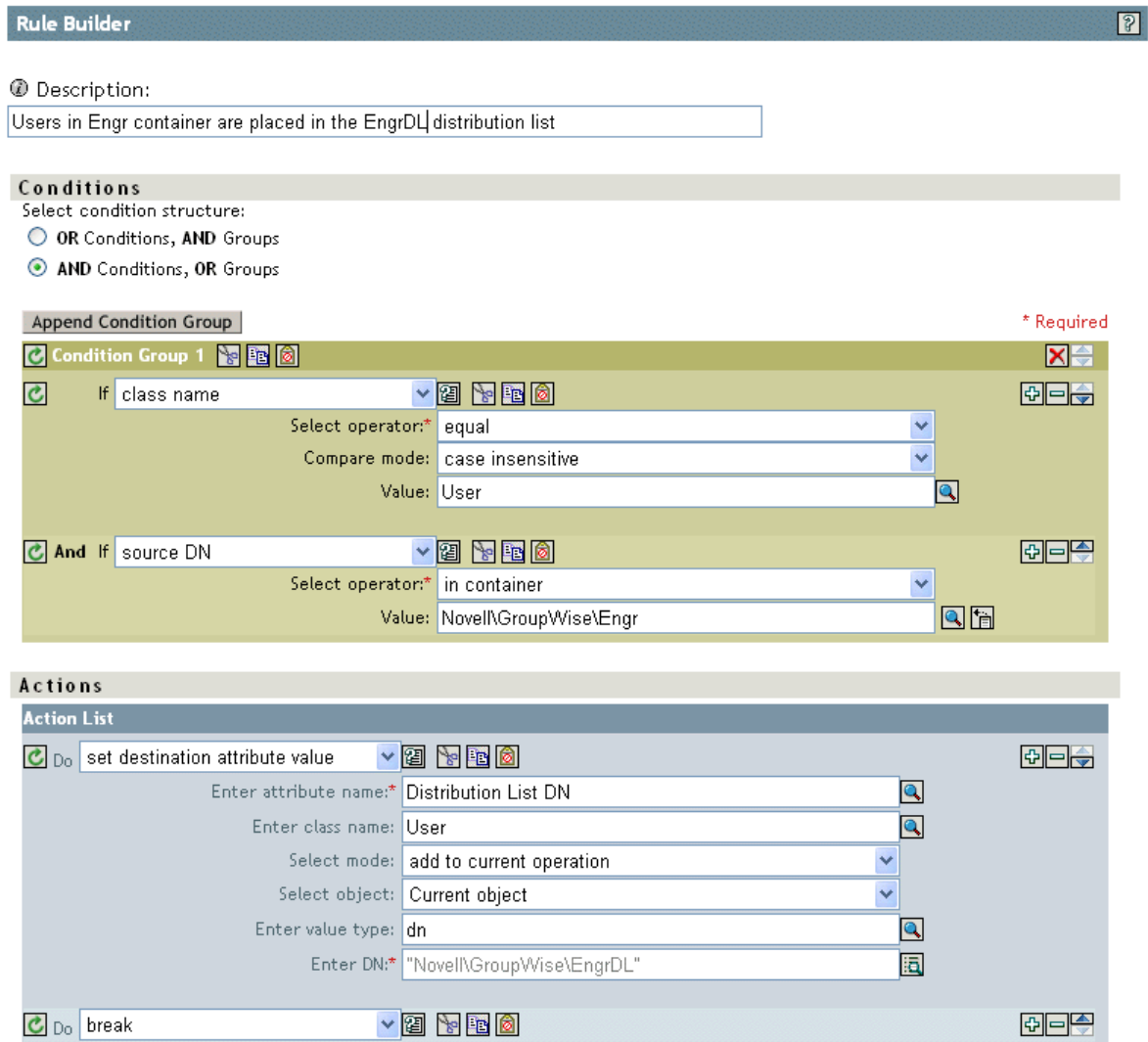
The policies in this section, created by using the Policy Builder, show how to configure the following actions:

- ♦ [“Creating a New User as a Member of a Distribution List Based on the User’s Identity Vault Container” on page 34](#)
- ♦ [“Adding a User as a Blind Copy or Carbon Copy Participant in a Distribution List” on page 34](#)
- ♦ [“Adding a User to a Distribution List When He or She Becomes a Manager” on page 35](#)
- ♦ [“Removing a User from a Distribution List When the User is No Longer a Manager” on page 36](#)
- ♦ [“Removing a User from All Distribution Lists” on page 37](#)

In the 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 Identity Vault Container

Figure 5-3 Create Policy



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 5-4 Adding a User to a Distribution List

The screenshot shows the 'Rule Builder' interface 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 5-5 Removing a User from a Distribution List

The screenshot displays a configuration interface with two main sections: a condition and an action list.

Condition Section:

- Operation: **And If**
- Attribute: **operation attribute**
- Enter name: **isManager**
- Select operator: **changing from**
- Compare mode: **case insensitive**
- Value: **true**

Actions Section:

Action List

- Operation: **Do**
- Action: **remove 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 All Distribution Lists

Figure 5-6 Removing a User from All Distribution Lists

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

- Description:** Remove a user from all distribution lists
- Conditions:**
 - Select condition structure: AND Conditions, OR Groups
 - Append Condition Group: * Required
 - Condition Group 1:
 - If class name: [dropdown]
 - Select operator: equal
 - Compare mode: case insensitive
 - Value: User
- Actions:**
 - Action List:
 - Do clear destination attribute value [dropdown]
 - Enter attribute name: Distribution List DN
 - Enter class name: User
 - Select mode: add to current operation
 - Select object: Current object

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

5.3.3 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 the Identity Vault and GroupWise. When the Identity Vault user object contains a corresponding attribute, it must be set. It is important that attribute values are set in both the Identity Vault and GroupWise. If the attribute is set only in GroupWise, it could be overwritten with the value in the Identity Vault. You must customize the driver to update values in the Identity Vault; the driver does not do this by default.

The following example sets the Description attribute in the Identity Vault and GroupWise. The attribute write-back = "true" causes the attribute to also be written in the Identity Vault.

```

<rule>
  <description>GroupWise Account Required Attributes</description>
  <conditions>
    <and>
      <if-class-name op="equal">User</if-class-name>
    </and>
  </conditions>
  <actions>
    <do-set-default-attr-value name="Description" write-back="true">
      <arg-value type="string">
        <token-text xml:space="preserve">eDirectory User synchronized by
GroupWise Driver</token-text>
      </arg-value>
    </do-set-default-attr-value>
  </actions>
</rule>

```

5.3.4 Configuring the GroupWise UserID

The CN attribute in the Identity Vault is used to name the GroupWise account. You must include this in the Create policy as a required attribute. The CN value from the Identity Vault can be ignored in the Subscriber Create policy and a CN based on other attributes can be generated. An example of 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 45](#) for more information.

```

<rule>
  <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>

```

5.3.5 Creating Mappings for Additional Attributes

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

The Schema Mapping rule code segment below connects the Identity Vault 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.

5.3.6 Getting a Record Count from a Query

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

```
<nds dtdversion="2.0" ndsversion="8.x">
  <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>

      <!-- 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.

5.3.7 Deleting the GroupWise User without Deleting the Identity Vault User

After deleting the user in GroupWise, the driver cleans up the GroupWise attributes in the Identity Vault. 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>

```

5.3.8 Creating a GroupWise Nickname

GroupWise nicknames can be automatically created when an Identity Vault 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 Identity Vault rename occurs or when a GroupWise account is moved. When you set this option to False, nicknames are not created. Nickname creation requires GroupWise 8.0 or higher agents to be running.

5.3.9 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.)

Example 1

```
<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>
```

Example 2

```
<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>
```

5.3.10 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 to substitute for the default user. Using the Output Transformation policy, the Identity Vault 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 with the override owner, the resources are automatically assigned to the default user specified in the driver options. The DirXML Script 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-owner-dn">
        <arg-string>
          <token-text
xml:space="preserve">\GWDRIVERTREE\novell\users\sales\ResourceOwner</token-text>
          </arg-string>
        </do-set-xml-attr>
      </actions>
    </rule>
  </policy>
```

5.3.11 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 Identity Vault 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 to substitute for the default user. Using the Output Transformation policy, the Identity Vault 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 with 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 Disable</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="modify-attr[@attr-name='50058']"
name="gw:resource-owner-dn">
        <arg-string>
          <token-text
xml:space="preserve">\GWDRIVERTREE\novell\users\sales\ResourceOwner>
          </arg-string>
        </do-set-xml-attr>
      </actions>
    </rule>
  </policy>

```

5.3.12 Controlling Creation of GroupWise Accounts

There might be situations where an Identity Vault user is created and you do not want to create a corresponding GroupWise account. In addition, not all Identity Vault 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 by using an extended attribute such as createGroupWiseAccount.

The Identity Vault schema must be extended to include the createGroupWiseAccount attribute. 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>

```

5.3.13 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 8.0 or higher snap-ins for user moves.

When the Output Transformation style sheet is configured to move GroupWise accounts, we recommend that user moves be made in the Identity Vault and that the driver assign the object to a new post office in GroupWise. The DirXML script 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-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>
```

5.3.14 Adding Additional Attributes to Be Synchronized

You can map up to twenty user Identity Vault 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 Identity Vault 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.

5.3.15 Renaming Users

We recommend that you rename users by changing the naming attribute in the Identity Vault 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. In Example 1 below, the Identity Vault attribute Given Name is used to name the GroupWise account. When Given Name is modified, a GroupWise rename is generated. In Example 2 below, the Identity Vault User object is renamed. 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 8.0 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>
```

5.3.16 Creating a Gateway Alias

The following DirXML Script 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>

```

5.3.17 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. This creates two nickname records (User2a and User2b) that both reference User2c. The following DirXML Script sample code queries the User of the current event for nicknames.

Code Sample

```

<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>
    <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="4.0" ndsversion="8.x">
  <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>
    <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>

```

5.3.18 Querying for a Gateway Alias

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

Code Sample

```
<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="4.0" ndsversion="8.x">
  <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>
```

5.3.19 Querying for Internet EMail Address

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

Code Sample

```
<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="4.0" ndsversion="8.x">
  <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>
```

5.3.20 Synchronizing GroupWise External Users

In your business, you might have several different e-mail applications. Although not all employees 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.

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 following sections explain how to implement this functionality:

- ♦ [“Creating External Users” on page 50](#)
- ♦ [“Specifying an External Post Office in an Add Event” on page 50](#)
- ♦ [“Creating External Post Offices” on page 51](#)
- ♦ [“Specifying a Non-GroupWise Domain in an Add Event” on page 51](#)

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 Identity Vault object associated with the external post office. For additional information, refer to [“Creating External Post Offices” on page 51](#).
- ♦ Identify the external post office by [“Specifying an External Post Office in an Add Event” on page 50](#).
- ♦ Create a user in an organizational unit associated with the External GroupWise Post Office. For more information, see [“Synchronize eDir OrgUnit To GroupWise External Post Office:” on page 116](#).

When you create accounts in the Identity Vault for a non-GroupWise user, make sure that `gw:classification=“external”` attribute 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 [Synchronize GroupWise External Entity Objects](#) and [Synchronize eDir OrgUnit to GroupWise External Post Office](#) 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 Identity Vault object, such as an Organizational Unit (recommended). Select [Synchronize eDir OrgUnit to GroupWise External Post Office](#) 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 51](#).

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 [“Synchronize eDir OrgUnit To GroupWise External Post Office:” on page 116](#), 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>
```

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 you create 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>

```

5.3.21 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. Use the following example to first query if an e-mail address is in use, then based on the query results, it tests if it was in use or not.

```

<rule>
  <description> Query to see if e-mail address is unique in GroupWise</description>
  <actions>
    <do-set-local-variable name="PROPOSED-EMAIL" scope="policy">
      <arg-string>
        <token-text xml:space="preserve">Lee.Kristen@KristensRUs.com</token-text>
      </arg-string>
    </do-set-local-variable>
    <do-set-local-variable name="EMAIL" scope="policy">
      <arg-node-set>
        <token-query class-name="User">
          <arg-match-attr name="Internet EMail Address">
            <arg-value type="string">
              <token-local-variable name="PROPOSED-EMAIL"/>
            </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>
    <do-if>
      <arg-conditions>
        <and>
          <if-xpath op="true">$EMAIL</if-xpath>
        </and>
      </arg-conditions>
      <arg-actions>
        <do-trace-message>
          <arg-string>
            <token-text xml:space="preserve">Email address is in use by the user </
token-text>
          <token-xpath expression="$EMAIL/@src-dn"/>
          </arg-string>
        </do-trace-message>
      </arg-actions>
      <arg-actions>
        <do-trace-message>
          <arg-string>
            <token-text xml:space="preserve">Email address not found, you are free
to use it.</token-text>
          </arg-string>
        </do-trace-message>
      </arg-actions>
    </do-if>
  </actions>
</rule>

```

5.4 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 5.4.1, “Using Policies to Set Client Options,” on page 53](#)
- ♦ [Section 5.4.2, “Client Options,” on page 55](#)

NOTE: Some client options cannot be set through the GroupWise driver. Only the client options that can be controlled by the driver are covered in this guide. For a list of the client options that can be set through the driver, see [Section 5.5, “Client Options Quick Reference,” on page 94](#).

5.4.1 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 53](#)
- ♦ [“Example Procedure” on page 54](#)

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*.

Action 1

Do:

Specify attribute name: *

Specify class name:

Select mode:

Select object:

Specify value type:

Enter components: *

- 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.

5.4.2 Client Options

To view the client options:

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



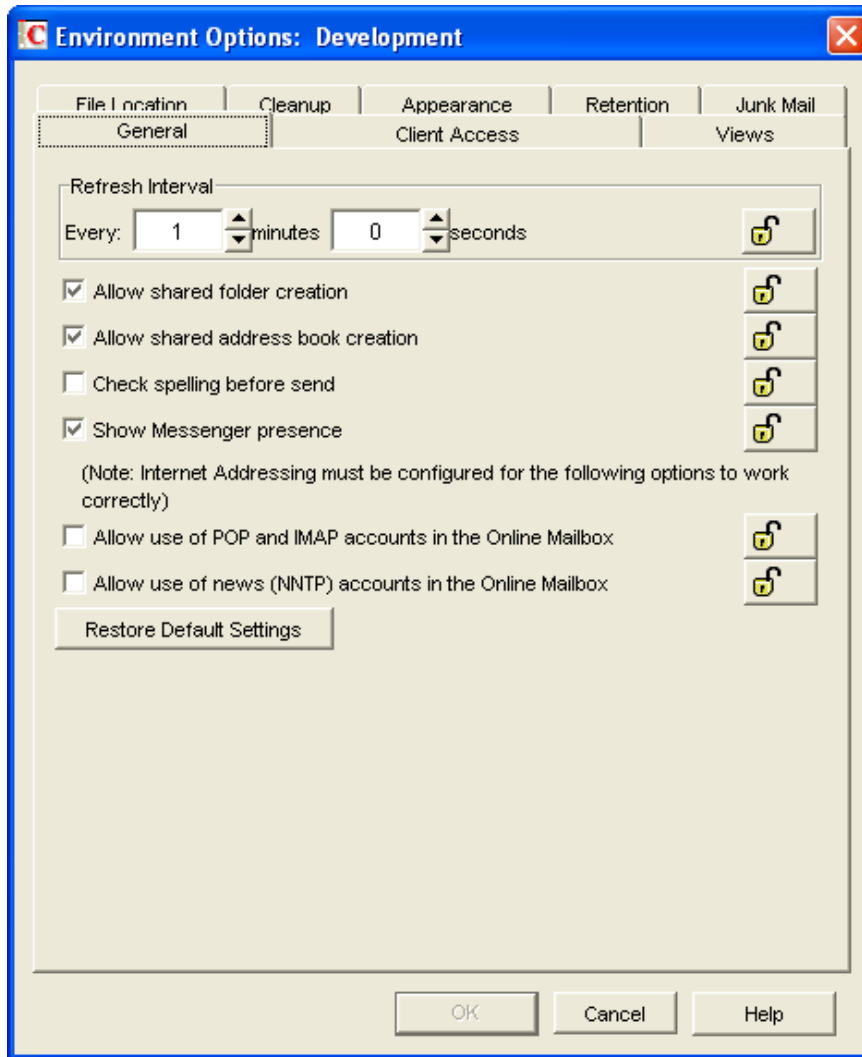
Use the following information to create policies to set the GroupWise client options on user objects.

- ◆ [Section 5.4.3, “Environment > General,” on page 56](#)
- ◆ [Section 5.4.4, “Environment > Client Access,” on page 59](#)
- ◆ [Section 5.4.5, “Environment > Views,” on page 61](#)
- ◆ [Section 5.4.6, “Environment > File Location > Archive Directory,” on page 63](#)
- ◆ [Section 5.4.7, “Environment > Cleanup,” on page 65](#)
- ◆ [Section 5.4.8, “Send > Send Options,” on page 67](#)
- ◆ [Section 5.4.9, “Send > Mail,” on page 71](#)
- ◆ [Section 5.4.10, “Send > Appt,” on page 74](#)
- ◆ [Section 5.4.11, “Send > Task,” on page 77](#)
- ◆ [Section 5.4.12, “Send > Note,” on page 79](#)
- ◆ [Section 5.4.13, “Send > Security,” on page 82](#)
- ◆ [Section 5.4.14, “Send > Disk Space Management,” on page 84](#)
- ◆ [Section 5.4.15, “Date and Time > Calendar,” on page 87](#)
- ◆ [Section 5.4.16, “Date and Time > Calendar > Alarm Options,” on page 89](#)
- ◆ [Section 5.4.17, “Date and Time > Busy Search,” on page 91](#)

5.4.3 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 5-7 Environment Options 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>
  <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.

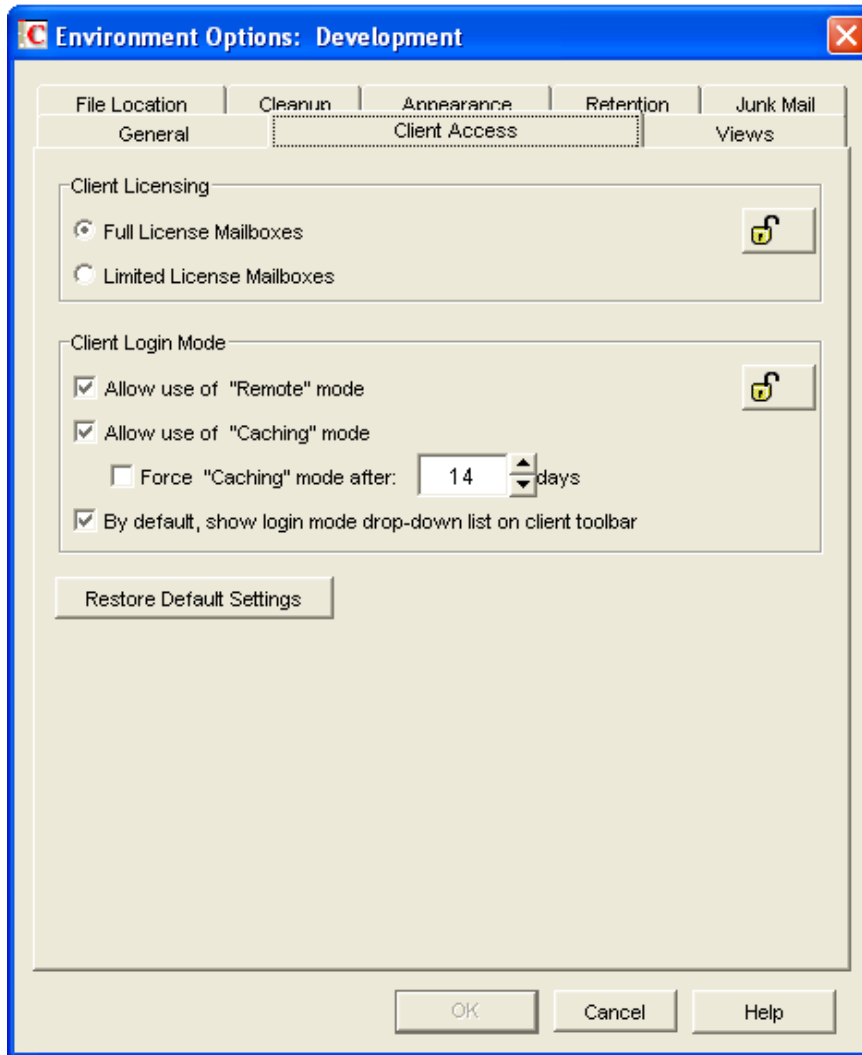
Show Messenger Presence

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.

5.4.4 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 5-8 Environment Options 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:

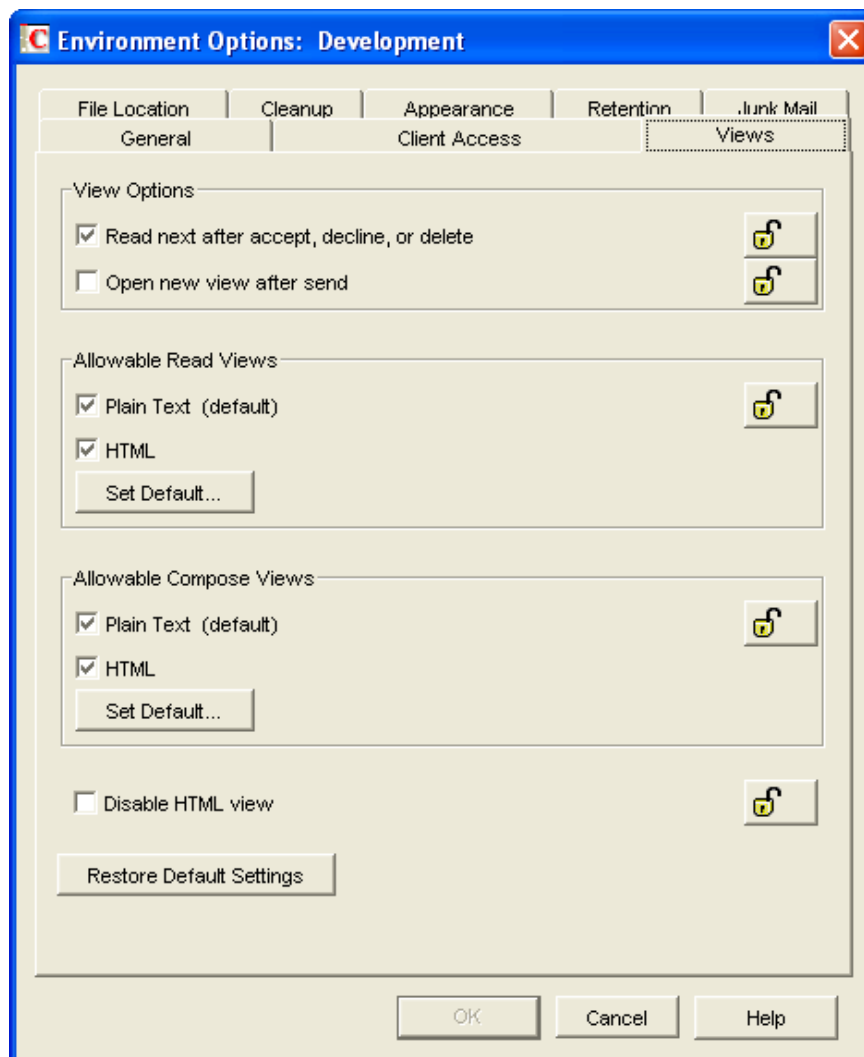
- ♦ The GroupWise WebAccess client (including wireless devices)
- ♦ A GroupWise client (Windows or WebAccess) via the Proxy feature
- ♦ A GroupWise client (Windows or WebAccess) via the Busy Search feature
- ♦ A POP or IMAP client

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.

5.4.5 Environment > Views

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

Figure 5-9 Environment Options 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:

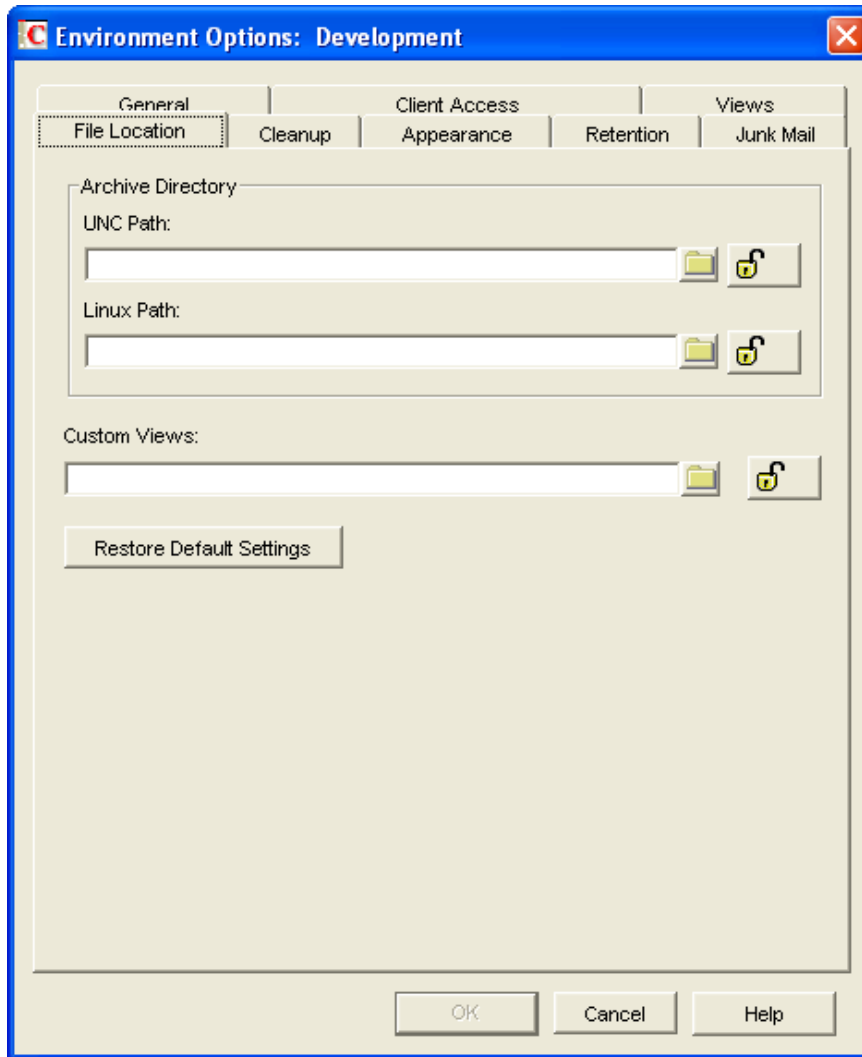
- ♦ **Plain Text:** Setting the value to `Text` allows users to compose items in plain text.
- ♦ **HTML:** Setting the value to `HTML` allows users to compose items in HTML.

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

5.4.6 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 5-10 Environment Options 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

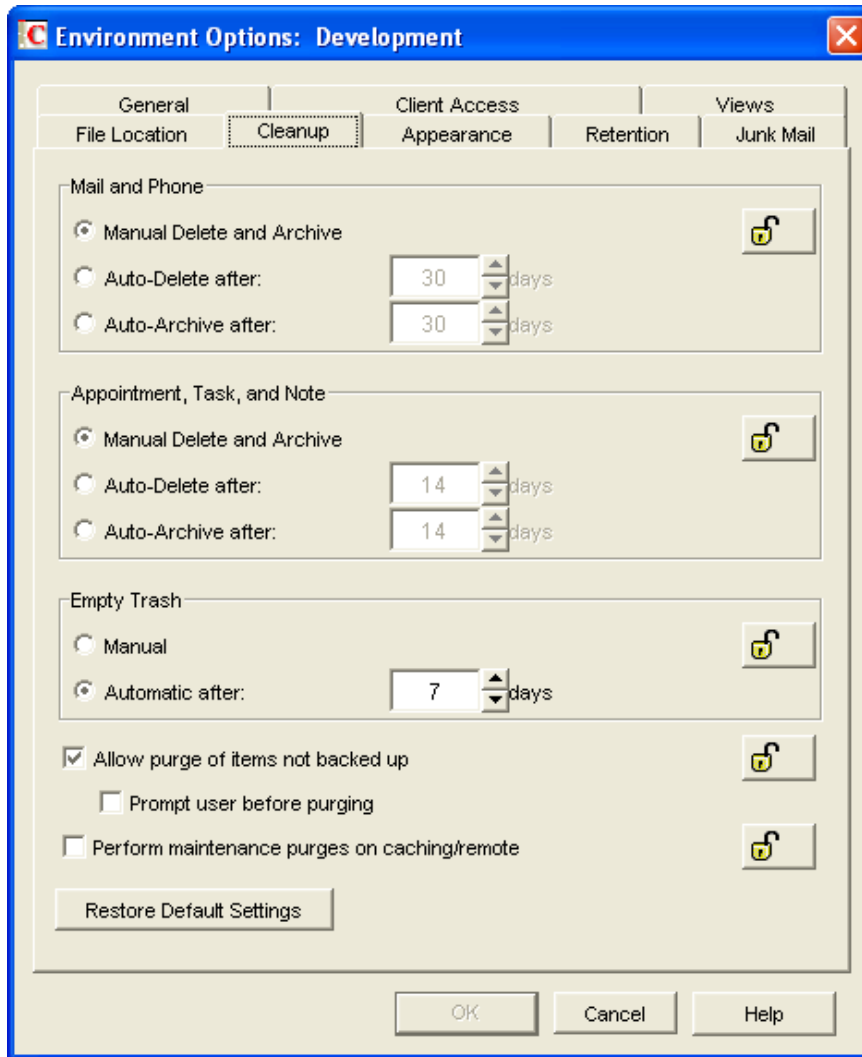
The `archiveLocationLinux` field is the Linux path of a local or personal directory where archived messages are stored for Linux/Mac clients.

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.

5.4.7 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 5-11 Environment Options 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 5.4.14, "Send > Disk Space Management,"](#) on page 84.

```
<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:

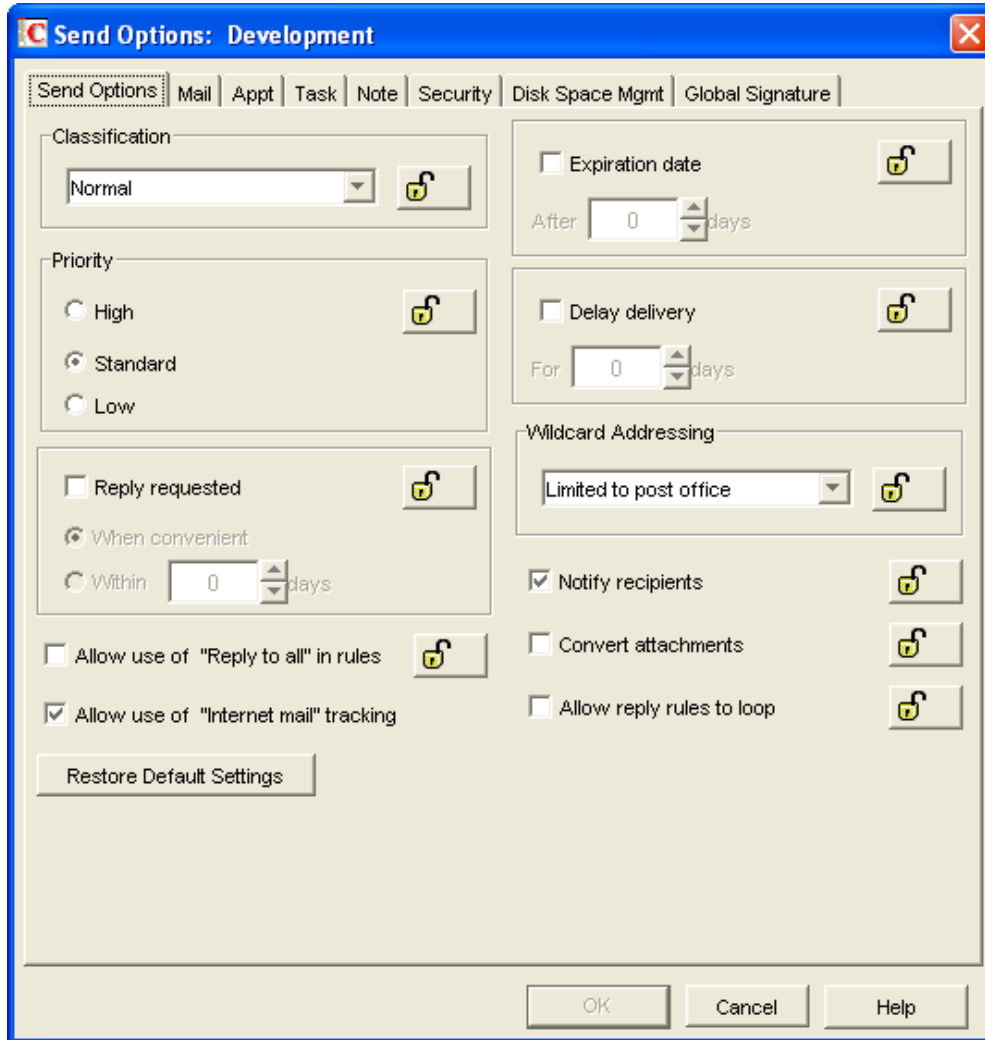
```
<attr attr-name="DiscardSettings">
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">AutoPurgeAfterTrashDays</component>
    <component name="field">trashPurge</component>
  </value>
  <value type="structured">
    <component name="value">7</component>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

5.4.8 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 5-12 Send Options 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 5.4.9, "Send > Mail,"](#) on page 71.

```
<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 the 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`.

IMPORTANT: The lock level must not be set on this field. This means that 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>
  <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.

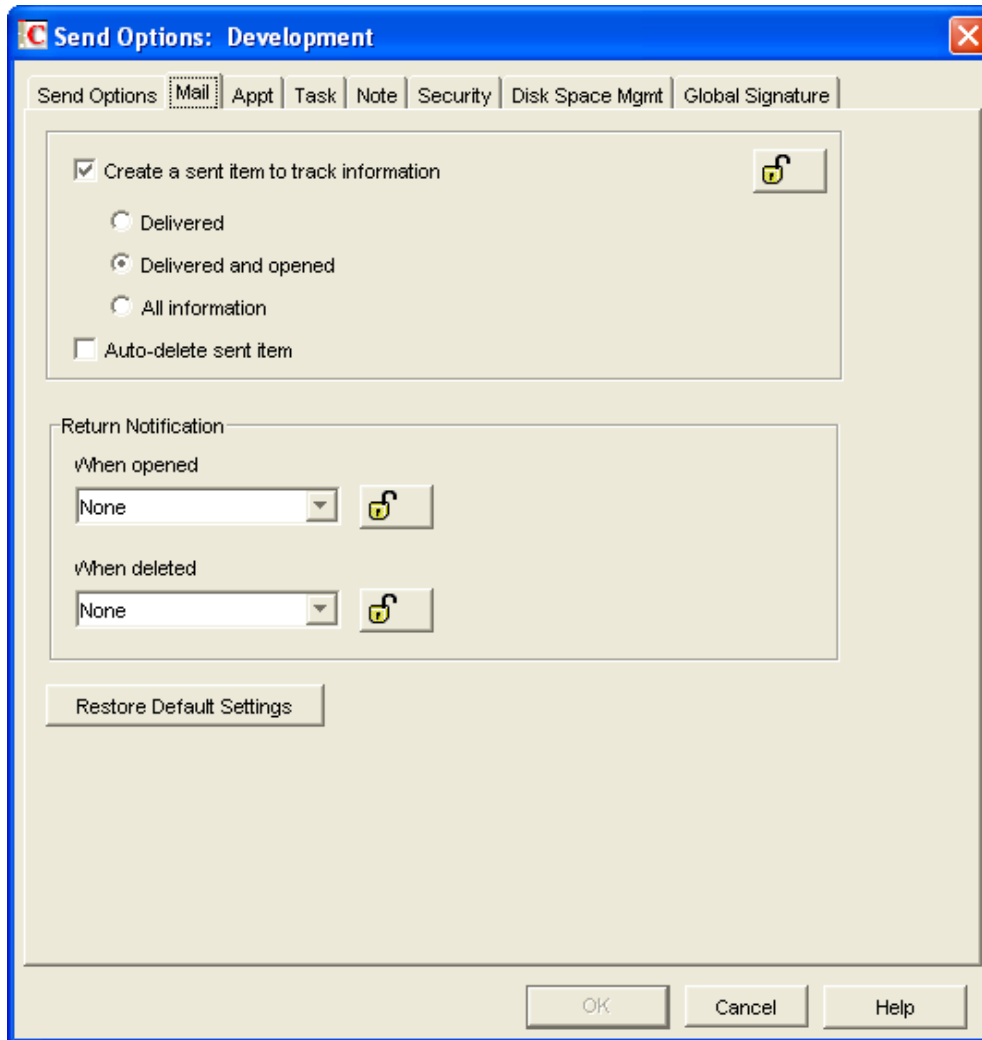
Notify Recipients

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.

5.4.9 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 5-13 Send Options 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

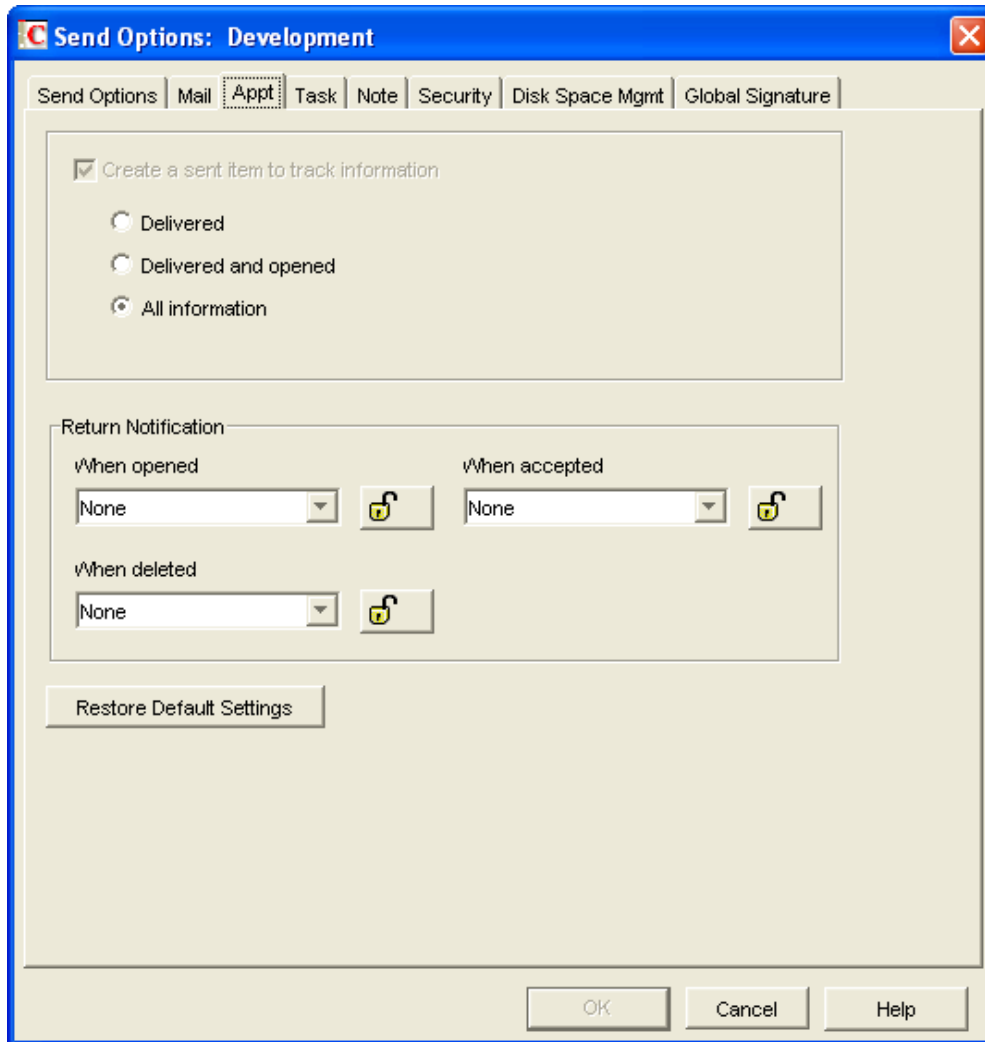
The mailReturnDelete field allows users to be notified when a mail message is deleted. There are four different notification options:

- ♦ **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.

5.4.10 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 5-14 Send Options 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 71](#).

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

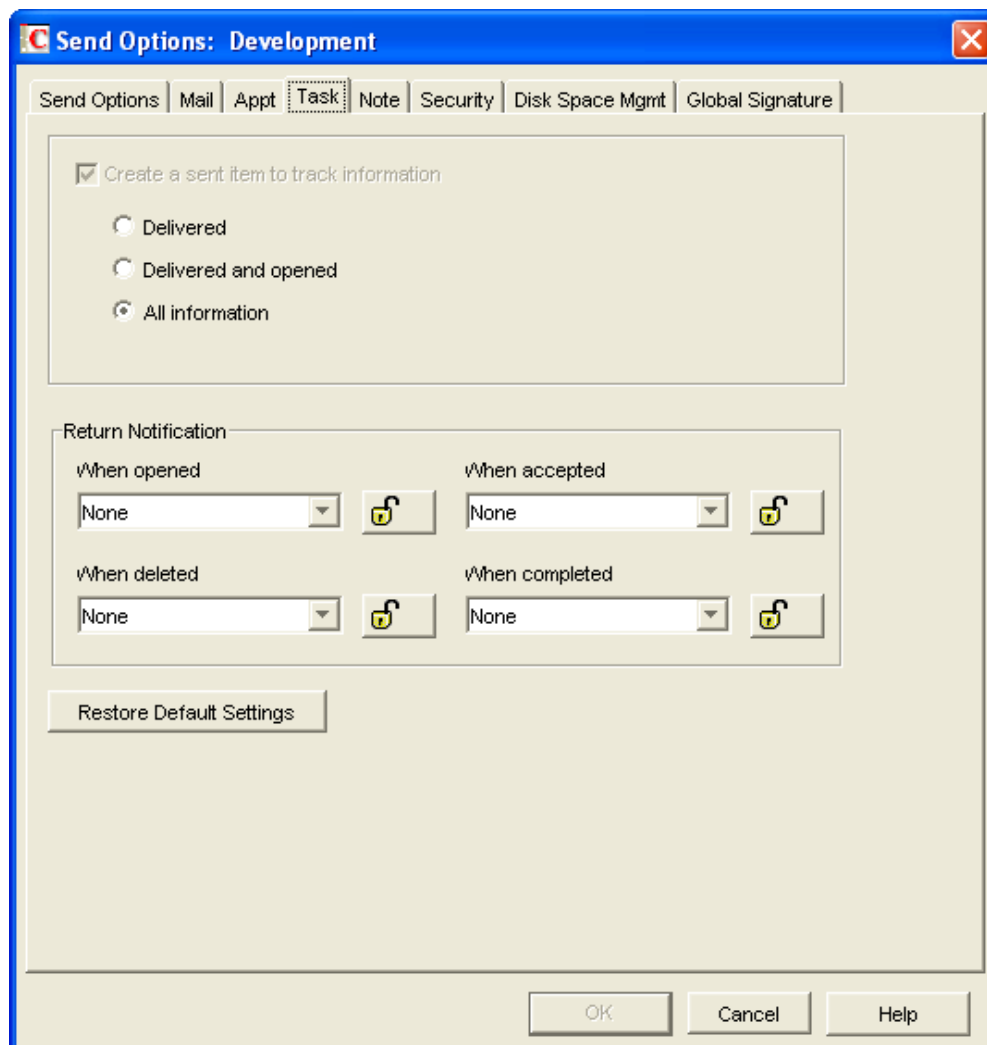
The appointmentReturnAccept field allows users to be notified when an appointment is accepted. There are four different notification options:

- ♦ **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.

5.4.11 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 5-15 Send Options 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>
  <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 5.4.9, "Send > Mail," on page 71](#).

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

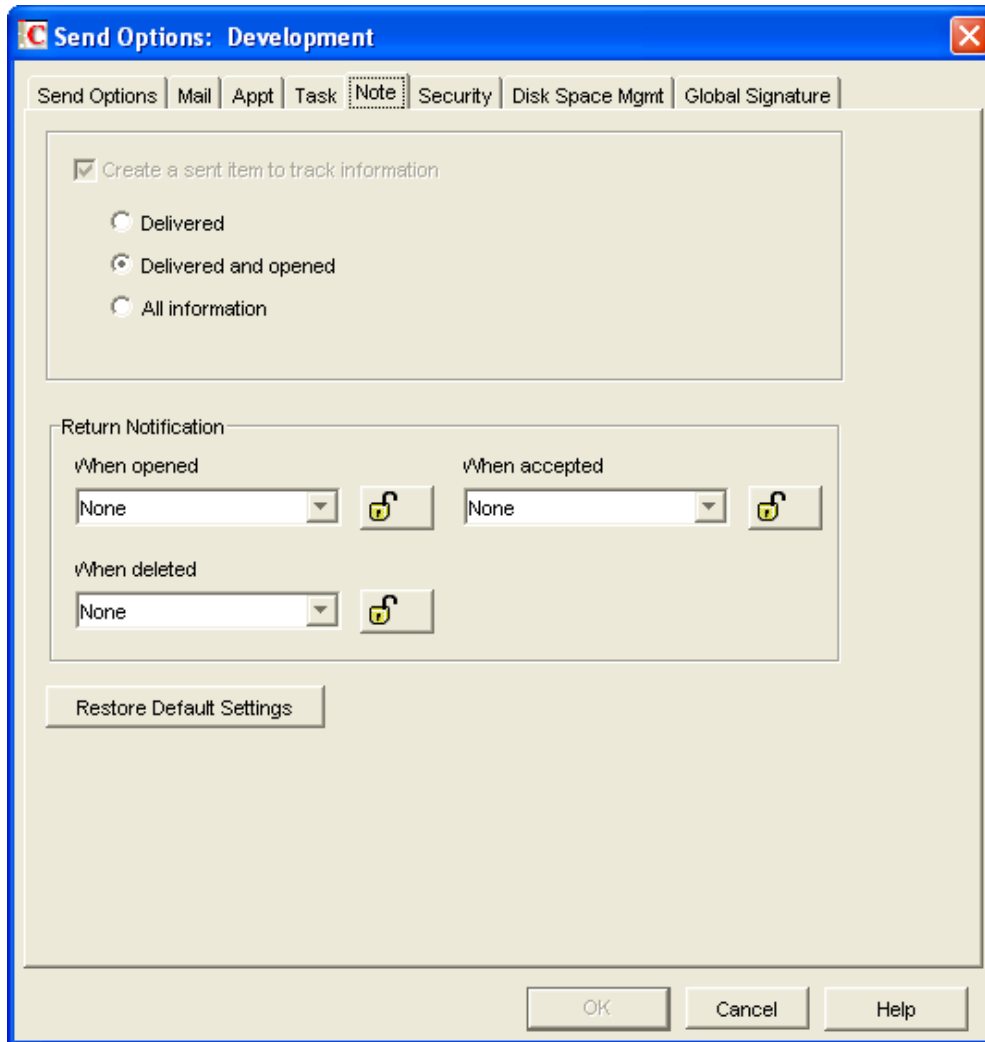
The taskReturnCompleted field allows users to be notified when a task is completed. There are four different notification options:

- ♦ **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.

5.4.12 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 5-16 Send Options 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 5.4.9, "Send > Mail," on page 71](#).

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

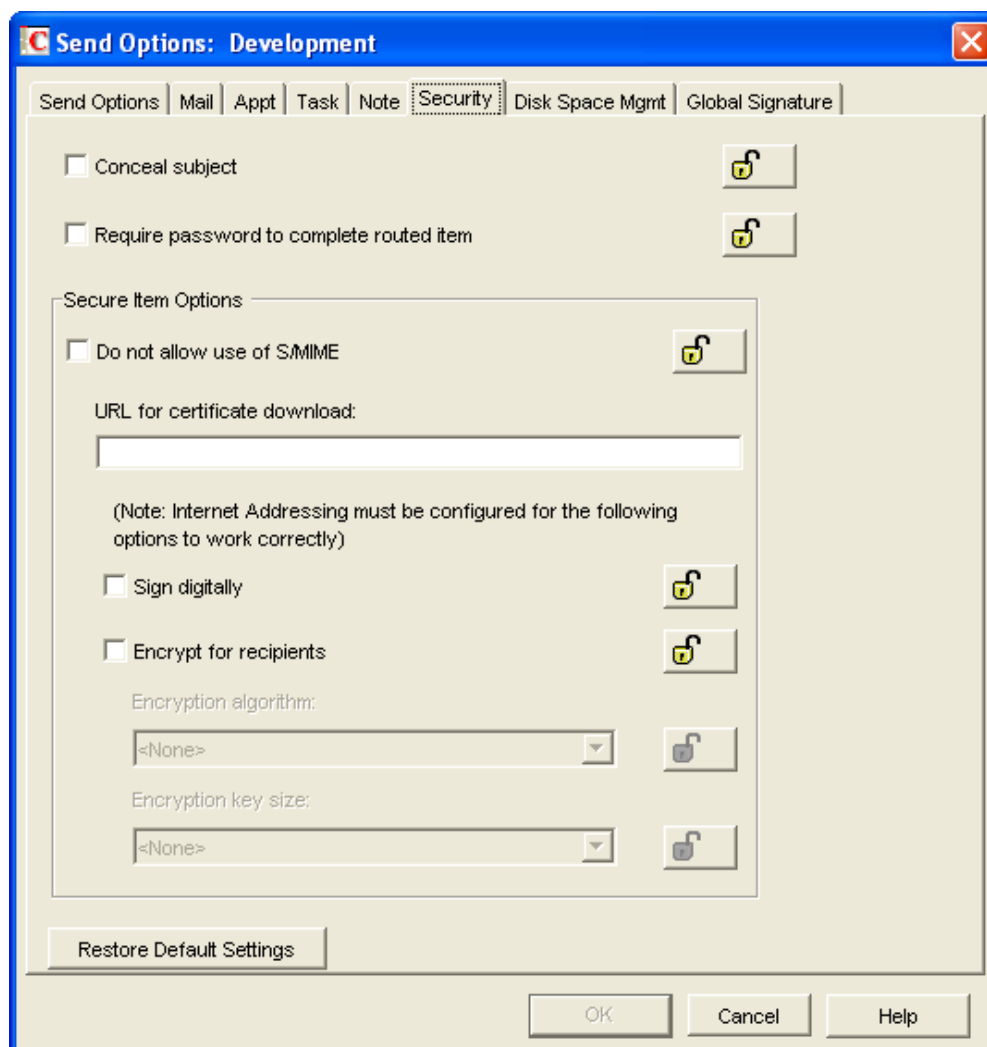
The noteReturnAccept field allows users to be notified when a note is accepted. There are four different notification options:

- ♦ **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.

5.4.13 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 5-17 Send Options 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.

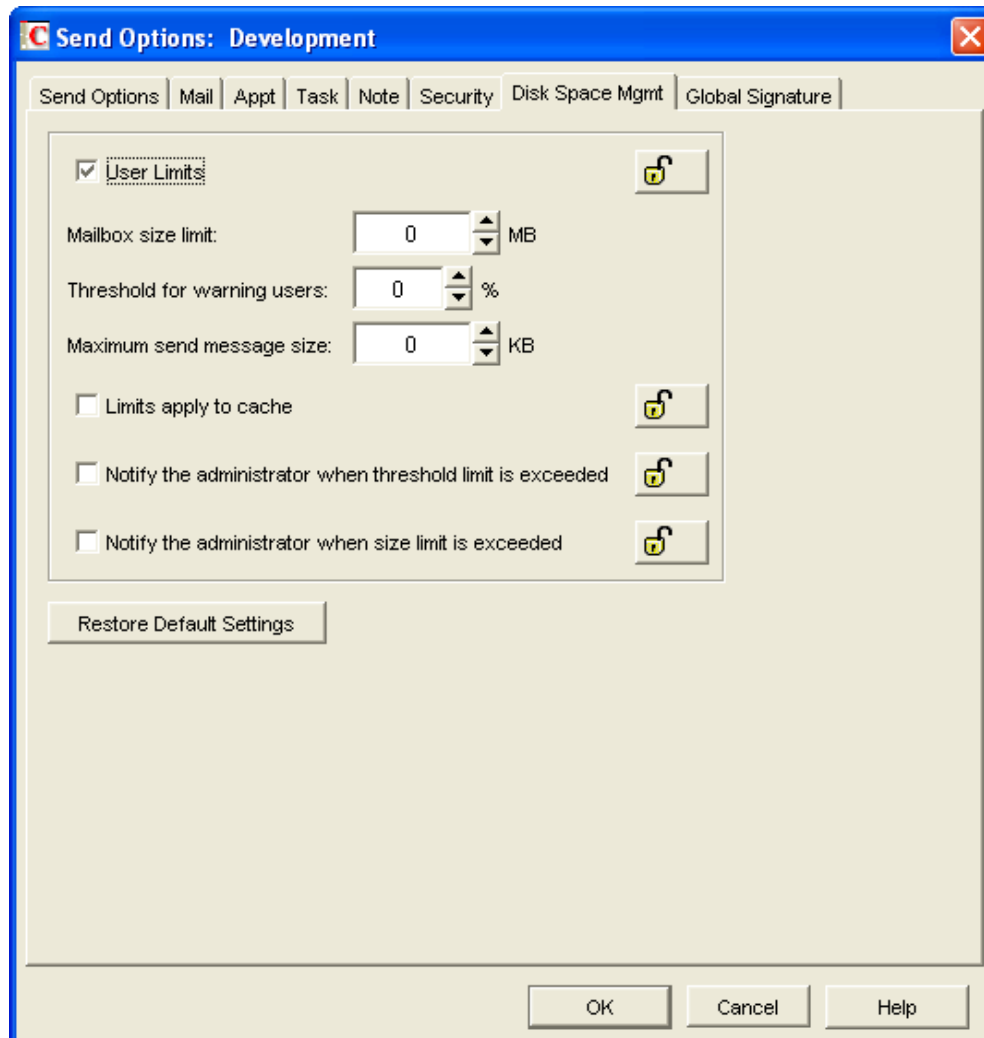
Encrypt for Recipients

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.

5.4.14 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 5-18 Send Options 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 5.4.7, “Environment > Cleanup,”](#) on page 65.

```

<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>
  <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">enableBoxThresholdNotificaion</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">enableBoxSizeNotificaion</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 options listed below ; 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.

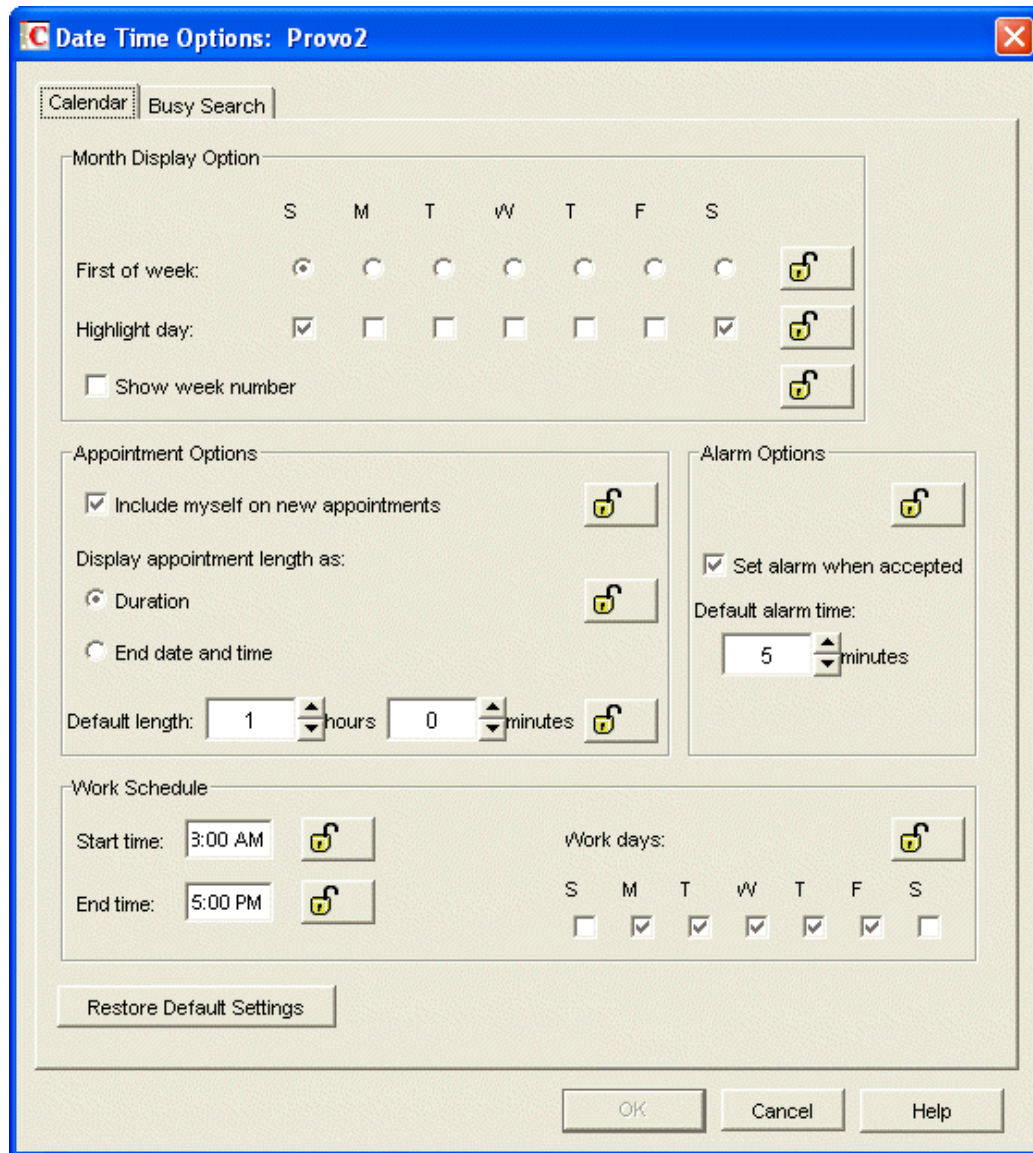
The `enableBoxSizeNotification` field is set to 0 or 1. 0 is No and 1 is Yes.

IMPORTANT: If you lock this field, the lock level must be set on a domain or post office, not on users or external entities.

5.4.15 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 5-19 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>
  <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 hilightDaysOfWeek 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.

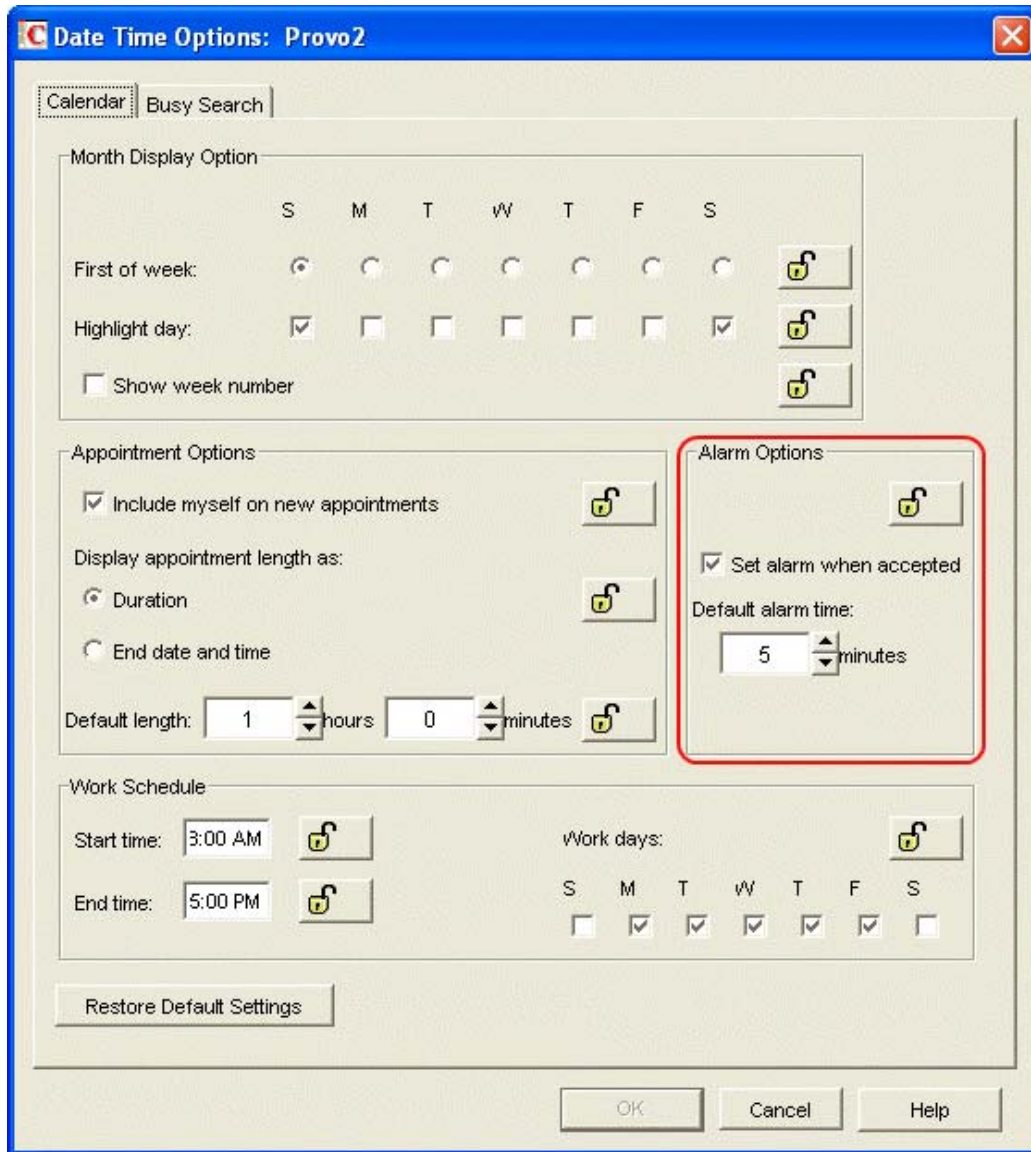
Work Schedule > Work Days

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.

5.4.16 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 5-20 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.

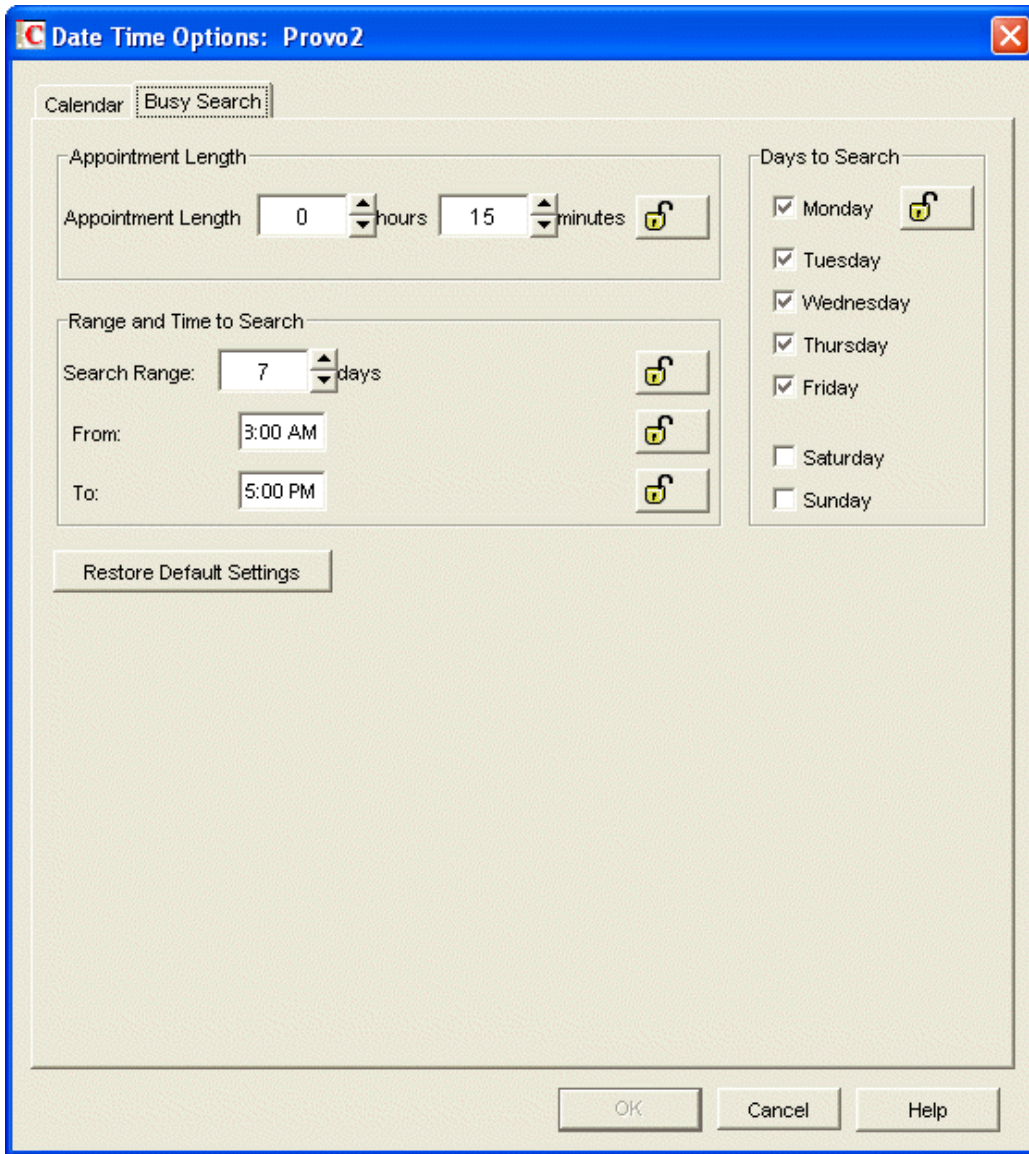
Default Alarm Time

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.

5.4.17 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 5-21 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>
  </value>
</attr>
```

```

        <component name="field">busyInterval</component>
    </value>
    <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 5.4.15, "Date and Time > Calendar," on page 87](#)).

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.

5.5 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 5.5.1, “Environment,” on page 94](#)
- ♦ [Section 5.5.2, “Send,” on page 95](#)
- ♦ [Section 5.5.3, “Date and Time,” on page 96](#)

5.5.1 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 5-1](#) shows the ConsoleOne options with a with their corresponding XML field names.

Table 5-1 GroupWise Client Options: Environment

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

ConsoleOne Option	XML Field
<i>Cleanup > Empty Trash > days</i>	<i>trashDays</i>

5.5.2 Send

The send options allows you to change how users send mail, appointments, notes, and tasks. [Table 5-2](#) shows the ConsoleOne options with their corresponding XML field names.

Table 5-2 GroupWise Client Options: Send

ConsoleOne Option	XML Field
<i>Send Options > Classification</i>	<i>sendSecurity</i>
<i>Send Options > Delay delivery</i>	<i>delayDelivery</i>
<i>Send Options > Convert attachments</i>	<i>itemConversions</i>
<i>Send Options > Wildcard Addressing</i>	<i>asteriskSendRestriction</i>
<i>Send Options > Allow reply rules to loop</i>	<i>allowRuleReplyMoreThanOnce</i>
<i>Send Options > Allow use of Internet mail tracking</i>	<i>internetStatusTracking</i>
<i>Send Options > Priority</i>	<i>mailPriority</i>
<i>Send Options > Reply requested</i>	<i>Send Options > Reply requested</i>
<i>Send Options > Expiration date</i>	<i>mailExpireDays</i>
<i>Send Options > Notify recipients</i>	<i>notifyRecipient</i>
<i>Mail > Create a sent item to track information</i>	<i>outboxInsert</i>
<i>Mail > Create a sent item to track information > option</i>	<i>mailStatusInfo</i>
<i>Mail > Auto-delete sent item</i>	<i>mailAutoDelete</i>
<i>Mail > Return Notification > When opened</i>	<i>mailReturnOpen</i>
<i>Mail > Return Notification > When deleted</i>	<i>mailReturnDelete</i>
<i>Appt > Create a sent item to track information options</i>	<i>appointmentStatusInfo</i>
<i>Appt > Return Notification > When opened</i>	<i>appointmentReturnOpen</i>
<i>Appt > Return Notification > When deleted</i>	<i>appointmentReturnDelete</i>
<i>Appt > Return Notification > When accepted</i>	<i>appointmentReturnAccept</i>
<i>Task > Create a sent item to track information options</i>	<i>taskStatusInfo</i>
<i>Task > Return Notification > When opened</i>	<i>taskReturnOpen</i>
<i>Task > Return Notification > When accepted</i>	<i>taskReturnAccepted</i>
<i>Task > Return Notification > When deleted</i>	<i>taskReturnDelete</i>
<i>Task > Return Notification > When completed</i>	<i>taskReturnCompleted</i>
<i>Note > Create a sent item to track information options</i>	<i>noteStatusInfo</i>

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

5.5.3 Date and Time

The Date and Time options allows you to control how the calendar is displayed, and how busy searches are conducted. [Table 5-3](#) shows the ConsoleOne options with their corresponding XML field names.

Table 5-3 GroupWise Client Option: Date and Time

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

ConsoleOne Option	XML Field
<i>Busy Search > Range and Time to Search > To</i>	busyEndTime
<i>Busy Search > Range and Time to Search > Search Range</i>	busySearchRange
<i>Busy Search > Appointment Length</i>	busyInterval
<i>Busy Search > Days to Search</i>	busyDays

6 Managing the Driver

As you work with the GroupWise driver, there are a variety of management tasks you might need to perform:

- ♦ [Section 6.1, “Using Anti-Virus Software on a GroupWise System,” on page 99](#)
- ♦ [Section 6.2, “Synchronizing Group Objects,” on page 99](#)
- ♦ [Section 6.3, “Synchronizing GroupWise Distribution List Objects,” on page 100](#)
- ♦ [Section 6.4, “Using the GroupWise Snap-Ins to Remove a GroupWise Account,” on page 100](#)
- ♦ [Section 6.5, “Re-associating a GroupWise Account with an Identity Vault User,” on page 100](#)
- ♦ [Section 6.6, “Renaming Users,” on page 101](#)
- ♦ [Section 6.7, “Common Management Tasks,” on page 101](#)

The first six sections describe tasks that are specific to the GroupWise driver. The last section lists tasks that are common for all drivers.

6.1 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).

6.2 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 the Identity Vault and then links the two together. If the group is renamed, the description is modified, or users are added to or removed 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 Distribution 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 33](#) for more information.

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

6.3 Synchronizing GroupWise Distribution List Objects

The driver synchronizes GroupWise distribution list objects. The Filter policy and the Schema Mapping policy include the GroupWise distribution list objects. The GroupWise distribution list is updated and maintained by the driver just like the Group objects. For more information see, [“Synchronize GroupWise Distribution Lists:” on page 116.](#)

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

You can delete an Identity Vault 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 Identity Vault 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 by using the GroupWise snap-ins, because the object might have already been removed 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 the Identity Vault, 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 Identity Vault 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 the Identity Vault, Identity Manager discards the modify request.

- 2 Delete the GroupWise account.

- 3 To re-create the GroupWise account, delete the association.

- 4 Change an Identity Vault attribute for the user that the driver watches for modifications or resynchronization.

6.5 Re-associating a GroupWise Account with an Identity Vault User

Administrators sometimes delete the value of the GroupWise ID attribute (disassociate it) from an Identity Vault user and then re-associate (graft) it. This action resets the relationship between an Identity Vault 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 Identity Vault 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 \(http://www.novell.com/documentation/gw7/pdfdoc/gw7_admin/gw7_admin.pdf\)](http://www.novell.com/documentation/gw7/pdfdoc/gw7_admin/gw7_admin.pdf) for known issues and precautions.

6.6 Renaming Users

Using the GroupWise snap-ins to rename users is not recommended. Rename the user object in the authoritative data source and let the driver rename the account in GroupWise.

6.7 Common Management Tasks

The following list includes management tasks that are common to all Identity Manager drivers. For details about how to perform these tasks, see the [NetIQ Identity Manager Driver Administration Guide](#).

- ◆ Starting, stopping, and restarting the driver
- ◆ Viewing driver version information
- ◆ Using Named Passwords to securely store passwords associated with the driver
- ◆ Monitoring the driver's health
- ◆ Backing up the driver
- ◆ Inspecting the driver's cache files
- ◆ Viewing the driver's statistics
- ◆ Using the DirXML Command Line utility to perform management tasks through scripts
- ◆ Securing the driver and its information
- ◆ Synchronizing objects
- ◆ Migrating and resynchronizing data

7 Troubleshooting the Driver

The following sections provide information to help troubleshoot issues with the GroupWise driver.

- ♦ [Section 7.1, “Avoiding Data Corruption,” on page 103](#)
- ♦ [Section 7.2, “Troubleshooting Driver Processes,” on page 103](#)
- ♦ [Section 7.3, “Error Messages,” on page 103](#)

7.1 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*.

7.2 Troubleshooting Driver Processes

Viewing driver processes is necessary to analyze unexpected behavior. To view the driver processing events, use DStTrace. You should only use it during testing and troubleshooting the driver. Running DStTrace while the drivers are in production increases the utilization on the Identity Manager server and can cause events to process very slowly. For more information, see [“Viewing Identity Manager Processes”](#) in the *NetIQ Identity Manager Driver Administration Guide*.

7.3 Error Messages

For each event or operation received from the engine, the driver returns an XML document containing a status report in DStTrace. See [Section 7.2, “Troubleshooting Driver Processes,” on page 103](#) 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.

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 A.1.5, “Driver Parameters,” on page 113](#) 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 A.1.5, “Driver Parameters,” on page 113](#) 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 A.1.5, “Driver Parameters,” on page 113](#) 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 A.1.5, “Driver Parameters,” on page 113](#) 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 A.1.5, “Driver Parameters,” on page 113](#) 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 on 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 A.1.5, "Driver Parameters," on page 113](#) 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 on 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 A.1.5, "Driver Parameters," on page 113](#) 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 ID) for this value.

Action: Verify that the driver parameters are configured correctly. See [Section A.1.5, "Driver Parameters," on page 113](#) 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 A.1.5, "Driver Parameters," on page 113](#) 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 [Chapter 2, "Installing the Driver Files," on page 15](#) 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 [Chapter 2, "Installing the Driver Files," on page 15](#) 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 A.1.5, "Driver Parameters," on page 113](#) 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 A.1.5, "Driver Parameters," on page 113](#) 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. For more information, see [Configuring the Remote Loader and Drivers](#) in the *NetIQ Identity Manager Setup Guide*.

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 NetIQ 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.

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

The Admin user object is most often used to supply these rights. However, you might want to create a DriversUser (for example) and assign security equivalence to that user. Whatever rights that the driver needs to have on the server, the DriversUser object must have the same security rights.

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 a 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 5.3, "Modifying Policies," on page 30](#) for more information.

Level: Warning (for the 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 not 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

A Driver Properties


This section provides information about the Driver Configuration and Global Configuration Values properties for the GroupWise driver. These are the only unique properties for drivers. All other driver properties (Named Password, Engine Control Values, Log Level, and so forth) are common to all drivers. Refer to “[Driver Properties](#)” in the *NetIQ Identity Manager Driver Administration Guide* for information about the common properties.

The information is presented from the viewpoint of iManager. If a field is different in Designer, it is marked with a Designer icon.

- ♦ [Section A.1, “Driver Configuration,” on page 111](#)
- ♦ [Section A.2, “Global Configuration Values,” on page 114](#)

A.1 Driver Configuration

In iManager:

- 1 Click  to display the Identity Manager Administration page.
- 2 Open the driver set that contains the driver whose properties you want to edit:
 - 2a In the *Administration* list, click *Identity Manager Overview*.
 - 2b If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.
 - 2c Click the driver set to open the Driver Set Overview page.
- 3 Locate the driver icon, then click the upper right corner of the driver icon to display the *Actions* menu.
- 4 Click *Edit Properties* to display the driver’s properties page.

By default, the Driver Configuration page is displayed.

In Designer:

- 1 Open a project in the Modeler.
- 2 Right-click the driver icon or line, then select click *Properties > Driver Configuration*.

The Driver Configuration options are divided into the following sections:

- ♦ [Section A.1.1, “Driver Module,” on page 112](#)
- ♦ [Section A.1.2, “Driver Object Password,” on page 112](#)
- ♦ [Section A.1.3, “Authentication,” on page 112](#)
- ♦ [Section A.1.4, “Startup Option,” on page 113](#)
- ♦ [Section A.1.5, “Driver Parameters,” on page 113](#)
- ♦ [Section A.1.6, “ECMAScript,” on page 114](#)
- ♦ [Section A.1.7, “Global Configurations,” on page 114](#)

A.1.1 Driver Module

The driver module changes the driver from running locally to running remotely or the reverse.

Java: 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 `classes` directory as a class file, or in the `lib` directory as a `.jar` file. If this option is selected, the driver is running locally.

The name of the driver's Java class is: `com.novell.gw.dirxml.driver.gw.GWdriverShim`

Native: This option is not used with the GroupWise driver.

Connect to Remote Loader: Used when the driver is connecting remotely to the connected system. Designer includes two suboptions:

- ♦ **Remote Loader Client Configuration for Documentation:** Includes information on the Remote Loader client configuration when Designer generates documentation for the driver.
- ♦ **Driver Object Password:** Specifies a password for the Driver object. If you are using the Remote Loader, you must enter a password on this page. Otherwise, the remote driver does not run. The Remote Loader uses this password to authenticate itself to the remote driver shim.

A.1.2 Driver Object Password

Driver Object Password: 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.

A.1.3 Authentication

The authentication section stores the information required to authenticate to the connected system.

Authentication ID: Specify a user application ID. This ID is used to pass Identity Vault subscription information to the application.

Example: `Administrator`

Authentication context: This option is not used with the GroupWise driver.

Remote Loader Connection Parameters: Used only if the driver is using the Remote Loader. The parameter to enter is `hostname=xxx.xxx.xxx.xxx port=xxxx kmo=certificatename`, when the host name is the IP address of 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 `kmo` entry is optional. It is only used when there is an SSL connection between the Remote Loader and the Metadirectory engine.

Application Password: This option is not used with the GroupWise driver.

NOTE: The application password is not required if the Groupwise driver and the Groupwise server are running on the same system. However, if the Groupwise driver and the Groupwise server are running on separate servers, ensure that the values for authentication ID and application password are specified. In this scenario, the driver running on one server authenticates to the other server (Groupwise server) to access the files system containing the domain folder, hence the windows server account and password are expected to be specified in the driver configuration.

Remote Loader Password: Used only if the driver is using 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.

Cache limit (KB): Specify the maximum event cache file size (in KB). If it is set to zero, the file size is unlimited. Click *Unlimited* to set the file size to unlimited in Designer.

A.1.4 Startup Option

The Startup Option section allows you to set the driver state when the Identity Manager server is started.

Auto start: The driver starts every time the Identity Manager server is started.

Manual: The driver does not start when the Identity Manager server is started. The driver must be started through Designer or iManager.

Disabled: 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.

Do not automatically synchronize the driver: 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.

A.1.5 Driver Parameters

The Driver Parameters section lets you configure the driver-specific parameters. When you change driver parameters, you tune driver behavior to align with your network environment.

The parameters are:

Domain Server: Specify the name or IP address of the server where the GroupWise domain database (`wpdomain.db`) resides. 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.

Domain Path: Specify the path to the directory containing the GroupWise domain database (`wpdomain.db`). Using the primary domain database is recommended. The domain path format is different, depending upon where the driver is located relative to the domain database:

- ◆ Driver and database on same server:

Windows example: `c:\Novell\GroupWise\Domain`

Linux example: `/Novell/GroupWise/Domain`

- ◆ Driver and database on different servers:

Windows example: `c$\Novell\GroupWise\Domain`

NetWare example: `volume\Novell\GroupWise\Domain`

These are only examples of path formats. Your actual path will probably be different.

Enforce Admin Lockout Setting: 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, the domain settings are used. This means that the GroupWise driver must be running with GroupWise support files equal to or later than these settings. Select *True* to enable this lockout setting, or select *False* to disable this lockout setting.

Create Nicknames: Select *True* if you want the driver to create GroupWise nicknames when GroupWise accounts are renamed or moved to another post office.

Reassign Resource Ownership: Select *True* if you want the driver to reassign ownership of resources when the GroupWise accounts are disabled or expired.

Default Resource Owner User ID: Specify the default user who becomes the new owner of resources that are reassigned.

GroupWise Domain Database Version: Specify the version of the GroupWise Domain database version the driver connects to. The options are:

- ♦ *GroupWise 8*
- ♦ *GroupWise 2012*

Cleanup Group Membership: Cleans up Identity Vault Group memberships when removing a user from all GroupWise Distribution Lists. Select *True* or *False*.

Synchronize GroupWise External Entity Objects: Select *True* to synchronize eDirectory's GroupWise External Entry objects with external users in GroupWise. By default, it is set to *False*.

Publisher Heartbeat Interval: Specifies the Publisher channel heartbeat interval in minutes. Specify 0 to disable the heartbeat.

A.1.6 ECMAScript

Displays an ordered list of ECMAScript resource files. The files contain extension functions for the driver that Identity Manager loads when the driver starts. You can add additional files, remove existing files, or change the order the files are executed.

A.1.7 Global Configurations

Displays an ordered list of Global Configuration objects. The objects contain extension GCV definitions for the driver that Identity Manager loads when the driver is started. You can add or remove the Global Configuration objects, and you can change the order in which the objects are executed.

A.2 Global Configuration Values

Global configuration values (GCVs) are values that can be used by the driver to control functionality. GCVs are defined on the driver or on the driver set. Driver set GCVs can be used by all drivers in the driver set. Driver GCVs can be used only by the driver on which they are defined.

The GroupWise driver includes many GCVs. You can also add your own if you discover you need additional ones as you implement policies in the driver.

To access the driver's GCVs in iManager:


- 1 Click  to display the Identity Manager Administration page.

- 2 Open the driver set that contains the driver whose properties you want to edit.
 - 2a In the *Administration* list, click *Identity Manager Overview*.
 - 2b If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.
 - 2c Click the driver set to open the Driver Set Overview page.
- 3 Locate the driver icon, click the upper right corner of the driver icon to display the *Actions* menu, then click *Edit Properties*.

or

To add a GCV to the driver set, click *Driver Set*, then click *Edit Driver Set properties*.

To access the driver's GCVs in Designer:

- 1 Open a project in the Modeler.
- 2 Right-click the driver icon  or line, then select *Properties > Global Configuration Values*.

or

To add a GCV to the driver set, right-click the driver set icon , then click *Properties > GCVs*.

The global configuration values are organized as follows:

- ♦ [Section A.2.1, "Driver Configuration," on page 115](#)
- ♦ [Section A.2.2, "Entitlements," on page 117](#)
- ♦ [Section A.2.3, "Account Tracking," on page 119](#)
- ♦ [Section A.2.4, "Password Synchronization," on page 119](#)
- ♦ [Section A.2.5, "Managed System Information," on page 120](#)

A.2.1 Driver Configuration

GroupWise Domain Database Version: The version of the GroupWise domain database to which this driver should connect.

- ♦ *GroupWise 8*
- ♦ *GroupWise 2012*

Default Sync Destination: GroupWise Post Office 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: `GW\GWSystem\PO1`.

Enforce Admin Lockout Setting: Enforces the Minimum Snap-in Release Version and 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, the domain settings are used. This means that the GroupWise driver must be running with GroupWise support files equal to or later than these settings.

Normally, it is set to *True*. You might need to set it to *False*, if the GroupWise support pack is installed and ConsoleOne is configured to lock out previous versions. *True* enforces this lockout setting. *False* disables this lockout setting.

Synchronize Groups: Allows the driver to synchronize eDirectory groups to GroupWise distribution lists. *True* enables the synchronization. *False* disables the synchronization.

Cleanup Group Membership: Available only if *Synchronize Groups* is set to *True*. Removes the user from the Group Membership attribute when the user is removed from the GroupWise distribution lists.

Synchronize GroupWise Distribution Lists: Select *True* if you want this driver to synchronize eDirectory's GroupWise Distribution List objects with distribution lists in GroupWise. By default, it is set to *False*.

Sync GroupWise External Entities to this Domain: Available only if *Synchronize GroupWise Distribution Lists* is set to *True*. Specify a non-GroupWise domain name that exists within the GroupWise system. This domain must host at least one external post office, defined in *Sync GroupWise External Entities to this External Post Office*.

Synchronize GroupWise External Entity Objects: Select *True* to synchronize eDirectory's GroupWise External Entity objects with external users in GroupWise. By default, it is set to *False*.

Sync GroupWise External Entities to this External Post Office: Available only if *Synchronize GroupWise Distribution Lists* is set to *True*. Specify an external post office name that exists within the GroupWise system. This post office must be subordinate to the GroupWise domain defined in *Sync GroupWise External Entities to this Domain*.

Synchronize eDir OrgUnit To GroupWise External Post Office: Allows the driver to synchronize eDirectory organizational units to GroupWise external post offices. *True* enables the synchronization. *False* disables the synchronization.

Create External Post Offices in the Non-GroupWise Domain: Available only if *Synchronize eDir OrgUnit to GroupWise External Post Office* is set to *True*. 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.

Create Nicknames: Allows the driver to create GroupWise nicknames when GroupWise accounts are renamed or moved to another post office. *True* creates nicknames when the accounts are renamed or moved. *False* 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.

Reassign Resource Ownership: The driver reassigns ownership of resources when GroupWise accounts are disabled or expired.

True 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. *False* is the default.

Default Resource Owner User ID: 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 *Reassign Resource Ownership* option is *False*. 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.

Create Accounts During Migration: Allows the driver to create new GroupWise accounts for users without a current account during a migration from eDirectory. *True* allows the accounts to be created. *False* does not create the accounts.

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 *True*, the driver creates a GroupWise account. When *False* is specified, the Add event is ignored and the driver issues a warning that this option is set to *False*. The default value is *False*.

Migration sets the driver association on all users with GroupWise accounts. See [Section 3.3, “Associating Identity Vault Users and GroupWise Users,”](#) on page 26 for more information.

Action On eDirectory GroupWise External Entity Delete: Select the action you want the driver to take on an associated GroupWise account (mailbox), when a GroupWise external entity is deleted in eDirectory. The options are:

- ◆ *Disable the GroupWise account*
- ◆ *Delete the GroupWise account*
- ◆ *Expire the GroupWise account*
- ◆ *Disable and Expire the GroupWise account*

Action On eDirectory GroupWise External Entity Expire/Unexpire: Select the action you want the drive to take on the associated GroupWise account (mailbox), when an expired or unexpired GroupWise external entity logs into eDirectory. The options are:

- ◆ *Expire/Unexpire the GroupWise Account*
- ◆ *Disable/Enable the GroupWise Account*
- ◆ *Disable/Enable and Expire/Unexpire the GroupWise Account*

Action On eDirectory GroupWise External Entity Disable/Enable: Select the action you want the driver to take on the associated GroupWise account (mailbox), when a disabled or enabled GroupWise external entity logs into eDirectory. The options are:

- ◆ *Expire/Unexpire the GroupWise Account*
- ◆ *Disable/Enable the GroupWise Account*
- ◆ *Disable/Enable and Expire/Unexpire the GroupWise Account*

Remove GroupWise External Entity from all Distribution Lists on expire: Select *True* if you want the driver to remove the GroupWise external entity from all distribution lists when the GroupWise account is expired; otherwise, select *False*.

Remove GroupWise External Entity from all Distribution Lists on disable: Select *True* if you want the driver to remove the GroupWise external entity from all distribution lists when the GroupWise account is disabled; otherwise, select *False*.

Publisher Heartbeat interval: Specify the Publisher channel heartbeat interval in minutes. Enter 0 to disable the heartbeat.

A.2.2 Entitlements

There are multiple sections in the *Entitlements* tab. Depending on which packages you installed, different options are enabled and displayed. This section documents all of the options.

- ◆ [“Entitlements Options” on page 118](#)
- ◆ [“Data Collection” on page 118](#)
- ◆ [“Role Mapping” on page 118](#)
- ◆ [“Resource Mapping” on page 118](#)

Entitlements Options

Use Driver GWAccount Entitlement: Select *True* to allow the driver to manage GroupWise accounts based on the GroupWise account entitlement. Select *False* to not use the GroupWise account entitlement.

If you select *False*, the following options are not displayed.

Account On GroupWise Account Entitlement Add: Select the action you want the driver to take on the associated GroupWise account (mailbox), when a user is created in the Identity Vault with a GroupWise account entitlement. The options are:

- ♦ *Enable the GroupWise account*
- ♦ *Disable the GroupWise account*

Action On GroupWise Account Entitlement Remove: Select the action you want the driver to take on the associated GroupWise account (mailbox), when a user's GroupWise account entitlement is removed. The options are:

- ♦ *Disable the GroupWise account*
- ♦ *Delete the GroupWise account*
- ♦ *Expire the GroupWise account*
- ♦ *Disable and expire the GroupWise account*

Data Collection

Data collection enables the Identity Report Module to gather information to generate reports. For more information, see the [NetIQ Identity Reporting Module Guide](#).

Enable data collection: Select *Yes* to enable data collection for the driver through the Data Collection Service by the Managed System Gateway driver. If you are not going to run reports on data collected by this driver, select *No*.

Allow data collection from user accounts: Select *Yes* to allow data collection by the Data Collection Service through the Managed System Gateway driver for the user accounts.

Role Mapping

The Role Mapping Administrator allows you to map business roles with IT roles.

Enable role mapping: Select *Yes* to make this driver visible to the Role Mapping Administrator.

Allow mapping of user accounts: Select *Yes* if you want to allow mapping of user accounts in the Role Mapping Administrator. An account is required before a role, profile, or license can be granted through the Role Mapping Administrator.

Resource Mapping

The Roles Based Provisioning Module allows you to map resources to users. For more information, see the [NetIQ User Application: User Guide](#).

Enables resource mapping: Select *Yes* to make this driver visible to the Roles Based Provisioning Module.

Allow mapping of user accounts: Select *Yes* if you want to allow mapping of user accounts in the Roles Based Provisioning Module. An account is required before a role, profile, or license can be granted.

A.2.3 Account Tracking

Account tracking is part of the Identity Reporting Module. For more information, see the [NetIQ Identity Reporting Module Guide](#).

Enable account tracking: Set this to *True* to enable account tracking policies. Set it to *False* if you do not want to execute account tracking policies.

Realm: Specify the name of the realm, security domain, or namespace in which the account name is unique.

Object Class: Add the object class to track. Class names must be in the application namespace.

Identifiers: Add the account identifier attributes. Attribute names must be in the application namespace.

NOTE: A new identifier, *LDAPDN*, has been added to the Identifiers list. You must add it manually because the package upgrade doesn't add it to the Account Tracking GCV.

Status attribute: Name of the attribute in the application namespace to represent the account status.

Status active value: Value of the status attribute that represents an active state.

Status inactive value: Value of the status attribute that represents an inactive state.

Subscription default status: Select the default status the policies assume when an object is subscribed to the application and the status attribute is not set in the Identity Vault.

Publication default status: Select the default status the policies assume when an object is published to the Identity Vault and the status attribute is not set in the application.

A.2.4 Password Synchronization

The following GCVs control the flow of passwords between GroupWise and the Identity Vault. For more information about how to use the Password Management GCVs, see “[Configuring Password Flow](#)” in the [NetIQ Identity Manager Password Management Guide](#).

Set the initial/default GroupWise password on account creation: If *True*, the GroupWise initial/default password is set when an account is created. The initial password value is specified in the Create policy. If *False*, the initial password is not set.

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.

Synchronize the eDirectory password to the GroupWise regular password: If *True*, allows passwords to flow from eDirectory to GroupWise. If *False*, the regular password is not set.

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.

A.2.5 Managed System Information

These settings help the Identity Reporting Module function to generate reports. For more information, see the [NetIQ Identity Reporting Module Guide](#).

ID: Specify a unique ID for the GroupWise system. This ID is displayed in the reports.

Name: Specify a descriptive name for this GroupWise system. The name is displayed in the reports.

Description: Specify a brief description of this GroupWise system. The description is displayed in the reports.

Type: Specify the type of system the GroupWise system provides in your environment. This information is displayed in the reports.

Classification: Specify the classification for this GroupWise system in your environment. For example, Mission-Critical. This information is displayed in the reports.

Vendor: Select *NetIQ, Inc.* as the vendor of this system. The vendor information is displayed in the reports.

Version: Specify the version of this GroupWise system. The version is displayed in the reports.

Business Owner: Select a user object in the Identity Vault that is the business owner of this GroupWise system. This can only be a user object, not a role, group, or container.

Application Owner: Select a user object in the Identity Vault that is the application owner for this GroupWise system. This can only be a user object, not a role, group, or container.

Location: Specify the physical location of the GroupWise system. This information is displayed in the reports.

Environment: Specify the type of environment the GroupWise system provides. For example, development, test, or production. This information is displayed in the reports.

Authentication IP Address: Specify the IP address used to authenticate to the GroupWise system.

Authentication Port: Specify the port used to authenticate to the GroupWise system.

Authentication ID: Specify the user ID used to authenticate to the GroupWise system.

B Class and Attribute Descriptions

The table in this section lists each Identity Vault (eDirectory) class and attribute used by the GroupWise driver. 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
	50094	Net ID	This can either be a fully distinguished name or the common name.
	58004	DS_DN	This is always the fully distinguished name.
	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 use a value of 62 (0x3E).</p>

eDirectory Class or Attribute	GroupWise Attribute	Description	Secondary Effects
GroupWise External Entity	50157	Exclusive use of Internet domain name	0 = Off. Requires setting an Internet domain name: 50045. 1 = On. Only recognizes the domain name set in the Internet domain name: 50045.
	50319	Preferred Internet eMail ID	Example: JohnDoe "map]" is not allowed because it is reserved. 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.)
	50045	Internet domain name	Example: MyDomain.com
	59028	LDAP authentication ID in typeful format	Example: cn=admin, o=novell
	59073	Internet Free/Busy URL	
	50013	Preferred Internet address format (numeric value)	0 - Full (Name.PostOffice.Domain@IDomain.com) 1 - Host and User ID (Name.PostOffice@IDomain.com) 2 - User ID (Name@IDomain.com) 3 - Lastname.firstname 4 - Firstname.lastname 5 - No setting (reserved) 6 - First initial and last name
	50320	Disallowed Internet address formats (bit settings)	0 - None 1 - Full (never set this bit) 2 - Host 4 - User ID 8 - Lastname.Firstname 16 - Firstname.Lastname 32 - First initial and last name You should not set bit one in this attribute value. It is an illegal operation to disallow the Full format. You can "or" values together. For instance, to allow only full name you use a value of 62 (0x3E).
	50157	Exclusive use of Internet domain name	0 = Off (requires setting an Internet domain name: 50045) 1 = On (only recognizes the domain name set in the Internet domain name: 50045)
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.

eDirectory Class or Attribute	GroupWise Attribute	Description	Secondary Effects
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.
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 attribute 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	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.
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.

eDirectory Class or Attribute	GroupWise Attribute	Description	Secondary Effects
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.	<p>The eDirectory attribute names must be added to the filter. The eDirectory and GroupWise attribute names must be added to the Schema Mapping rule.</p> <p>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.</p>
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 34.
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 34.

IMPORTANT: When the GroupWise Visibility 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 examples 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 by 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>
        <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 -
  ->
  </actions>
</rule>
```



```
<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>
```

C Trace Levels

The driver supports the following trace levels:

Level	Description
0	Status messages (success/failure/warning)
1	Informational messages about what Identity Manager is doing
2	Adds dumps of the XML that is passed to/from the driver
3	Adds XML dumps after a policy is applied, and adds more verbose output during policy evaluation
4	Informational messages about the application
5	Debugging messages and messages about application progress and password synchronization information

For information about setting driver trace levels, see [“Viewing Identity Manager Processes”](#) in the *NetIQ Identity Manager Driver Administration Guide*.

