



# NetIQ® Identity Manager Driver for GroupWise Implementation Guide

October 2019

## **Legal Notice**

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

**Copyright (C) 2019 NetIQ Corporation. All rights reserved.**

---

# Contents

<b>About this Book and the Library</b>	<b>7</b>
<b>About NetIQ Corporation</b>	<b>9</b>
<b>1 Introduction</b>	<b>11</b>
Identity Manager GroupWise Driver	11
Supported GroupWise Versions	11
How the Driver Works	11
Data Transfer Between Systems	12
Key Features	12
Local Platforms	12
Remote Platforms	12
Entitlements	13
Password Synchronization	13
Data Synchronization	13
Driver Shim	13
Driver Packages	14
Checklist for Enabling User and Group Objects Synchronization	14
<b>2 Installing the Driver Files</b>	<b>15</b>
Prerequisites	15
Installing the Driver Shim	15
<b>3 Creating a New Driver Object</b>	<b>17</b>
Creating the Driver Object in Designer	17
Importing the Driver Packages	17
Installing the Driver Packages	18
Configuring the Driver Object	21
Deploying the Driver	21
Associating Identity Vault with GroupWise System	22
Starting the Driver	24
Activating the Driver	24
<b>4 Upgrading an Existing Driver</b>	<b>25</b>
Upgrading an Existing Driver to GroupWise Driver	25
Upgrading the Driver Shim	25
Upgrading the Existing Driver Packages	26
<b>5 Customizing the Driver by Using Policies and Filters</b>	<b>27</b>
Default Driver Actions	27
Modifying Default Settings in Policies and the Filter	27
Modifying the Driver Filter	28
Adding Entries to the Schema Mapping Policy	28

Modifying the Create Policy . . . . .	28
Modifying the Matching Policy . . . . .	28
Modifying Policies . . . . .	29
Specifying the GroupWise Post Office . . . . .	29
Configuring the GroupWise UserID . . . . .	30
Creating Mappings for Additional Attributes . . . . .	31
Getting a Record Count from a Query . . . . .	31
Creating a GroupWise Nickname . . . . .	32
Creating a GroupWise Nickname Record . . . . .	32
Controlling Creation of GroupWise Accounts . . . . .	34
Moving Users from One Post Office to Another Post Office . . . . .	34
Adding Additional Attributes to Be Synchronized . . . . .	36
Renaming Users . . . . .	36
Creating a Gateway Alias . . . . .	37
Using the Wildcard Query . . . . .	38
Querying for a Nickname . . . . .	39
Querying for a Email Address from a Nickname . . . . .	41
Querying for a Gateway Alias . . . . .	42
Querying for Internet Email Address . . . . .	43
Synchronizing GroupWise External Users . . . . .	45
Verifying if an E-Mail Address or Gateway Alias Is Unique . . . . .	46
Converting String Attributes to Structured Attributes . . . . .	48
Setting GroupWise Client Options with the Driver . . . . .	49
Using Policies to Set Client Options . . . . .	50
Client Options . . . . .	53
Environment > General . . . . .	54
Environment > Client Access . . . . .	56
Environment > Views . . . . .	57
Environment > Cleanup . . . . .	58
Environment > File Location . . . . .	59
Send > Send Options . . . . .	61
Send > Mail . . . . .	64
Send > Appt . . . . .	66
Send > Task . . . . .	68
Send > Note . . . . .	70
Send > Security . . . . .	72
Send > Disk Space Management . . . . .	74
Calendar > General . . . . .	76
Calendar > Alarm Options . . . . .	78
Calendar > Busy Search . . . . .	79
Client Options Quick Reference . . . . .	80
Environment . . . . .	80
Send . . . . .	81
Calendar . . . . .	82
<b>6 Securing Driver Communication</b>	<b>85</b>
<b>7 Managing the Driver</b>	<b>87</b>
<b>8 Troubleshooting the Driver</b>	<b>89</b>
Attributes 50045 And 50157 Have Changed from String to Structured Format . . . . .	89
Errors are Displayed After Modifying the External Entity Objects on the Upgraded Driver . . . . .	89

Passing the Value of the GroupWise PostOffice Default Sync Destination GCV in Slash Format . . . . .	89
Uninstalling the Driver on Windows Reports a Java Virtual Machine Error . . . . .	90
Issue with Encrypting the OU Attribute . . . . .	90
Passwords Not Synchronized . . . . .	90
Exception Reported When Running Groupwise Driver and Google Apps Driver on the Same Server. . . . .	90
Troubleshooting Driver Processes . . . . .	91
<b>A Driver Properties</b>	<b>93</b>
Driver Configuration . . . . .	93
Driver Module . . . . .	93
Driver Object Password . . . . .	94
Authentication . . . . .	94
Startup Option . . . . .	95
Driver Parameters . . . . .	95
ECMAScript. . . . .	96
Global Configurations . . . . .	96
Global Configuration Values. . . . .	96
Driver Configuration . . . . .	97
Entitlements. . . . .	98
Account Tracking . . . . .	100
Password Synchronization. . . . .	101
Managed System Information . . . . .	101
GCVs Applicable for the Upgraded Driver . . . . .	102
<b>B Class and Attribute Descriptions</b>	<b>105</b>
<b>C Trace Levels</b>	<b>115</b>



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

## Other Information in the Library

For more information about the library for Identity Manager, see the following resources:

- ♦ [Identity Manager documentation website](#)
- ♦ [Identity Manager drivers documentation website](#)





# 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.

<b>Worldwide:</b>	<a href="http://www.netiq.com/about_netiq/officelocations.asp">www.netiq.com/about_netiq/officelocations.asp</a>
<b>United States and Canada:</b>	1-888-323-6768
<b>Email:</b>	<a href="mailto:info@netiq.com">info@netiq.com</a>
<b>Web Site:</b>	<a href="http://www.netiq.com">www.netiq.com</a>

## Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

## 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](http://www.netiq.com/documentation). You can also email [Documentation-Feedback@netiq.com](mailto: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](http://community.netiq.com).

# 1 Introduction

Novell GroupWise is a cross-platform, corporate email system that provides secure messaging, calendaring, and scheduling. GroupWise also includes task management, contact management, document management, and other productivity tools that are secure, highly available, and easily accessible. For more information, visit [GroupWise Documentation](#) website.

- ♦ [“Identity Manager GroupWise Driver” on page 11](#)
- ♦ [“Data Transfer Between Systems” on page 12](#)
- ♦ [“Key Features” on page 12](#)
- ♦ [“Checklist for Enabling User and Group Objects Synchronization” on page 14](#)

## Identity Manager GroupWise Driver

The NetIQ Identity Manager GroupWise driver is designed to work with GroupWise server. The GroupWise Identity Manager driver leverages the GroupWise REST services and provides the following benefits:

- ♦ It is architecture agnostic.
- ♦ It can run locally on the Identity Manager engine or in a Remote Loader configuration.
- ♦ It replaces the native JNDI communication layer by using the REST commands sent to the GroupWise Administration Service.
- ♦ It is enhanced and virtually eliminates the limitations of previously shipped GroupWise drivers. For example, on Linux, you no longer need to run the driver on the same server where GroupWise Domain is running. Also, you do not need to use ConsoleOne to access the GroupWise server.

## Supported GroupWise Versions

GroupWise driver supports the following versions:

- ♦ GroupWise 2014 SP1 and later supported packs
- ♦ GroupWise 18

## How the Driver Works

The GroupWise driver synchronizes data between the Identity Vault and GroupWise. It manages GroupWise accounts and account information. When a user or a group object is created, modified, renamed, or deleted in the Identity Vault, the driver synchronizes these changes with GroupWise.

When an event is generated in the Identity Vault, the driver processes the event and transforms the received XDS document by applying appropriate rules and policies. The transformed XDS document is passed to driver shim for further processing.

# Data Transfer Between Systems

There are two data transfer channels between the Identity Vault and GroupWise: Subscriber channel and Publisher channel. The driver supports communication in one-way only on Subscriber channel.

- ♦ **Subscriber Channel:** Transfers data and events from the Identity Vault to the GroupWise system.

The Subscriber channel controls data transfer as follows:

- ♦ It monitors the Identity Vault for new objects and any change to the existing objects.
- ♦ It sends the relevant changes to the driver shim to be executed in the GroupWise system.
- ♦ **Publisher Channel:** This channel is not supported for the driver. However, the driver automatically synchronizes **EEmail Address** and **Internet EEmail Address** attributes on the channel. A user add event on the Subscriber channel fetches these attributes from the GroupWise system that in turn trigger a Publisher event which synchronizes the attributes to the Identity Vault unless the attributes are not disabled in the driver filter.

---

**IMPORTANT:** Some Identity Vault attributes contain multiple values for which GroupWise allows only one value. When you modify a multivalued attribute in the Identity Vault, the driver overwrites the value for this attribute in GroupWise. If you delete any value from a multivalued attribute from the Identity Vault, the driver deletes the attribute from GroupWise.

---

## Key Features

This section discusses the following key features of the driver:

- ♦ [“Local Platforms” on page 12](#)
- ♦ [“Remote Platforms” on page 12](#)
- ♦ [“Entitlements” on page 13](#)
- ♦ [“Password Synchronization” on page 13](#)
- ♦ [“Data Synchronization” on page 13](#)
- ♦ [“Driver Shim” on page 13](#)
- ♦ [“Driver Packages” on page 14](#)

## Local Platforms

A local installation is an installation of the driver on the Identity Manager server. You can install the GroupWise driver on all operating systems supported for the Identity Manager server.

## Remote Platforms

The GroupWise driver can use the Remote Loader service to run on a server other than the Identity Manager server. The Remote Loader enables the driver to communicate with the Identity Manager server.

## Entitlements

The GroupWise driver supports the following entitlements by default:

- ♦ **UserAccount:** This entitlement grants or revokes a GroupWise account for a specified user. When this entitlement is granted, the driver provides an enabled logon account. When this entitlement is revoked, the driver either disables or deletes the logon account, depending on the driver configuration.
- ♦ **Group:** This entitlement grants or revokes membership to a group in GroupWise. When the entitlement is revoked, Identity Manager removes the user from the group.

If you upgrade a lower version of the GroupWise driver to the latest GroupWise driver, the upgraded driver performs the following actions by using the entitlements:

- ♦ Adds user object accounts
- ♦ Removes, disables, or expires user object accounts
- ♦ Adds members to a group
- ♦ Removes members from a group
- ♦ Adds members to a distribution list
- ♦ Removes members from a distribution list

## Password Synchronization

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

## Data Synchronization

The GroupWise driver synchronizes users, groups, and organizational unit.

If you upgrade a lower version of the GroupWise driver to the latest GroupWise driver, the upgraded driver synchronizes users, groups, distribution lists, external entities, organizational unit, and post offices.

## Driver Shim

The driver uses a Java based driver shim to communicate between the Identity Manager engine and GroupWise REST APIs. The driver shim converts the XML-based Identity Manager command and event language (XDS) to the protocols and REST API calls required to interact with GroupWise.

The shim for GroupWise is `com.novell.gw.dirxml.driver.rest.shim.GWdriverShim`. For information about installing the driver shim, see [“Installing the Driver Shim” on page 15](#).

## Driver Packages

The GroupWise driver packages are available on the Package Update site. When the driver is created with packages in Designer, a set of policies and rules are created suitable for synchronizing with GroupWise.

For creating a new driver, use the following packages:

- ♦ GroupWise REST Account Tracking version 3.0.0
- ♦ GroupWise REST Audit Entitlements version 3.0.0
- ♦ GroupWise REST Base version 3.2.0
- ♦ GroupWise REST Default Configuration version 3.2.0
- ♦ GroupWise REST Entitlements version 3.1.0
- ♦ GroupWise REST Managed System Information version 3.0.0
- ♦ GroupWise REST Password Synchronization version 3.2.0

For upgrading to the latest GroupWise driver, use the following packages:

- ♦ GroupWise Account Tracking version 2.5.1
- ♦ GroupWise Audit Entitlements version 2.5.0
- ♦ GroupWise Base version 2.6.0
- ♦ GroupWise Entitlements version 2.5.1
- ♦ GroupWise Managed System Information version 2.5.0
- ♦ GroupWise Password Synchronization version 2.6.0

---

**IMPORTANT:** Use these packages only if you are upgrading your existing driver to the latest GroupWise driver. They are not meant for connecting to GroupWise 2012 or lower versions of GroupWise. Download these packages from the [Package Update site](#).

To configure your driver to connect to GroupWise 2012 or lower versions, use packages with versions less than 2.5 from the [Package Update site](#).

---

## Checklist for Enabling User and Group Objects Synchronization

Use the following checklist to verify that you complete the following tasks in order to have a complete solution with the driver.

- ♦ Ensure that you have installed the software mentioned in [“Prerequisites” on page 15](#).
- ♦ Install the driver shim. For more information, see [“Installing the Driver Shim” on page 15](#).
- ♦ Create and configure the driver. For more information, see [Chapter 3, “Creating a New Driver Object,” on page 17](#).

# 2 Installing the Driver Files

You can install the GroupWise driver on different systems and platforms. To verify the system requirement list, see [System Requirements for Identity Manager 4.8](#).

The installation and configuration process for the driver requires access to the GroupWise server, Identity Manager and/or Remote Loader, and Designer for Identity Manager.

To install the driver, you first need to install the driver files, install the driver packages, and then modify the driver configuration to suit your environment. This section describes how to install the driver files. For information on installing and configuring driver packages, see [Chapter 3, “Creating a New Driver Object,”](#) on page 17.

- ♦ [“Prerequisites”](#) on page 15
- ♦ [“Installing the Driver Shim”](#) on page 15

## Prerequisites

- ♦ Identity Manager 4.6 or later.
- ♦ Designer 4.6 or later
- ♦ GroupWise 2014 SP1 or later, and GroupWise 18

---

**IMPORTANT:** Log in to the GroupWise Administration console and verify that the Identity Vault information is correctly linked with the GroupWise server. For more information, see [“Associating Identity Vault with GroupWise System”](#) on page 22

---

## Installing the Driver Shim

By default, the driver files are installed on the Identity Manager server at the same time as the Identity Manager engine. The installation program extends the Identity Vault’s schema and installs the driver shim and the driver configuration file. It does not create the driver in the Identity Vault or upgrade an existing driver’s configuration.

You can install the driver on the Identity Manager server, or connect to the Identity Manager engine through a Remote Loader from a remote server. In this configuration, you install the Remote Loader and the driver files on a non-Identity Manager server where you want to run the driver. For more information, see in the [Configuring the Remote Loader and Drivers](#) in the *NetIQ Identity Manager Driver Administration Guide*. After the driver files are installed, create the driver. For more information, see [Chapter 3, “Creating a New Driver Object,”](#) on page 17.





# 3 Creating a New Driver Object

To create the driver in the Identity Vault, ensure that the driver files are installed on the server from where you want to run the driver (see [Chapter 2, “Installing the Driver Files,”](#) on page 15). Install the driver packages and then modify the driver configuration to suit your environment.

- ♦ [“Creating the Driver Object in Designer”](#) on page 17
- ♦ [“Activating the Driver”](#) on page 24

## Creating the Driver Object in Designer

Create the GroupWise driver by installing the driver packages and then modifying the configuration to suit your environment. After you create and configure the driver, you need to deploy it to the Identity Vault and start it.

- ♦ [“Importing the Driver Packages”](#) on page 17
- ♦ [“Installing the Driver Packages”](#) on page 18
- ♦ [“Configuring the Driver Object”](#) on page 21
- ♦ [“Deploying the Driver”](#) on page 21
- ♦ [“Associating Identity Vault with GroupWise System”](#) on page 22
- ♦ [“Starting the Driver”](#) on page 24

## Importing the 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. NetIQ recommends that you have the latest packages in the Package Catalog before creating a new driver object.

You can update driver packages at any time. They are stored in the Package Catalog. Packages are initially imported into the Package Catalog when you create a project, import a project, or convert a project. It is important to verify you have the latest packages imported into the Package Catalog before you install the driver.

To verify that Package Catalog has the most recent version of the driver packages, perform the following steps:

- 1 Open Designer.
- 2 In the toolbar, click **Help > Check for Package Updates**.  
Ensure that you have the latest version of the Common Settings packages in the Package Catalog.
- 3 Click **OK** to update the packages  
or

Click **OK** if the packages are up-to-date.

- 4 Continue with [“Installing the Driver Packages”](#) on page 18.

## Installing the Driver Packages

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**.  
or  
Drag and drop the GroupWise driver from the palette into the Modeler space.
- 3 Select **GroupWise REST Base**, then click **Next**.
- 4 Select the optional features to install the GroupWise driver. All options are selected by default. The options are:
  - Default Configuration:** These packages contain the default configuration information for the GroupWise driver. This is a mandatory package. Always leave this option selected.
  - Password Synchronization:** These packages contain the policies required to synchronize passwords to GroupWise.
  - Entitlements:** These packages contain the policies and entitlements required to enable the driver for account creation and management with entitlements.
  - Data Collection:** These packages contain the policies that enable the driver to collect data for reports. If you are using the Identity Reporting, verify that this option is selected. For more information, see the [Administrator Guide to NetIQ Identity Reporting](#).
  - 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 [Administrator Guide to NetIQ Identity Reporting](#).
- 5 Click **Next**.
- 6 (Conditional) Click **OK** to install the Password Synchronization Notification package dependency.
- 7 (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 Advanced Java Class and Common Settings packages, if you have not installed any other packages into the selected driver set.
- 8 (Conditional) If not already configured, fill in the following fields on the Common Settings page, then click **Next**:
  - 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 On the Install GroupWise REST Base page, specify the name of the driver, then click **Next**.

11 On the Install GroupWise REST Base page, fill in the following fields, then click **Next**:

**Authentication ID:** Specify the user ID used to authenticate to the GroupWise system. By default, it is the GroupWise Administrator user.

**Connection Information:** Specify the IP address and the decimal port number (for example, `IP Address:port`) to connect to GroupWise. By default, it runs on port 9710 (Administration Service port). The Administration Service running on the GroupWise primary domain is used as the connection address in the driver configuration.

---

**NOTE:** If you specify GroupWise server host name instead of IP address, ensure that **Set Bind Exclusive** setting is changed to **false** in the Message Transfer Agent of the GroupWise server. To do this, log in to Administration Service, change the setting and then restart the Administration Service.

---

**Password:** Specify the admin user password to authenticate to GroupWise.

**Always accept server certificate:** By default, this is set to **No**. Specify the values for the following parameters to use the keystore:

- ◆ **Keystore path for SSL certificates:** Specify the full path to the keystore file containing the SSL certificates.
- ◆ **Keystore Password:** Specify the password for accessing the keystore file containing the SSL certificates.

For more information about setting up SSL connections, See [Chapter 6, “Securing Driver Communication,”](#) on page 85.

Select **Yes** if you want the driver to accept the GroupWise server's certificate for establishing SSL connection with the Identity Manager server. This avoids the need for manually maintaining a keystore.

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

**Default Sync Destination GroupWise Post Office:** Specify the GroupWise post office name in dot format. The newly added Identity Vault objects are created in this GroupWise post office. For example: `GWDomain.PostOffice`. In earlier GroupWise drivers, the GroupWise post office name was specified in slash format.

13 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.

If you select **No**, skip to [Step 17](#). If you select **Yes**, provide 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 where the Remote Loader is installed and is running for this driver. The default value is 8090.

**KMO:** Specify the Key Name of the Key Material Object (KMO) that contains the keys and certificates the Remote Loader uses for an SSL connection. This parameter is only used when you use SSL for connections between the Remote Loader and the Identity Manager engine.

**Other parameters:** Specify any other parameters required to connect to the Remote Loader. Any parameters specified must use a key-value pair format, as follows:

```
paraName1=paraValue1 paraName2=paraValue2
```

**Remote Loader Password:** Specify the Remote Loader's password as defined in the Remote Loader. The Identity Manager server (or Remote Loader shim) requires this password to authenticate to the Remote Loader.

**Driver Password:** Specify the driver object password that is defined in the Remote Loader service. The Remote Loader requires this password to authenticate to the Identity Manager server.

- 14 (Conditional) Provide the following fields on the Managed System Information page, then click **Next**:

**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.

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

**Vendor:** Select **NetIQ Corporation** 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.

---

**NOTE:** This page is only displayed if you installed the Managed System package.

---

- 15 (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.

---

**NOTE:** This page is only displayed if you installed the Managed System package.

---

- 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.

**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.

---

**NOTE:** This page is only displayed if you installed the Managed System package.

---

- 17 (Conditional) Provide the following field on the Account Tracking Information page, then click **Next**:

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

---

**NOTE:** This page is only displayed if you installed the Account Tracking package.

---

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

The driver is now created. To modify the configuration settings, proceed to the section [“Configuring the Driver Object”](#) on page 21.


## Configuring the Driver Object

After installing the driver packages, you can configure the driver to suit your environment. 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.

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

## 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 Review 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 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, “[Associating Identity Vault with GroupWise System](#)” on page 22.

## Associating Identity Vault with GroupWise System

You must associate Identity Vault with the GroupWise system.

**1** In the GroupWise Administration console, click **System > LDAP Servers**, then click **New Directory**.

**New Directory** Close X

**General** LDAP Authentication Email Publishing

Name: idm4x\_tree1

Description: This Identity Vault server is associated with GroupWise system.

Type: eDirectory

Address: 192.126.34.23

Port: 389  Use SSL

SSL Certificate: [Empty] [Search] [Delete] [Edit]

LDAP User: cn=admin,ou=sa,o=system

LDAP User Password: [Masked]

[Test Connection]

Base DN: o=data

Sync Domain: gw\_domain

Enable Synchronization

[Sync]

[?] [OK] [Cancel]


- 2 In the **General** tab, fill in the following fields, then click **Test Connection** to verify that you have provided accurate information about Identity Manager server:
  - 2a **Name:** Specify the name of your Identity Vault (eDirectory tree).
  - 2b **Description:** Provide a description for eDirectory.
  - 2c **Type:** Select the directory type. In this case, it is eDirectory.
  - 2d **Address:** Enter the IP address of your eDirectory server (Your eDirectory server must be set to allow clear text in order to use port 389).
  - 2e **SSL Certificate:** This is an optional field. Use it if you want the GroupWise server to communicate with a backend server in SSL mode.
  - 2f **LDAP User:** Specify the admin user name.
  - 2g **LDAP User Password:** Specify the password for the admin user.
  - 2h **Test Connection:** Click this button to verify that you have provided accurate information about Identity Manager server.
  - 2i **Base DN:** Specify the container where the objects reside in Identity Vault. For example, o=data.

- 2j **Sync Domain:** The GroupWise domains are populated in the drop-down list. Select the value that matches the domain name that you specified for the `Default Sync Destination GroupWise Post Office` parameter in [Step 12 on page 19](#).
- 2k **Enable Synchronization:** Uncheck this option.
- 3 Click **OK** to complete the configuration.
- 4 Click **Close** to return to the main Administration console window.

## 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 will not 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**.

## Activating the Driver

The Identity Manager driver for GroupWise does not need a separate activation. If you create the driver in a driver set where you have already activated the Identity Manager server and service drivers, the driver inherits the activation from the driver set.

If you create the driver in a driver set that has not been previously activated, the driver will run in the evaluation mode for 90 days. You must activate the driver during the evaluation period; otherwise, the driver will be disabled. If you try to run the driver, the trace displays an error message indicating that you need to reactivate the driver to use it. For information on activation, refer to [Activating Identity Manager](#) in the *NetIQ Identity Manager Overview and Planning Guide*.



# 4 Upgrading an Existing Driver

The GroupWise driver communicates with the GroupWise system. Ensure that earlier versions of GroupWise are upgraded to GroupWise 2014 SP1 or later versions, or GroupWise 18, before running the driver upgrade. The GroupWise upgrade program automatically associates GroupWise server with the Identity Vault. However, you should verify whether the Identity Vault is correctly linked with the upgraded GroupWise server.

- 1 Log in to the Administration console.
- 2 Navigate to the LDAP Server Configuration page.
- 3 Verify the **Name** field populates the name of the Identity Vault (eDirectory tree).
- 4 Specify other Identity Vault configuration information and save the settings.

For more information, see [“Associating Identity Vault with GroupWise System” on page 22](#).

## Upgrading an Existing Driver to GroupWise Driver

To upgrade an existing driver to the supported GroupWise driver, you need to upgrade the following driver components:

- ♦ Driver shim
- ♦ Driver packages
- ♦ [“Upgrading the Driver Shim” on page 25](#)
- ♦ [“Upgrading the Existing Driver Packages” on page 26](#)

### Upgrading the Driver Shim

To upgrade the driver shim, perform the following actions:

- 1 Stop the driver instance by using Identity Console, Designer, or dxcmd by performing one of the following actions:
  - ♦ If the driver is running locally, stop the driver instance and the Identity Vault.
  - ♦ If the driver is running with a Remote Loader instance, stop the driver and the Remote Loader instance.

For example, go to a command prompt on Linux and run `ndsmanage stopall`

- 2 Download the driver patch file to a temporary folder on your server.
- 3 Extract the contents of the driver patch file.
- 4 Update the driver files:
  - ♦ Linux: Open a command prompt and run the following command to upgrade the existing RPM:

```
rpm -U (image-path)/novell-DXMLGWRest.rpm
```

- ♦ **Windows:** Navigate to the <Extracted Driver Patch File Temporary Location>\windows folder and copy the GWRestShim.jar file to <IdentityManager installation>\RemoteLoader\lib folder.

- 5 (Conditional) If the driver is running locally, start the Identity Vault and the driver instance.  
For example, open a command prompt on Linux and run `ndsmanage startall`
- 6 (Conditional) If the driver is running with a Remote Loader, start the Remote Loader and the driver instance.

## Upgrading the Existing Driver Packages

You must upgrade the existing GroupWise driver packages to GroupWise 2.5 packages.

1. Download all GroupWise 2.5 or 2.6 packages from the [Package Update site](#).

Ensure that the package version is 2.5 or 2.6. For more information about the packages needed for the driver upgrade, see [“Driver Packages” on page 14](#).

2. Right-click the driver, then click **Properties**.
3. Click **Packages**, and select the packages to upgrade.

---

**IMPORTANT:** Performing a partial upgrade of the packages might break the existing driver functionality.

If you want to install the legacy GroupWise driver after installing the upgraded packages, you need to manually select 2.0.x packages during package installation because 2.5 packages will become the default packages for the GroupWise driver. You must ignore 2.5 packages for creating a legacy GroupWise driver.

- 
4. Follow the driver configuration steps from [“Installing the Driver Packages” on page 18](#).
  5. Click **Next**.
  6. In the driver configuration page, update the GroupWise **Driver Class** name to `com.novell.gw.dirxml.driver.rest.shim.GWdriverShim`.

---

**NOTE:** Change the name of the driver module if you are running the driver locally. If you are running the driver remotely, modify the Remote Loader instance configuration with the new class name before starting the driver instance.

- 
7. Deploy the driver.
  8. Start the driver.

---

**IMPORTANT:** GroupWise does not support Distribution List and External Entities objects. However, the upgraded driver supports the Modify operation for them. For a list of GCVs applicable for the upgraded driver, see [“GCVs Applicable for the Upgraded Driver” on page 102](#).

---

# 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.

- ♦ [“Default Driver Actions” on page 27](#)
- ♦ [“Modifying Default Settings in Policies and the Filter” on page 27](#)
- ♦ [“Modifying Policies” on page 29](#)
- ♦ [“Setting GroupWise Client Options with the Driver” on page 49](#)
- ♦ [“Client Options Quick Reference” on page 80](#)

## 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.

## 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, NetIQ recommends 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 28](#) 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 28](#) for more information.

3. Modify the Subscriber Create policy. See [“Modifying the Create Policy” on page 28](#) for more information.
4. Modify the Subscriber Placement policy. See [“Modifying Policies” on page 29](#).

---

**IMPORTANT:** Ensure that you set the GroupWise attributes by using the do-add-dest-attr-value action instead of do-set-dest-attr-value action. An exception occurs if you set the attributes by using the do-set-dest-attr-value action. [“Creating a Gateway Alias” on page 37](#) provides an example code using this action.

---

## 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.

If you add classes or attributes to the filter, you must append the `merge-authority="edir"` string to the added attribute in the Filter.

For example:

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

## 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.

## 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 for a User object and CN for a Group object.

## Modifying the Matching Policy

Matching policies define the minimum criteria that two objects must meet to be considered the same.

# Modifying Policies

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

- ♦ [“Specifying the GroupWise Post Office” on page 29](#)
- ♦ [“Configuring the GroupWise UserID” on page 30](#)
- ♦ [“Creating Mappings for Additional Attributes” on page 31](#)
- ♦ [“Getting a Record Count from a Query” on page 31](#)
- ♦ [“Creating a GroupWise Nickname” on page 32](#)
- ♦ [“Creating a GroupWise Nickname Record” on page 32](#)
- ♦ [“Controlling Creation of GroupWise Accounts” on page 34](#)
- ♦ [“Moving Users from One Post Office to Another Post Office” on page 34](#)
- ♦ [“Adding Additional Attributes to Be Synchronized” on page 36](#)
- ♦ [“Renaming Users” on page 36](#)
- ♦ [“Creating a Gateway Alias” on page 37](#)
- ♦ [“Using the Wildcard Query” on page 38](#)
- ♦ [“Querying for a Nickname” on page 39](#)
- ♦ [“Querying for a Email Address from a Nickname” on page 41](#)
- ♦ [“Querying for a Gateway Alias” on page 42](#)
- ♦ [“Querying for Internet Email Address” on page 43](#)
- ♦ [“Synchronizing GroupWise External Users” on page 45](#)
- ♦ [“Verifying if an E-Mail Address or Gateway Alias Is Unique” on page 46](#)
- ♦ [“Converting String Attributes to Structured Attributes” on page 48](#)

## 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.

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

```

<rule>
  <description>Users in Sales container are placed in Post Office P01</
description>
  <conditions>
    <and>
      <if-class-name op="equal">User</if-class-name>
      <if-src-dn op="in-container">data\users\Sales</if-src-dn>
    </and>
  </conditions>
  <actions>
    <do-set-op-dest-dn>
      <arg-dn>
        <token-text xml:space="preserve">GWDomain.P01</token-text>
      </arg-dn>
    </do-set-op-dest-dn>
    <do-break/>
  </actions>
</rule>
<rule>
  <description>Users in Engineering container are placed in Post Office
P02</description>
  <conditions>
    <and>
      <if-class-name op="equal">User</if-class-name>
      <if-src-dn op="in-container">data\users\Engr</if-src-dn>
    </and>
  </conditions>
  <actions>
    <do-set-op-dest-dn>
      <arg-dn>
        <token-text xml:space="preserve">GWDomain.P02</token-text>
      </arg-dn>
    </do-set-op-dest-dn>
    <do-break/>
  </actions>
</rule>

```

## 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.) 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 36](#) 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>
```

## 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. 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 Web Console. You should configure the same mappings in GroupWise as you do in the driver mappings.

## 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>pol</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 GroupWise system. This search can be altered to apply to other search criteria.

## 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 Identity Console 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.

## 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.)



## Example 1

```
<add class-name="GroupWise Nickname" dest-dn="domain.po" 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">Usernl</value>
  </add-attr>
  <!-- name of nickname record -->
  <add-attr attr-name="50073" >
    <value type="string">nnl</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">Usernl</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">nnl</value>
  </add-attr>
</add>
```

## 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.

NetIQ recommends that you use the UserAccount entitlement to control the creation of an account. When this entitlement is granted, the driver provides an enabled logon account. When this entitlement is revoked, the driver either disables or deletes the logon account, depending on the GCV configuration of entitlements.

Alternatively, you can control the creation of an account by triggering the account creation through 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>
```

## Moving Users from One Post Office to Another Post Office

When the Output Transformation style sheet is configured to move GroupWise accounts, NetIQ recommends that user moves be made in the Identity Vault and that the driver assigns 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 Post Office</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">GWDomain.salesPO</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">GWDomain.engineeringPO</token-
text>
          </arg-string>
        </do-set-xml-attr>
      </arg-actions>
    </do-if>
  </actions>
</rule>

```

The following example shows how to move a user to a new post office based on an attribute change:

```

<rule>
  <description>Post Office Move</description>
  <conditions>
    <or>
      <if-class-name mode="nocase" op="equal">User</if-class-name>
    </or>
    <or>
      <if-op-attr name="Description" op="changing-to">NYC</if-op-attr>
    </or>
  </conditions>
  <actions>
    <do-move-dest-object class-name="User">
      <arg-dn>
        <token-text xml:space="preserve">domain.po</token-text>
      </arg-dn>
    </do-move-dest-object>
  </actions>
</rule>

```

## 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 add these Identity Vault attributes to the filter and Schema Mapping policy.

## Renaming Users

NetIQ recommends 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.

## 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>
```

## 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>

```

where SMTP specifies the gateway alias type and UserOne@novell.com is the gateway alias address.

## Using the Wildcard Query

Wildcard (\*) query is supported for all attributes except Internet Email Address and Email Address.

### Code Sample

```

<nds dtdversion="4.0" ndsversion="8.x">
  <source>
    <product edition="Advanced" version="4.5.0.0">DirXML</product>
    <contact>NetIQ Corporation</contact>
  </source>
  <input>
    <query class-name="User" event-id="0" scope="subtree">
      <search-class class-name="User"/>
      <search-attr attr-name="50089">
        <value type="string">AAA*</value>
      </search-attr>
      <read-attr attr-name="50089"/>
    </query>
  </input>
</nds>

```

## Result

```
<nds dtdversion="2.0" ndsversion="8.x">
  <source>
    <product build="20160208_0216" instance="GroupWise REST
Driver"version="4.0.2.0">DirXML Driver for GroupWise</product>
    <contact>NetIQ Corporation</contact>
  </source>
  <output>
    <instance class-name="User" event-id="0" src-dn="gwdomain.pol.user1">
      <association>gwdomain.pol.user1{106}{B1D8F380-1429-0000-B673-
757234396331}6012EC01-18B5-0000-8300-1F8D6C64A072</association>
      <attr attr-name="OU">
        <value type="string">AAA-ENGINEERING</value>
      </attr>
    </instance>
    <instance class-name="User" event-id="0" src-dn="gwdomain.pol.user2">
      <association>gwdomain.pol.user2{106}{3AC06E00-1595-0000-B673-
757234396331}6012EC01-18B5-0000-8300-1F8D6C64A072</association>
      <attr attr-name="OU">
        <value type="string">AAA-SALES</value>
      </attr>
    </instance>
    <status event-id="0" level="success"/>
  </output>
</nds>
```

---

**NOTE:** Groupwise Rest API returns an error if the `search-attr` contains `?(question mark)` or `=(equals to)` literals.

---

## 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>
        </token-query>
      </arg-node-set>
    </do-set-local-variable>
  </actions>
</rule>
```



```

    <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">
  <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>

```

## Querying for a Email Address from a Nickname

The following DirXML script code segment shows how to query the email address from a user nickname.

## Code Sample

```
<nds dtdversion="4.0" ndsversion="8.x">
  <source>
    <product edition="Advanced" version="4.5.3.0">DirXML</product>
    <contact>NetIQ Corporation</contact>
  </source>
  <input>
    <query class-name="User" event-id="0" scope="subtree">
      <search-class class-name="User"/>
      <search-attr attr-name="Internet EMail Address">
        <value>user@domain.com</value>
      </search-attr>
      <read-attr attr-name="Internet EMail Address"/>
      <read-attr attr-name="50073"/>
    </query>
  </input>
</nds>
```

## Result

```
<nds dtdversion="2.0" ndsversion="8.x">
  <source>
    <product build="20160208_0216" instance="GroupWise REST
Driver" version="4.0.2.0">DirXML Driver for GroupWise</product>
    <contact>NetIQ Corporation</contact>
  </source>
  <output><instance class-name="User" event-id="0" src-
dn="gwdomain1.pol.user1">
    <association>gwdomain1.pol.user1{106}{98A43B80-129F-0000-8A67-
777838626530}1975BF80-18BE-0000-BA4E-0D7666A11154</association>
    <attr attr-name="Internet EMail Address">
      <value type="string">user@domain.com</value>
    </attr>
    <attr attr-name="CN">
      <value type="string">user</value></attr>
    </instance><status event-id="0" level="success"/>
  </output>
</nds>
```

## 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>
      <if-association op="associated"/>
    </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">
  <output>
    <instance class-name="User" event-id="0" src-
dn="TaoDom.TaoPO.User1{106}{640D4300-049C-0000-9F67-777433313534}50D4B180-
061B-0000-9A29-2264EBF4B491">
      <association>TaoDom.TaoPO.User1{106}{640D4300-049C-0000-9F67-
777433313534}50D4B180-061B-0000-9A29-2264EBF4B491</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>
```

## 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">
  <output>
    <instance class-name="User" event-id="0"
      src-dn="TaoDom.TaoPO.User2{106}{640D4300-049C-0000-9F67-
777433313534}50D4B180-061B-0000-9A29-2264EBF4B491">
    <association>TaoDom.TaoPO.User2{106}{640D4300-049C-0000-9F67-
777433313534}50D4B180-061B-0000-9A29-2264EBF4B491</association>
      <attr attr-name="Internet EMail Address">
        <value type="string">User2@domain.com</value>
      </attr>
    </instance>
    <status level="success"/>
  </output>
</nds>
```

## 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 45](#)
- ◆ [“Specifying an External Post Office in an Add Event” on page 46](#)
- ◆ [“Creating External Post Offices” on page 46](#)

## 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 46](#).
- ◆ Identify the external post office by [“Specifying an External Post Office in an Add Event” on page 46](#).
- ◆ Create a user in an organizational unit associated with the External GroupWise Post Office.

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 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 GroupWise Web administration console.

---

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

---

To specify placement when creating external post offices, specify the name of the non-GroupWise domain in which to create the external post office in the Placement policy.

## 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>

```

## Converting String Attributes to Structured Attributes

GroupWise supports some of the attributes only in the structured format. You need to convert them to the structured type that GroupWise supports. For example, attributes 50045. The attribute 50045 looks similar to the following in the JSON format:

```

"internetDomainName" : {
  "inherited" : false,
  "value" : "some value",
  "exclusive" : false
}

```

The true or false value for the `inherited` and `exclusive` components of this attribute depends on the configuration of the GroupWise system. For example,

```

<add-attr attr-name="50045">
  <value type="structured">
    <component name="inherited">true</component>
    <component name="value">company.com</component>
    <component name="exclusive">>false</component>
  </value>
</add-attr>

```

For more information about how GroupWise handles these attributes, see [GroupWise SDK: Administration REST API Guide](#).

To transform a string attribute type to a structured type, create a Transformation policy similar to the example shown below and add it to the Output Transformation policy of the driver. Also, ensure that you add the structured attributes to the Schema Mapping policy and the Subscriber filter of the driver.

The following example converts the 50045 attribute from a string value to a structured value. To override the preferred Internet domain name that the post office has inherited from its domain, the component `inherited` is set to `false`.



```

<rule>
  <description>Convert 50045 attribute from string to structured format</
description>
  <comment xml:space="preserve">The GroupWise REST interface
requires this attribute in the structured format.</comment>
  <conditions>
    <and>
      <if-op-attr name="50045" op="changing"/>
      <if-xpath op="true">node()[@attr-name='50045']//value/
@type='string'</if-xpath>
    </and>
  </conditions>
  <actions>
    <do-reformat-op-attr name="50045">
      <arg-value type="structured">
        <arg-component name="inherited">
          <token-text xml:space="preserve">>false</token-text>
        </arg-component>
        <arg-component name="value">
          <token-local-variable name="current-value"/>
        </arg-component>
        <arg-component name="exclusive">
          <token-text xml:space="preserve">>false</token-
text>
          </arg-component>
        </arg-value>
      </do-reformat-op-attr>
    </actions>
  </rule>

```

---

**NOTE:** In the GroupWise driver, you can set the Exclusive Use of Internet Domain Name by using the attribute 50045. In the legacy GroupWise driver, it could be done by using the attribute 50157. To set the Exclusive Use of Internet Domain Name by using the attribute 50045, set the component `exclusive` to `true` for the 50045 attribute in the above example policy.

---

## 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. Normally, the client options are set by the administrator through the GroupWise Administration Console.

- ♦ [“Using Policies to Set Client Options” on page 50](#)
- ♦ [“Client Options” on page 53](#)
- ♦ [“Environment > General” on page 54](#)
- ♦ [“Environment > Client Access” on page 56](#)
- ♦ [“Environment > Views” on page 57](#)
- ♦ [“Environment > Cleanup” on page 58](#)
- ♦ [“Environment > File Location” on page 59](#)
- ♦ [“Send > Send Options” on page 61](#)

- ♦ “Send > Mail” on page 64
- ♦ “Send > Appt” on page 66
- ♦ “Send > Task” on page 68
- ♦ “Send > Note” on page 70
- ♦ “Send > Security” on page 72
- ♦ “Send > Disk Space Management” on page 74
- ♦ “Calendar > General” on page 76
- ♦ “Calendar > Alarm Options” on page 78
- ♦ “Calendar > Busy Search” on page 79

---

**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 [“Client Options Quick Reference” on page 80](#).

---

## 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 GroupWise Administration console. However, you can access the client options in GroupWise Administration console, 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 the in the policy.

- ♦ [“Considerations” on page 50](#)
- ♦ [“Example Procedure” on page 51](#)

## 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 GroupWise Administration console. 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. The following lock levels are available in GroupWise Administration console:
  - ♦ 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 Administration console. 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.
  - ♦ 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 GroupWise Administration console.
  - ♦ 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

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 \(https://www.netiq.com/documentation/identity-manager-46/policy\\_designer/data/pbaccessing.html\)](https://www.netiq.com/documentation/identity-manager-46/policy_designer/data/pbaccessing.html).
- 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.

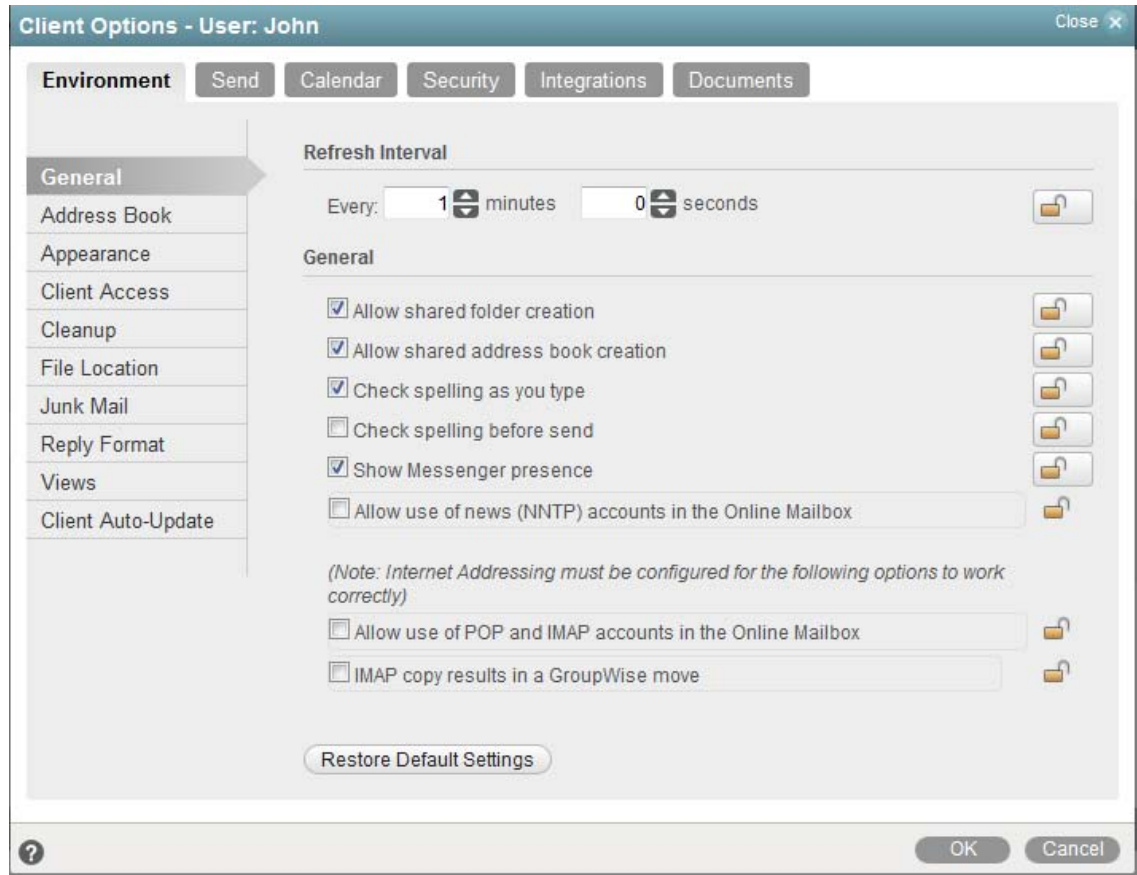
Name	Values							
<input type="text" value="lock-level"/>	<input type="text" value="0"/>							
<input type="text" value="value"/>	<input type="text" value="0"/>							
<input type="text" value="field"/>	<input type="text" value="autoSpellCheck"/>							

- 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.

# Client Options

To view the client options:

- 1 In GroupWise Administration console, select a Domain, Post Office, or User object, then click **Client Options**.



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

- ◆ “Environment > General” on page 54
- ◆ “Environment > Client Access” on page 56
- ◆ “Environment > Views” on page 57
- ◆ “Environment > Cleanup” on page 58
- ◆ “Environment > File Location” on page 59
- ◆ “Send > Send Options” on page 61
- ◆ “Send > Mail” on page 64
- ◆ “Send > Appt” on page 66
- ◆ “Send > Task” on page 68
- ◆ “Send > Note” on page 70
- ◆ “Send > Security” on page 72
- ◆ “Send > Disk Space Management” on page 74

- ♦ [“Calendar > General” on page 76](#)
- ♦ [“Calendar > Alarm Options” on page 78](#)
- ♦ [“Calendar > Busy Search” on page 79](#)

## 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 GroupWise Administration console through the GroupWise client options under **Environment > General**.

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.

---

## 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.

---

## Show Messenger Presence

The showIMPpresence 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.

## 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 GroupWise Administration console through the GroupWise client options under **Environment > Client Access**.

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.

## Environment > Views

The **Views** options are found in GroupWise Administration console through the GroupWise client options under **Environment > Views**. The **Views** Environment options determine when items open, and whether or not users can read and compose messages in HTML.

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>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">TEXT,HTML</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.

---

## 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.

## 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. The default view must be specified in the `defaultViewCompose` field.

## 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 GroupWise Administration console through the GroupWise client options under **Environment > Cleanup**.

The `DiscardSettings` attribute is used for the **Cleanup** options as well as the **Disk Space Management** options. For more information, see [“Send > Disk Space Management” on page 74](#).

```
<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">AUTO_PURGE</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:

- ♦ **Manual Delete and Archive:** Setting this value requires the user to delete and archive the mail and phone messages manually.
- ♦ **Auto-Delete after:** Setting this value allows GroupWise to delete the mail and phone messages after the days specified in the list box is elapsed. The maximum limit is 10,000 days.
- ♦ **Auto-Archive after:** Setting this value allows GroupWise to archive the mail and phone messages after the days specified in the list box is elapsed. The maximum limit is 10,000 days.

## Days

If you use the AUTO\_PURGE 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">AUTO_PURGE</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.

## Environment > File Location

The **File Location** option determines the archive locations for the GroupWise Windows and Linux clients. The location can either be a local drive or a network drive. The **File Location** settings are found in GroupWise Administration console through the GroupWise client options under **Environment > File Location**.

**For Windows:**

```

<do-set-dest-attr-value name="LocationsSettings">
  <arg-value type="structured">
    <arg-component name="lock-level">
      <token-text xml:space="preserve">NONE</token-text>
    </arg-component>
    <arg-component name="value">
      <token-text xml:space="preserve">C:\GWAREHIVE</token-text>
    </arg-component>
    <arg-component name="field">
      <token-text xml:space="preserve">archiveLocation</token-text>
    </arg-component>
    <arg-component name="itemLocked">
      <token-text xml:space="preserve">true</token-text>
    </arg-component>
  </arg-value>
</do-set-dest-attr-value>

```

#### **For Linux:**

```

<do-set-dest-attr-value name="LocationsSettings">
  <arg-value type="structured">
    <arg-component name="lock-level">
      <token-text xml:space="preserve">NONE</token-text>
    </arg-component>
    <arg-component name="value">
      <token-text xml:space="preserve">\\sles11gw2014\archive</token-text>
    </arg-component>
    <arg-component name="field">
      <token-text xml:space="preserve">archiveLocationLinux</token-text>
    </arg-component>
    <arg-component name="itemLocked">
      <token-text xml:space="preserve">true</token-text>
    </arg-component>
  </arg-value>
</do-set-dest-attr-value>

```

## **Archive Directory**

**UNC Path:** Specify the location where archived messages will be saved on GroupWise Windows clients.

**Linux Path:** Specify the location where archived messages will be saved on GroupWise Linux and Mac clients.

## **Custom Views**

**Custom Views:** Specify the folder where user-created views will be saved.

## 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 GroupWise Administration console through the GroupWise client options under **Send > Send Options**.

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 [“Send > Mail” on page 64](#).

```
<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">LIMITED_TO_POST_OFFICE</component>
    <component name="field">asteriskSendRestriction</component>
  </value>
  <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
- ◆ TOP\_SECRET

- ♦ FOR\_YOUR\_EYES\_ONLY
- ♦ 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:

- ♦ **LIMITED\_TO\_SYSTEM:** Setting the value to `LIMITED_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`.
- ♦ **LIMITED\_TO\_POST\_OFFICE:** Setting the value to `LIMITED_TO_POST_OFFICE` 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.
- ♦ **LIMITED\_TO\_DOMAIN:** Setting the value to `LIMITED_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.
- ♦ **UNLIMITED:** Setting the value to `UNLIMITED` 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.
- ♦ **NOT\_ALLOWED:** Setting the value to `NOT_ALLOWED` 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.

## 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.

## Send > Mail

The **Mail** options apply to mail messages only. The **Mail** options are found in GroupWise Administration console 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.

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">DELIVERED_OPENED</component>
    <component name="field">mailStatusInfo</component>
  </value>
</attr>
```



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

- ♦ **DELIVERED\_OPENED:** Setting the value to `DELIVERED_OPENED` tracks the delivered and opened status only. The user can open the Properties window of the sent message to view the status.
- ♦ **ALL\_INFORMATION:** Setting the value to `ALL_INFORMATION` 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">NONE</component>
    <component name="field">mailReturnOpen</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">NONE</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 `NONE` for the user to not receive a notification when the mail message is opened.
- ♦ **MAIL\_RECEIPT:** Set the value to `MAIL_RECEIPT` for the user to receive a mail message stating that the recipient opened the mail message.
- ♦ **NOTIFY:** Set the value to `NOTIFY` for the user to receive notification through GroupWise Notify when the recipient opens the mail message.

- ♦ **NOTIFY\_MAIL:** Set the value to NOTIFY\_MAIL 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 NONE for the user to not receive a notification when the mail message is deleted.
- ♦ **MAIL\_RECEIPT:** Set the value to MAIL\_RECEIPT for the user to receive a mail message stating that the recipient deleted the mail message.
- ♦ **NOTIFY:** Set the value to NOTIFY for the user to receive notification through GroupWise Notify when the recipient deletes the mail message.
- ♦ **NOTIFY\_MAIL:** Set the value to NOTIFY\_MAIL for the user to receive notification through GroupWise Notify and a mail message when the recipient deletes the mail message.

## Send > Appt

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

The AppointmentMessageSettings attribute stores this information.

```
<attr attr-name="AppointmentMessageSettings">
  <value type="structured">
    <component name="value">ALL_INFORMATION</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 64](#).

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:

- ♦ **DELIVERED\_OPENED:** Setting the value to `DELIVERED_OPENED` only tracks the delivered and opened status. The user can open the Properties window of the sent appointment to view the status.
- ♦ **ALL\_INFORMATION:** Setting the value to `ALL_INFORMATION` 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\_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\_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\_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.

## Send > Task

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

The `TaskMessageSettings` attribute stores this information.

```
<attr attr-name="TaskMessageSettings">
  <value type="structured">
    <component name="value">ALL_INFORMATION</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">taskReturnAccepted</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 [“Send > Mail” on page 64](#).

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:

- ♦ **DELIVERED\_OPENED:** Setting the value to `DELIVERED_OPENED` tracks only the delivered and opened status. The user can open the Properties window of the sent task to view the status.
- ♦ **ALL\_INFORMATION:** Setting the value to `ALL_INFORMATION` 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\_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\_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 taskReturnAccepted 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\_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\_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.

## Send > Note

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

The NoteMessageSettings attribute stores this information.

```

<attr attr-name="NoteMessageSettings">
  <value type="structured">
    <component name="value">DELIVERED_OPENED</component>
    <component name="field">noteStatusInfo</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">NONE</component>
    <component name="field">noteReturnOpen</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">NONE</component>
    <component name="field">noteReturnDelete</component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">NONE</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 [“Send > Mail” on page 64](#).

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:

- ◆ **DELIVERED\_OPENED:** Setting the value to `DELIVERED_OPENED` only tracks the delivered and opened status. The user can open the Properties window of the sent note to view the status.
- ◆ **ALL\_INFORMATION:** Setting the value to `ALL_INFORMATION` 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\_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 NONE for the user to not receive a notification when the note is deleted.
- ♦ **MAIL\_RECEIPT:** Set the value to MAIL\_RECEIPT for the user to receive a mail message stating that the recipient deleted the note.
- ♦ **NOTIFY:** Set the value to NOTIFY for the user to receive notification through GroupWise Notify when the recipient deletes the note.
- ♦ **NOTIFY\_MAIL:** Set the value to NOTIFY\_MAIL 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 NONE for the user to not receive a notification when the note is accepted.
- ♦ **MAIL\_RECEIPT:** Set the value to MAIL\_RECEIPT for the user to receive a mail message stating that the recipient accepted the note.
- ♦ **NOTIFY:** Set the value to NOTIFY for the user to receive notification through GroupWise Notify when the recipient accepted the note.
- ♦ **NOTIFY\_MAIL:** Set the value to NOTIFY\_MAIL for the user to receive notification through GroupWise Notify and a mail message when the recipient accepts the note.

## Send > Security

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



```

<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 a boolean value of `true` or 1. To disallow the use of S/MIME, set the value to `false` or 0.

---

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

---

## 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.

## Send > Disk Space Management

The disk space management settings are found in GroupWise Administration console 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.

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 [“Environment > Cleanup” on page 58](#).

```
<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="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">enableBoxThresholdNotification</
component>
  </value>
  <value type="structured">
    <component name="lock-level">0</component>
    <component name="value">0</component>
    <component name="field">enableBoxSizeNotification</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 and boxThresholdLimit fields.

---

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

---

### 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.

### 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.

---

## 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 GroupWise Administration console. 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.

---

## 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 GroupWise Administration console. 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.

---

## Calendar > General

The **Calendar** options determine basic settings for the GroupWise Calendar. The **Calendar** options are found in GroupWise Administration console through the GroupWise client options under **Calendar > General**.

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">highlightDaysOfWeek</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>
</attr>
```

```

    <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 all letters of the day capitalized. The value field can store only one day.

## Month Display Option > Highlight Day

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

## Month Display Option > Show Week Number

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

## Appointment Options > Include Myself on New Appointments

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

## Appointment Options > Default Length

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

```

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

```

## Work Schedule > Start Time

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

## Work Schedule > End Time

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

## Work Schedule > Work Days

The `workdays` field applies the start time and end time to each work day. Specify the desired work days in the value field. For example, MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY. The value is the days of the week in English, separated by a comma.

## 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 GroupWise Administration console through the GroupWise client options under **Calendar > Alarm Options**.

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.

## Calendar > 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 GroupWise Administration console through the GroupWise client options under **Calendar > Busy Search**.

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">01:30</component>
    <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>
</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.

## 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 [“Calendar > General” on page 76](#)).

## 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.

## Client Options Quick Reference

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

- ♦ [“Environment” on page 80](#)
- ♦ [“Send” on page 81](#)
- ♦ [“Calendar” on page 82](#)

## Environment

The environment options allow you to change how a users interacts with the GroupWise client. These options control views, access, appearance, junk mail settings, retention, and cleanup. [Table 5-1](#) shows the GroupWise Administration console options with a with their corresponding XML field names.

**Table 5-1** Client Options: Environment

Client Option	XML Field
General > Check spelling before send	autoSpellCheck
General > Allow shared folder creation	allowSharedFolders
General > Allow shared address book creation	allowSharedAddressBooks
General > Allow use of POP and IMAP accounts in the Online Mailbox	allowPOP_IMAPAccounts
General > Allow use of news (NNTP) accounts in the Online Mailbox	allowNNTPAccounts
General > Show Messenger presence	showIMPresence
Client Access > Client Licensing	clientLicense
Views > Allowable Read Views	allowableViewRead



Client Option	XML Field
Views > Allowable Read Views > Set Default	defaultViewRead
Views > Allowable Compose Views	alloableViewCompose
Cleanup > Empty Trash	trashPurge
Cleanup > Empty Trash > days	trashDays

## Send

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

**Table 5-2** GroupWise Client Options: Send

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

Client Option	XML Field
Task > Return Notification > When accepted	taskReturnAccepted
Task > Return Notification > When deleted	taskReturnDelete
Task > Return Notification > When completed	taskReturnCompleted
Note > Create a sent item to track information options	noteStatusInfo
Note > Return Notification > When opened	noteReturnOpen
Note > Return Notification > When deleted	noteReturnDelete
Note > Return Notification > When accepted	noteReturnAccept
Security > Conceal Subject	concealedSubject
Security > Require password to complete routed item	routePasswordRequired
Security > Secure Item Options > Do not allow use of S/MIME	disallowSMIME
Security > Secure Item Options > Encrypt for recipients	encryptMessages
Disk Space Mgmt > User Limits	userLimitSet
Disk Space Mgmt > Mailbox size limit	boxSizeLimit
Disk Space Mgmt > Threshold for warning users	boxThresholdLimit
Disk Space Mgmt > Limit apply to cache	boxLimitAppliesToCache
Disk Space Mgmt > Notify the administrator when threshold limit is exceeded	enableBoxThresholdNotification
Disk Space Mgmt > Notify the administrator when size limit is exceeded	enableBoxSizeNotification

## Calendar

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

**Table 5-3** GroupWise Client Option: Calendar

Client Options	XML Field
General > Month Display Option > First of week	firstDay
General > Month Display Option > Highlight day	highlightDaysOfWeek
General > Month Display Option > Show week number	showWeekNumber
General > Appointment Options > Include myself on new appointments	appointmentIncludeSelf
General > Appointment Options > Default length	appointmentDefaultLength
General > Work Schedule > Start time	startOfWorkday
General > Work Schedule > End time	endOfWorkday

---

<b>Client Options</b>	<b>XML Field</b>
General > Work Schedule > Work days	<a href="#">workdays</a>
General > Alarm Options > Set alarm when accepted	<a href="#">appointmentAlarmSet</a>
General > Alarm Options > Default alarm time	<a href="#">appointmentAlarmMinutes</a>
Busy Search > Range and Time to Search > From	<a href="#">busyStartTime</a>
Busy Search > Range and Time to Search > To	<a href="#">busyEndTime</a>
Busy Search > Appointment Length	<a href="#">busyInterval</a>
Busy Search > Days to Search	<a href="#">busyDays</a>

---



# 6 Securing Driver Communication

The GroupWise driver uses REST APIs to communicate with Groupwise. Groupwise internally uses an SSL connection. SSL connections encrypt all traffic on the TCP/IP socket by using a public/private key pair.

You can configure the driver to always accept the GroupWise server's certificate for establishing a SSL connection with the Identity Manager server. To do so, change the **Always accept server certificate** setting to **True** during driver configuration. For more information, see [Step 11 on page 19](#). If you leave the setting as is, you can use an alternative method and import the server certificate from GroupWise into a keystore on your Identity Manager server.

- 1 Import the server certificate from GroupWise and save it to a file in the `der` format.
  - 1a Open a web browser and connect to GroupWise with administrator rights at the first time. The browser prompts you to accept the server certificate.
  - 1b Go to the properties of the browser and download the certificate to your Identity Manager server in the `der` format.
  - 1c Save the file to a local file system.

- 2 Add the `.der` file to the keystore by using the following command at the command line:

```
keytool -import -file PATH_OF_DERFile\PublicKeyCert.der -keystore  
KEYSTOERPATH\NAME.keystore -storepass keystorepass
```

NetIQ recommends that you use Java 1.7 keytool. The command might not work with versions earlier than Java 1.7.

- 3 When you are asked to trust this certificate, select **Yes**.
- 4 Copy the `.keystore` file to any directory on the same file system where Identity Manager is running.
- 5 In Identity Console, Click **IDM Administration**.
- 6 Select the driverset where your driver is running and then click the GroupWise driver icon.
- 7 Navigate to **Configuration > Driver Parameters**.
- 8 In the **Subscriber Settings**, enter the complete path to the `keystore` file.
- 9 Specify the keystore password.
- 10 Click **Save** to save the configuration.



# 7 Managing the Driver

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





# 8 Troubleshooting the Driver

Refer to the following sections if you are experiencing a problem with the GroupWise driver:

- ♦ [“Attributes 50045 And 50157 Have Changed from String to Structured Format” on page 89](#)
- ♦ [“Errors are Displayed After Modifying the External Entity Objects on the Upgraded Driver” on page 89](#)
- ♦ [“Passing the Value of the GroupWise PostOffice Default Sync Destination GCV in Slash Format” on page 89](#)
- ♦ [“Uninstalling the Driver on Windows Reports a Java Virtual Machine Error” on page 90](#)
- ♦ [“Issue with Encrypting the OU Attribute” on page 90](#)
- ♦ [“Passwords Not Synchronized” on page 90](#)
- ♦ [“Exception Reported When Running Groupwise Driver and Google Apps Driver on the Same Server” on page 90](#)
- ♦ [“Troubleshooting Driver Processes” on page 91](#)

## Attributes 50045 And 50157 Have Changed from String to Structured Format

If you experience an error while attempting to set attribute 50045 or 50157, see [Converting String Attributes to Structured Attributes](#). For more information about how GroupWise handles these attributes, see [GroupWise SDK: Administration REST API Guide](#).

## Errors are Displayed After Modifying the External Entity Objects on the Upgraded Driver

The user object contains the DirXML-Accounts attribute in the Identity Vault. This attribute is not applicable for the External Entity objects. An External Entity object is represented as User {106} in GroupWise. When the modify association event is triggered for the External Entity object on the upgraded driver, the account tracking policy tries to update the account tracking attribute and results in error.

It is safe to ignore the error because it does not cause any functionality loss.

## Passing the Value of the GroupWise PostOffice Default Sync Destination GCV in Slash Format

After the driver upgrade, if you see the following trace message when a user is added, verify that the value of the Default Sync Destination: GroupWise PostOffice is in dot format:

```
DirXML Log Event -----  
  
Driver   = \GW12-LNX86\system\driverset1\GroupWise-Jun10_2014  
  
Thread  = Subscriber  
  
Object   = \GW12-LNX86\data\users\user (DOMAIN\PO1)  
  
Level    = error  
  
Message = <code>java.lang.IllegalArgumentException: Placement Rule  
Destination string DOMAIN\PO1 was not found</code>
```

## Uninstalling the Driver on Windows Reports a Java Virtual Machine Error

The driver uninstallation program only supports a 32-bit Java path. Ensure that you set the 32-bit Java path in the environmental variables to load the uninstallation program for a 64-bit Windows operating system.

## Issue with Encrypting the OU Attribute

The Organizational Unit (OU) attribute of a user in the Identity Vault is mapped to the CN attribute of GroupWise's Post Office class. When this attribute is encrypted in the Identity Vault, it also encrypts the value of the CN attribute in the driver trace.

There is no workaround at this time.

## Passwords Not Synchronized

If the password changes do not reflect in the Identity Vault, set the **Synchronize the eDirectory password to the GroupWise regular password** GCV to **false** to synchronize the password.

## Exception Reported When Running Groupwise Driver and Google Apps Driver on the Same Server

**Issue:** The default configuration of the Google Apps driver modifies the Java API which creates a compatibility issue with the GroupWise driver when both the drivers are running on the same server. As a result, the GroupWise driver reports the following error while processing events on the Subscriber channel:.

```
13:22:28 E9C03700 Drvrs: gw2014 ST:
DirXML Log Event -----
Driver: \WGSDVAULT\SD\driverset\GroupWise2014
Channel: Subscriber
Object: \WGSDVAULT\SD\Teachers\aegerter
Status: Error
Message: Code(-9010) An exception occurred:
javax.xml.transform.TransformerFactoryConfigurationError: Provider
javax.xml.transform.sax.SAXTransformerFactory could not be instantiated:
java.lang.IllegalAccessException: Class javax.xml.transform.FactoryFinder
can not access a member of class
javax.xml.transform.sax.SAXTransformerFactory with modifiers "protected"
```

**Workaround:** Set **Override JAXP Factory** to false on the Google Apps driver, or run the GroupWise Driver and Google Apps Driver on different servers.

## Troubleshooting Driver Processes

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



# 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 Identity Console. If a field is different in Designer, it is marked with the Designer icon.

- ♦ [“Driver Configuration” on page 93](#)
- ♦ [“Global Configuration Values” on page 96](#)
- ♦ [“GCVs Applicable for the Upgraded Driver” on page 102](#)

## Driver Configuration

In Identity Console:

- 1 Click the **IDM Administration** tile.
- 2 Select the driver set that contains the driver whose properties you want to edit.
- 3 Click the driver icon to display the driver’s properties page.

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:

- ♦ [“Driver Module” on page 93](#)
- ♦ [“Driver Object Password” on page 94](#)
- ♦ [“Authentication” on page 94](#)
- ♦ [“Startup Option” on page 95](#)
- ♦ [“Driver Parameters” on page 95](#)
- ♦ [“ECMAScript” on page 96](#)
- ♦ [“Global Configurations” on page 96](#)

## 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.rest.shim.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.

## 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.

## Authentication

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

**Authentication ID:** Specifies the user ID used to authenticate to the GroupWise system. By default, this is the GroupWise Administrator user.

**Connection Information:** Specifies the IP address and the decimal port number (for example, *IP Address:port*) to connect to GroupWise. By default, it runs on port 9710 (Administration Service port). The Administration Service running on the GroupWise primary domain is used as the connection address in the driver configuration.

**Remote Loader Connection Parameters:** Used when the driver is connecting remotely to the connected system. 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 Identity Manager engine.

**Application Password:** Specifies the admin user password to authenticate to GroupWise system.

**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):** Specifies 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.

## 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 Identity Console.

**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.

## 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:

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

**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:** Specifies the default user who becomes the new owner of resources that are reassigned.

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

**Always accept server certificate:** By default, this is set to **No**. To use the keystore, specify the values for the following parameters:

- ♦ **Keystore path for SSL certificates:** Specify the full path to the keystore file containing the SSL certificates.
- ♦ **Keystore Password:** Specify the password for accessing the keystore file containing the SSL certificates.
- ♦ **Reenter Keystore password:** Specify the password again to confirm it.

Select **Yes** if you want the driver to accept the GroupWise server's certificate for establishing SSL connection with the Identity Manager server. This avoids the need for manually maintaining a keystore. For more information on setting up SSL connections, See [Chapter 6, "Securing Driver Communication,"](#) on page 85.

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

## 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.

## 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.

## 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 Identity Console:

- 1 Click the **IDM Administration** tile.
- 2 Select the driver set that contains the driver whose properties you want to edit.
- 3 Locate the driver icon, then click the driver icon to display the driver's properties page.
- 4 Click **Global Config Values** drop down to display the GCV page.

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:

- ♦ [“Driver Configuration” on page 97](#)
- ♦ [“Entitlements” on page 98](#)
- ♦ [“Account Tracking” on page 100](#)
- ♦ [“Password Synchronization” on page 101](#)
- ♦ [“Managed System Information” on page 101](#)



## Driver Configuration

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

**Default Sync Destination: GroupWise Post Office:** Specify the GroupWise post office name in dotted form. The newly added Identity Vault objects are created in this GroupWise post office. For example: `GWDomain.PostOffice`.

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

**Cleanup Group Membership:** This option is 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 eDir OrgUnit To GroupWise External Post Office:** This option allows the driver to synchronize eDirectory organizational units to GroupWise external post offices. To enable synchronization, select **True** and specify a non-GroupWise domain name that exists within the GroupWise system in the **Create External Post Offices in this Non-GroupWise Domain** setting.

To disable synchronization, click **False**.

**Create External Post Offices in this Non-GroupWise Domain:** 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.

**Delete All Nicknames:** Allows the driver to delete GroupWise nicknames when GroupWise accounts are renamed or moved to another post office. **False** does not delete nicknames when the accounts are renamed or moved. Select **True** to delete them.

**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 [“Associating Identity Vault with GroupWise System” on page 22](#) for more information.

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

**Disassociate User in GroupWise on Deletion in ID Vault:** When a user is deleted in the Identity Vault, the corresponding user account is disassociated in the GroupWise server. The default value is **False**.

**GroupWise Web Service (SOAP) URL:** Specify the URL for the GroupWise Web Service (SOAP) API. Identity Manager engine can verify the synced password to GroupWise server in the Identity Vault using **password synchronization status** capability.

Example: `http://<ipaddress>:7191/soap`

## 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 98](#)
- ◆ [“Data Collection” on page 99](#)
- ◆ [“Role Mapping” on page 99](#)
- ◆ [“Resource Mapping” on page 100](#)
- ◆ [“Parameter Format” on page 100](#)
- ◆ [“Entitlement Extensions” on page 100](#)

## 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.

**Enable Login Disabled attribute sync:** Select **True** if the changes made to the LoginDisabled attribute in the Identity Vault should synchronize even if the User Account entitlement (Account) is enabled.

**Parameter Format:** Specify the parameter format the entitlement agent must use. You can pass the entitlement parameters in the legacy format or as a Jason string arranged in a `{"name":"value"}` format.

**Action 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**

**Use Group Entitlement:** Select whether the driver manages group membership for users with the gwGroup entitlement. By default, this is set to **True**. This allows the driver to manage GroupWise group membership based on the gwGroup entitlement. Select **False** if you do not want the driver to manage group membership for users based on the gwGroup entitlement.

**Parameter Format:** Specify the parameter format the entitlement agent must use. You can pass the entitlement parameters in the legacy format or as a Jason string arranged in a { "name" : "value" } format.

**Advanced Settings:** Select show to display the entitlement options that allow or deny additional functionality like data collection and others. These settings should rarely be changed.

## Data Collection

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

**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.

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

## Role Mapping

NetIQ Identity Applications allow you to map business roles with IT roles.

**Enable role mapping:** Select **Yes** to make this driver visible to Identity Applications.

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

**Allow mapping of groups:** Select **Yes** if you want to allow mapping of groups in Identity Applications.

## Resource Mapping

Identity Applications allow you to map resources to users.

**Enables resource mapping:** Select **Yes** to make this driver visible to Identity Applications.

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

**Allow mapping of groups:** Select **Yes** if you want to allow mapping of groups in Identity Applications.

## Parameter Format

**Format for Account entitlement:** Select the parameter format the entitlement agent must use. The options are **Identity Manager 4** or **Legacy**.

**Format for Group entitlement:** Select the parameter format the entitlement agent must use. The options are **Identity Manager 4** or **Legacy**.

## Entitlement Extensions

**Groupwise account extensions:** The content of this field is added below the entitlement element in the EntitlementConfiguration resource object.

**Group extensions:** The content of this field is added below the entitlement element in the EntitlementConfiguration resource object.

## Account Tracking

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

**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.

## Password Synchronization

The following GCVs control the follow 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.

## Managed System Information

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

### General Information

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

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

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

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

**Vendor:** Select **NetIQ** 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.

### System Ownership

**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.

### System Classification

**Classification:** Specify the classification for this GroupWise system in your environment. For example, Mission-Critical. 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.

## Connection And Miscellaneous Information

**Connection and miscellaneous information:** Select **show** to display the following settings:

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

**Type:** Specifies the type of the managed system.

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

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

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

## GCVs Applicable for the Upgraded Driver

The following GCVs are retained from the existing driver setup after the driver upgrade. They are applicable only for the upgraded driver. They don't apply to a new driver.

**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:** This option is 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:** This option is 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**.

**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 driver 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**.

**Use Distribution Lists Entitlement:** Select **True** if you want the driver to manage GroupWise distribution lists based on the gwDistLists Entitlement; otherwise, select **False**.

**Synchronize the eDirectory password to the GroupWise regular password:** Select **True** to allow passwords to flow from eDirectory to GroupWise. Select **False** if you do not want to set the regular password.

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.





# B

## Class and Attribute Descriptions

Table B-1 lists the GroupWise attributes included in the Schema Mapping policy. You might need to customize them to meet your requirement.

**Table B-1** *Classes and Attributes Included in the Schema Mapping Policy*

eDirectory Class or Attribute	GroupWise Attribute	Description
<b>User</b>		
CN	None	Common Name of a User object. This attribute is not included in the Schema Mapping policy, but the driver internally maps it with a corresponding GroupWise attribute.  When a GroupWise account is created or renamed, this value is used to name the GroupWise account. For all other operations, this value is ignored.
Given Name	50091	User's first name  Synchronizes from eDirectory to GroupWise on Create and Modify events.
Surname	50093	User's last name  Synchronizes from eDirectory to GroupWise on Create and Modify events.
Title	50096	User's title  Synchronizes from eDirectory to GroupWise on Create and Modify events.
OU	50089	User's department  Synchronizes from eDirectory to GroupWise on Create and Modify events.
Telephone Number	50095	User's telephone number  Synchronizes from eDirectory to GroupWise on Create and Modify events.
Facsimile Telephone Number	50145	User's facsimile telephone number  Only synchronizes the telephone number portion from eDirectory to GroupWise on Create and Modify events.
Company	50310	User's company  Synchronizes from eDirectory to GroupWise on Create and Modify events.

eDirectory Class or Attribute	GroupWise Attribute	Description
Initials	50322	Middle initials, up to 8 characters
Generational Qualifier	50323	Jr., III, and so forth, up to 8 characters
personalTitle	50324	Dr., Mr., Ms., and so forth, up to 8 characters
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	50138	Synchronizes from eDirectory to GroupWise on Create and Modify events. Setting the GroupWise 50138 attribute to 1 expires the GroupWise account.
OU	50089	User's department.  Synchronizes from eDirectory to GroupWise on Create and Modify events.
<b>Group</b>		
Member of a group	Member To	On eDirectory user Modify events, a set of distribution lists can be specified. The user can be added as a Member, BC, or CC. 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.
<b>Organizational Unit</b>		
OU	CN	User's department  Synchronizes from eDirectory to GroupWise on Create and Modify events.

Table B-2 lists the attributes that are available in the upgraded GroupWise driver. You might need to customize them to meet your requirement.

**Table B-2** Classes and Attributes Included in the Schema Mapping Policy for the Upgraded Driver

eDirectory Class or Attribute	GroupWise Attribute	Description
<b>User</b>		
Given Name	50091	User's first name  Synchronizes from eDirectory to GroupWise on Create and Modify events.

eDirectory Class or Attribute	GroupWise Attribute	Description
Surname	50093	User's last name  Synchronizes from eDirectory to GroupWise on Create and Modify events.
Title	50096	User's title  Synchronizes from eDirectory to GroupWise on Create and Modify events.
OU	50089	User's department  Synchronizes from eDirectory to GroupWise on Create and Modify events.
Telephone Number	50095	User's telephone number  Synchronizes from eDirectory to GroupWise on Create and Modify events.
Facsimile Telephone Number	50145	User's facsimile telephone number  Only synchronizes the telephone number portion from eDirectory to GroupWise on Create and Modify events.
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.  This attribute takes its value from the CN attribute. 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: <ul style="list-style-type: none"> <li>◆ Email Address</li> <li>◆ Internet Email Address</li> <li>◆ NGW: GroupWise ID</li> <li>◆ Identity Manager association key</li> </ul>
NGW Account ID	50116	Optional field for accounting. It can contain a cost account used for posting charges to this user.  Normally the driver does not set this value. However, this attribute can be set through the Create rule or Create style sheet.
NGW: Gateway Access	59001	Normally the driver does not set this value. However, this attribute can be set through the Create rule or style sheet.
NGW: Mailbox Expiration Time	50138	This attribute is used to set the NGW: Expiration Time attribute which in turn will set the GroupWise attribute 50058.

eDirectory Class or Attribute	GroupWise Attribute	Description
Login Disabled	50058	<p>A Boolean value that indicates whether eDirectory login (authentication) is allowed.</p> <p>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.</p>
NGW: File ID	50038	<p>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.</p> <p>A Move event could cause this attribute to change. This attribute should not be modified in any style sheet.</p>
NGW: Visibility	50076	<p>Used to specify the databases into which an object should be replicated. Controls whether objects appear in the address book.</p> <p>This attribute can be set through the Create rule or style sheet. To set it, add code to the Create rule. Use SYSTEM for global visibility, or NONE for no visibility. The value to set the visibility for Post Office is POST_OFFICE and Domain is DOMAIN.</p>
<b>Group</b>		
NGW: Visibility	50076	<p>Used to specify the databases into which an object should be replicated. Controls whether objects appear in the address book.</p> <p>This attribute can be set through the Create rule or style sheet. To set it, add code to the Create rule. Use SYSTEM for global visibility, or NONE for no visibility. The value to set the visibility for Post Office is POST_OFFICE and Domain is DOMAIN.</p>
Member	Member To	<p>On eDirectory user Modify events, a set of distribution lists can be specified. The user can be added as a Member, BC, or CC. 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.</p>
<b>GroupWise Distribution List</b>		
NGW: Visibility	50076	<p>Used to specify the databases into which an object should be replicated. Controls whether objects appear in the address book.</p> <p>This attribute can be set through the Create rule or style sheet. To set it, add code to the Create rule. Use SYSTEM for global visibility, or NONE for no visibility. The value to set the visibility for Post Office is POST_OFFICE and Domain is DOMAIN.</p>
Member	Member To	<p>On eDirectory user Modify events, a set of distribution lists can be specified. The user can be added as a Member, BC, or CC. 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.</p>

eDirectory Class or Attribute	GroupWise Attribute	Description
NGW: Carbon Copy Member	Member CC	Use the gw:participation="cc" attribute to have the driver set this information.
NGW: Blank Copy Member	Member BC	Use the gw:participation="bc" attribute to have the driver set this information.
<b>GroupWise External Entity</b>		
Given Name	50091	User's first name  Synchronizes from eDirectory to GroupWise on Create and Modify events.
Surname	50093	User's last name  Synchronizes from eDirectory to GroupWise on Create and Modify events.
Title	50096	User's title  Synchronizes from eDirectory to GroupWise on Create and Modify events.
OU	50089	User's department  Synchronizes from eDirectory to GroupWise on Create and Modify events.
Telephone Number	50095	User's telephone number  Synchronizes from eDirectory to GroupWise on Create and Modify events.
Facsimile Telephone Number	50145	User's facsimile telephone number  Only synchronizes the telephone number portion from eDirectory to GroupWise on Create and Modify events.
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.  This attribute takes its value from the CN attribute. 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: <ul style="list-style-type: none"> <li>◆ Email Address</li> <li>◆ Internet Email Address</li> <li>◆ NGW: GroupWise ID</li> <li>◆ Identity Manager association key</li> </ul>

eDirectory Class or Attribute	GroupWise Attribute	Description
NGW Account ID	50116	Optional field for accounting. It can contain a cost account used for posting charges to this user.  Normally the driver does not set this value. However, this attribute can be set through the Create rule or Create style sheet.
NGW: External Net ID	50094	
NGW: Mailbox Expiration Time	50138	This attribute is used to set the NGW: Expiration Time attribute which in turn will set the GroupWise attribute 50058.
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.
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.  A Move event could cause this attribute to change. This attribute should not be modified in any style sheet.
NGW: Visibility	50076	Used to specify the databases into which an object should be replicated. Controls whether objects appear in the address book.  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 SYSTEM for global visibility, or NONE for no visibility.  The value to set the visibility for Post Office is POST_OFFICE and Domain is DOMAIN.
<b>GroupWise Resource</b>		
NGW: Owner	50081	The user (NGW: Object ID) that owns the resource. An owner is identified by its Object Name.
<b>Organizational Unit</b>		
CN	OU	The corresponding GroupWise class is GroupWise Post Office.

Table B-3 lists additional GroupWise attributes that you can customize through policies to meet your business requirements.

**Table B-3** Custom Attributes That Are Not Part of the Default Schema Mapping Policy

eDirectory Class or Attribute	GroupWise Attribute	Description
<b>User</b>		
	50319	<p>Preferred Internet eMail ID. For 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	<p>Internet domain name</p> <p>The attribute 50045 takes a string value. Ensure that you convert this attribute to a structured attribute because GroupWise accepts some attributes only in a structured format. For more information, see <a href="#">“Converting String Attributes to Structured Attributes” on page 48.</a></p> <p>Example: MyDomain.com</p>
	50094	<p>Net ID</p> <p>This can either be a fully distinguished name or the common name.</p>
	58004	<p>DS_DN</p> <p>This is always the fully distinguished name.</p>
	58056	<p>LDAP authentication ID in typeful format. For example: cn=admin, o=novell</p>
	50013	<p>Preferred Internet address format</p> <p>(numeric value)</p> <p>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</p>
	50320	<p>Allowed Addressing formats</p> <p>(bit settings)</p> <p>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</p> <p>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).</p>

eDirectory Class or Attribute	GroupWise Attribute	Description
	50157	<p>Exclusive use of Internet domain name</p> <p>You can set the Exclusive Use of Internet Domain Name by using the 50157 attribute in the legacy GroupWise driver and 50045 attribute in the GroupWise driver. The attribute 50045 takes a string value. Ensure that you convert this attribute to a structured attribute because GroupWise accepts some attributes only in a structured format. For more information, see <a href="#">“Converting String Attributes to Structured Attributes” on page 48.</a></p> <p>True. Requires setting an Internet domain name: 50045. False. Only recognizes the domain name set in the Internet domain name: 50045.</p>
<b>GroupWise External Entity</b>		
	50319	<p>Preferred Internet eMail ID</p> <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	<p>Internet domain name</p> <p>Example: MyDomain.com</p> <p>The attribute 50045 takes a string value. Ensure that you convert this attribute to a structured attribute because GroupWise accepts some attributes only in a structured format. For more information, see <a href="#">“Converting String Attributes to Structured Attributes” on page 48.</a></p>
	58056	<p>LDAP authentication ID in typeful format</p> <p>Example: cn=admin, o=novell</p>
	50013	<p>Preferred Internet address format.</p> <p>(numeric value)</p> <p>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</p>



eDirectory Class or Attribute	GroupWise Attribute	Description
	50320	<p>Allowed addressing formats.</p> <p>(bit settings)</p> <p>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</p> <p>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).</p>
	50157	<p>Exclusive use of Internet domain name.</p> <p>You can set the Exclusive Use of Internet Domain Name by using the 50157 attribute in the legacy GroupWise driver and 50045 attribute in the GroupWise driver. The attribute 50045 takes a string value. Ensure that you convert this attribute to a structured attribute because GroupWise accepts some attributes only in a structured format. For more information, see <a href="#">“Converting String Attributes to Structured Attributes” on page 48.</a></p> <p>True. Requires setting an Internet domain name: 50045. False. Only recognizes the domain name set in the Internet domain name: 50045.</p>
Description	50032	<p>Provides additional information.</p> <p>Synchronizes from eDirectory to GroupWise on Create and Modify events.</p>



# 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*.

