



DriveLock 5 in Novell Environments

Whitepaper



Copyright

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

© 2007 CenterTools Software GmbH. All rights reserved.

CenterTools and DriveLock and others are either registered trademarks or trademarks of CenterTools GmbH or its subsidiaries in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

1	Introduction.....	4
2	Software Prerequisites.....	5
3	Deploying DriveLock Configuration	6
4	Deploying DriveLock Agents	10
4.1	Deploy the DriveLock Agent Using Novell ZENworks	10
4.2	Upgrading Existing Agent Installations	16
5	Using Novell Users and Groups in DriveLock.....	17
5.1	Select NDS Users or Groups	17
5.2	Mixed mode.....	19
5.3	Offline usage	20
6	Configuration Traffic.....	21

1 Introduction

CenterTools DriveLock is the perfect solution to prevent unauthorized data transfer controlling the use of all types of ports and devices on all computers in an entire network. Access to particular devices can be granted to specific users and groups that exist within the network.

In Novell networks, you can use Novell ZENworks which allows for easy centralized configuration of device control across an entire enterprise network.

This document provides technical information about interoperability between CenterTools DriveLock and Novell Directory Services/ZENworks.

Because careful planning and evaluation is essential for successfully deploying DriveLock throughout the enterprise, this whitepaper also describes best practices and examples of policy settings to help you achieve the specific needs of your organization.

2 Software Prerequisites

CenterTools recommends using Novell ZENworks when deploying DriveLock in a Novell environment. This whitepaper covers the requirements for successfully deploying DriveLock Agents to client computers and for distributing the client configuration.

System Requirements:

- Novell Directory Service (eDirectory), Novell Enterprise Server (Linux), Netware
- ZENworks 4.x or higher (recommended for software distribution)
- Supported client operating systems: Windows 2000, XP, 2003, Vista
- Novell Client

3 Deploying DriveLock Configuration

The two methods for centrally deploying the DriveLock configuration are:

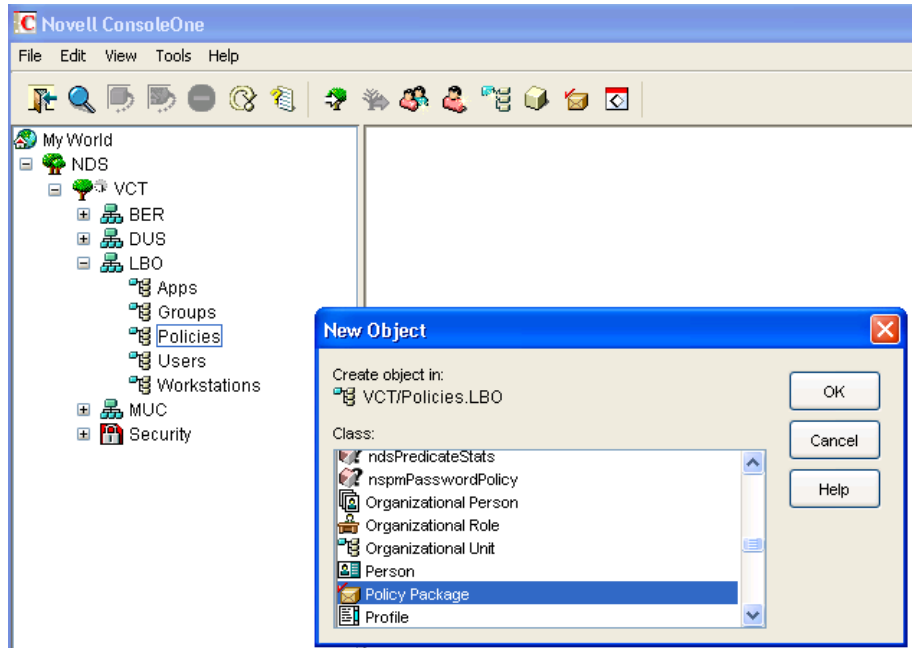
1. An Agent configuration file that contains the settings that are applied by the Agent. This is stored on a server and can be retrieved by Agents using an UNC path, FTP or HTTP.
2. A group policy created with ZENworks that is assigned to the Agents. This is a more powerful and elegant solution than working with configuration files.

Perform the following steps to implement each configuration methods:

- 1.) Configuration using a configuration file: This method can be implemented more quickly but provides less flexibility in the long run.
 - a. Configure DriveLock using the DriveLock Management console on an administrative workstation. Use the console node “Configuration files” to create a new configuration file.
 - b. Publish the configuration file. (Refer to the chapter “Create a configuration file” in the DriveLock manual for details. “DriveLock 5.0 Planning – Installation – Deployment”)
 - c. Create a customized DriveLock Agent installation package using the Deployment Wizard (Refer to the chapter “Deployment Wizard” in the DriveLock manual for details. “DriveLock 5.0 Planning – Installation – Deployment”)
 - d. Deploy the Agent as described in the next chapter
- 2.) Configuration using ZENworks Group Policy: This is method of configuring DriveLock in your Novell environment provides more flexibility in the long run.
 - a. Start Console One
 - b. Create a new policy package in your OU/Organisation structure

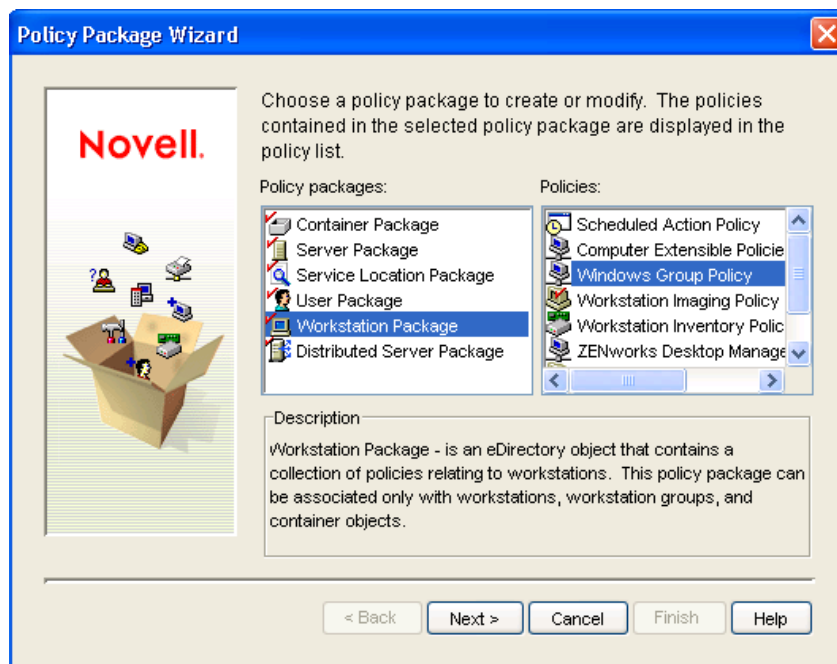


If you have already an existing Policy Package assigned to workstations you can instead use the existing Windows Group Policy. To edit the policy, the DriveLock Management Console must be installed on the computer where you are editing the DriveLock policy. If the Management Console is not installed, DriveLock configuration settings are not displayed and can't be edited.



- c. Select *Workstation Package* and then select *Windows Group Policy*.

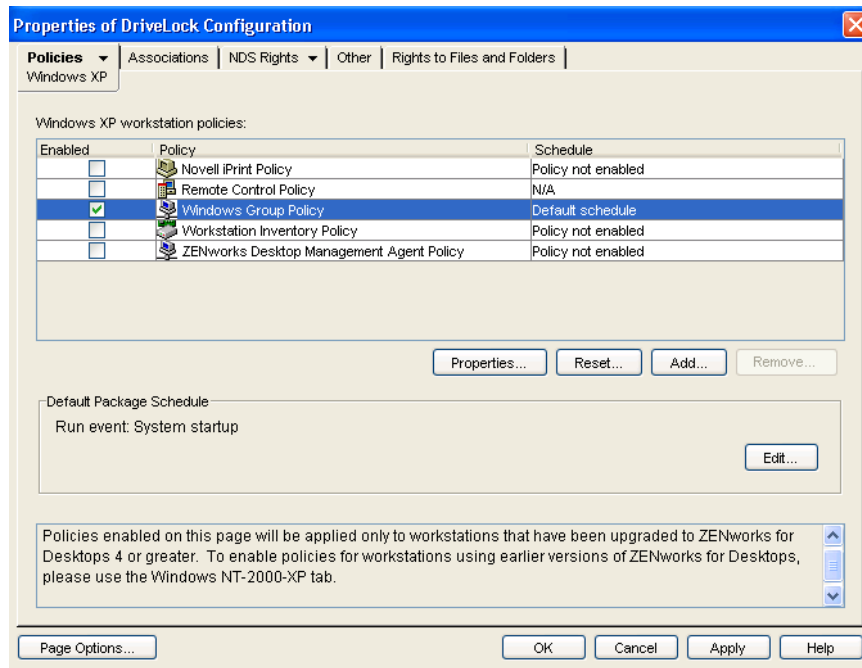
Note: The DriveLock configuration is stored in the computer settings of the policy and must be assigned to computers, not to users.



- d. Type a name for the policy package

Note: Note that only a single policy package can be assigned to a computer.

- e. Select the check box "*Define additional settings*" and then click **Finish**.
- f. On the Select "*Windows XP*" from the "*Policies*" menu.

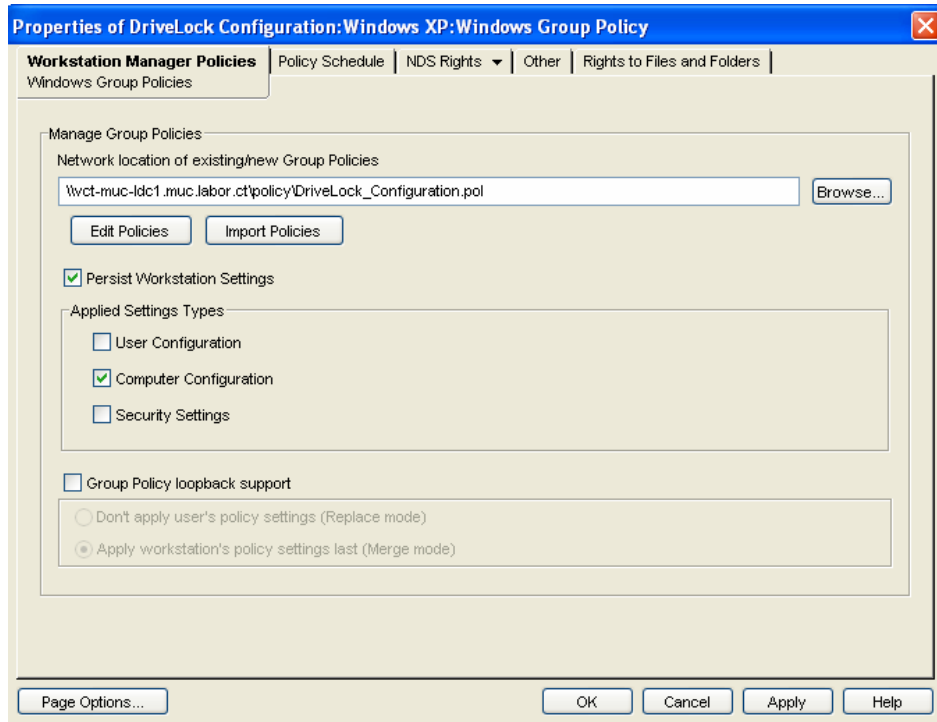


- g. Ensure that the “*Default Package Schedule*” is configured to run at System start-up (Run event: System start-up).
- h. Select the checkbox “*Windows Group Policy*” and then click **Properties**.
- i. Select the path for storing the group policy. Note that network traffic is created each time the group policy is applied.

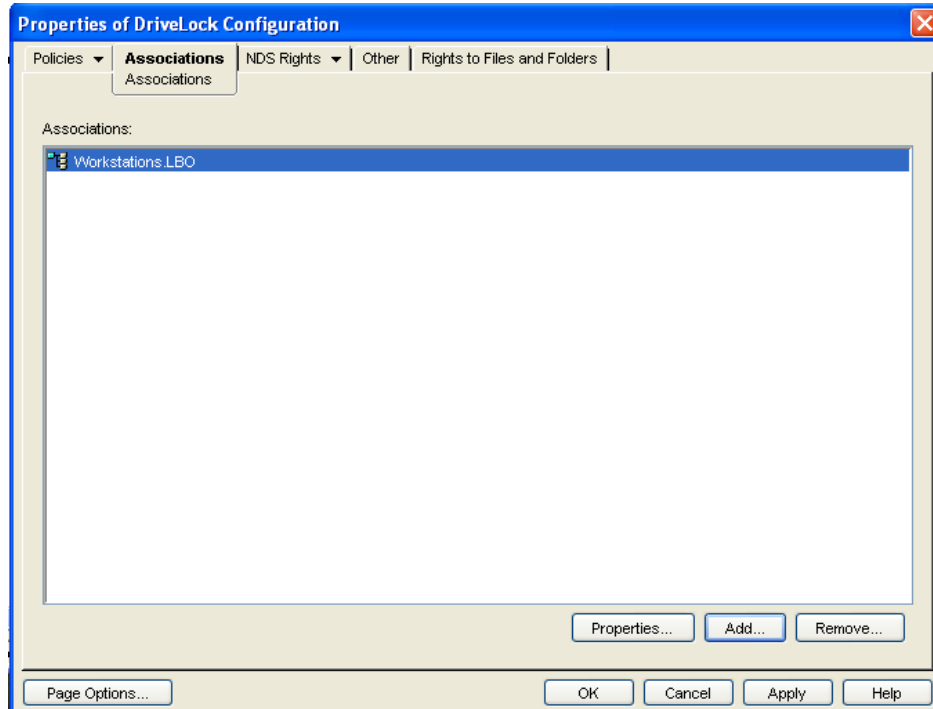


The group policy files should be placed on a share which is accessible to the computer account. For example, create a folder named Policies and a subfolder for each policy in the SYS share of an NDS Linux or NetWare server and save the policy file to this location.

- j. After selecting a location for storing the policy, you can edit the policy settings. To create the DriveLock configuration, select the checkbox “*Persist Workstation Settings*”, and then click **Edit Policies**. When finished editing the policy settings, close the policy.



- k. Once all policy settings have been configured, the policy must be assigned to computers. To do this, click **OK** in the “*Manage Group Policies*” dialog box, and then select the appropriate organizational unit in the “*Associations*” dialog box of the group policy.



4 Deploying DriveLock Agents

You can deploy DriveLock Agents using your ZENworks environment or third-party deployment software. To deploy DriveLock using third-party deployment software, follow the instructions in the DriveLock manual “DriveLock 5.0 Planning – Installation – Deployment”.

4.1 Deploy the DriveLock Agent Using Novell

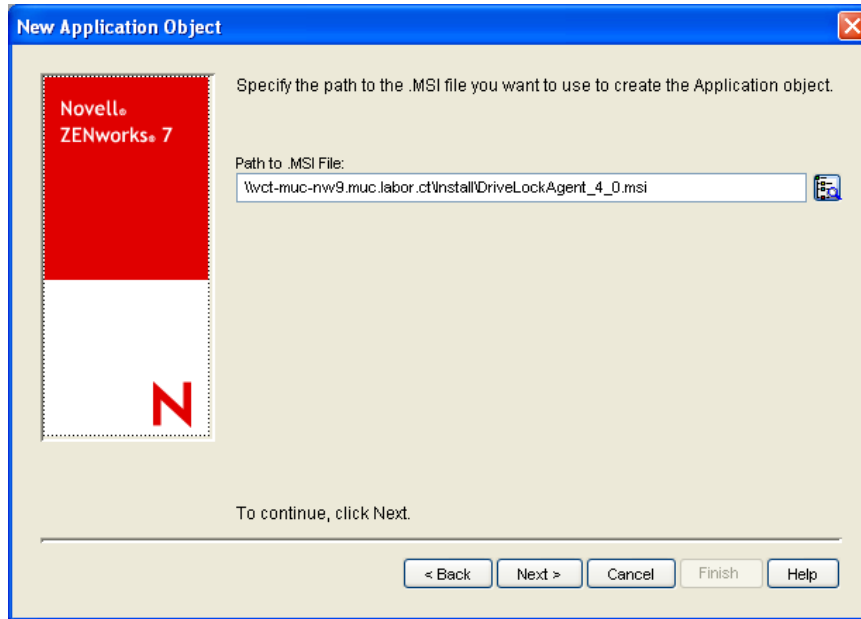
ZENworks

To deploy the DriveLock Agent using Novell ZENworks copy the Agent installation file (an MSI file) from the DriveLock CD or from the DriveLock download site to a shared folder.

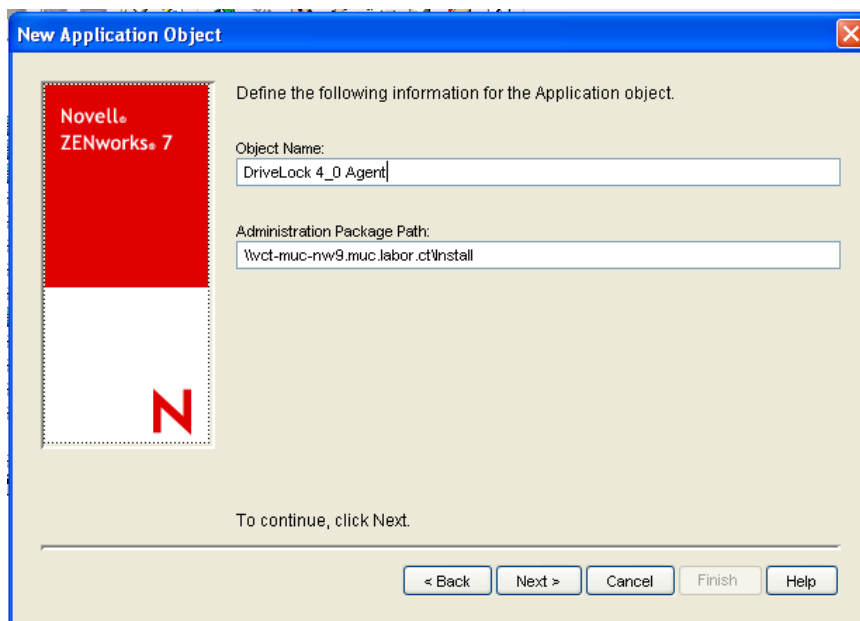
1. Start “Console One”.
2. Create a new “Application Package”.
3. Complete the “New Application Object” wizard using the following settings:
 - a. Select “*An application that has an .MSI file*”.
 - b. Select the network path where you copied the DriveLock Agent installation file.



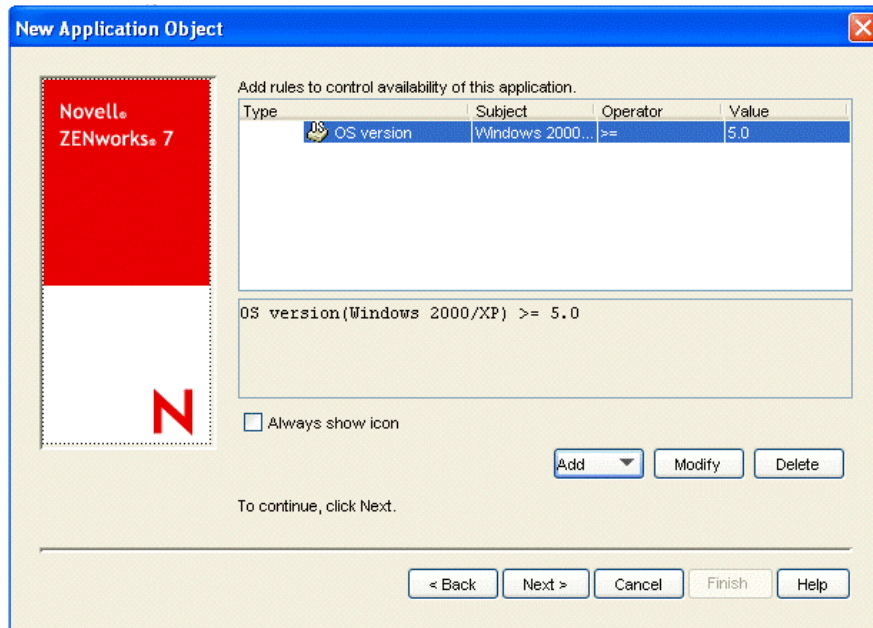
Before starting, place the Agent installation file in a share that is accessible to the computer account. For example, create a folder Apps and a subfolder named DriveLock in the SYS share of an NDS Linux or NetWare server and save the policy file to this location.



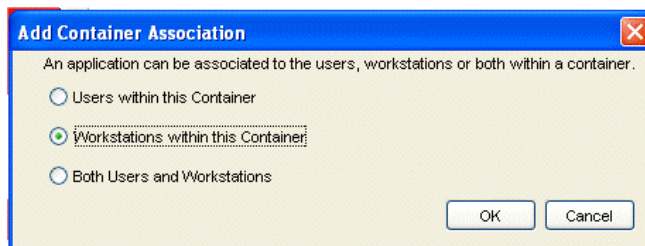
- c. Type a name for the package and specify the administrative location of the MSI installation package (normally the same path specified above).



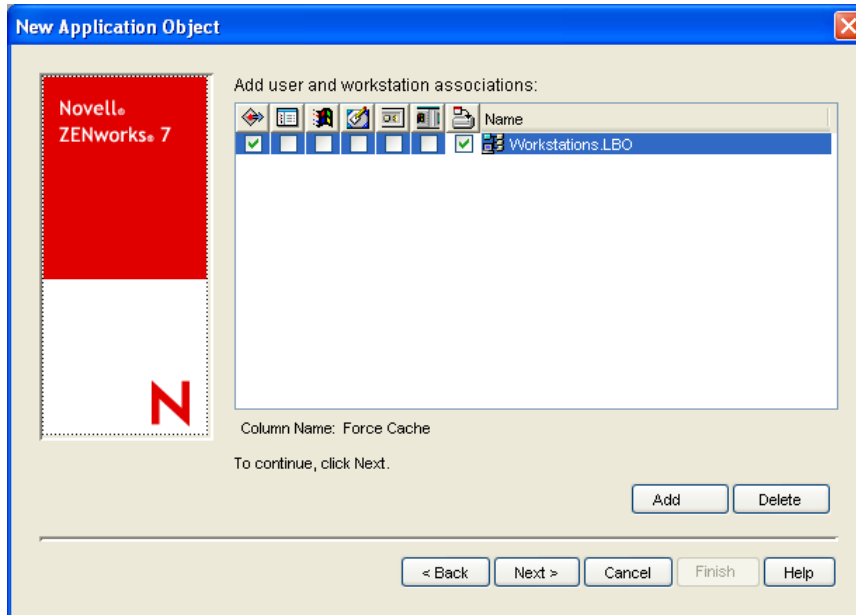
- d. Optionally you can add a rule to limit the distribution of the Agent to computers running Windows 2000 and Windows XP only. Otherwise, keep the default configuration (not selected)



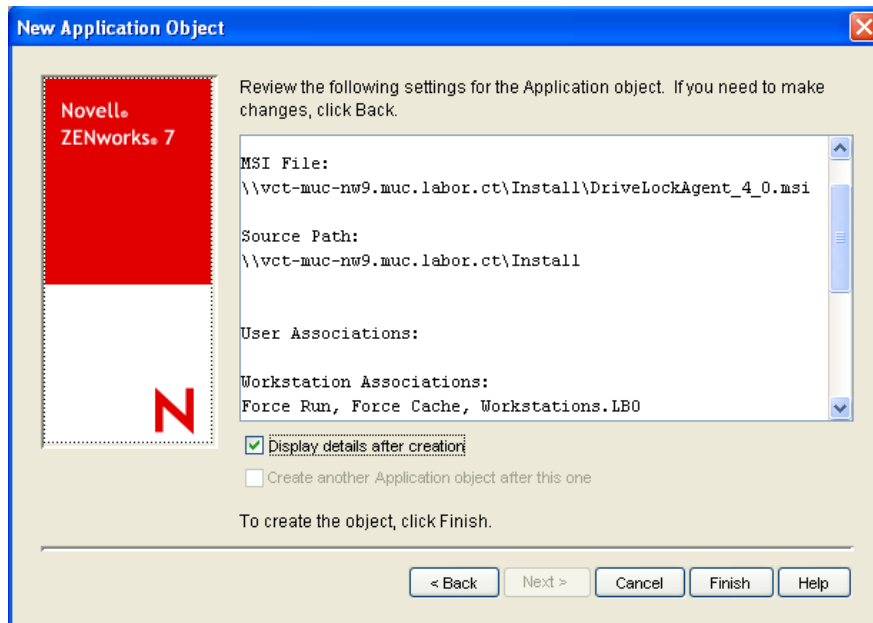
- e. The next step assigns the Application package to computer accounts. Select the container with the computer accounts in NDS and then select the option to associate the policy with workstations only.



- f. Under "Distribution Option", select the check boxes "Force run" and "Force Cache" and then clear the check box "App Launcher" as shown in the following screenshot:

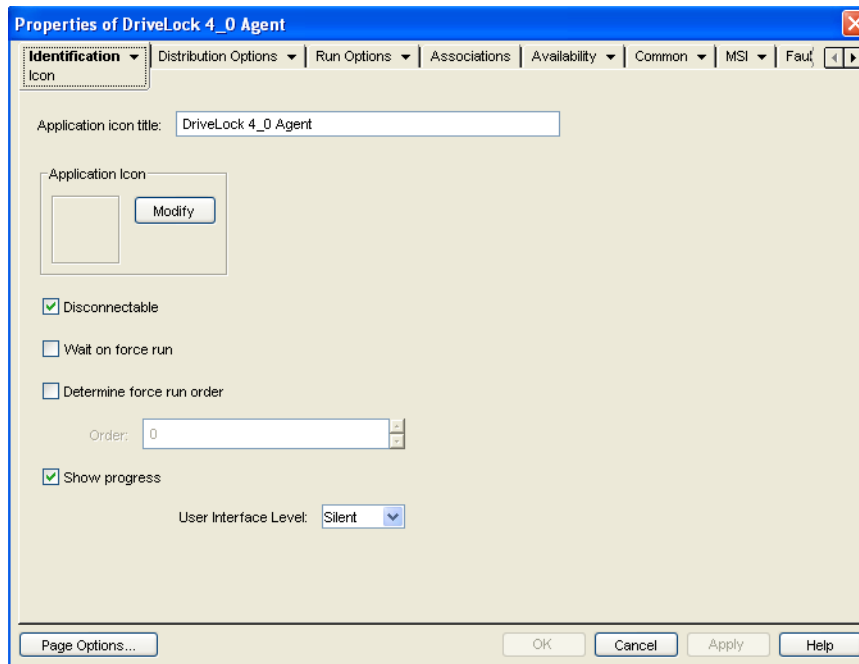


- g. Review the summary and then select the checkbox “*Display details after creation*” to configure additional settings.

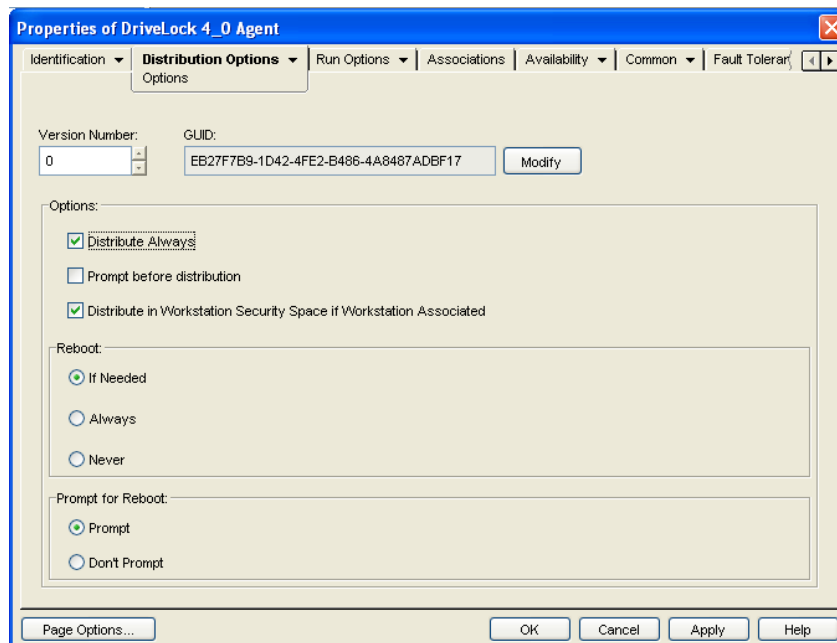


4. Customize the package properties

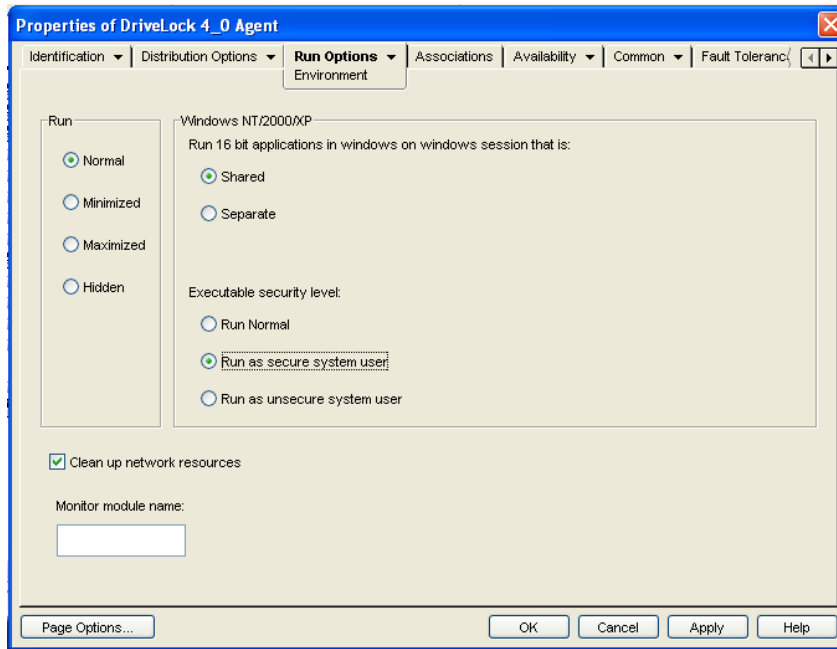
- a. On the “*Identification – Icon*” page, on the “*User Interface Level*” menu, click **Silent**.



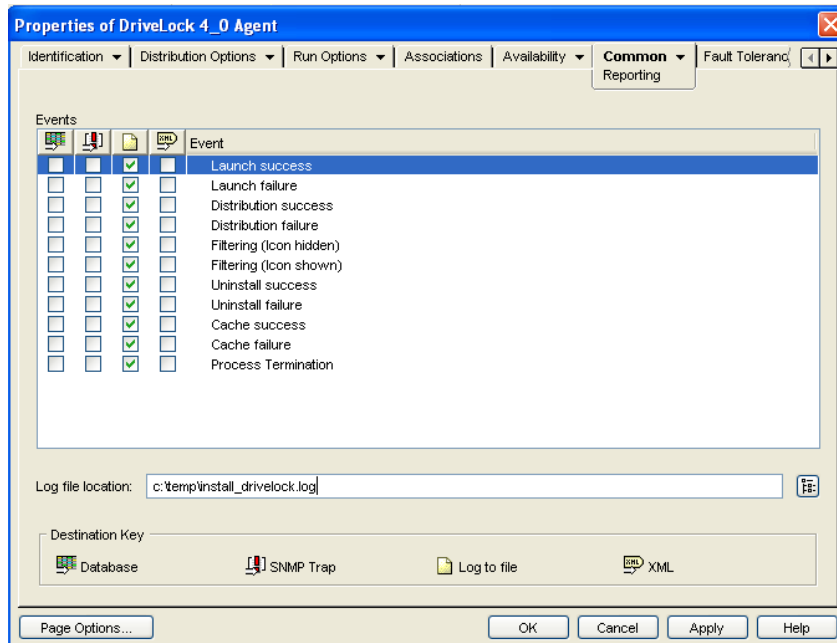
- b. On the “*Distribution Options*” page, select the “*Distribute always*” and “*Distribute in Workstation Security Space if Workstation Associated*” check boxes.



- c. In the “*Run Options – Environment*” dialog box, select “*Run as secure system user*”. This is required because the local system account installs the software package - not the user (you must select this setting if users don’t have local administrative rights on client computers).



- d. Optional logging can be activated to confirm that the package ran properly. To do this, open the “Common – Reporting” dialog as shown in the following screenshot.



- e. Click **OK** to confirm the settings, and then check client computers to confirm that the Agent is being installed successfully.

4.2 Upgrading Existing Agent Installations

To deploy a newer version of the DriveLock Agent to client computers, perform the following steps:

1. Copy the Agent installation file (an MSI file) from the DriveLock CD or from the DriveLock download site to a shared folder. Ensure that the computer accounts have Read permissions on the network share to be able to install the Agent.
2. Undo the assignment of the existing DriveLock package
 - a. Open the existing package.
 - b. Go to the “Associations” page and record the current settings.
 - c. Create a new Application package as described in the previous chapter of this document ([Deploy the DriveLock Agent Using Novell ZENworks](#))
 - d. Assign the new package to computers using the settings you recorded in Step 2b.
 - e. Once the new package is assigned it will upgrade the Agents. You don't need to uninstall the previous version first.

5 Using Novell Users and Groups in DriveLock

A DriveLock policy can include several types of rules that apply to specific users or groups. For example, you can use users and groups to define exceptions to company-wide rules for drive locking. With DriveLock 5.0 you can choose from users and groups that are defined in Novell NDS.

CenterTools highly recommends enabling Dynamic User Login. Otherwise all users log on as the same Windows user (Administrator) and everyone has administrative permissions. Refer to the Novell ZENworks documentation for how to enable and configure “Dynamic Local User”.



When Dynamic User Login is activated, a local windows user account is created during the Novell Login process. The name of the local user account is identical to the name of the NDS user account (for example, NDS user “John” logs in and a Windows user “John” is created and automatically logged on instead of the local “Administrator” account).

5.1 Select NDS Users or Groups

Requirements:

- Microsoft Windows 2000, XP, 2003 or Vista
- Installed Novell Client
- Permissions to open the Policy Package with the DriveLock Configuration (to edit the existing configuration)

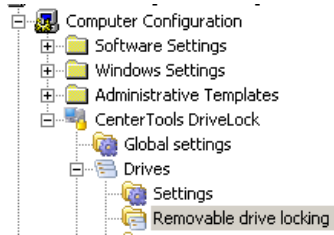
Procedures:

In DriveLock, users and groups can be selected in many places. The following steps are an example of selecting Novell NDS users and groups. The procedure for selecting users and groups in other configuration scenarios is identical to this example.

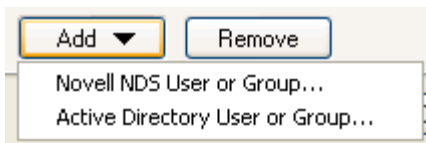
This example shows how to lock all USB removable drives (USB removable media, USB hard disks, etc.) by default, but to allow the DriveLock Administrator group to use USB drives.

1. Open your DriveLock configuration (explained in the previous chapter) “CenterTools DriveLock”
2. Go to “Drives”

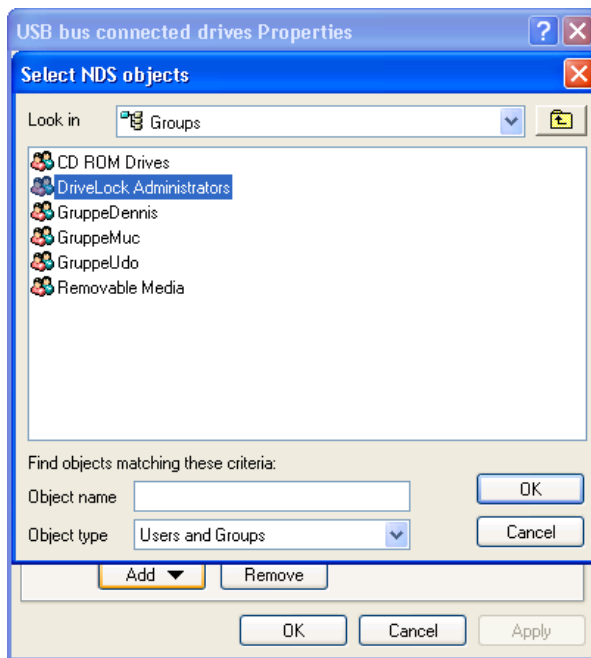
3. Go to “Removable drive locking”



4. In the right pane double click on **USB Bus connected drives** to open the settings page for USB drives
5. If the Novell Client is installed on the same machine where the DriveLock configuration is edited, advanced **Add** Button with the Drop-Down menu is displayed:



6. From the list, select **Novell NDS User or Group** to open a window where you can select a user or group. In this example the group “*DriveLock Administrators*” is selected.









7. Confirm the selection by clicking **OK** twice
8. Save your configuration. Now USB drives are locked for everyone except the members of the NDS group “*DriveLock Administrators*”.

Follow the same procedure, when configuring user-based rules anywhere in the DriveLock Management Console.

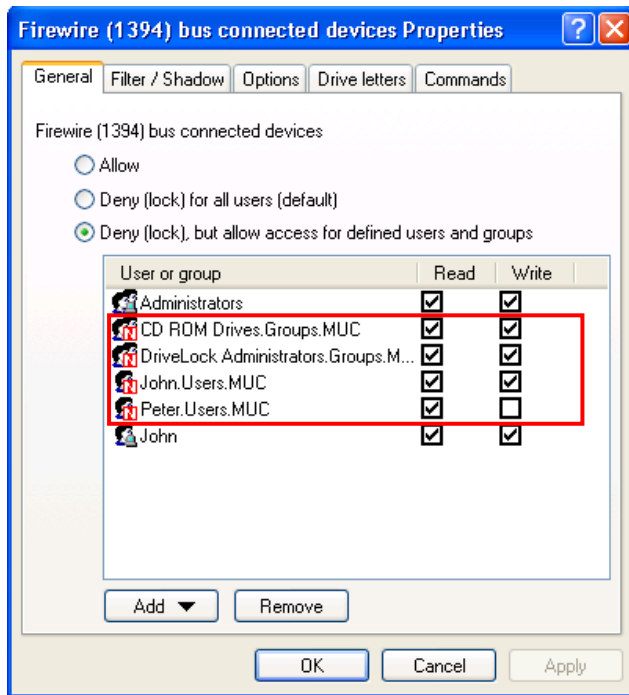
5.2 Mixed mode

It is possible to select users or groups from the local machines user account database, from Microsoft Active Directory, from Novell NDS or a combination of users from multiple sources.

Each entry that is added to the list is identified by an icon. The following table shows which directory the user or group icon corresponds to:

Icon	Indicates
	Active Directory user
	Active Directory group
	Local machine user
	Local machine group
	NDS user
	NDS group

The highlighted area of the following figure shows how icons are displayed in the DriveLock Management Console.



Combining permissions for users and groups that a user belongs to can result in unexpected behaviour, For example, user “John” is member of the group “USB drive users”. John has read/write permissions on “USB bus connected drives” but the group “USB drive users” has only read permissions. The result can be that John finally only has read permissions.

5.3 Offline usage

An additional step is required to ensure correct policy enforcement when a computer has no network connection to the NDS directory. In this case the logged-on Novell user cannot be verified and DriveLock can only use local user and groups used. As a result, DriveLock ignores rule settings that are based on NDS users and groups when offline.

Example: CD-drives are locked except for the NDS group “CD-ROM users”. Members of this group can access the CD-drive when they’re online. After the laptop goes offline “CD-ROM users” can no longer access the CD drive (there’s no NDS server available to check if user / group has permissions).

To work around this issue, use local users or groups in a DriveLock policy. When doing this, ensure that Dynamic User Login is enabled so that Novell users log into Windows with their user name instead of Administrator. Refer to the Novell ZENworks documentation for how to enable and configure “Dynamic Local User”.

6 Configuration Traffic

To help you assess the impact on your network of applying group policy settings from the NDS Server or via HTTP or FTP, the following table lists the approximate size of several rules and other policy settings:

Settings		Used space (KB)
General	General settings (Includes all general settings like event handling, encryption etc.)	0.5
Drives	Default settings (Includes general settings such as locking of drive types USB, Firewire, CD/DVD etc.)	1.1
	Exceptions (Whitelist rules)	0.4 (per exception)
Devices	Default settings (Includes general settings such as state of device classes)	2.7
	Templates	22.1 (per template)
	Whitelist rules (no template-generated rules)	0.4 (per rule)

As the table above shows the space required for a group policy object that contains DriveLock settings heavily depends on the number and types of settings configured. A standard DriveLock group policy object uses approximately 5 KB (no templates defined). DriveLock settings are relatively static (usually policies are not changed frequently). As a result, after initial replication and adoption by client computers has been completed, network traffic due to replication drops sharply.