

The logo for CenterTools features a red swoosh that starts from the left edge of the page and curves upwards and to the right, ending under the word "Tools".

CenterTools

DriveLock Quick Start Guide

Be secure in less than 4 hours

CenterTools Software GmbH

© 2012

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.

© 2012 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

INTRODUCTION.....	4
SYSTEM REQUIREMENTS	4
INSTALLING DRIVELOCK COMPONENTS	5
INSTALLING THE DRIVELOCK MANAGEMENT CONSOLE	5
INSTALLING THE DRIVELOCK ENTERPRISE SERVICE	7
INSTALLING THE DRIVELOCK CONTROL CENTER	16
CONFIGURING THE DRIVELOCK COMPONENTS	18
SETUP THE DRIVELOCK CONTROL CENTER	18
CREATING A GROUP POLICY OBJECT	20
CONFIGURING POLICY SETTINGS	21
INSTALLING THE DRIVELOCK AGENT	31
SUMMARY	35

Introduction

As your IT infrastructure is getting increasingly complex, the task of providing comprehensive network security is also becoming more involved. However, providing comprehensive protection doesn't need to be difficult or time-consuming if you are using intelligent tools to accomplish the task. DriveLock can help make data security easy. It only takes a few simple steps to install and configure DriveLock 6 to help eliminate the dangers to your sensitive data posed by the uncontrolled use of USB ports and other open ports on client computers.

This document guides you through the process of installing and configuring DriveLock to control access to removable drives. It also includes the steps that are required to centrally deploy the DriveLock Agent to all client computers where device access needs to be enforced and to centrally monitor user access to removable drives. The entire process, including the configuration of prerequisites, typically takes well under 4 hours.

System Requirements

The following are required to perform the steps described in this guide. For more detailed information, refer to the DriveLock documentation.

Administrative Workstation:

The DriveLock Management Console must be installed on an administrative workstation. Generally, this is the computer from where you perform most day-to-day management tasks. The computer should be running any version of Windows XP, Windows Vista or Windows 7, except Home editions. Because you will configure Group Policy settings, the Microsoft Group Policy Management Console (GPMC) must be installed on this computer. You can also install the DriveLock Management Console on a computer running Windows Server, but it is recommended to not use a server to perform management tasks. Unless you are installing DriveLock for a 30-day evaluation, the administrative workstation should access to the Internet for activating the license.

DriveLock Enterprise Server:

The optional DriveLock Enterprise Service consolidates client events for central monitoring. It needs to be installed on a computer running Windows Server 2003 or newer. Installation on a domain controller is not supported.

The DriveLock Enterprise Service also needs to create a Microsoft SQL Server database. You can use an existing instance of SQL Server or install a dedicated instance on the DriveLock Enterprise Server or a different server. You can use any edition of Microsoft SQL Server 2005 or 2008, including the free Express editions.

The DriveLock Enterprise Service logs on using a domain user account. You need to create this account before you start the installation. It is recommended that you configure the account's password to never expire. No further configuration is required for this account.

To enable distribution of the DriveLock Agent to client computers using Group Policy, you will need to create a shared folder on the DriveLock Enterprise Server or any other server. Both file and share permissions need to be configured to allow Read access for the Everyone or Authenticated Users groups.

If the Windows Firewall is enabled on the server you will also need to configure firewall exceptions to allow clients computers to send event information and for administrators to create reports. For more information about the required firewall exceptions, refer to the DriveLock documentation.

Software:

You will need the following DriveLock components. The easiest way to obtain them is to download the DriveLock 7.1 ISO image and burn a CD from it. Alternatively, you can download each component separately:

- DriveLock Management Console
- DriveLock Enterprise Service
- DriveLock Control Center
- DriveLock Agent

Unless you are installing DriveLock for a 30-day evaluation, you will also need access to the DriveLock license file that was provided to you when you purchased DriveLock.

Installing DriveLock Components

Before you can configure device control rules and monitoring you need to install the administration console. For central monitoring you should also install the optional DriveLock Enterprise Service and DriveLock Control Center.

Depending on your operating system use the 32Bit or the 64Bit installation packages.

In case the User Account Control (UAC) is active accept all Windows notification messages.

Alternatively you start a command line via „Run as administrator“ and use the `msiexec` commands e.g. `msiexec /I DriveLock_MMC.msi`

Installing the DriveLock Management Console

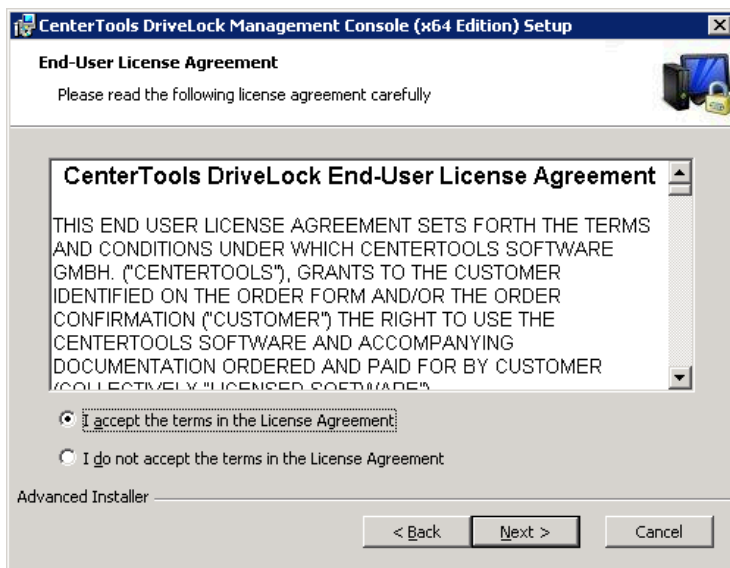
You use the DriveLock Management Console to configure all DriveLock Settings and perform most administration tasks. You need to install the management console on the administrative workstation.

Estimated time required: **10 minutes**.

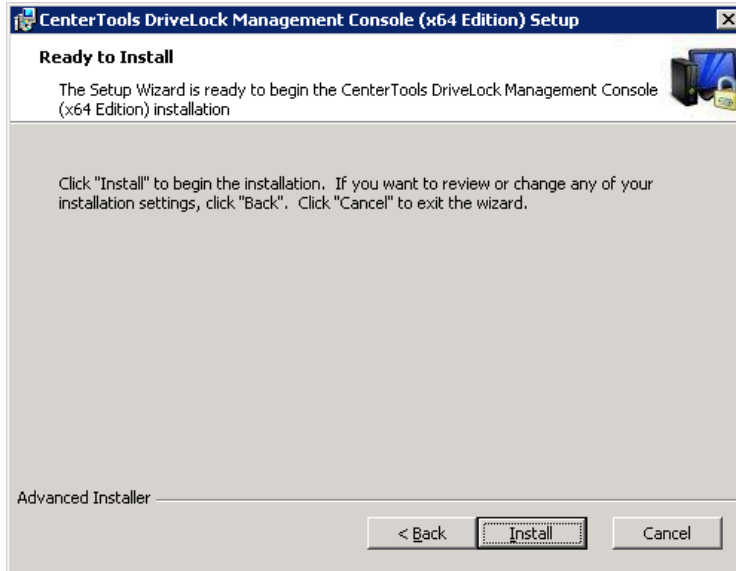
To start the installation, run *Setup.exe*.



Click **Next**.



Accept the license terms and click **Next**.



Click **Install** to start the installation.



After successful installation click **Finish** to close the installation wizard.

Installing the DriveLock Enterprise Service

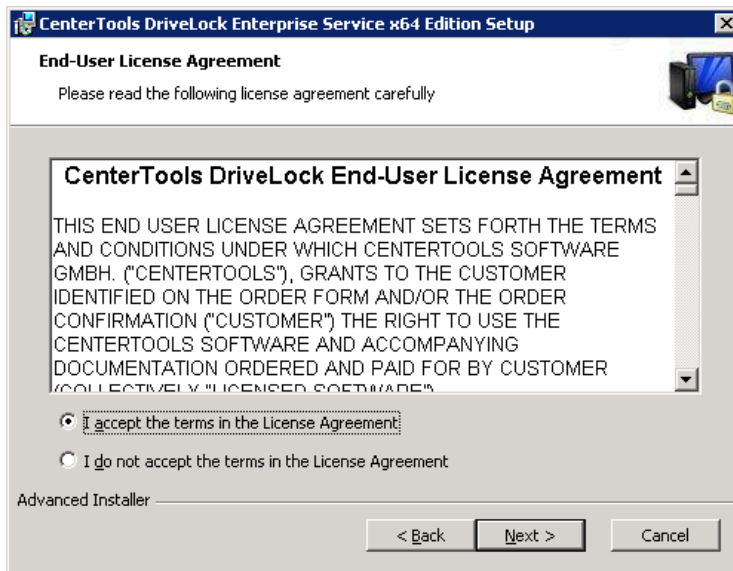
The DriveLock Enterprise Service (DES) receives event information from all DriveLock clients and stores them in a central database. It can also store recovery data for encryption and provides access to the data for reporting and analysis via the DriveLock Control Center (DCC) console. For detailed information about the DES and DCC, refer to the DriveLock documentation.

Estimated time required: **25 minutes**

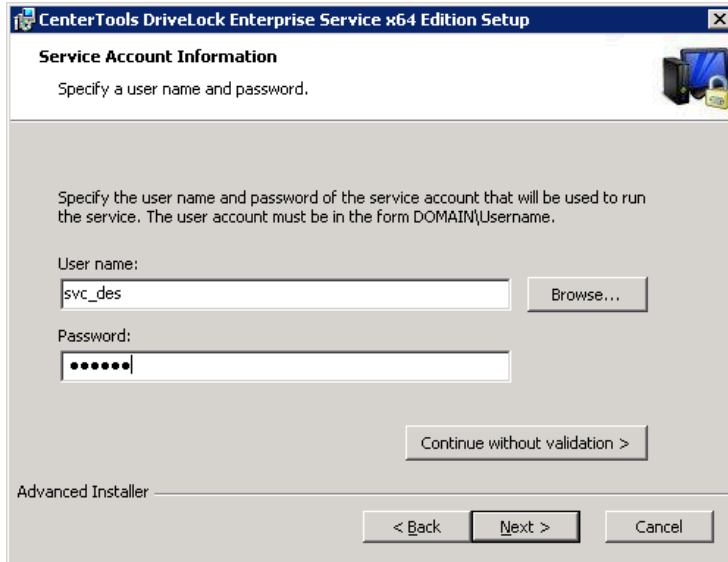
Start the DriveLock Enterprise Service setup on the server computer.



Click **Next** to start installation.



Accept the license terms and click **Next**.

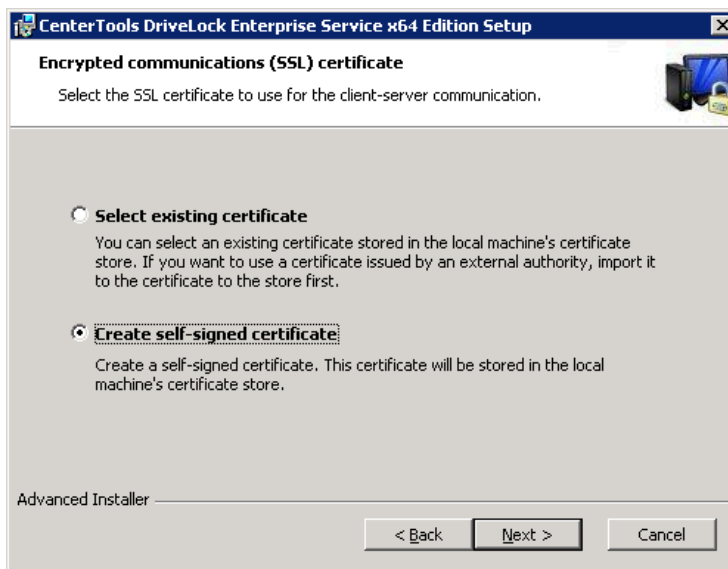


Type the user name and password of the service account used to run the DriveLock Enterprise Service or click **Browse** to select an existing account.

Click **Next** to continue installation.



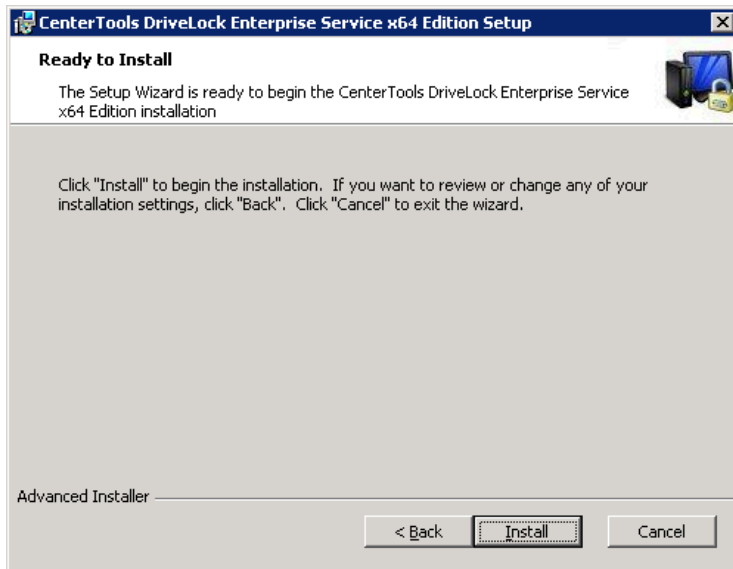
Use the *Continue without validation* checkbox only if the user account can't be verified but you are certain that the account exists and that you want to proceed with the installation.



A certificate is required for the encrypted client-server communication.

Click *Select existing certificate* if the SSL certificate you want to use is already in the computer's certificate store. Click **Next**, select the certificate from the list, and then click **OK** to confirm.

To have DriveLock create a certificate, click *Create self-signed certificate* and then click **Next**.

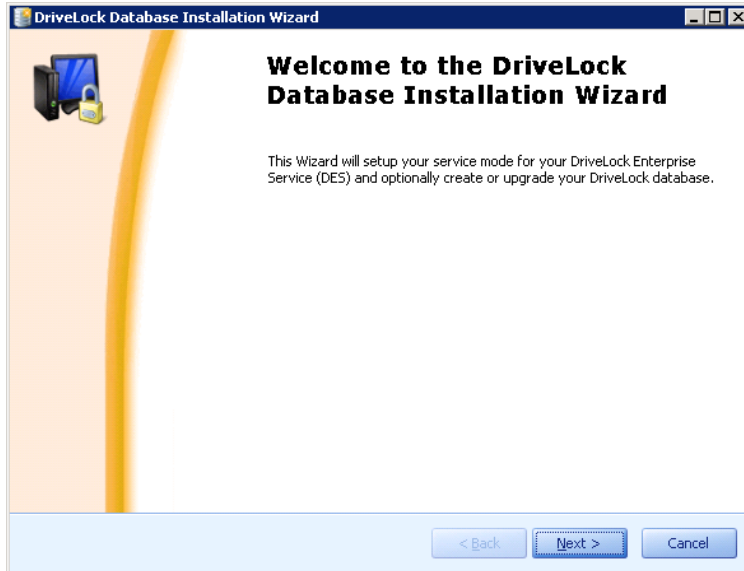


Click **Install** to start DriveLock Enterprise Service installation.



When the installation has completed, click **Finish** to close the wizard.

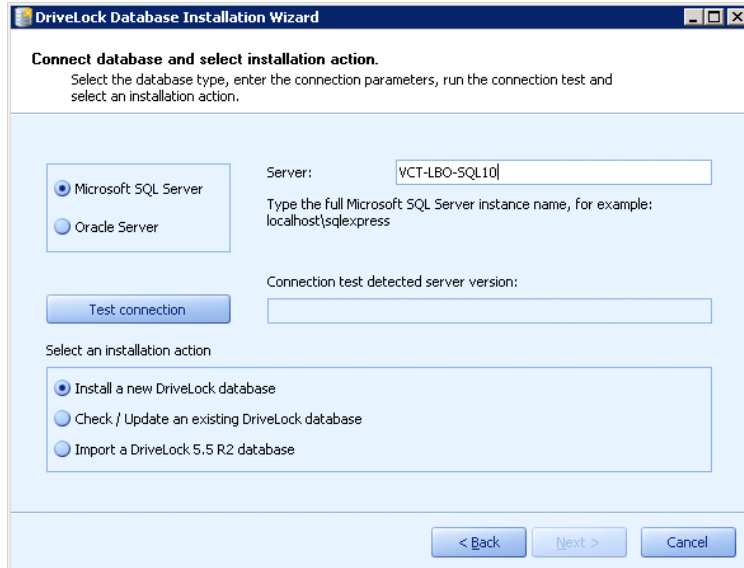
When the installation is complete, the Database Installation Wizard starts. This wizard guides you through the process of installing, configuring or updating the DriveLock Enterprise Service database. You can also use the wizard to change the DriveLock Enterprise Service mode for branch offices deployments.



Click **Next** to start the wizard.



Choose "Central DriveLock Enterprise Service" and click **Next**.



The screenshot shows the 'DriveLock Database Installation Wizard' window. The title bar reads 'DriveLock Database Installation Wizard'. The main heading is 'Connect database and select installation action.' Below this, there is a sub-heading: 'Select the database type, enter the connection parameters, run the connection test and select an installation action.'

On the left, there are two radio buttons: 'Microsoft SQL Server' (which is selected) and 'Oracle Server'. To the right of these buttons is a 'Server:' label and a text input field containing 'VCT-LBO-SQL10'. Below this is a smaller text input field with the placeholder text 'Type the full Microsoft SQL Server instance name, for example: localhost\sqlexpress'. Below that is another label 'Connection test detected server version:' followed by an empty text input field.

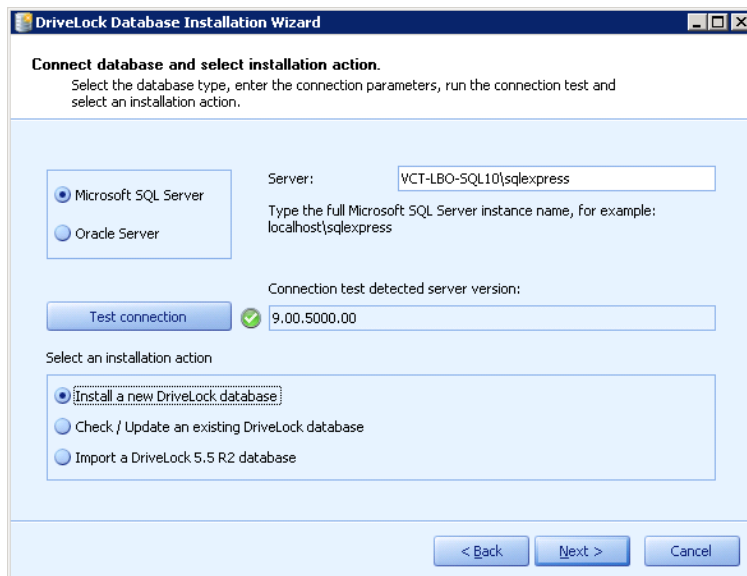
Below the server information is a 'Test connection' button. Underneath that is the heading 'Select an installation action' followed by three radio buttons: 'Install a new DriveLock database' (selected), 'Check / Update an existing DriveLock database', and 'Import a DriveLock 5.5 R2 database'.

At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

Fill in our SQL servername.

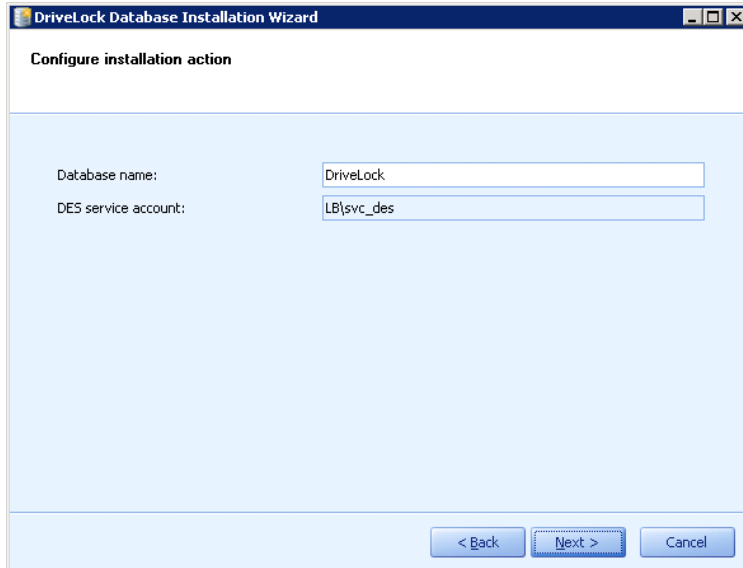


In case you use a SQL-Express server you have to type the correct instance name. e.g. SQLEXPRESS as you can see in our example below.

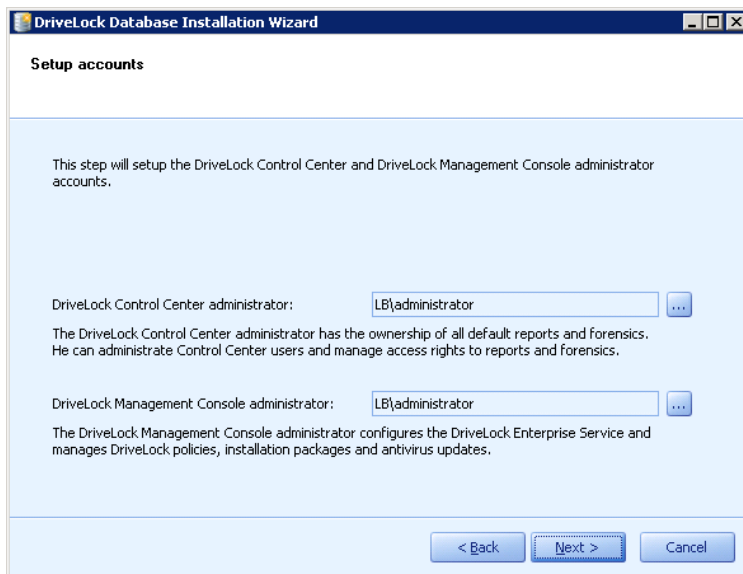


This screenshot is similar to the previous one, but with more information filled in. The 'Server:' field now contains 'VCT-LBO-SQL10\sqlexpress'. The 'Connection test detected server version:' field now contains '9.00.5000.00' and has a green checkmark icon to its left. The 'Test connection' button is now disabled. The 'Install a new DriveLock database' radio button is still selected.

Select the database server type, Microsoft SQL Server. Type the name of the database server and, if required, the name of the database instance. To confirm that DES can connect to the server, click **Test Connection**. Finally select whether to create a new DriveLock database and then click **Next**.



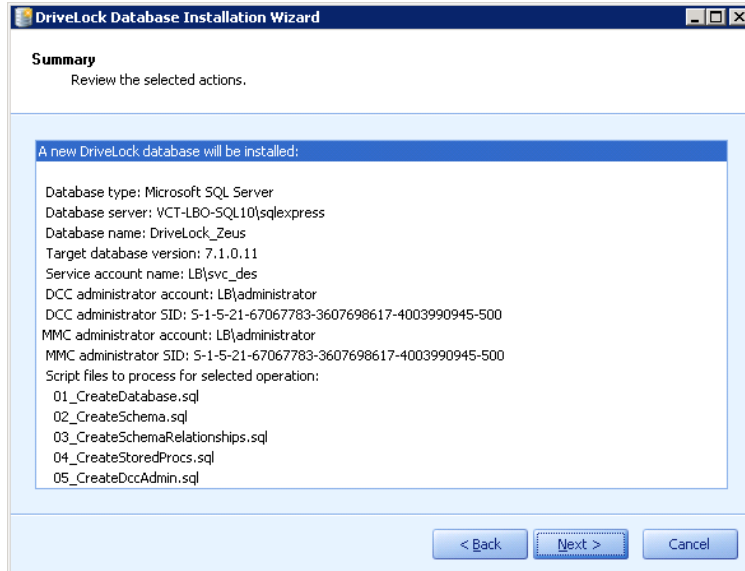
Type the database name click **Next**.



Next select a group or user and corresponding security identifier (SID) that will initially be assigned permissions to use the DriveLock Control Center. You can change this account or add additional users and groups in the Control Center after the database installation has completed.

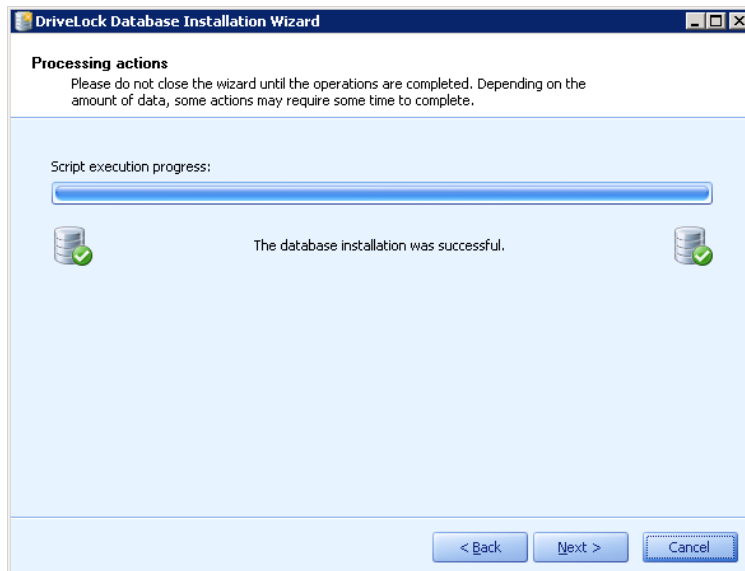
The service account that the DriveLock Enterprise Service use to connect to the database was specified during the installation.

Click **Next** to continue.



Review the summary of the installation settings and then click **Next** to start the installation.

Depending on the size of the database, the installation may take several minutes.



When the installation is complete, click **Next**.



To complete the installation, click **Finish**.

Installing the DriveLock Control Center

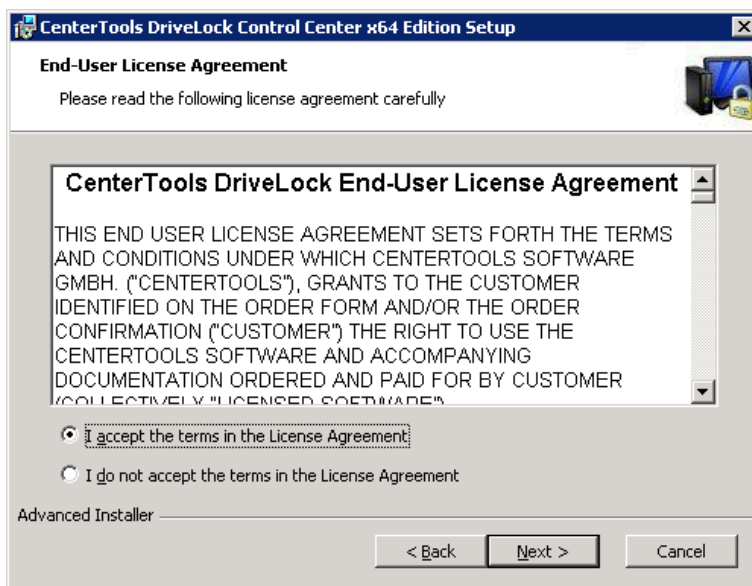
The DriveLock Control Center is a console that provides access to the DriveLock Enterprise Service for monitoring and reporting. It is recommended that you install the DriveLock Control Center on the administrative workstation.

Estimated time required: **10 minutes**

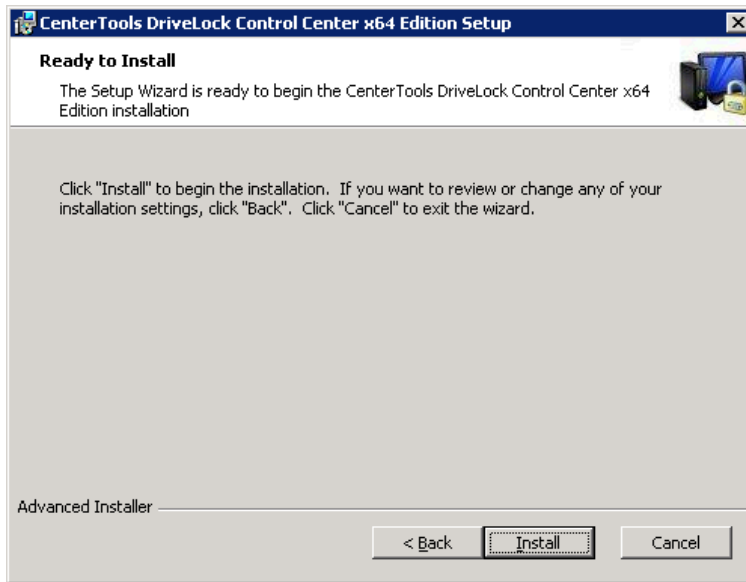
Start the DriveLock Control Center setup on the administrative workstation.



Click **Next** to start installation wizard.



Accept the license terms and click **Next**.



To start the installation click **Install**.



When the installation has completed, click **Finish** to close the wizard.

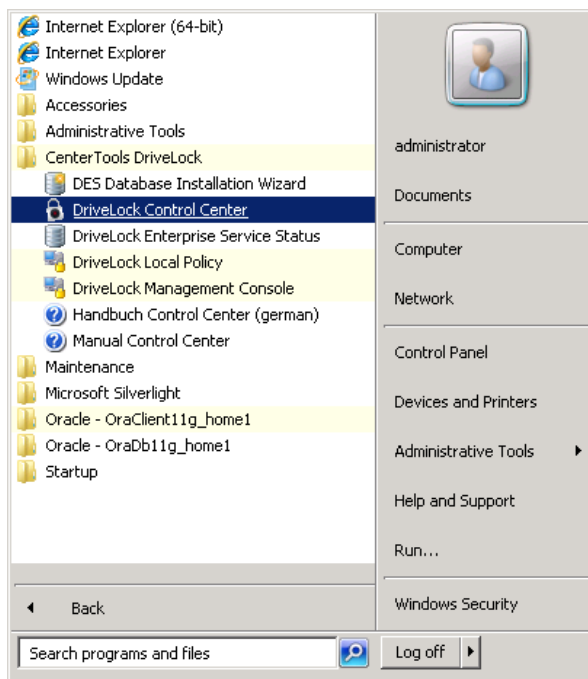
Configuring the DriveLock Components

Before you can monitor client events and create reports you need to configure the DriveLock Control Center to use the correct DriveLock Enterprise Service.

Setup the DriveLock Control Center

Estimated time required: **10 minutes**

Start the DriveLock Control Center.

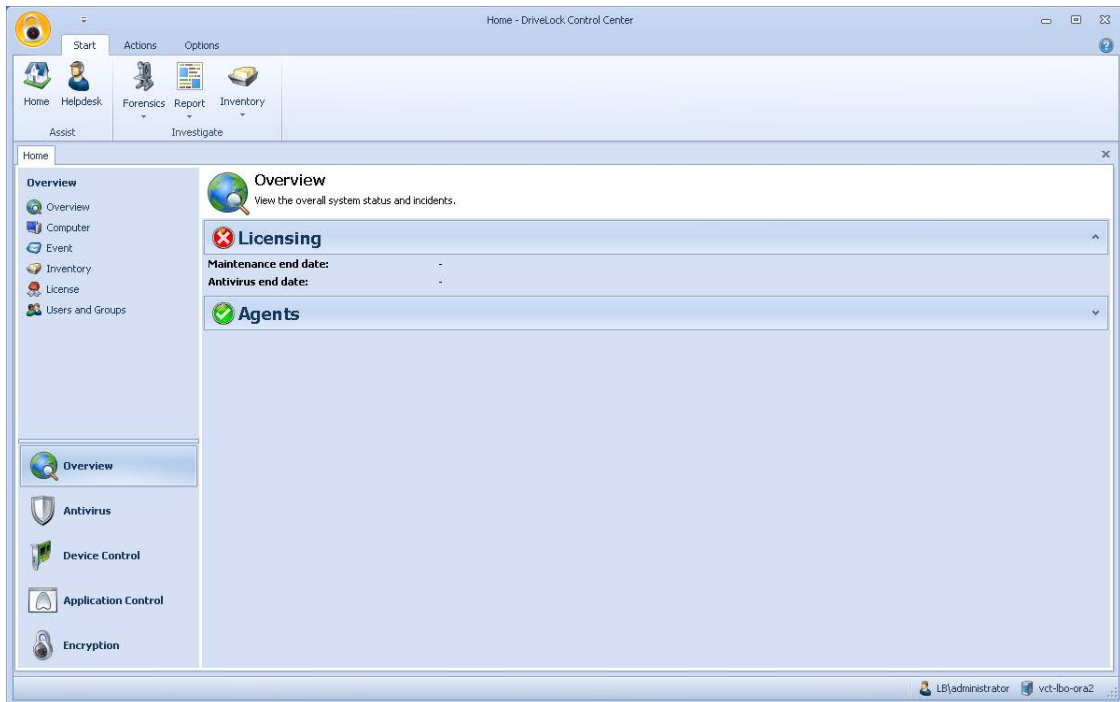


When you start the DriveLock Control Center for the first time, you are prompted to select a DriveLock Enterprise Service.



Type the DNS or NetBIOS name of the DriveLock Enterprise Service, alternatively select a DriveLock Enterprise Service from the poll down menu, leave all other settings unchanged, and then click **OK**.

The DriveLock Control Center starts. Because no client events have connected to the DriveLock Enterprise Service yet, no events are displayed.



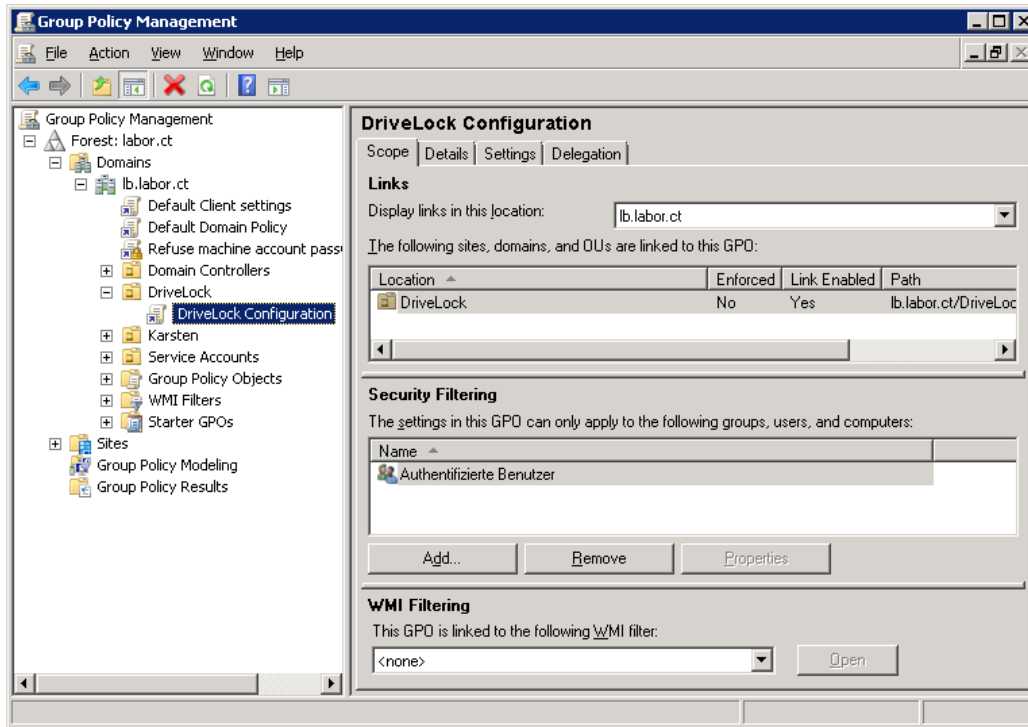
Creating a Group Policy Object

Once all administration and monitoring components are in place you can configure the policy settings that will be applied on client computers.

To centrally configure all DriveLock settings in your network you need to create a Group Policy Object (GPO) in Active Directory. You will configure all client settings in this GPO.

Estimated time required: **10 minutes**

Start the Microsoft Group Policy Management Console (GPMC).



The GPO must apply to client computer accounts that will be protected by DriveLock. If all these client computers are already in a single Organizational Unit (OU), you can link the GPO to this OU. Otherwise, you should re-organize your OU structure to consolidate client computer accounts or link the GPO to the root of your domain.

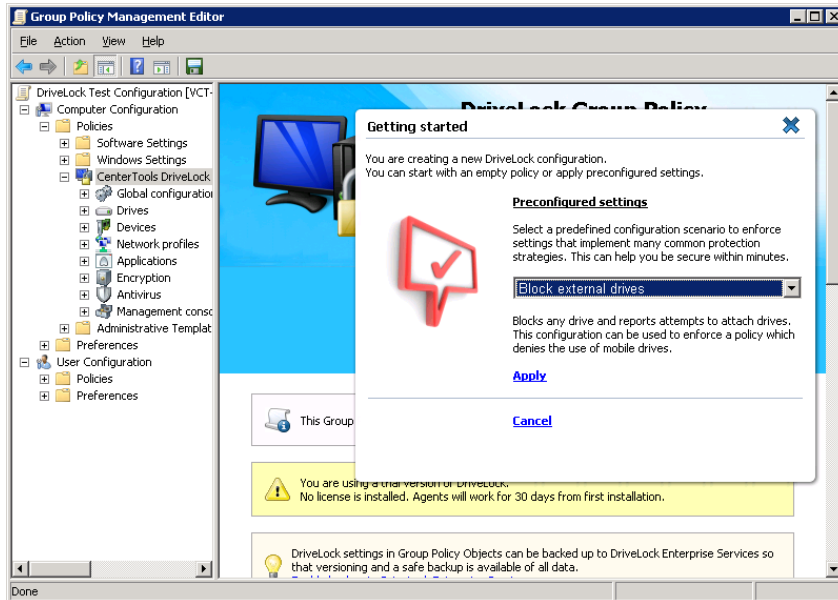
Right-click the OU that the GPO will apply to and then click **Create a GPO in this domain, and Link it here**. Provide a name for the GPO and then click **OK**.

Configuring Policy Settings

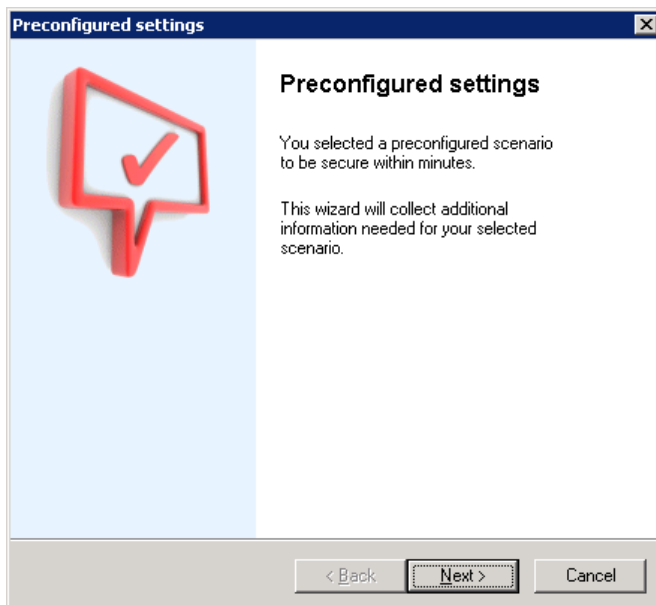
After you have created the GPO you can configure DriveLock settings in it. To do this, the DriveLock Management Console must be installed on the computer where you edit the GPO.

Estimated time required: **60 minutes**.

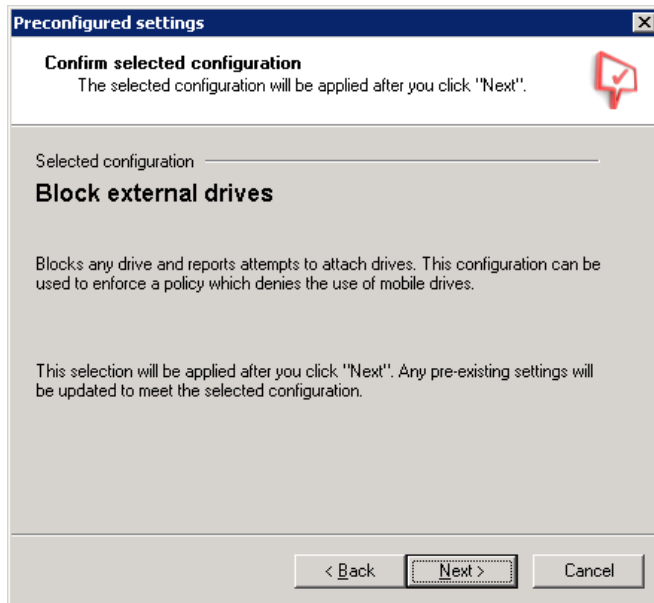
Right-click the GPO you created and then click **Edit**. In the Group Policy Management Editor, expand **Computer Configuration** and then click **CenterTools DriveLock**.



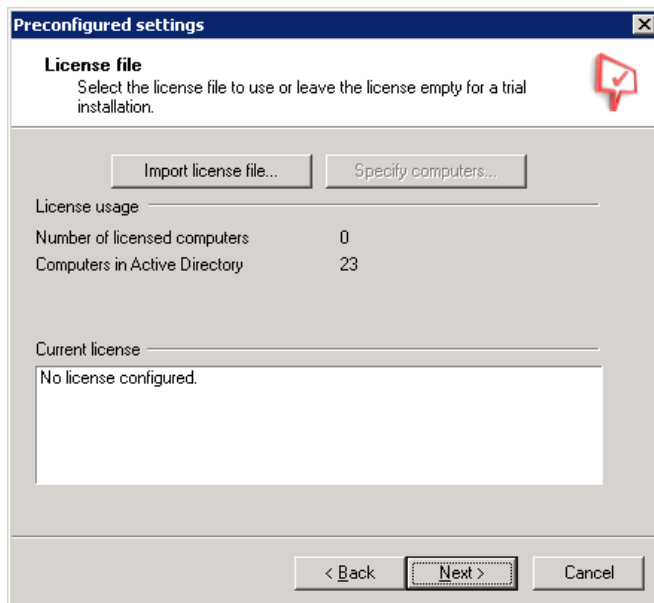
In the Getting Started dialog box, select “Block external drives” and click **Apply**.



You can now start to configure client settings.



In this example we configure basic settings to block any drive and reports attempts to attach drives.

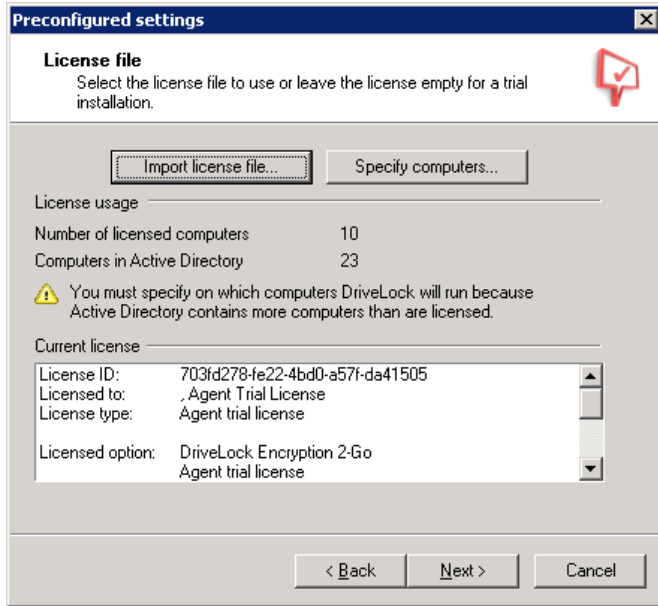


Please import your license file with "Import license file" button.

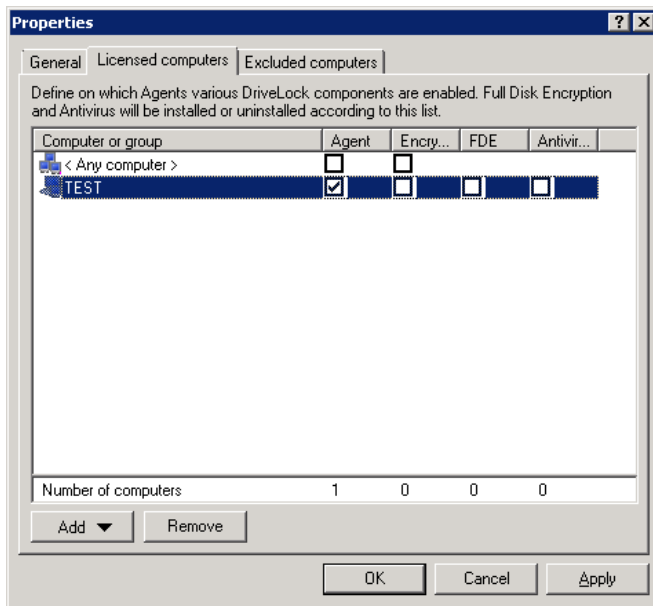


The DriveLock download package includes a trial Agent license that is valid for up to 10 Agents. You can find this license file *AgentTrial.lic* in the default installation folder "C:\Program Files\CenterTools\DriveLock\Tools". DriveLock Full Disk Encryption (FDE) is not included in this trial license.

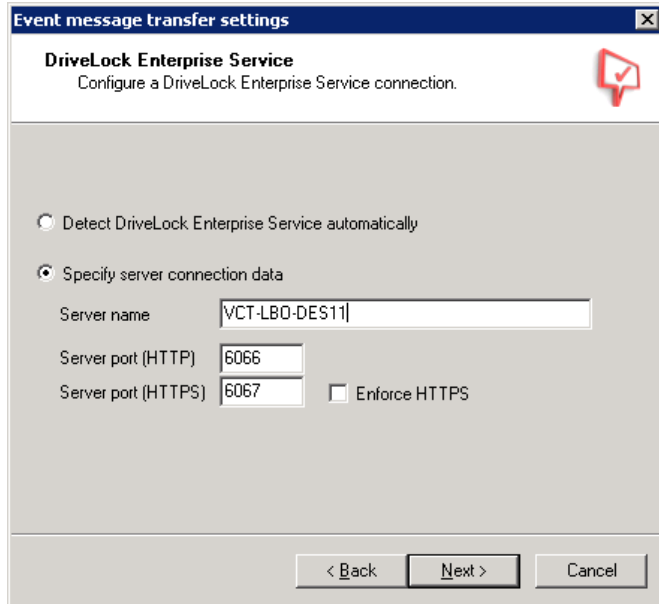
Click Import license file, and then follow the instructions to select your DriveLock license file and activate the license.



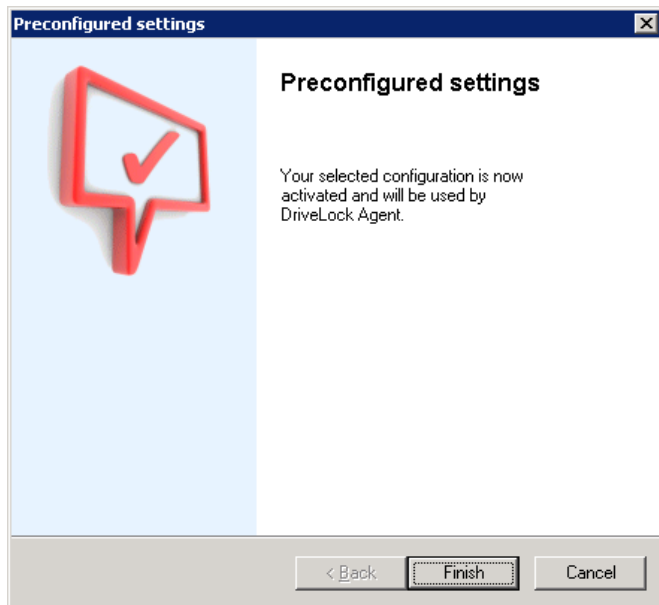
In case there are more computers in your Active Directory listed as in the trial license licensed, then click on **Specify computers**.



and configure at least one PC.

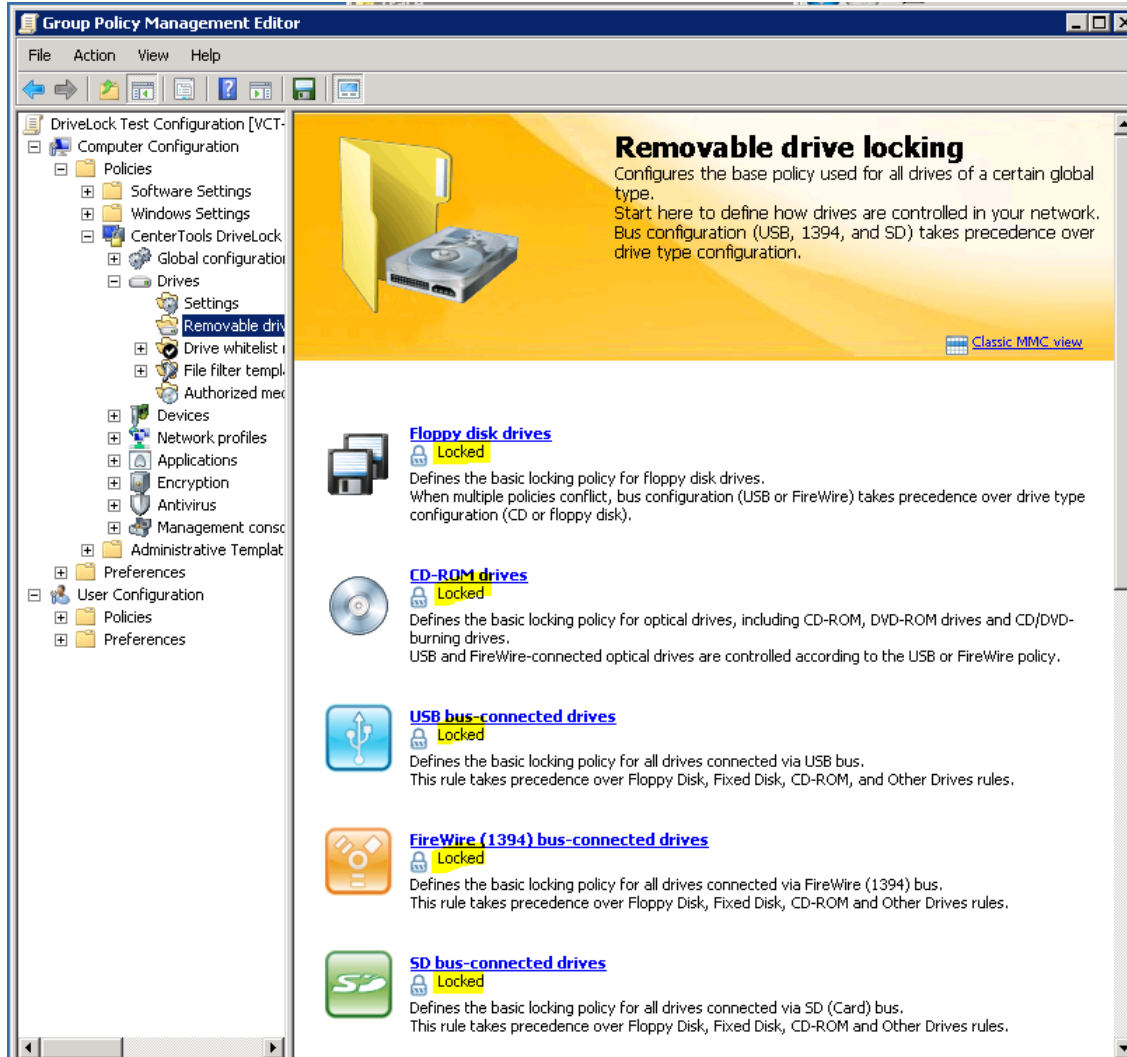


Final check “*Detect DriveLock Enterprise Service automatically*” and click **Next**. Optional you can edit the DES settings manually. In our scenario you have to edit the local server name.



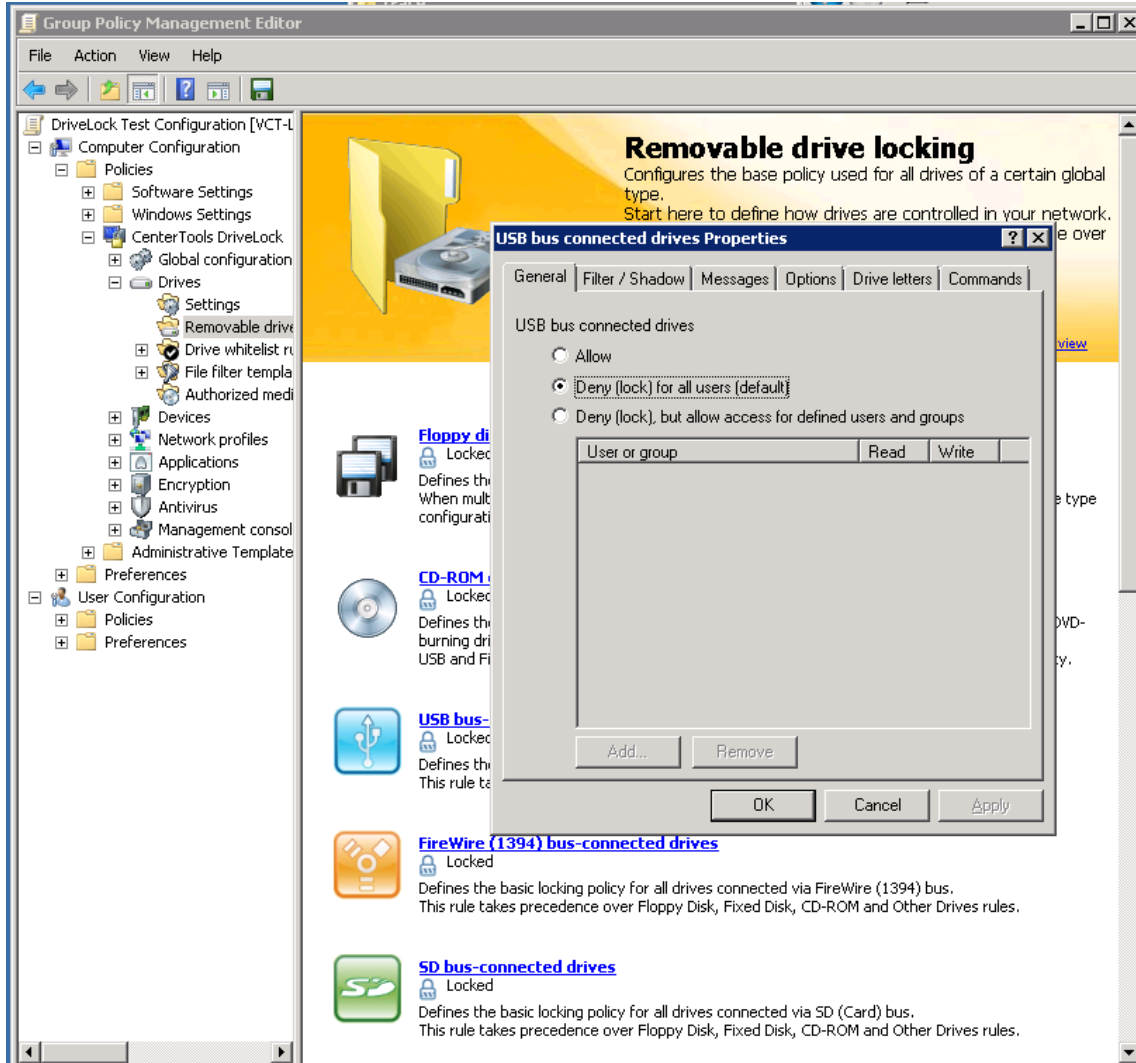
Now the basic settings are configured, click **Finish** to close the wizard.

To validate the DriveLock settings open the MMC node Drives – Removable drive locking.

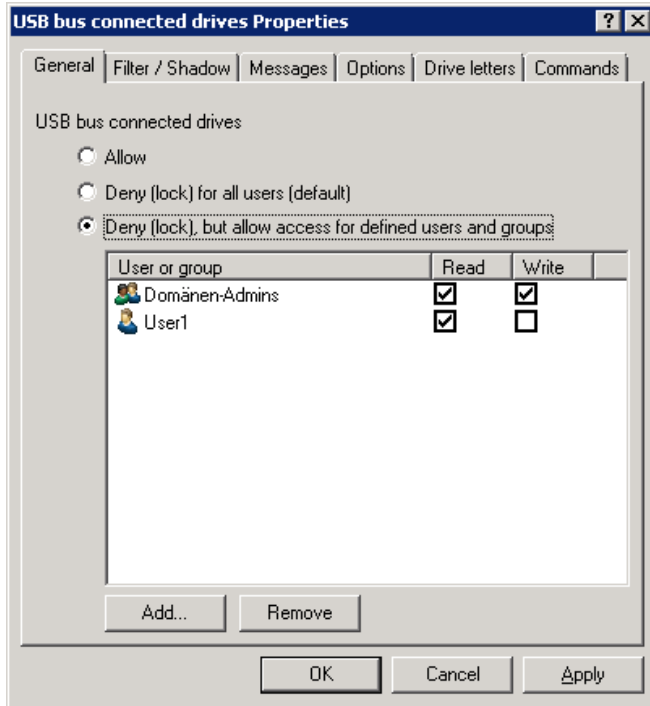


Based on the lock symbol you can identify that the basic setting block all access to removable drives, except fixed hard disks.

To change the settings for a drive type, click the drive category, such as USB drives.

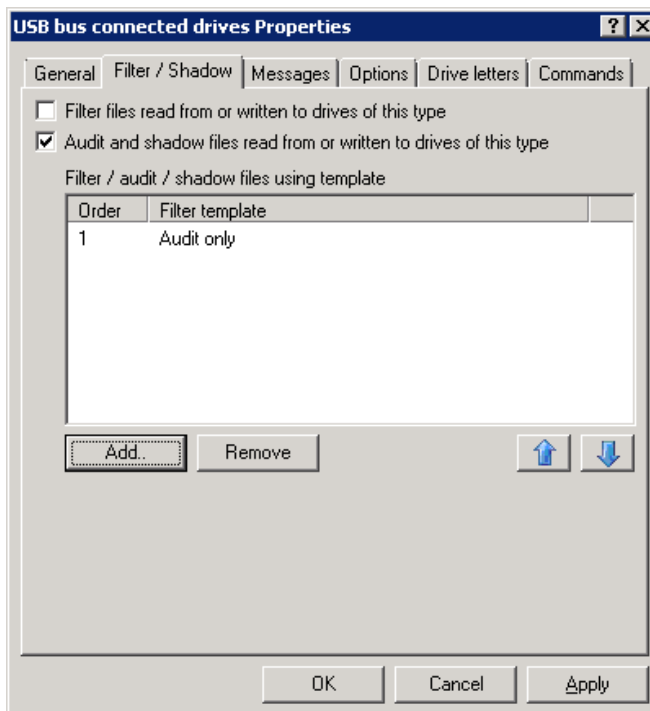


A dialog box appears that lets you configure access settings. For example, to allow write access for USB-connected drives for administrators only while allowing only read access for User1, configure the settings in the following graphic.

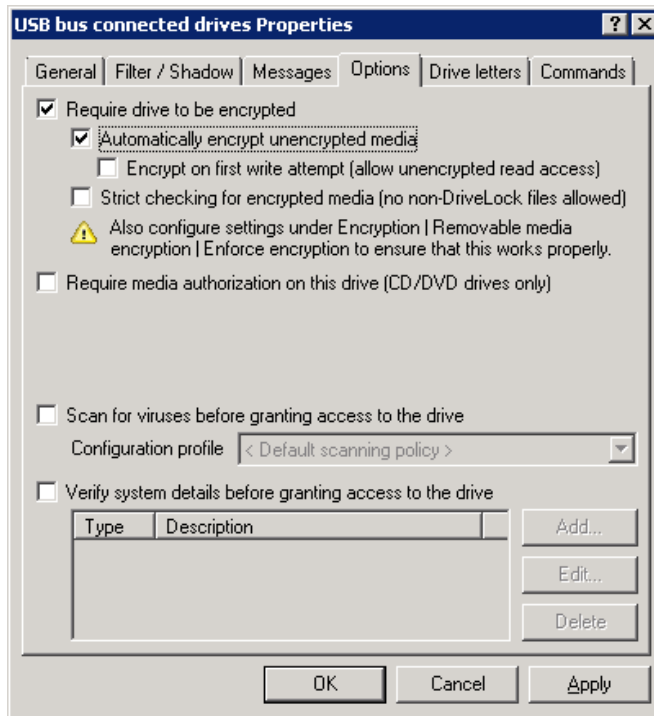


Next click on the tab “Filter / Shadow”. Now you can activate the auditing of file that are read from or written to USB-connected drives.

To do this mark “Audit and shadow files read from or written to drives of this type” and select via “Add” button the template “Audit only”.

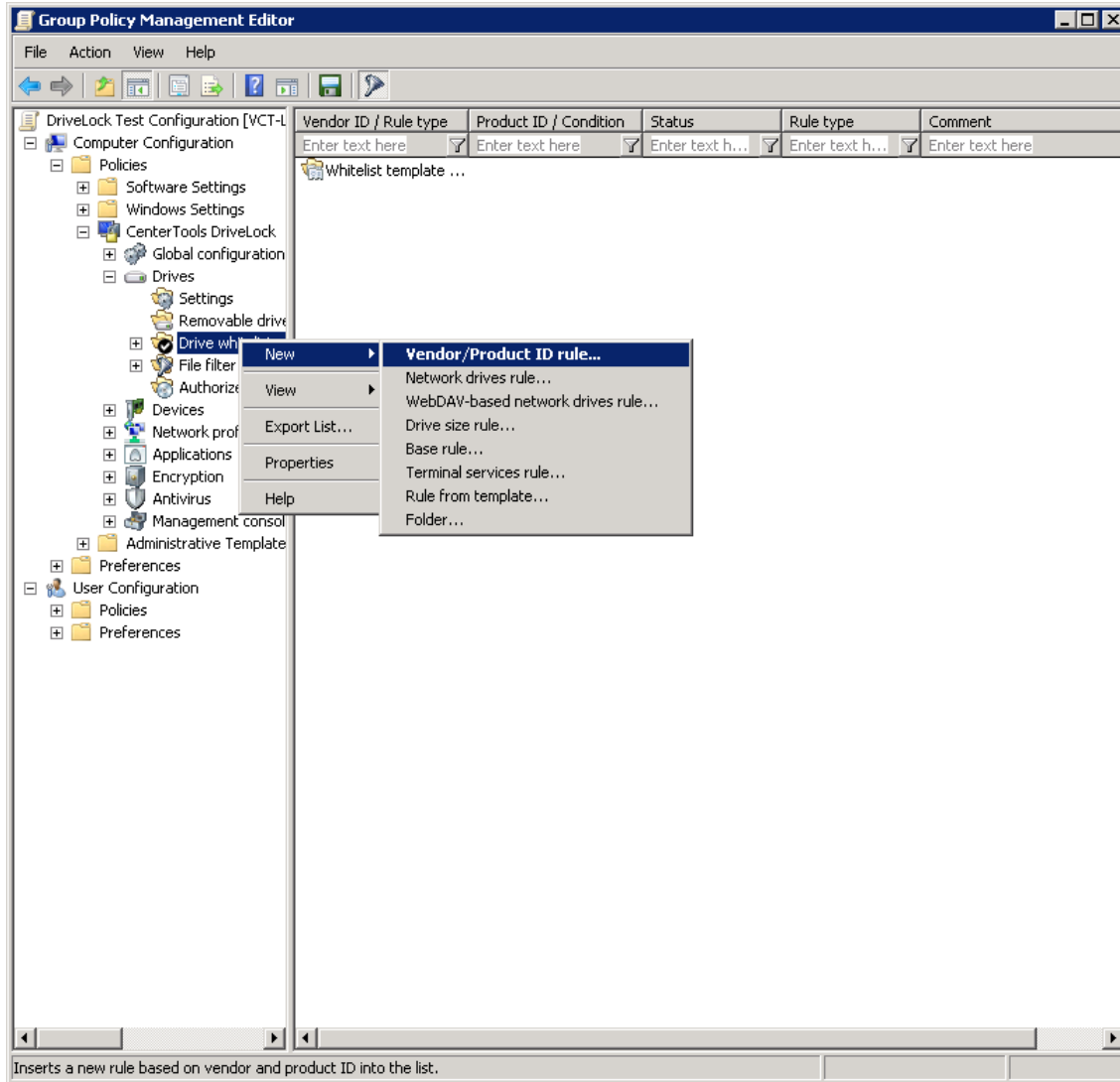


If you want to ensure that users can only access drives that have been encrypted by DriveLock, select the *Option* and mark “*Require drive to be encrypted*” and “*Automatically encrypt unencrypted media*”.

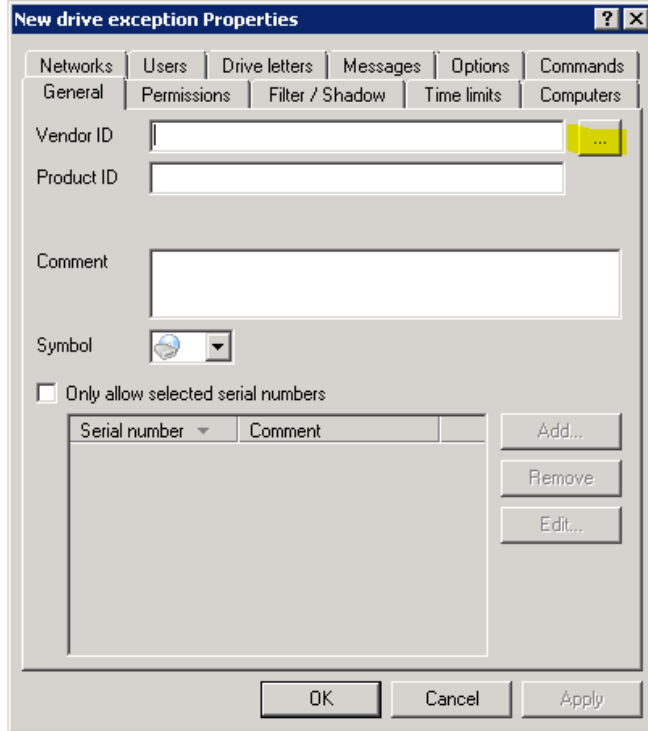


To configure settings for additional drive types, repeat the previous steps for each of them.

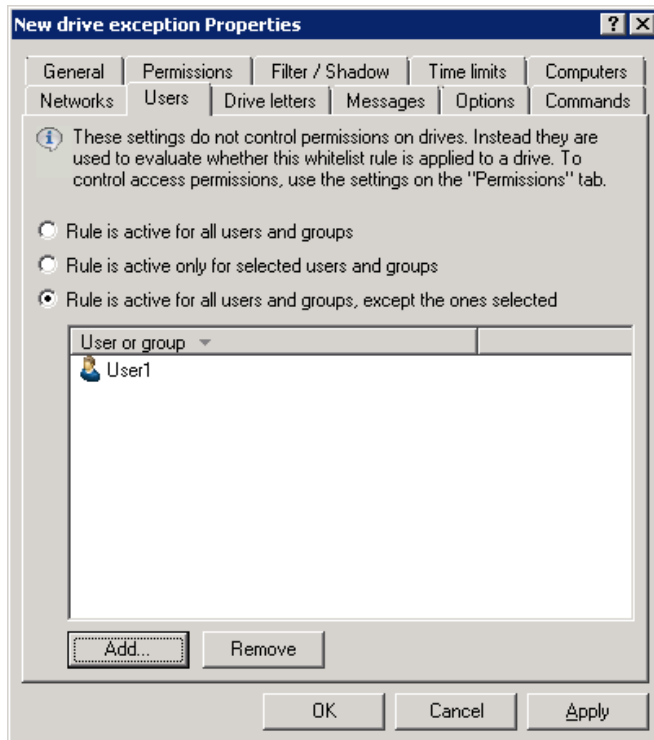
To create exceptions to the policy for a drive type, you can configure whitelist rules. For example, you can use whitelist rules to allow users to access only authorized removable media. To create a new drive whitelist rule, right click **Drive whitelist rule – New – Vendor/Product ID rule....**



You can select the drive to which the whitelist rule applies from drives that are currently connected to your administrative workstation or a client computer running the DriveLock Agent. To do this, click the ... button.



Select the local computer or connect to a client computer running the DriveLock Agent. Select the drive from the list of currently connected drives and then click **OK**. The drive appears in the whitelist rules. You can configure access to this drive on the Permissions and Options tabs.



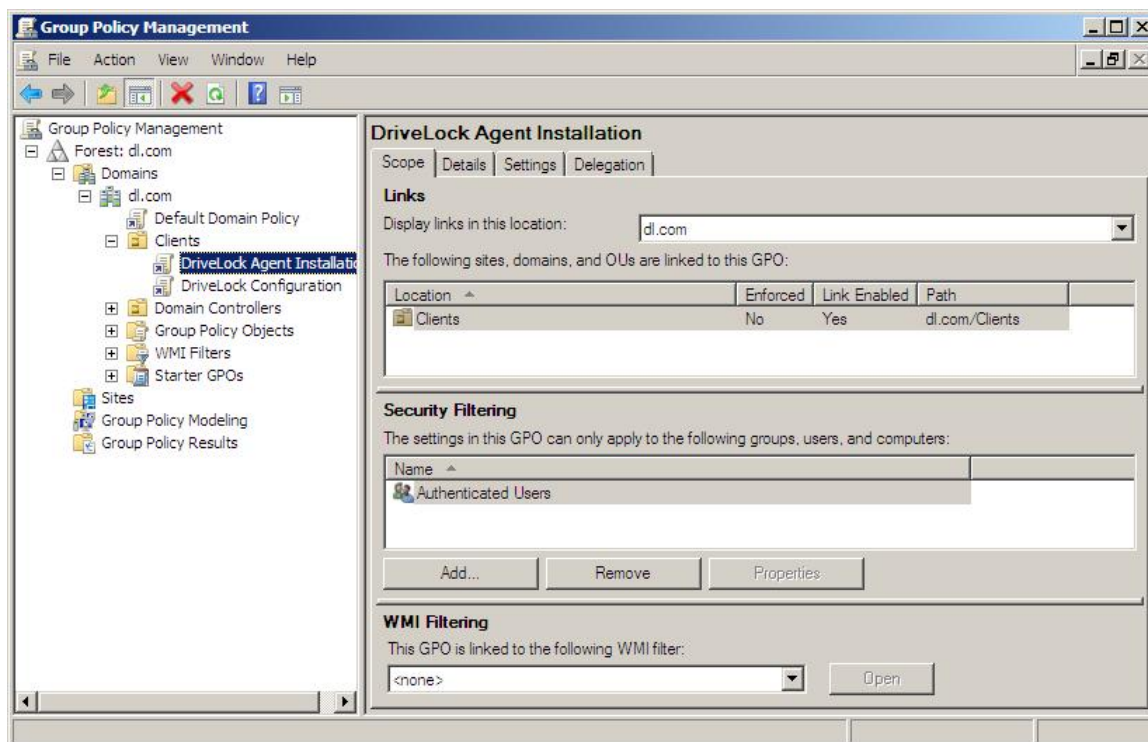
Installing the DriveLock Agent

Once all Group Policy settings are configured, the Windows Group Policy mechanism automatically distributes them to the client computers. Once you install the DriveLock Agent on these computers, it will start applying and enforcing these settings. You will distribute and install the Agent using Group Policy.

Estimated time required: **20 minutes**.

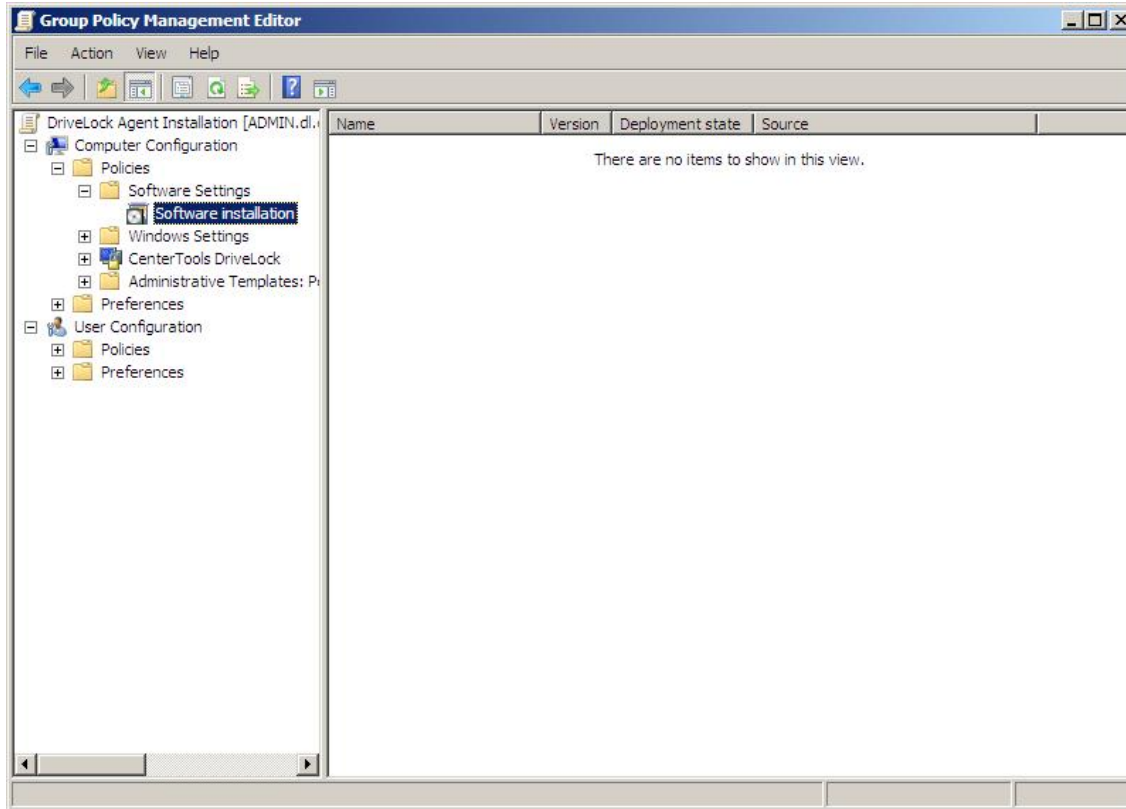
Before you can distribute the DriveLock Agent using Group Policy, you need to copy the Agent installation package (DriveLockAgent.msi) to a shared folder on a server. Ensure that both file and share permissions are configured to allow Read access for the Everyone or Authenticated Users groups.

CenterTools recommends the use of separate GPOs for DriveLock policy settings and software installation. You will create a software distribution policy. On the administrative workstation, start the Microsoft Group Policy Management Console (GPMC).

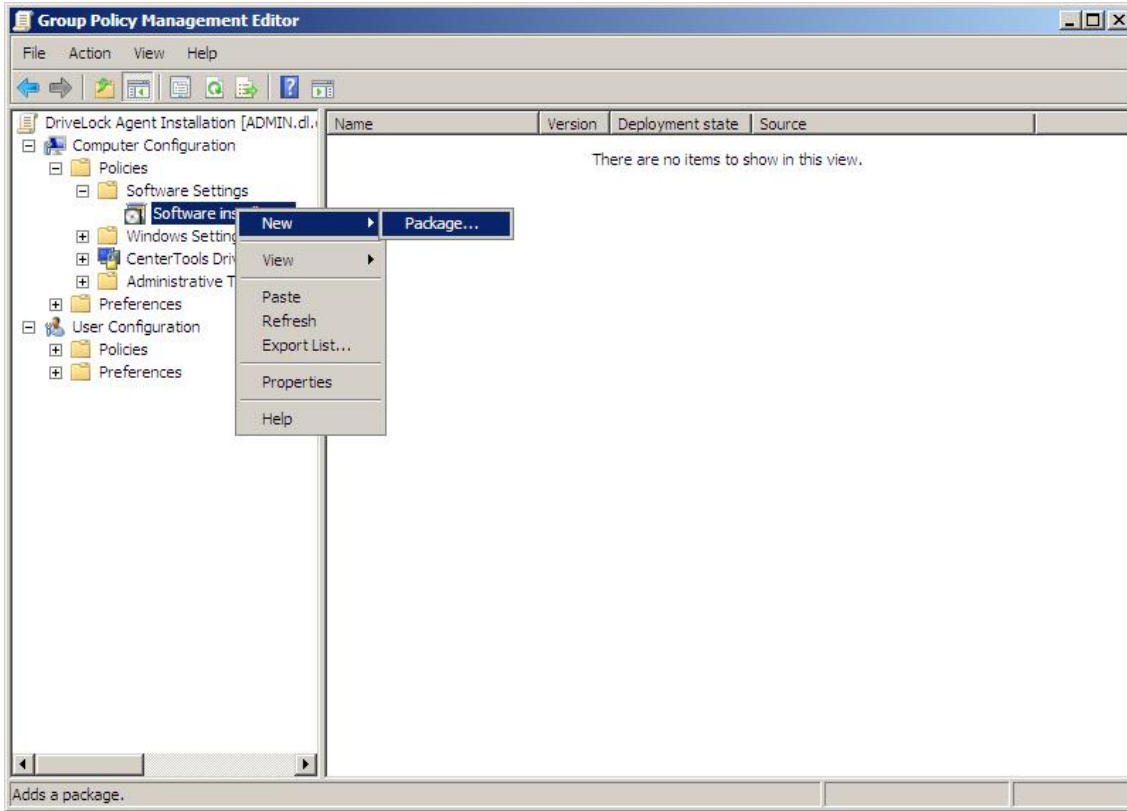


The GPO must apply to client computers that will be protected by DriveLock. Right-click the appropriate OU and then click **Create and Link a GPO here**. Provide a name for the GPO and then click **OK**.

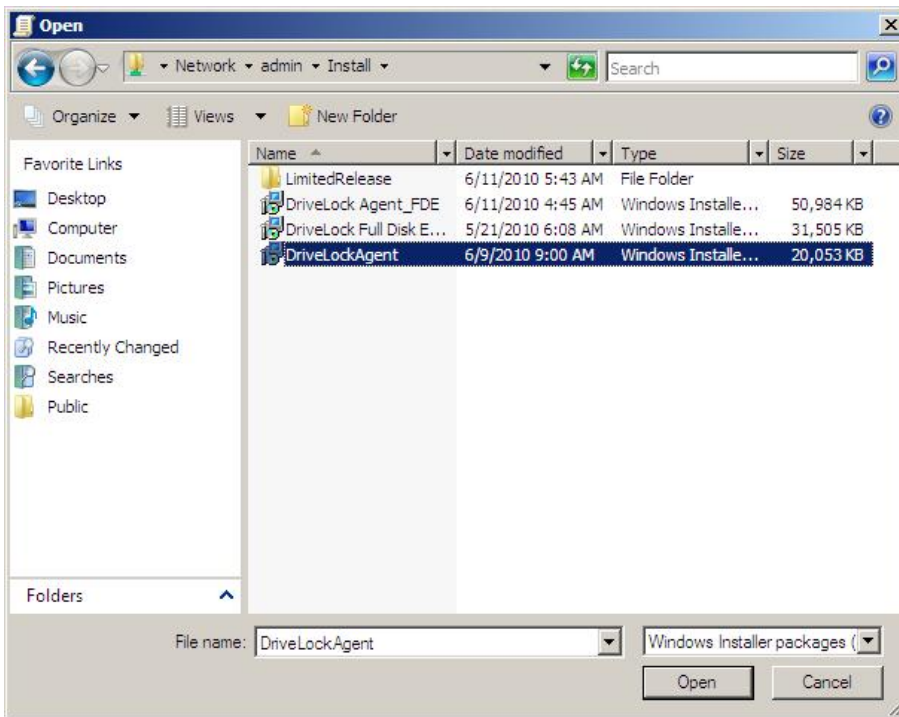
Right-click the GPO you created and then click **Edit**. In the Group Policy Management Editor, expand **Computer Configuration**, expand **Policies** and then click **Software Installation**.



To create a new software installation package, right-click **Software Installation**, point to **New** and then click **Package**.



Navigate to the shared folder where you saved the DriveLock Agent installation file, select the file and then click **Open**.



Ensure that **Assigned** is selected and then click **OK**.

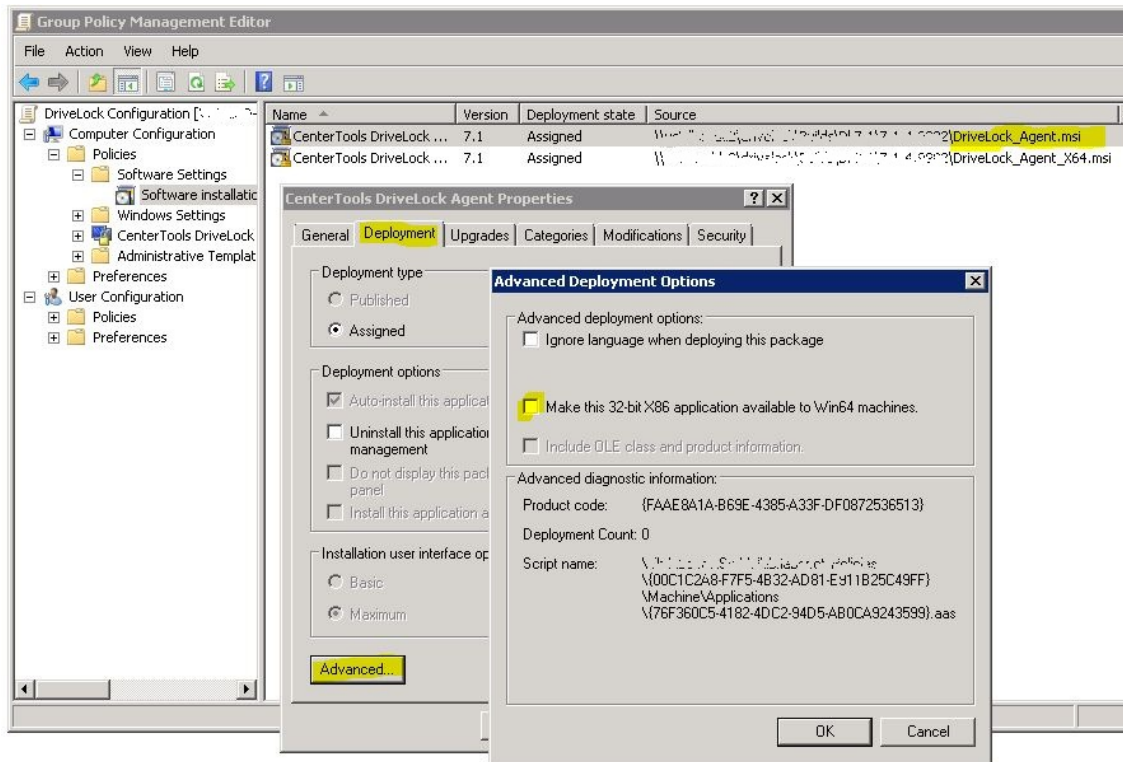
Once the software distribution policy is configured, all client computers that the GPO applies to will automatically install the Agent. Client computers will receive the policy settings during the next regular group policy refresh interval. You can also initiate an immediate Group Policy refresh on the client computer using the Windows `gpupdate` command. The installation of the Agent starts the next time the client computer restarts after the Group Policy refresh has been completed.

Once the DriveLock Agent is installed, it will immediately start applying the drive control settings you configured and start reporting events to the DriveLock Enterprise Service.



If you install the DriveLock Agent by using Group Policy, it can't be uninstalled from the Add/Remove Programs application in Control Panel. Instead, remove the software package from the GPO.

If you use a Windows Server 64Bit operating system you can distribute both 32Bit and 64Bit installation msi packages with one GPO. In this case take notice of one point. For the 32Bit installation package unmark the "Make this 32-bit X86 application available to Win64 machines". See screenshot below.



With this setting the 32Bit DriveLock agent will be installed on 32Bit PCs and the 64Bit DriveLock agent will be installed on 64Bit PCs.

Summary

The total estimated time required to install, configure and deploy DriveLock to control drive access and provide central reporting, as described in this document, is 2 hours and 25 minutes. Even when adding the time required for configuring the prerequisites, such as installing Microsoft SQL Server, a comprehensive drive control solution can be rolled out in well under 4 hours.