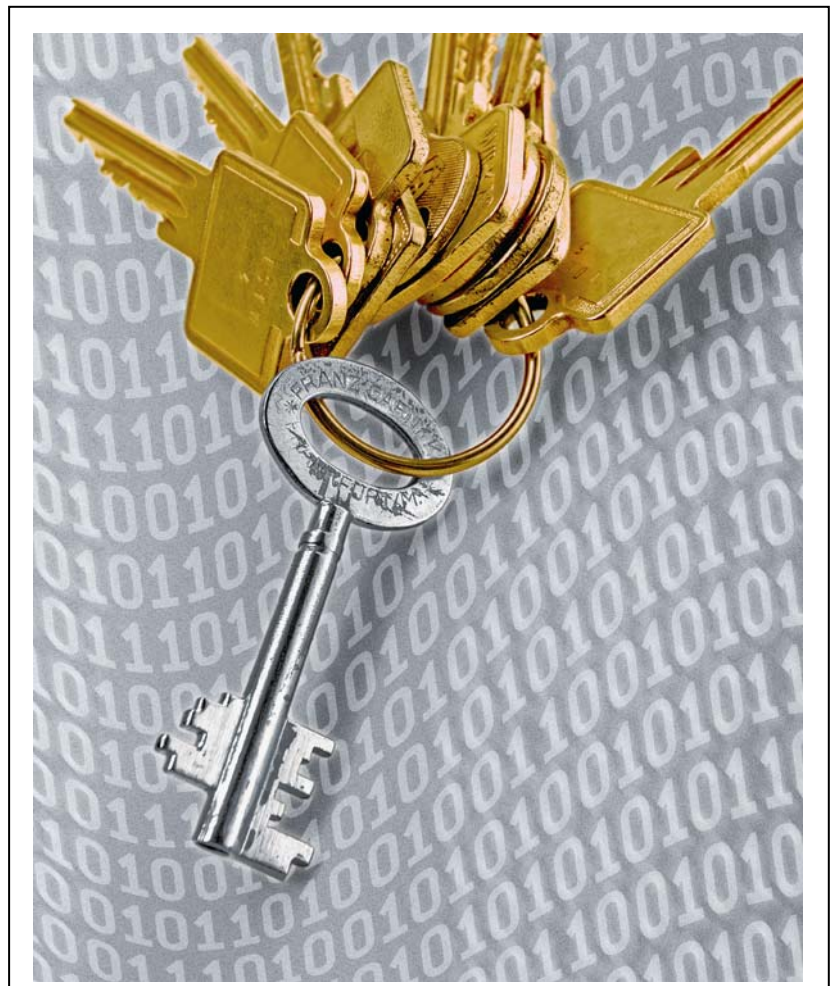




# DriveLock 5.5

Planning – Installation – Deployment



### 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.

© 2008 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

<b>0</b>	<b>About This DriveLock Documentation .....</b>	<b>5</b>
0.1	Content .....	5
0.2	Document Conventions .....	6
<b>1</b>	<b>Introduction.....</b>	<b>7</b>
1.1	Threats and Challenges.....	7
1.1.1	New risks .....	7
1.1.2	Legal challenges.....	8
1.1.3	Endpoint security threats .....	8
1.1.4	How to mitigate endpoint security threats.....	9
1.2	Securing Your Network with DriveLock.....	9
<b>2</b>	<b>Planning the DriveLock Deployment .....</b>	<b>11</b>
2.1	The DriveLock Components.....	11
2.1.1	The Agent.....	12
2.1.2	The DriveLock Management Console .....	12
2.1.3	The Security Reporting Center .....	12
2.2	The DriveLock Deployment.....	13
2.2.1	Design - Information is crucial.....	14
2.2.2	Setup - Rolling out the Agent software.....	15
2.2.3	Implementation - Tightening security.....	16
2.2.4	Operation - The day-to-day business .....	17
<b>3</b>	<b>Installing DriveLock.....</b>	<b>19</b>
3.1	System Requirements.....	19
3.2	Complete Installation .....	21
3.3	Installing the DriveLock Agent .....	24
3.3.1	Installing DriveLock by using Active Directory Group Policy .....	25

---

3.3.2	Installing the Agent by using configuration files .....	27
3.3.3	Manual DriveLock Agent installation .....	35
3.4	Installing the DriveLock Management Console.....	38
3.5	Updating DriveLock.....	38
3.5.1	Updating the Agent .....	38
3.5.2	Updating the Management Console.....	39
3.6	Removing DriveLock.....	39
3.7	Installing and updating the DriveLock Security Reporting Center .....	40
<b>4</b>	<b>Deploying DriveLock Configuration Settings.....</b>	<b>41</b>
4.1	Creating and Using a Local Policy .....	41
4.2	Deploying Policies by Using Group Policy.....	43
4.3	Deploying Policies by Using Configuration Files.....	47
4.3.1	Creating a configuration file .....	48
4.3.2	Editing a configuration file.....	49
4.3.3	Deploying a configuration manually .....	50

# 0 About This DriveLock Documentation

## 0.1 Content

This manual describes the steps that are required to deploy DriveLock securely and efficiently. The manual covers three main areas:

- General planning for deploying DriveLock and an overview of the DriveLock components are covered in Chapter 2.
- Installation of DriveLock and its components is covered in Chapter 3.
- Deploying the DriveLock configuration settings to client computers is covered in Chapter 4.

Configuring drive and device locking, whitelist rules, network profiles, application blocking, auditing and other features of DriveLock is covered in the document “*DriveLock Administration Guide*”.

The document “*DriveLock Encryption Guide*” covers DriveLock’s encryption functionality for mobile drives and how to use it.




The document “*DriveLock Full Disk Encryption Guide*” covers DriveLock’s Full Disk Encryption and how to deploy and configure it.

For information about the Security Reporting Center, see the document “*DriveLock Security Reporting Center Manual*”.

More information about DriveLock (such as video tutorials, whitepapers and other documentation) can be found on the DriveLock Web site ([www.drivelock.com](http://www.drivelock.com)).

## 0.2 Document Conventions

Throughout this document the following conventions and symbols are used to emphasize important points that you should read carefully, or menus, items or buttons you need to click or select.

	<p><b>Caution:</b> This symbol means that you should be careful to avoid unwanted results, such as potential damage to operating system functionality or loss of data</p>
	<p><b>Hint:</b> Useful additional information that might help you save time.</p>
	<p><b>Information:</b> Additional information about the current topic</p>
<p><i>italics</i></p>	<p>Italics represent fields, menu commands, and cross-references.</p>
<pre>C:\&gt;command</pre>	<p>A fixed-width typeface represents messages or commands typed at a command prompt.</p>
<p><b>Cancel</b></p>	<p><b>Bold type</b> represents a button that you need to click.</p>
<p>ALT + R</p>	<p>A plus sign between two keyboard keys means that you must press those keys at the same time. For example, ALT+R means that you must hold down the ALT key while you press R.</p>
<p>ALT, R, U</p>	<p>A comma between two or more keys means that you must press them consecutively. For example 'ALT, R, U' means that you must first press the Alt key, then the R key, and finally the U key.</p>

# 1 Introduction

## 1.1 Threats and Challenges

It was a nice birthday present: a brand new iPod with 80GB of internal storage. Now Jason, CEO of a medium sized company, is sitting in his office. He is listening to the music coming from the new gadget that is now connected to his laptop, while reviewing the new designs for a revolutionary upcoming product. Suddenly he realizes that it would take just seconds to copy this highly confidential information—or any other sensitive corporate data—to his iPod. Even worse, anyone in the company who has access to the data could do the same thing. At this point Jason realizes that he must take action to prevent the loss of this critical information, and that this threat to security must be stopped immediately.

### 1.1.1 New risks

The threat Jason just discovered is known as “pod slurping”—plugging a portable storage device, such as an iPod, into a computer and illicitly downloading large quantities of data from the computer. Because the computer is connected to the company’s network, a corporate firewall affords no protection against pod slurping or similar data theft methods. In October 2006 Apple announced, that they had sold over 39 million iPods during the previous twelve months (Preliminary Fourth Quarter Results, Apple, 18<sup>th</sup> Oct. 2006). Each of these iPods, and the billions of other music players and other portable storage devices in use today, represent a potential risk. As these storage devices become smaller, and their storage capacity increases, they represent a significant security risk to companies, government agencies and other organizations. However, most organizations underestimate the risk. Studies show that attacks from the inside are as likely as attacks from the outside. Furthermore, computer crime doesn’t occur only in large organizations. Many incidents affect small companies with new products or technologies that are of interest to the competition. Almost any device attached to a computer, such as USB sticks, flash drives, PDAs or iPods can lead to major security breaches and become a vehicle for the theft of confidential and private information.

By using a small USB flash drive, anyone can take control of a computer in seconds. This includes installing Trojan horse programs that can e-mail or transfer data to a remote location. Running undetected in the background, such programs may also enable remote access to the computer by installing backdoors or creating new administrator accounts. They can also infect any other removable media devices that are plugged into that computer. Such software is widely available on the Internet and is easy to use.

## 1.1.2 Legal challenges

An increasingly complex environment of government regulations and industry standards addresses the accuracy and protection of company data and information. This includes data about employees as well as customer, partner, and contractor data. In the US, organizations are faced with having to address compliance issues related to Sarbanes-Oxley (SOX), the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and other federal and state regulations and guidelines. Other countries have implemented similar requirements.

*"Security compliance and control solutions play a key role in enforcing security compliance, and these solutions help organizations to avoid violations of government and industry regulations, avoid the loss/leakage of intellectual property, and drive down the cost of compliance through integration, consolidation, and automation,"* says Rose Ryan, J.D., IDC research analyst, Security Products and Services (Source: Worldwide Security Compliance and Control 2006–2010 Forecast and Analysis: Going Beyond Compliance to Proactive Risk Management, IDC study, September 2006).

CEOs can no longer ignore these issues but have to address security threats, finding the best way to secure the IT environment that has become essential to business. Standard practices include the use of firewalls, anti-virus tools, and content scanners, tightening user access rights and following best-of-breed guidelines. Forrester Research says that organizations have felt the sting of focusing on the network perimeter while neglecting to secure the endpoints (such as desktops, laptops) in the enterprise. *"Endpoint security is here today, and it is more than personal firewalls and anti-virus."* (Source: Michael Rasmussen, Director of Research, Forrester)

## 1.1.3 Endpoint security threats

At the core of the problem are three types of endpoint security threats. First, there is corporate espionage. There are many documented cases of employees who have been recruited by rival companies or organized crime to steal confidential data. Such crimes may involve the theft of intellectual property, customer lists or even employee lists to be used by headhunters.

The second threat involves employees who are disgruntled or have been recently terminated, and as a result try to harm the company by disabling the network, destroying data, or stealing data for use in their next job.

The third threat is ignorance: many employees cause data breaches or jeopardize network security unintentionally. Examples include users who install unauthorized software and employees who plug a virus-infected USB flash drive into a corporate computer. Employees also may fall victim to social engineering schemes that are initiated via telephone, phishing scams or other attacks. One recent attack involved e-mail messages that appeared to be simple marketing offers promising free USB drives. The e-mails were targeted

at specific users in a company, and the drives that users received in the mail contained a Trojan horse program. This program gave criminals direct access to the user's computer and allowed them to run system scans, steal data and launch additional attacks.

### **1.1.4 How to mitigate endpoint security threats**

To address these threats, many security experts recommend implementing a security policy for using portable devices as one component of a comprehensive corporate security strategy. Some IT professionals advocate minimizing the risk by physically blocking ports or by completely banning all devices, such as iPods, USB sticks or cameras, from the workplace. However, such radical solutions can impede productivity, as many portable devices or cameras can be very useful for the company, or their use may even be mandatory (for example, a real estate agent has to copy pictures of houses from a digital camera to a computer). The optimal approach to controlling drives and devices is use software that is designed to provide granular control, such as DriveLock from CenterTools. DriveLock is not only able to control endpoint security in a very flexible manner; it can also be easily configured to implement your company's portable device security policy.

## **1.2 Securing Your Network with DriveLock**

CenterTools DriveLock is a lightweight software solution that helps you secure your desktop computers. It has a Multilingual User Interface (MUI), allowing you to select the desired language during installation or when running the program.

DriveLock offers dynamic, configurable access control for removable drives (floppy disk drives, CD-ROM drives, USB memory sticks, etc.). DriveLock also lets you control the use of most other device types, such as Bluetooth transmitters, Palm, Windows Mobile, BlackBerry, cameras, Smartphones, media devices and many more. By configuring whitelist rules based on device type and hardware ID you can define exactly who can access which device at which time. Removable drives can be controlled based on the drive's manufacturer, model and even serial number, allowing you to enforce very granular access control policies. Additional features let you unlock specific authorized media and to define time limits and computers for whitelist rules. For deal with unexpected situations, authorized administrators can temporarily suspend DriveLock's device control on a computer even when the computer is offline and not connected to a network.

Installation of the client software (the DriveLock Agent) and policy deployment can be achieved easily by using existing software deployment mechanisms or by using the Group Policy feature of Active Directory. Group Policy is also the preferred method for distributing policy settings to clients. Alternatively, you can distribute policies using configuration files for standalone computers or in environments without Active Directory (for example Novell).

DriveLock's auditing capabilities, coupled with its file shadowing functionality, give you the information you need to monitor and enforce policy compliance. By using the DriveLock Device Scanner you can detect any drive or device that has been used in your network, even if it's no longer connected to a computer. The DriveLock Agent doesn't need to be installed on the target computers to use the Device Scanner.

Encryption is another main feature of DriveLock. DriveLock can help secure sensitive information by enforcing encryption when data is copied to removable drives or by encrypting an entire hard disk. DriveLock can also erase sensitive data in a secure manner by overwriting data multiple times, using one of several industry-standard algorithms.

DriveLock's Application Launch Filter provides easy control over which applications users can run. You can allow or deny the launching of an application based on several criteria, for example user or groups, the current network environment or a computer.

The optional Security Reporting Center (SRC) is DriveLock's central database and reporting component. The SRC consolidates all DriveLock events and Device Scanner results in a SQL Server database. Administrators can then use this data to create dynamic reports for auditing and management purposes.

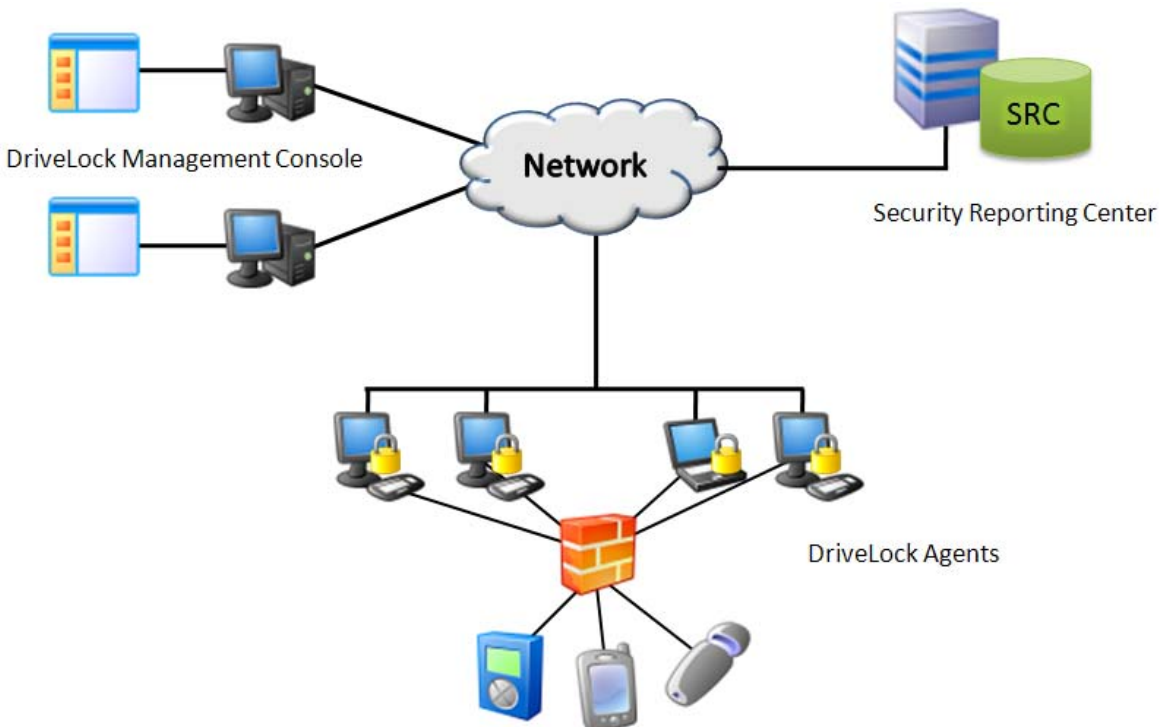
## 2 Planning the DriveLock Deployment

Before you begin to install the DriveLock Agent on your computers you should decide which components of DriveLock you will implement and how to use them. DriveLock is very flexible and almost anything can be customized to meet your needs. Therefore it is very important to understand how DriveLock works, how to perform configuration and deployment tasks, and how DriveLock can be used to assist you in securing your environment.

This chapter explains the different components of DriveLock and how they work together. It also describes an implementation process to help you set up your DriveLock deployment by following a step-by-step approach.

### 2.1 The DriveLock Components

The following diagram shows the DriveLock components and how they communicate with each other:



### 2.1.1 The Agent

The DriveLock Agent is the most important component of the DriveLock infrastructure. It implements and enforces your policy settings and must be installed on every computer where you want to control removable drives, devices or other settings. The Agent is a lightweight Windows service that runs in the background and maintains control over hardware ports and interfaces and enforces your security policy. To prevent unauthorized access or the bypassing of the security settings, regular users can't stop the service; only users who are specifically authorized by you can access and control the service.

### 2.1.2 The DriveLock Management Console

You use the DriveLock Management Console to configure the security settings for your clients, manage your environment and access other DriveLock components. This console is a Microsoft Management Console (MMC) snap-in that you can easily integrate into existing MMC console files that you may have already configured.

The DriveLock Management Console allows you to create a local configuration for the computer the console is running on, to define configurations using Active Directory Group Policy, and to save settings to a configuration file that you can import to another computer. You can also use the console to monitor the status of clients, access the DriveLock Agent on clients and remotely unlock an Agent, or—if the Agent is not connected to a network—by creating an offline access code that a user can type on the client computer. The Device Scanner and the Security Reporting Center (if installed) are also integrated into the DriveLock Management Console.



Only the Agent on a client computer and the Management Consoles running on an administrator's workstation are required to configure and secure your environment. DriveLock does not include or require any central component to enforce policies.

### 2.1.3 The Security Reporting Center

DriveLock's Security Reporting Center (SRC) allows you to consolidate DriveLock events on a central server and to create dynamic reports from this data. This lets you monitor mobile drives, devices and data transfers in aggregate or in detail. The SRC includes multi-client functionality which allows association of DriveLock events or Agents with specific customers (clients) or areas of responsibility (for example, a specific group of administrators is responsible for just one business unit). This feature is further enhanced by the option to assign individual permissions for data queries and reporting creation.

You can create reports about the use of removable media and device connection attempts, both allowed and prohibited. Other reports show which files have been written to or read from removable media. You can use the DriveLock policy settings to configure which details to record. All of these functions and the ability to generate graphical statistics make the SRC a very powerful monitoring and reporting tool.

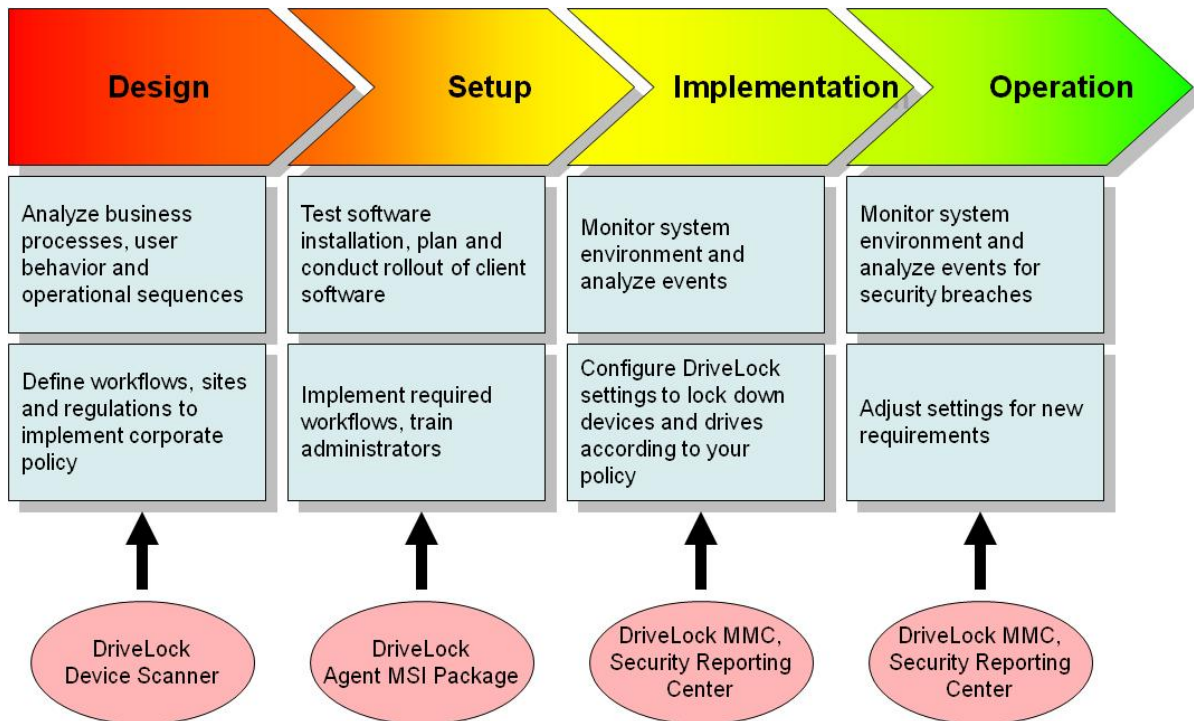
Starting with DriveLock Version 5.5, you can use the Security Reporting Center Management Console to monitor the current status of DriveLock Agents in your network. This includes information about the installation status (for example, whether the DriveLock Agent is installed on licensed computers) and the connection (for example, the last time an Agent communicated with the central Consolidator). You can quickly filter and group this data to create an easy-to use network-wide view of the status of DriveLock.

The SRC consists of three components: the SRC database, the DriveLock Web services, which require Microsoft Internet Information Server (IIS) 6.0, and the DriveLock Consolidator, which receives event messages from Agents and routes them to the database. All components of the SRC can be installed on a single server. This server can also hold the Microsoft SQL-Server database, which is required to store the event data.

## 2.2 The DriveLock Deployment

Deploying security measures can have a disruptive effect on business. The challenge is to create a balance between securing the network, preserving your company's flexibility and empowering users. DriveLock can be installed very easily and quickly even in large networks, and by thoroughly planning your deployment you can achieve better results and broader acceptance.

The following diagram illustrates some of the high-level considerations to keep in mind during the lifecycle of a DriveLock implementation and how to use each DriveLock component at each stage: Many CenterTools customers have found it helpful to follow this strategy when rolling out DriveLock in their network.



This implementation concept is based on best practices learned from existing deployments

### 2.2.1 Design – Information is crucial

Before you can start designing your DriveLock implementation, you must have collected information about your company's business processes and procedures. This includes answering the following questions:

1. What kind of access to client computers is required in my organization to meet business needs?
2. Which devices must be used based on these requirements?
3. Which devices can be kept out of the network without interfering with business requirements?

The more accurate and complete the answer to these questions, the better you are able to define the rules for DriveLock. Finding the answers requires knowledge of your IT environment, but you can also use the DriveLock Device Scanner to create an inventory of all devices that are currently in use and to project the consequences of blocking some or all of these devices.

Start the process by installing DriveLock on a single computer that is connected to your network. Use the Device Scanner to scan your network and use the results to quickly determine which devices have been in use on client computers up to this point. The results of the scan can be stored locally on your workstation, and you can later copy them to an administration workstation and create whitelist rules from them. When you compare the scan results with an existing inventory of devices, you can quickly identify which ones you were unaware of. This is crucial information that you need to continue with the design process.

The next step in designing the deployment is to categorize your findings by using the types of device classes that DriveLock uses to classify devices. These classes are shown in the DriveLock Management Console. When categorizing peripherals, distinguish between drives, interfaces and devices. Next, group devices according to device class (such as scanners, modems, PDAs, etc.). The following information that is provided by the Device Scanner can also help you group the results, starting with the general classification and moving to more details:

- Interface / drive
- Hardware / device type
- Manufacturer (manufacturer ID)
- Product (product ID)
- Serial number

Next you need to decide which groups of devices to allow, and which ones will be locked. To simplify your deployment it can be helpful to concentrate on just a few device classes that will be allowed. You can also assign user or group permissions to your inventory and grant or deny access, either unrestricted, or just during a certain time range (for example, Mondays and Wednesdays between 08:00 A.M. and 4:00 P.M.).

You can also decide which file transfers to or from portable drives to audit and whether to have DriveLock create shadow copies of those files (either entire files or just a portion) on a central location for later analysis.

When you have recorded all your answers, groups and settings, you can create your security policy for removable devices. It is important to document these rules because you may have to coordinate with others within your organization.

No matter how well the enforcement of device usage policies is designed and implemented, business routinely changes, and what works today will impede productivity in the future. Because of this you need an internal process to handle these changes. Having such a process in place enables you to react based on new requirements or new portable devices. In larger organizations, setting up those internal sequences may involve a long and involved process, so it's advisable to plan for change at an early stage.

### **2.2.2 Setup – Rolling out the Agent software**

The design phase is usually followed by the implementation. Before implementing your security controls using DriveLock's access control lists and whitelist rules, you need to install and configure your DriveLock environment properly.

It is recommended that you start the rollout with a basic configuration (such as language settings, event logging, etc.). You will lock devices and drives and create whitelist entries for specific items later during the implementation phase.



If you will be using configuration files instead of Active Directory Group Policy, you should create at least a simple configuration file prior to installing the Agent as you will have to specify the name and location of a configuration file during setup.

In larger network environments, software installation is more involved than in small organizations that only have few servers and clients. Often there are company policies and procedures for application testing and installation. Since the DriveLock Agent is installed by using a Microsoft Installer (.msi) package, it is easy to integrate the Agent installation into existing procedures and roll out the software to all clients in accordance with corporate policies. The use of a Microsoft Installer package also allows for a completely automated installation and upgrades that integrate with most corporate software deployment processes and technologies. Detailed information about how to install DriveLock can be found in Chapter 3.

Before you install the software, is also a good time to implement your internal organizational procedures if you haven't already done so already. Train your administrators and inform all affected users about changes to your security policy. Users will need to know that mobile devices use may be restricted and they must understand the reasons for the security improvement so they can adjust to the new environment.

### 2.2.3 Implementation – Tightening security

When everything is up and running you should start monitoring how DriveLock performs in your environment by using one of the following methods:

DriveLock can record many types of activities and incidents in the Windows Event Log (for example, when a new portable drive is attached or disconnected or when a device is used). Analyzing these logs, either by using the Event Viewer or consolidating events by using software such as NetIQ's Security Manager or Microsoft Operations Manager, can reveal useful information about user activities and DriveLock performance.

Another approach is to use the Security Reporting Center (SRC) to monitor DriveLock operations. You can configure the DriveLock Agent to send events to the SRC so that can analyze them by using the SRC Management Console with its powerful filters, search criteria and grouping capabilities.

After you've become familiar with DriveLock's operations, you can start locking down client computers. Start with the items you recorded during the design phase. By default, DriveLock blocks all devices in a category until you specify exceptions using whitelists. This makes it easy to block entire device types or interfaces that are not required in your network. For example, if you don't want to allow FireWire or Bluetooth connections at

all, or you want to prevent the use of all modems and mobile phones, you can create such a policy with just a few clicks.



Be careful not to lock network devices, human interface devices (keyboards and mice), or other critical system devices without first configuring whitelist rules.

Blocking these types of devices may prevent the computers from functioning correctly or from obtaining updated policy settings, including those that would re-enable the blocked devices.

Change the configuration according to your needs and closely watch for any events that are recorded. For example, attempts to access drives or devices you just have locked that appear in the Event Log or SRC could indicate that you forgot to add a required device to a whitelist. Carefully review all events to ensure correct operations.

The next step of the implementation phase is more complex. Assume that you need to lock USB ports but you have a number of devices and drives that need to be accessed. If you completed the design phase, you can create the required whitelist rules containing the settings required to tighten security. If you didn't create whitelist rules that allow the use of important devices, you may get inundated with phone calls from irate users. To set up whitelist rules you can use the information gathered with the Device Scanner during the design phase. To do this, simply copy the database file to your administrative workstation and open it from the DriveLock Management Console.

With the internal processes in place you can respond to helpdesk calls in a timely manner and maintain a high level of user satisfaction. If you adjust your rules incrementally you can use the SRC to keep track of what is going on, quickly adjust settings to fit changing requirements, and you won't get overwhelmed by user requests for policy exceptions.

## 2.2.4 Operation – The day-to-day business

After a successful implementation, day-to-day tasks take over and these tasks will be similar to those you encountered during implementation, except that policy changes are needed much less frequently.

During the Operation phase you monitor the SRC or the local Event Logs for unusual events that may indicate security breaches. You can use file filters or the shadowing feature of DriveLock to save important information about what files have been transferred to and from computers in your network. This data might be needed to investigate an incident or for forensic analysis.

You can also use the Management Console to monitor the status of your Agents or connect to the Agents by using Agent Remote Access. Sometimes it might be necessary to unlock drives or devices temporarily. (For

example, imagine that your CEO will have to give a speech in ten minutes and the slides for it are on a new USB stick that has not been added to a whitelist yet. In this scenario you can use the DriveLock console to enable temporary access to this device within seconds.

## 3 Installing DriveLock

You can install DriveLock from compact disc or using files downloaded from the CenterTools Web site. Typically, installation is performed by an administrator who wants to deploy Agents, configure the application in a centralized manner or use DriveLock as a standalone solution (for example, for test purposes).

To deploy DriveLock in your network when central configuration settings are already in place, use the Agent installer package, as described in the section “Installing the DriveLock Agent” in this chapter. This package only installs the Agent without policy configuration tools or administration documentation.

The following table describes the available installation packages:

<i>Setup.exe</i>	Installs the Agent and the DriveLock Management Console on an administrator workstation. You can also use this package to only install the Management Console.
<i>DriveLockAgent.msi</i>	Installs only the DriveLock Agent. This package is used for Agent deployment.
<i>Srcsetup.exe</i>	Installs the Security Reporting Center components on a central server.
<i>Srcmmcsetup.exe</i>	Installs the Security Reporting Center Management Console on an administrator workstation.
<i>DriveLock Full Disk Encryption.msi</i>	Installs the DriveLock Full Disk Encryption package ( <i>pdinstall.bin</i> ) on the Security Reporting Center or any client.
<i>DriveLock.iso</i>	Complete CD-image you can create an installation CD from and then use the files from the CD to install DriveLock and its components. It contains all the files mentioned above and all the DriveLock documentation (PDF).

### 3.1 System Requirements

CenterTools DriveLock works in the background and therefore only uses minimal hardware resources. DriveLock runs under all recent versions of the Windows operating system and requires no additional infrastructure. Configuration and Agent deployment are done primarily by using Active Directory. The DriveLock components also require the hardware and software listed in the following table:

	Agent	DriveLock Management Console	Security Reporting Center (Requirements may differ depending on your system environment and your database installation)
Minimum CPU speed	400 MHz	400 MHz	500 MHz
Minimum Memory	128 MB RAM	128 MB RAM	128 MB RAM
Minimum Hard Disk	25 MB	75 MB	95–300 MB for database (~275 MB for standard installation)
Supported operating systems	Windows XP SP2 or later Windows 2003 SP1 or later Windows Vista	Windows XP SP2 or later Windows 2003 SP1 or later Windows Vista	Windows 2003 Windows 2003 SP1 Windows 2003 R2
Additional Software	Microsoft XML Core Services 6.0  Microsoft Native WLAN API for Windows XP (required for feature: „Disable WiFi connections when connect to a LAN“)  Microsoft IMAPI 2.0 (for CD/DVD Encryption)	Microsoft XML Core Services 6.0  Microsoft Management Console 3.0  .NET Framework 2.0  .NET Framework 3.0 (for DriveLock Management Console and FDE only)  Microsoft IMAPI 2.0 (for CD/DVD Encryption)	Internet Information Services 6.0 (IIS) with ASP.NET 2.0  Microsoft SQL 2000 or 2005 Server  .NET Framework 2.0

CenterTools recommends that you always install the most current Service Pack and all security patches that are available for the version of the operating system you are using.

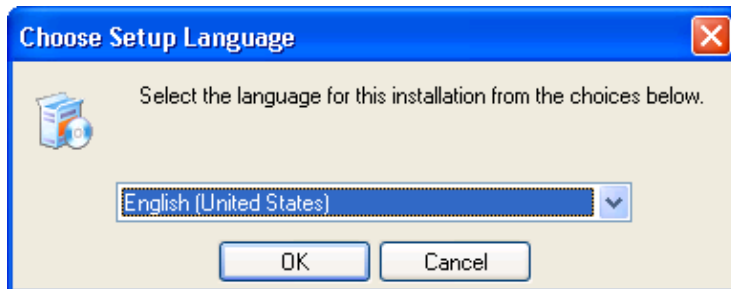
DriveLock also supports other network operation systems. For more information, see the chapter “Deploying Policies by Using Configuration Files”.

The Security Reporting Center requires a backend database. For more information, refer to the document "*DriveLock Security Reporting Center Manual*".

## 3.2 Complete Installation

This type of installation installs the DriveLock Agent and the DriveLock Management Console on a local computer and creates the corresponding Start menu entries. This is the recommended installation type for evaluating DriveLock.

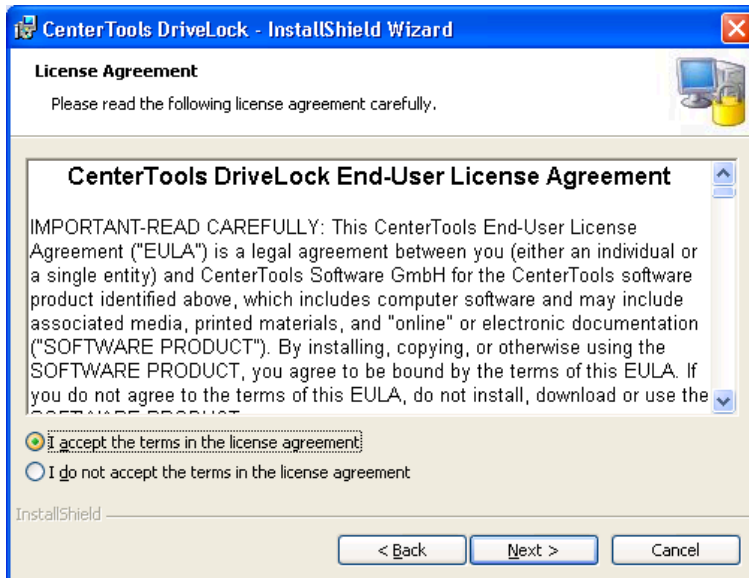
To start the installation, run *setup.exe* and follow the installation wizard through the next steps.



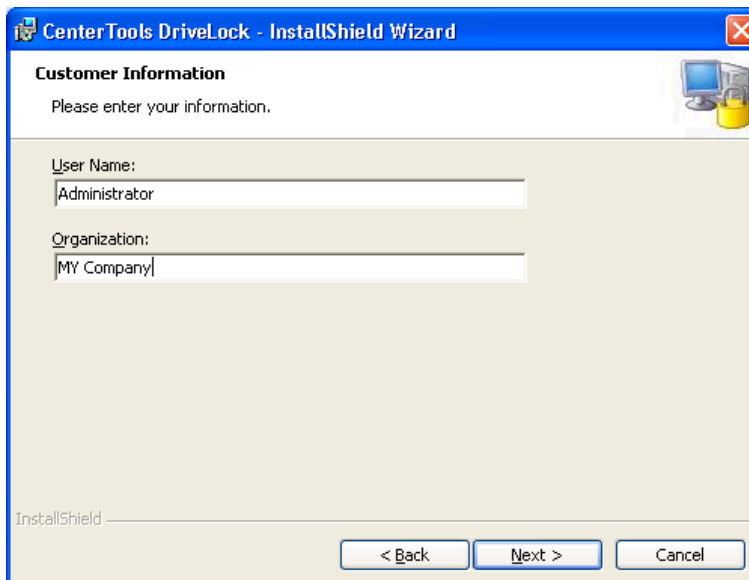
Select the desired language for the installation and click **OK**. Subsequently the DriveLock installation will be prepared by the Install Shield Wizard. Then the DriveLock installation starts automatically.



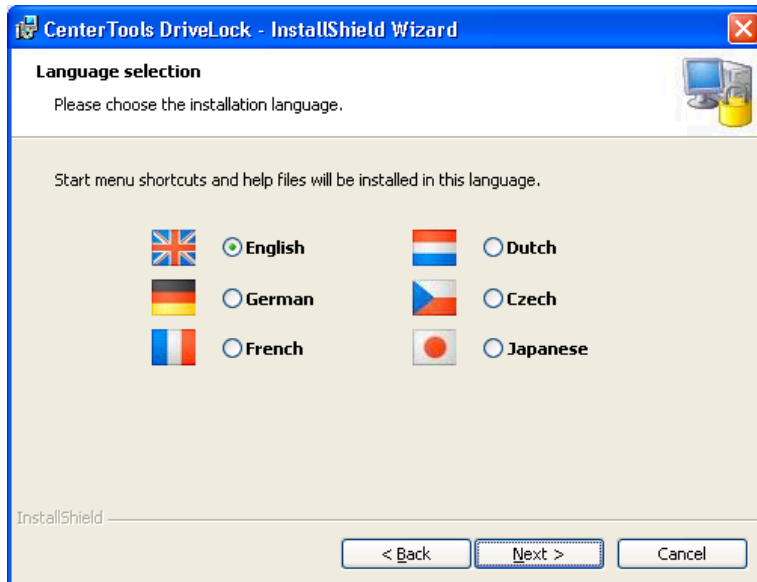
Click **Next**.



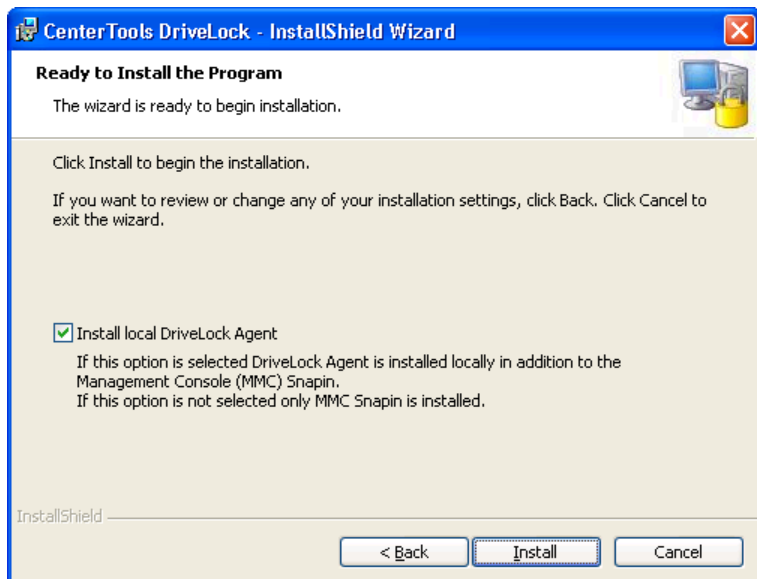
Read and accept the license agreement, and then click **Next**.



Type your name and company name, and then click **Next**.

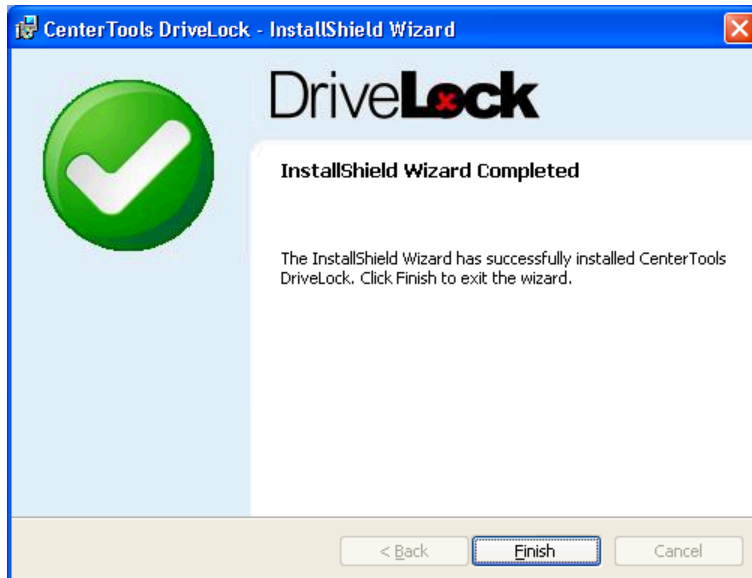


Select the desired language for the DriveLock user interface, and then click **Next**.



To evaluate DriveLock on a single computer, keep the option *“Install local DriveLock Agent”* checked. Deselect this option to install only the DriveLock Management Console.

Click **Install**. The complete installation may take several minutes.



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

After the installation, the “*CenterTools DriveLock*” service has been registered and is running.

The installation also created Start menu shortcuts to the documentation and the DriveLock Management Console. You can now start configuring DriveLock using the DriveLock Management Console (as described later in this document).



You can also install the package from a command line (silent installation). Use the MSI property “*LOCALAGENT*” to select whether or not an Agent will be installed locally. A value of 0 (not default) will install the Management Console only.

### 3.3 Installing the DriveLock Agent

The DriveLock Agent must be installed on each client computer where you want to control access to removable drives and devices.

A stand-alone Windows installer package is provided for installing the DriveLock Agent on client computers that are not administrative workstations. This installation package (*DriveLockAgent.msi*) installs the DriveLock Agent service without creating any entries in the Start menu.



The *DriveLockAgent.msi* package for the DriveLock Agent installation is located on the ISO-Image or can be downloaded separately from the DriveLock Web site.

Before you install the Agent on client computers, you must have created a policy that contains at least basic configuration settings and whitelist entries for required devices. This policy must be available to clients at the time of the installation. The Agent can access this policy either by using Group Policy or from a shared folder on the network.



If you install the Agent without a providing these configuration settings, either via Group Policy or a configuration file, you may inadvertently lock devices or drives that are required for proper operation of the client computers.

If you use Active Directory and Group Policy, you can install the Agent and configure and deploy Agent configuration settings by creating your own Group Policy Objects. You can also use configuration files stored in a central location to deploy your settings and specify the path to this file during Agent installation. The following sections describe the available Agent installation methods in more detail.

### 3.3.1 Installing DriveLock by using Active Directory Group Policy

A convenient way to deploy DriveLock Agents to target machines is by using Active Directory Group Policy.

Deploying DriveLock Agents by using Group Policy requires that the *DriveLockAgent.msi* Windows installer package is located in a shared folder that the client computer can access.

Additional information about using Group Policy Objects is available on the Microsoft TechNet Web site, including the following helpful documents:



Deploying and upgrading software (via GPO)

<http://technet2.microsoft.com/WindowsServer/en/library/fdbf74c6-2b98-4a79-815b-d831d8d757b51033.msp?mfr=true>

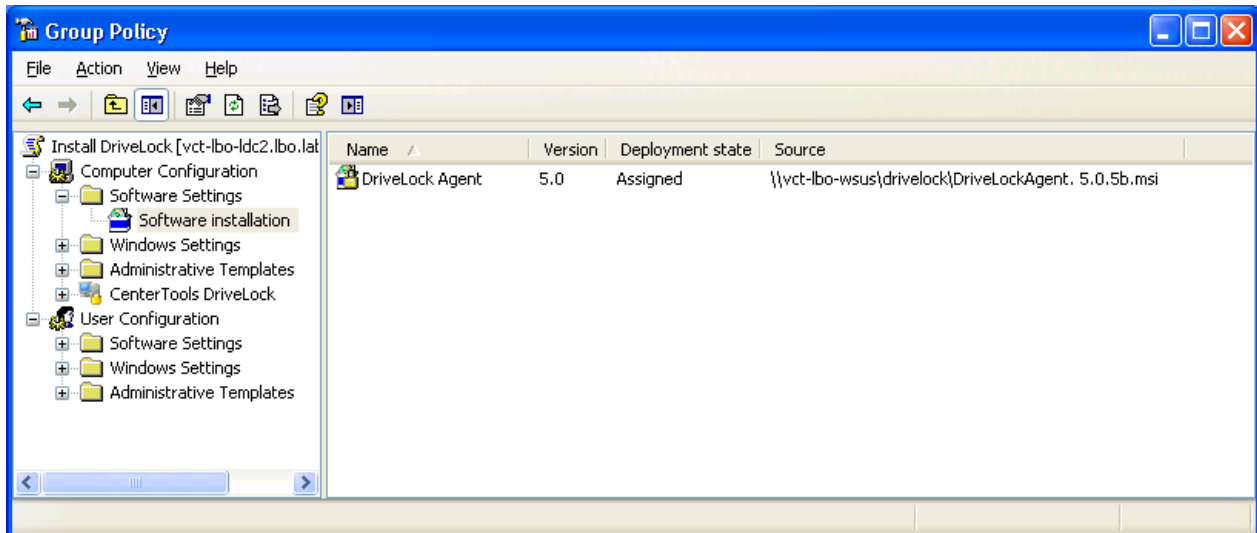
New ways to do familiar Group Policy tasks (pre-GPMC)

<http://technet2.microsoft.com/WindowsServer/en/library/f5860815-522a-4159-906b-bc606335948e1033.msp?mfr=true>

New ways to do familiar tasks using GPMC

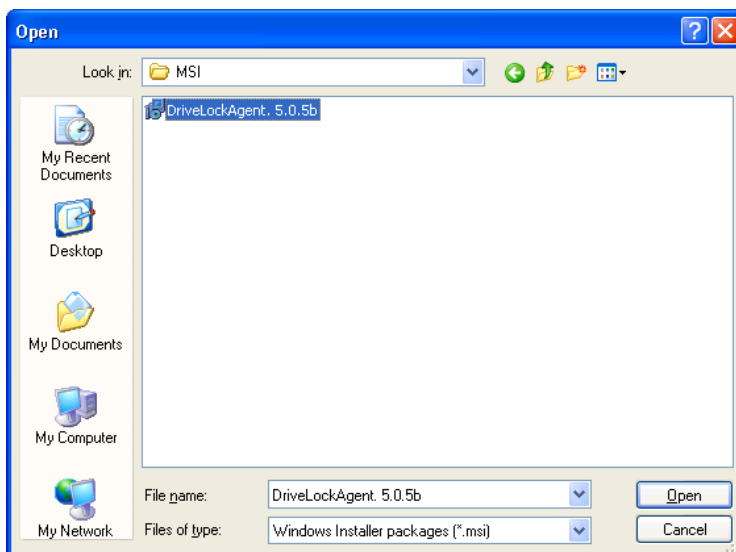
<http://technet2.microsoft.com/WindowsServer/en/library/7c73c060-3c97-4aad-95d3-2182d4692ded1033.msp?mfr=true>

To configure a software deployment policy, open an existing Group Policy Object or create a new one. In the Windows Group Policy Object Editor, in the console tree, navigate to *Computer Configuration* → *Software Settings* → *Software installation*.



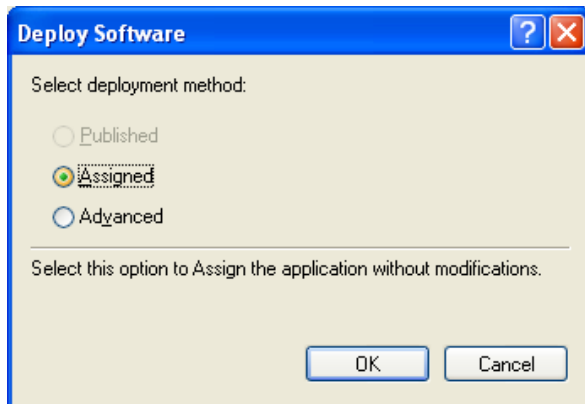
You can also use the DriveLock Management Console to open or create a Group Policy Object. This method is described in the section “Deploying Policies by Using Group Policy”.

Right-click **Software installation**, and then click **New** → **Package**.



Navigate to the shared folder that contains the installation package, select the *DriveLockAgent.msi* file and then click **Open**. Ensure that the file name is displayed in Universal Naming Convention (UNC) format (for example, "\\Server\driveLock\$\DriveLockAgent.msi").

Select *Assigned* as the deployment method options and then click **OK**.



The Group Policy Object is now configured and the Agent rollout will start after the policy is replicated to domain controllers and applied to the target machines.



DriveLock should not be assigned to the User Settings in a GPO, as DriveLock is a computer-focused application.

DriveLock configuration settings are not installed automatically with the software package. These settings, including a valid license file, must be provided separately as part of the same or a separate GPO.



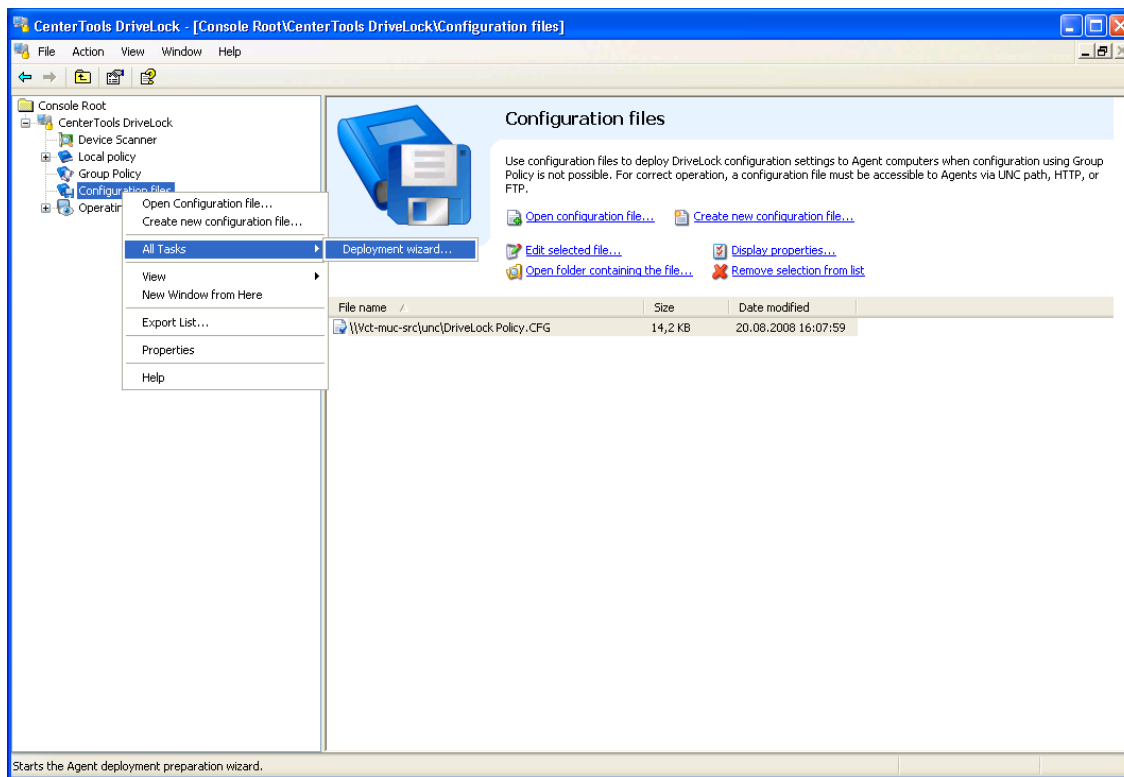
If you install the DriveLock Agent by using Group Policy, it can't be uninstalled from the Add/Remove Programs application in Control Panel. Instead, remove the software package from the GPO. For more information about assigning software using Group Policy, review the Group Policy documentation from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

### 3.3.2 Installing the Agent by using configuration files

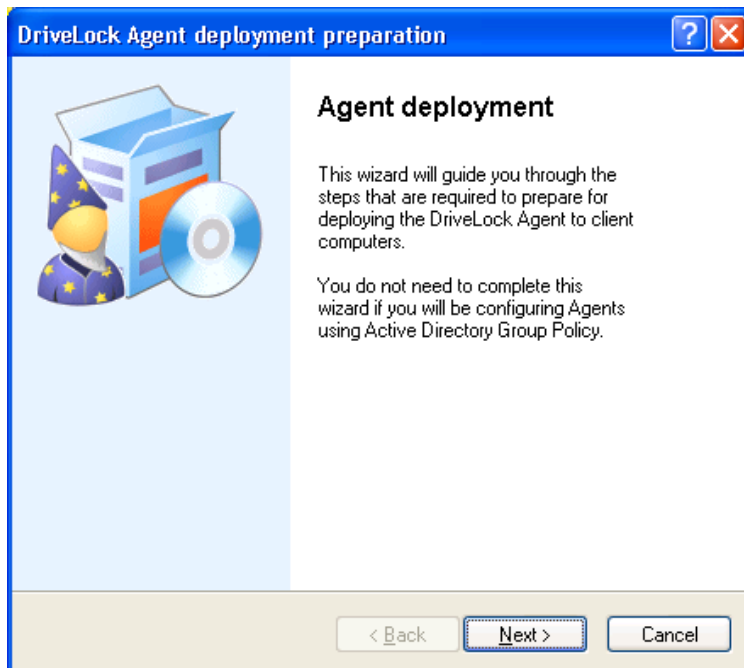
When you use a configuration file to deploy your DriveLock policy to client computers, copy this file to a shared folder and specify the network path to it during Agent installation. For information about using a configuration file, review the section "Deploying Policies by Using Configuration Files" in this manual.

### 3.3.2.1 Generating installation parameters by using the Deployment Wizard

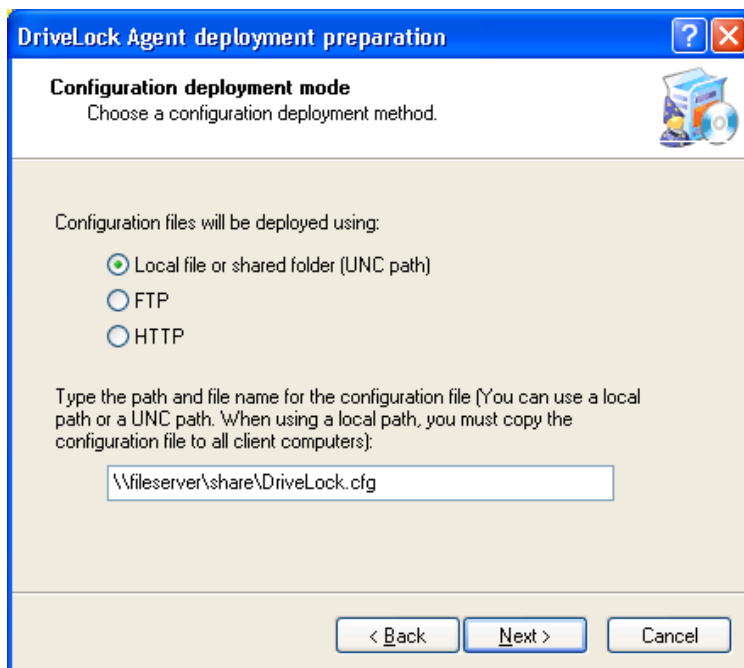
The DriveLock Deployment Wizard assists you in deploying the DriveLock Agent to computers in your network by using configuration files. The wizard helps you create the correct command line for Windows Installer, generates a modified Microsoft Installer package, or creates a Microsoft Installer Transform (.mst) file for your installation.



To launch the wizard, right-click **Configuration files**, point to **All Tasks** and then click **Deployment wizard...**.



Click **Next** to continue.

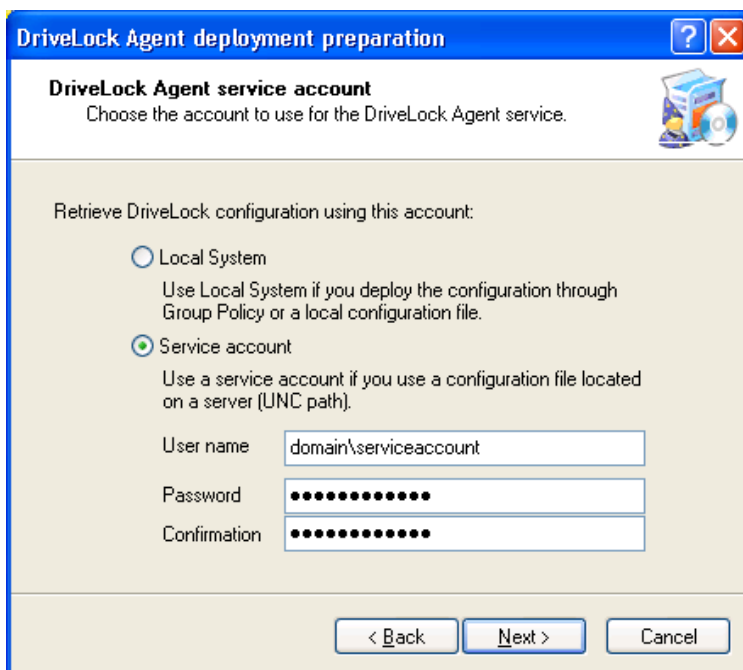


Specify the location from which the DriveLock Agent will retrieve the configuration file. You can specify a UNC path, an FTP location or an HTTP location. You can also specify a local path that can be accessed by the local System account (for example, *C:\Windows\DLConfig*).

After entering the location of the configuration file, click **Next**.

Next, specify the user credentials that are used to access the configuration file:

- **Local System:** DriveLock will connect to the configuration file by using the local System account on the client computer. This is the recommended setting if the configuration file is stored locally on client computers.
- **Service Account:** DriveLock will use the account you specify. This account must have permissions to access the file on the remote server. The account password will be stored in an encrypted format.
- **Anonymous:** If you have selected either an FTP or HTTP path, type *Anonymous* as the name of the service account and leave the password blank. The FTP or HTTP server must allow anonymous access to the configuration file.



**DriveLock Agent deployment preparation**

**DriveLock Agent service account**  
Choose the account to use for the DriveLock Agent service.

Retrieve DriveLock configuration using this account:

Local System  
Use Local System if you deploy the configuration through Group Policy or a local configuration file.

Service account  
Use a service account if you use a configuration file located on a server (UNC path).

User name: domain\serviceaccount

Password: ●●●●●●●●●●●●

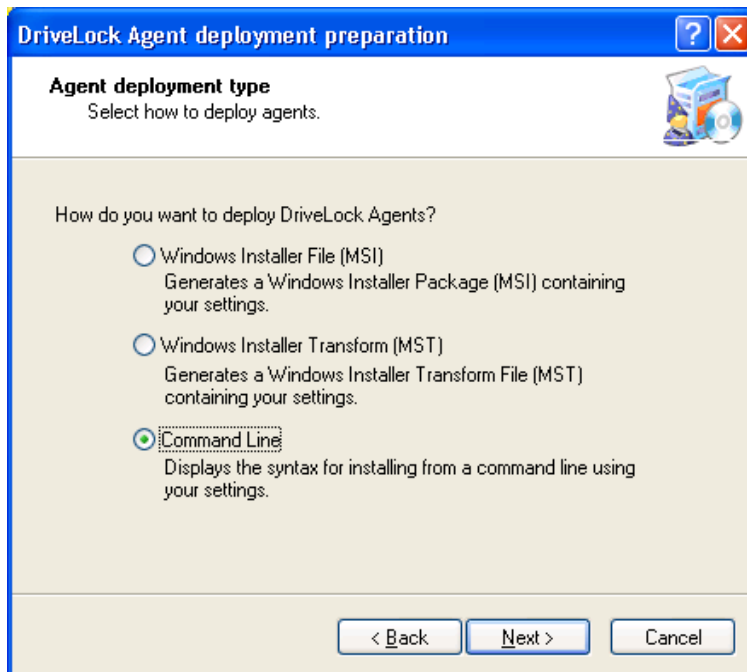
Confirmation: ●●●●●●●●●●●●

< Back   Next >   Cancel

Click **Next**

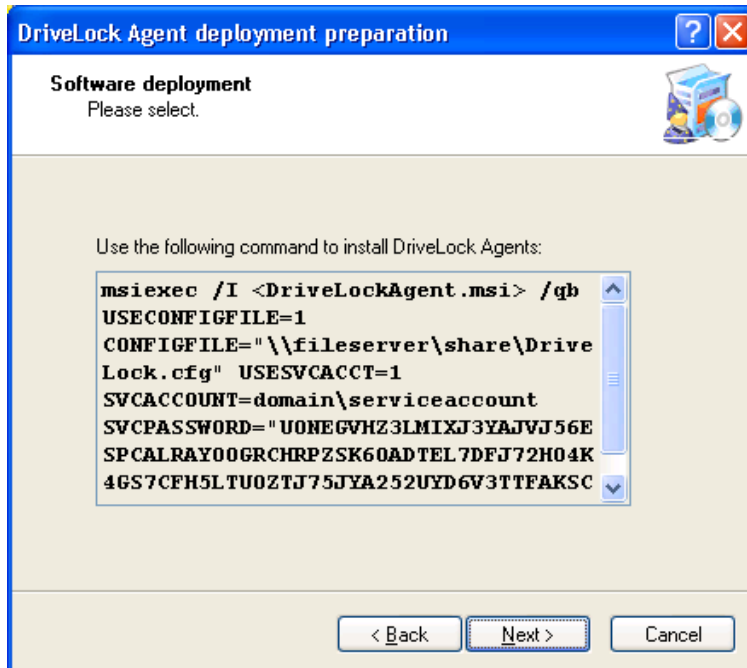
On the next page select the type of installation package that will be created by the wizard:

- **Microsoft Installer File (MSI):** Creates a new Microsoft Installer package that contains your settings.
- **Microsoft Installer Transform file (MST):** Creates a Microsoft Installer Transform (.mst) file that contains your settings. An MST file must be used in conjunction with the original MSI package that is included in the DriveLock installation.
- **Command line:** Shows the Microsoft Installer command line options for implementing the settings you have selected.

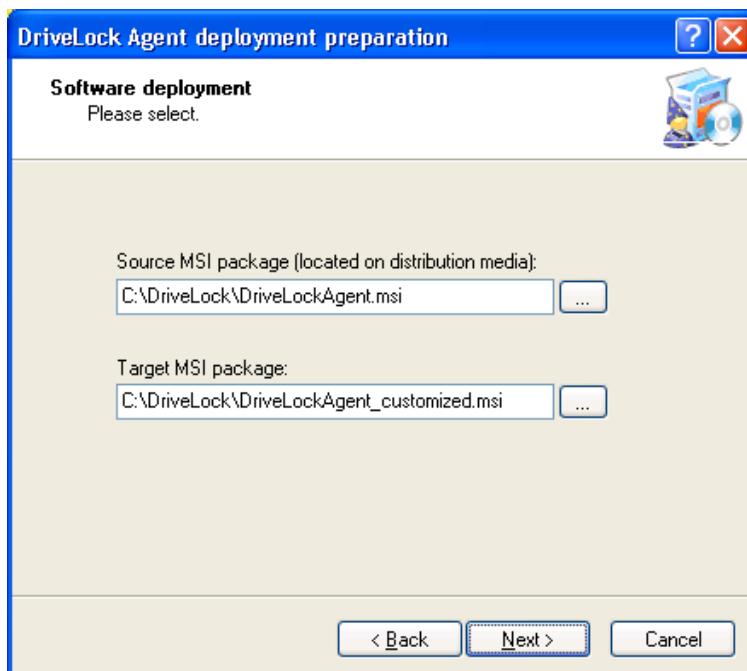


Click **Next**.

If you selected *Command Line*, the next page displays the command line you must use to install the DriveLock Agent. When using this command line, you must change “<DriveLockAgent.msi>” to the full path of DriveLockAgent.msi file.



If you selected the option to generate a new MSI file, you must provide the location and name of the original *DriveLockAgent.msi* file and the customized MSI file to be created.

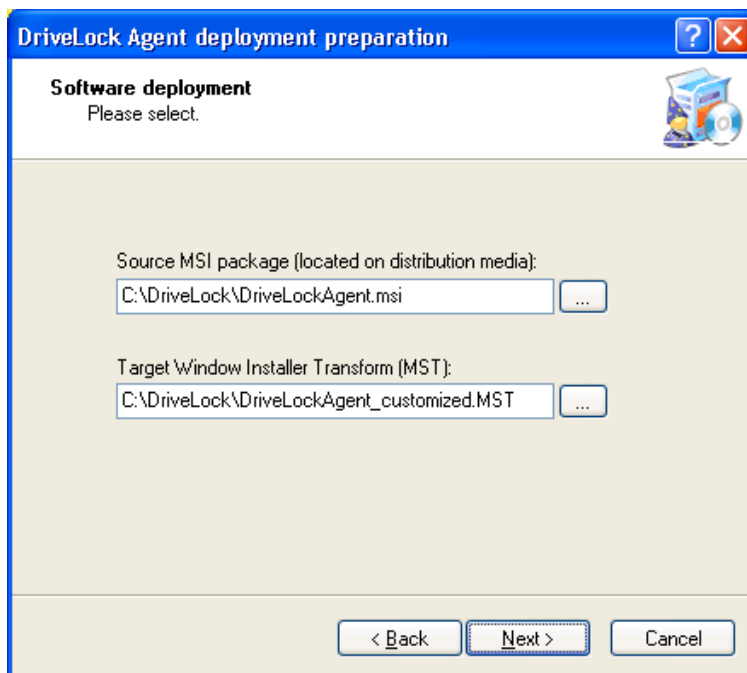


Type the name and location for both files, and then click **Next** to generate the new MSI file.



You can use the modified installer package you created to install an agent manually (see the section “Manual DriveLock Agent installation” of this manual for details) or for deployment using third-party deployment software.

If you want to generate a Microsoft Installer Transform (.mst) file you must provide the location and name original *DriveLockAgent.msi* file and the MST file.



Type the name and location for both files, and then click **Next** to generate the new MST file.

After you have completed the Agent Deployment Wizard you continue the deployment by using the command line.

### 3.3.2.2 Installation from a command prompt (silent installation)

If you install the Agent from a command prompt, you can specify additional options. The options allow you to specify from where the Agent will get its configuration settings and how this configuration is accessed.

To silently install the Agent without displaying the InstallShield Wizard and with the default configuration settings, use the following command:

```
Msiexec /i DriveLockAgent.msi /qn
```

If you must specify a configuration file location for the Agent, either use an installation package that has been modified by the wizard (.msi file), or use a wizard-generated command such as the following:

```
msiexec /i DriveLockAgent.msi /qn USECONFIGFILE=1
CONFIGFILE="\\fileserver\share\drivelock.cfg" USESVCACCT=1 SVCACCOUNT=domain\user
SVCPASSWORD="UCXUUZXY5LJLTJ2BAFPZTZ42JKBKPYCKCLVUXBEYYH2K6OZA"
```

The available options are:

<b>USECONFIGFILE=1</b>	Needed if you specify the location from where the Agent gets its configuration.
<b>CONFIGFILE="&lt;path&gt;"</b>	<p>&lt;path&gt; can be any valid UNC, FTP or HTTP path to the configuration file.</p> <p>Examples:</p> <p>UNC:    \\myserver\share\$\drivelock\dlconfig.cfg</p> <p>FTP:    myserver/pub/drivelock/dlconfig.cfg</p> <p>HTTP:   http://myserver/drivelock/dlconfig.cfg</p>
<b>CONFIGPROTOCOL=[0 1 2]</b>	<p>0: &lt;path&gt; is a file location</p> <p>1: &lt;path&gt; is an FTP location</p> <p>2: &lt;path&gt; is an HTTP location</p>
<b>USESVCACCT=1</b>	This parameter is needed if a user account is used to access the configuration file.
<b>SVCACCOUNT=&lt;account&gt;</b>	<p>Specifies the account that is used to access the configuration file.</p> <p>Example: SVCACCOUNT=mydomain\myuser)</p>
<b>SVCPASSWORD="&lt;encpwd&gt;"</b>	<encpwd> is the account's encrypted password that was created by the wizard.



To create the encrypted password, use the DriveLock Deployment Wizard.

You can also install DriveLock agents by using the original *DriveLockAgent.msi* in conjunction with a wizard-generated .mst file. The following command line installs the Agent on a computer using this method:

```
msiexec /i DriveLockagent.msi /qn TRANSFORMS=Your_MST_file.mst
```

### 3.3.3 Manual DriveLock Agent installation

Installing the DriveLock Agent manually on multiple computers is possible but not recommended because it can be time-consuming and increases the risk of making mistakes. You should use Group Policy or a third-party software deployment tool, such as Microsoft Systems Management Server (SMS) or NetInstall instead.

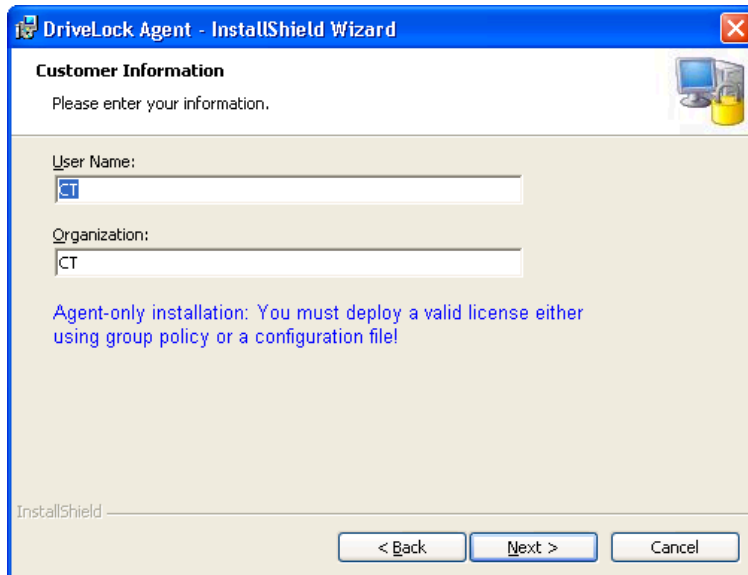
To start a manual installation, double-click the *DriveLockAgent.msi* file, and then follow the instructions in the InstallShield wizard.



The DriveLock Agent manual installation routine is available only in English.



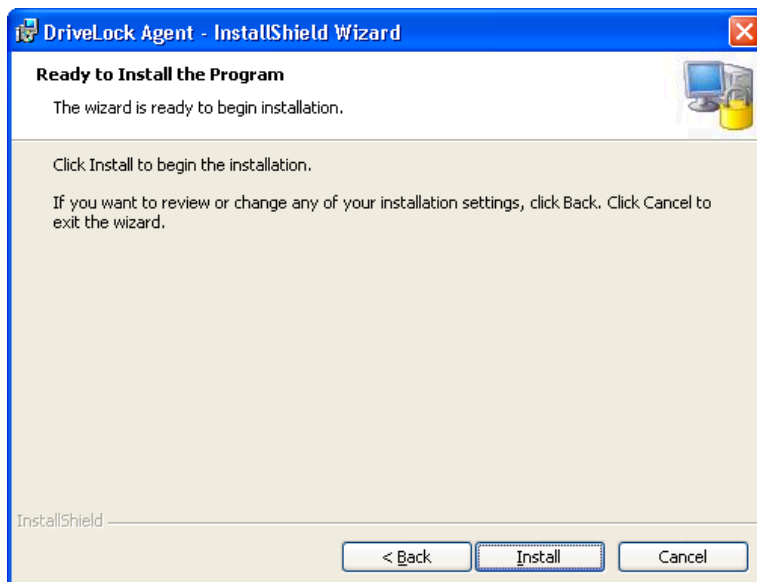
Click **Next**.



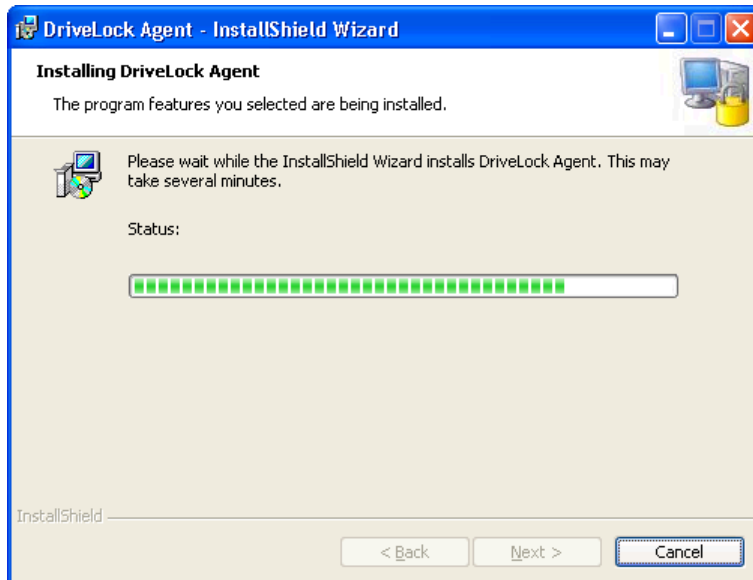
Type your name and company name, and then click **Next**.



In addition to installing the Agent, you need to deploy a valid license by using Group Policy or by using a DriveLock configuration file. For evaluating DriveLock you can use the trial license (AgentTrial.lic) that is located in the DriveLock installation folder on the computer where you installed the Management Console. (This license limits the use of Drivelock to 30 days from installation.)



Click **Install** to start the installation.



The installation normally takes 1 to 5 minutes, depending on your computer.



Click **Finish** to close the wizard.

Once the installation has completed, the *CenterTools DriveLock* service has been registered and is started. As the Agent has no user interface for configuration, you must deploy all configuration settings by using Group Policy or a configuration file.

## 3.4 Installing the DriveLock Management Console

You can configure DriveLock settings from any computer where the DriveLock Management Console is installed. The Agent does not need to be installed on this computer. You can also use the DriveLock MMC snap-in to create and edit Group Policy Objects, provided that you have the permissions required to edit a GPO.

To install only the DriveLock Management Console, follow the instructions in the section “Complete Installation” and select to not install a local Agent. When you install the Management Console without the Agent on a computer, the DriveLock service is not running and local drives and devices on the computer are not locked.

## 3.5 Updating DriveLock

CenterTools recommends that you update the DriveLock Management Console before updating the Agent. This enables you to make any required adjustments to your policy configuration before rolling out the updated Agent to client computers. Installing or updating the DriveLock Agent does not result in any changes to Group Policy Objects or configuration files.

To allow recovery from any unintended changes to existing configuration settings, export all local or Group Policy-based DriveLock policies to a file. For more information about exporting policies, see the chapter “Creating and Using a Local Configuration”.

### 3.5.1 Updating the Agent

Before installing an updated Agent by using Group Policy, select the existing GPO that you used for the initial deployment and add the new installation file (\*.MSI). After adding the installation file, on the Properties page of the software deployment policy, under “Updates” select the option “*Update existing packages*”. Then click **Add** and select the installation file for the previous version. Ensure that the default option “*Uninstall the existing package, then install the new package*” is selected.

If you install the new Agent by using a configuration file, follow the instructions in the chapter “Installing the Agent by using configuration files”. The installation process will detect if an older version of the Agent is installed and will update it automatically.



If you configured an uninstall password when you installed the previous version, you must provide this password for the update. Use the DriveLock Deployment Wizard to generate the encrypted version of this password.

### 3.5.2 Updating the Management Console

To update the Management Console, follow the instructions in the chapter “Installing the DriveLock Management Console”. The installation process detects if an older version of the Management Console is installed and will update it automatically.

## 3.6 Removing DriveLock

Unless you assigned DriveLock by using Group Policy, you can remove DriveLock from a computer by using the Add/Remove Programs application in Control Panel.

DriveLock Agents can also be uninstalled using the following command line, specifying the original installation package (.msi):

```
msiexec /x DriveLockagent.msi
```

If you have configured DriveLock to require a password for uninstalling, you must use the following command:

```
msiexec /x DriveLockagent.msi UNINSTPWD= encrypted-password
```



To create the encrypted password, use the DriveLock Deployment Wizard.



If you installed the DriveLock Agent by using Group Policy, you can't use the Add/Remove Programs application to uninstall DriveLock. Instead, remove DriveLock from the GPO to un-assign DriveLock from the computer. Alternatively, you can use the command line to uninstall DriveLock, but you have to ensure that there is no more GPO more that assigns DriveLock to the computer.

## 3.7 Installing and updating the DriveLock Security Reporting Center

The Security Reporting Center is the only component of the DriveLock product family that requires a central server. You can find Information about how to install, update and use the Security Reporting Center in the document “Security Reporting Center Manual”.

# 4 Deploying DriveLock Configuration Settings

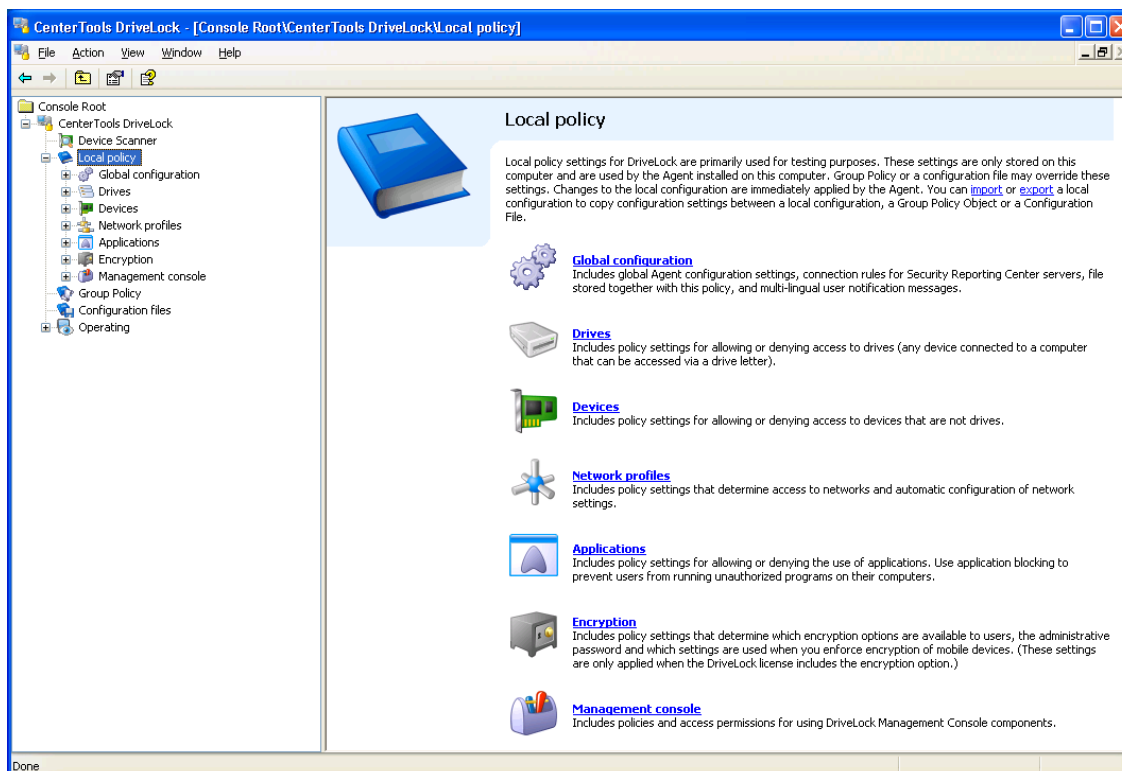
This chapter covers several methods for deploying configuration settings to client computers. You can also use the DriveLock Deployment Wizard, which is described the section “Generating installation parameters by using the Deployment Wizard”, to deploy configuration settings.



It is recommended that you become familiar with a local policy before you start deploying settings to multiple client computers in your network.

## 4.1 Creating and Using a Local Policy

To configure a standalone computer with the DriveLock Agent installed, use a local policy. This configuration is only applied to the computer on which you are running the DriveLock Management Console.

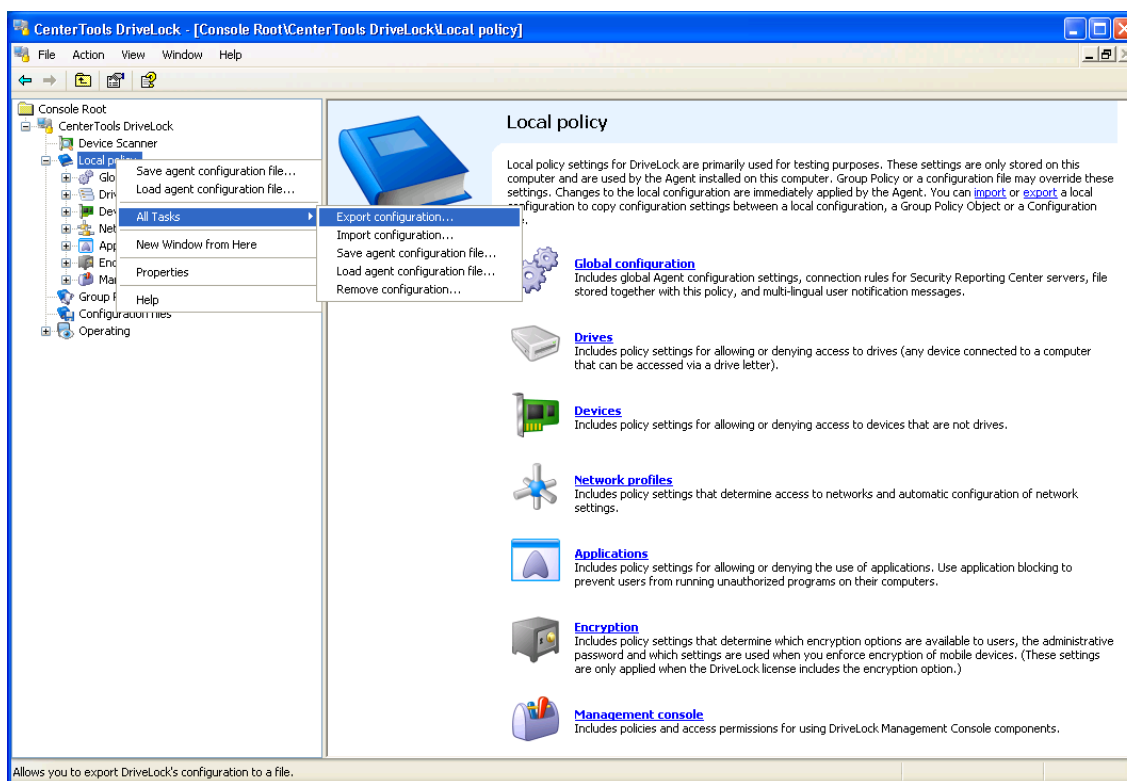


To access the local settings, in the DriveLock Management Console, in the console tree, select “*Local Policy*”.

You can configure global configuration settings, enable drive and device locking and create whitelists for drives or devices that you have identified on your computer by using the Device Scanner. Information about specific configuration settings can be found in the DriveLock Administration Guide.

A local policy can also be used to test a company-wide policy on a single computer before deploying it to the rest of the network. Once you are satisfied with your configuration, export the settings to a file, and then follow one of the following procedures (Export or Save).

To copy the local policy settings to a GPO you must first export the policy by performing the following steps.



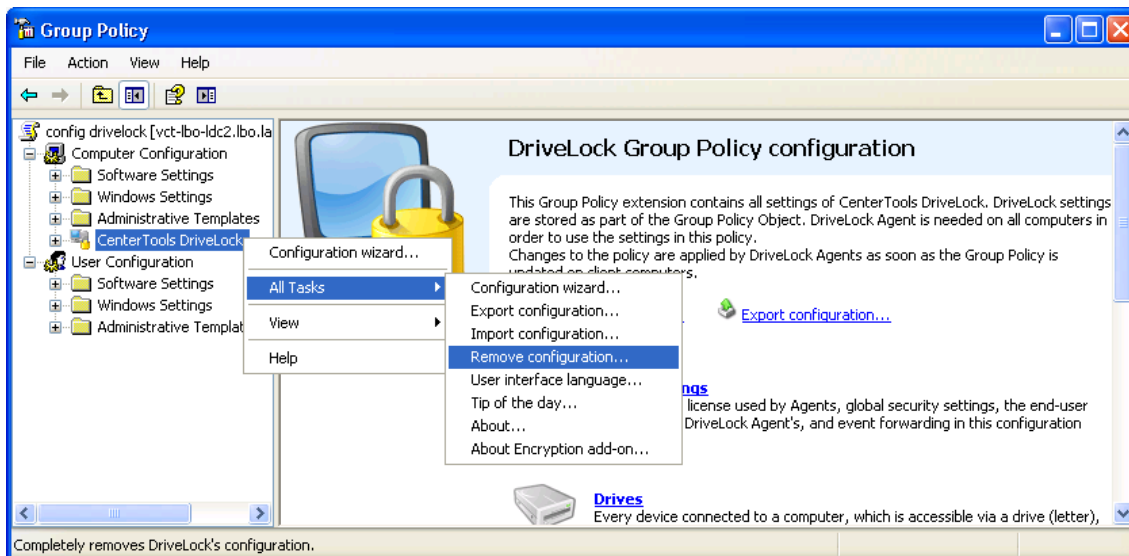
In the console tree, right-click **Local policy** and then click **All Tasks** → **Export configuration**. In the file selection dialog box, select the target directory and type the name of the export file. The configuration file has a .dlr extension.



To import the configuration, perform the following steps: Right-click **Local policy** and then click **All Tasks** → **Import configuration**. You can also export a policy from a GPO and import it into a local DriveLock policy. In addition, you can use the export procedure to back up your current configuration settings.

Selecting the option “*Save agent configuration file*” generates an Agent configuration file (.cfg). You can use the file to deploy a DriveLock configuration when you don’t want to use Group Policy or when you deploy DriveLock in a network without Active Directory.

To clear all configuration settings from an existing DriveLock policy, either local or GPO-based, perform the following procedure.

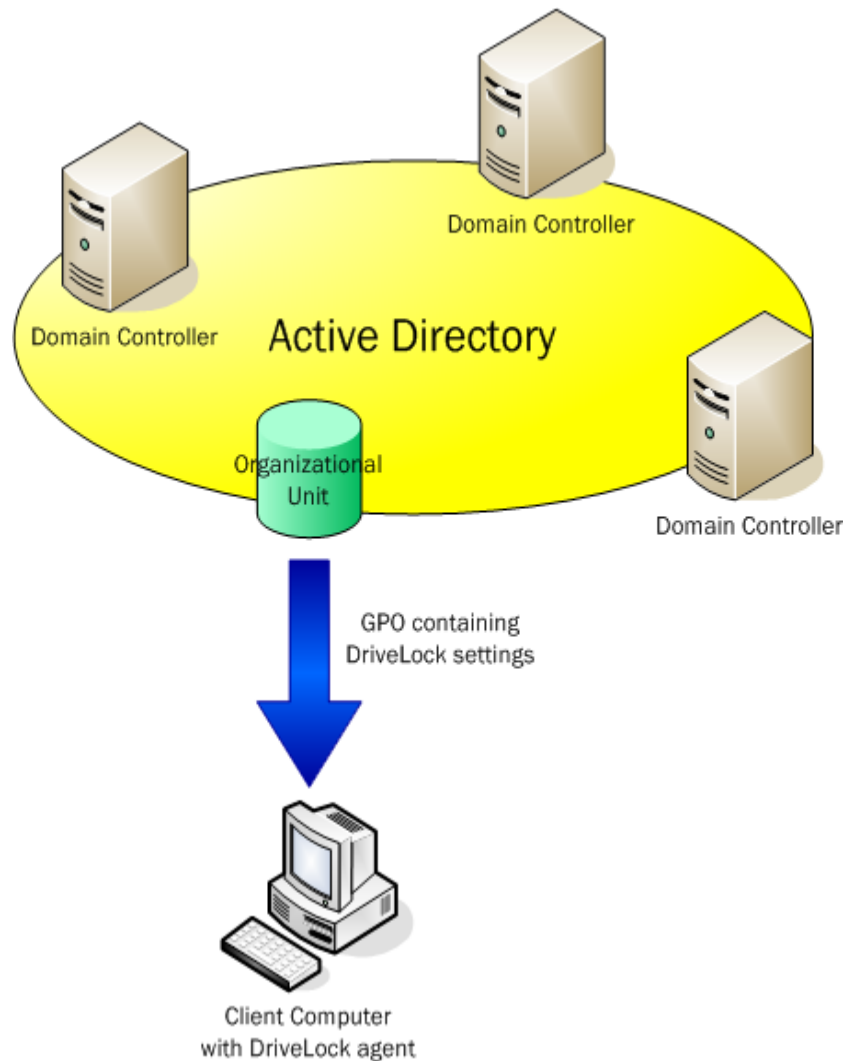


Right-click **CenterTools DriveLock** and then select *All Tasks* → *Remove configuration*.

## 4.2 Deploying Policies by Using Group Policy

The easiest way to configure the DriveLock Agent on multiple computers in a network is by using an Active Directory Group Policy. DriveLock can be configured by using the Group Policy Object Editor in conjunction with the DriveLock Microsoft Management Console (MMC) snap-in. This snap-in is automatically installed as part of the DriveLock installation.

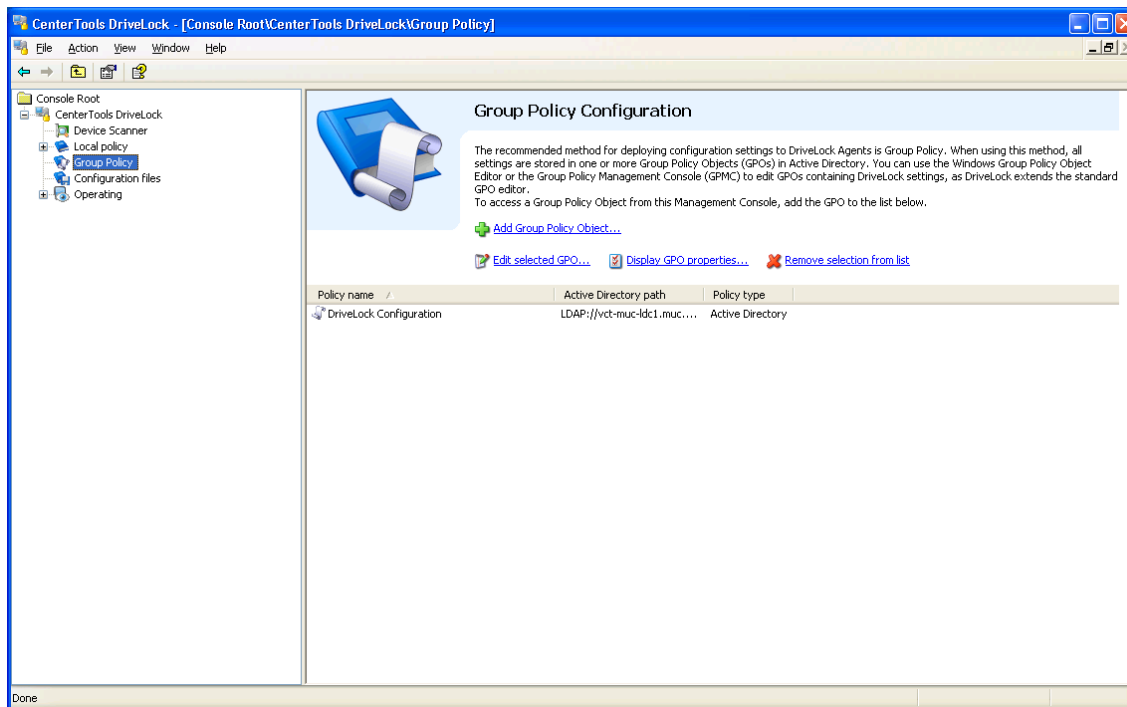
DriveLock can use Group Policy to deploy settings to computers that belong to an Active Directory domain. The DriveLock Agent running on these computers automatically applies all settings that are contained in the Group Policy Object.



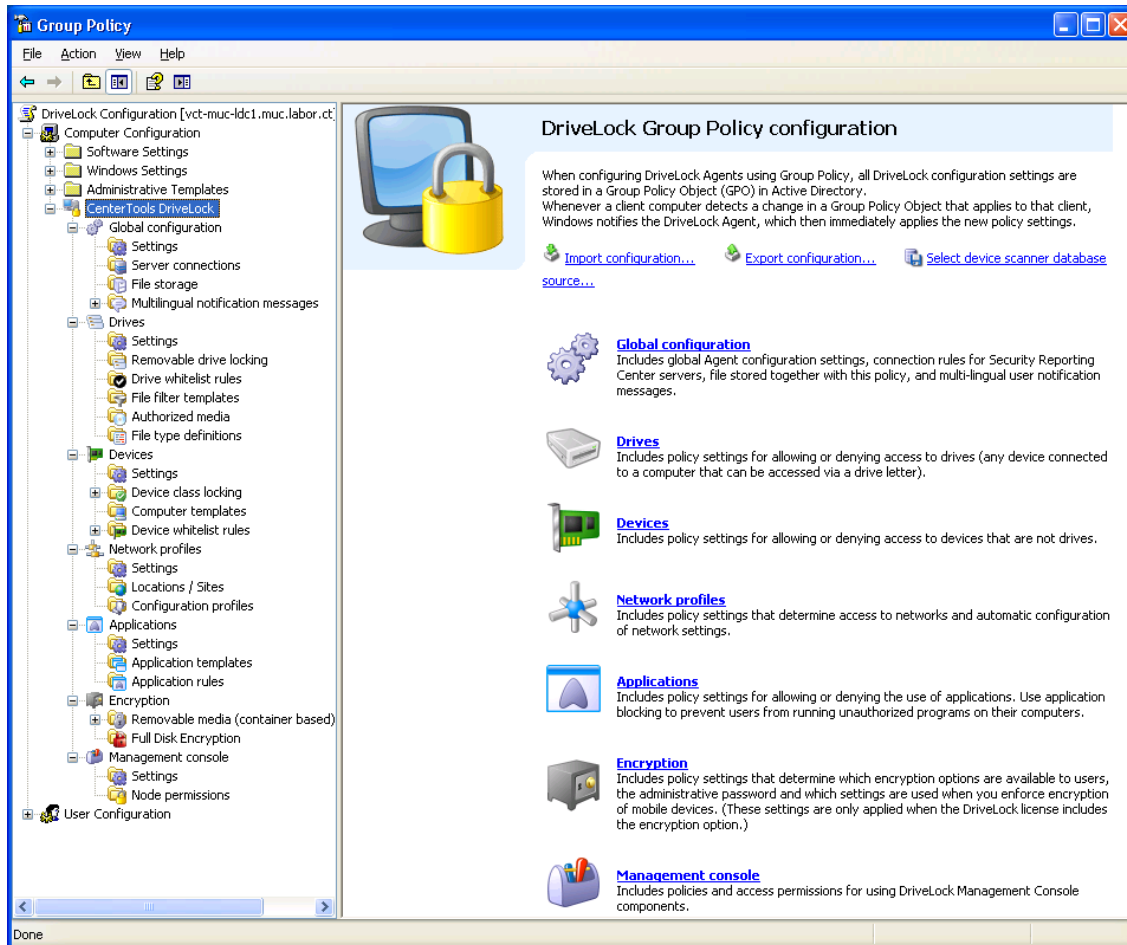
In Active Directory computers are often arranged in Organizational Units (OUs) to apply common settings to multiple computers. For example, an OU may contain all computers in a department or business unit. A DriveLock policy can be easily applied to all these computers by linking a Group Policy Objects containing DriveLock settings to the OU. Another reason to use OUs is delegation of administration tasks. Assigning GPOs to an OU instead of an entire domain or Active Directory site is a recommended practice because it allows you to maintain the appropriate protection level for each department or business unit. Because of these reasons, CenterTools recommends deploying DriveLock settings by using GPOs at the OU level.

The steps for configuring settings in a GPO are identical to those for configuring a local policy. You can configure the same parameters, create whitelists and configure networking settings.

To configure policy settings in the DriveLock Management Console, in the console tree, click *“Group Policy”*.



To add an existing GPO or create a new GPO that will contain DriveLock settings, in the console tree, click **Add Group Policy Object**. Next, select the GPO and then click **Edit selected GPO**. The Microsoft Group Policy Object Editor opens in a new window, allowing you to edit policy settings.



The Group Policy Object Editor displays the same DriveLock configuration items in the console tree that are available when you use a local configuration.

If you open the DriveLock policy on a Windows 2008 Server you will find the DriveLock configuration here:



The DriveLock Agent service applies configuration changes immediately after Windows receives updated Group Policy settings from a domain controller. Depending on the time until the next scheduled Group Policy update, it may take several minutes after you change the configuration until this update takes place. To apply changes to a GPO immediately, manually initiate a Group Policy update. To do this, on the client computer open a command prompt window and then type the following command:

```
gpupdate /force
```



You can find more information about how to use Group Policy to deploy a DriveLock configuration in the technical white paper "DriveLock Interaction with Active Directory", which is available on the DriveLock Web site ([www.drivelock.com](http://www.drivelock.com)). This white paper also contains replication traffic information and deployment tips.

## 4.3 Deploying Policies by Using Configuration Files

You can centrally install and configure DriveLock even in networks without Active Directory, such as networks using Novell NetWare. Since no Group Policy mechanism is available in such networks, you must distribute central DriveLock configuration settings by using a configuration file. This file can be placed on a central network drive (using a UNC path) or it can be accessed by using HTTP or FTP.

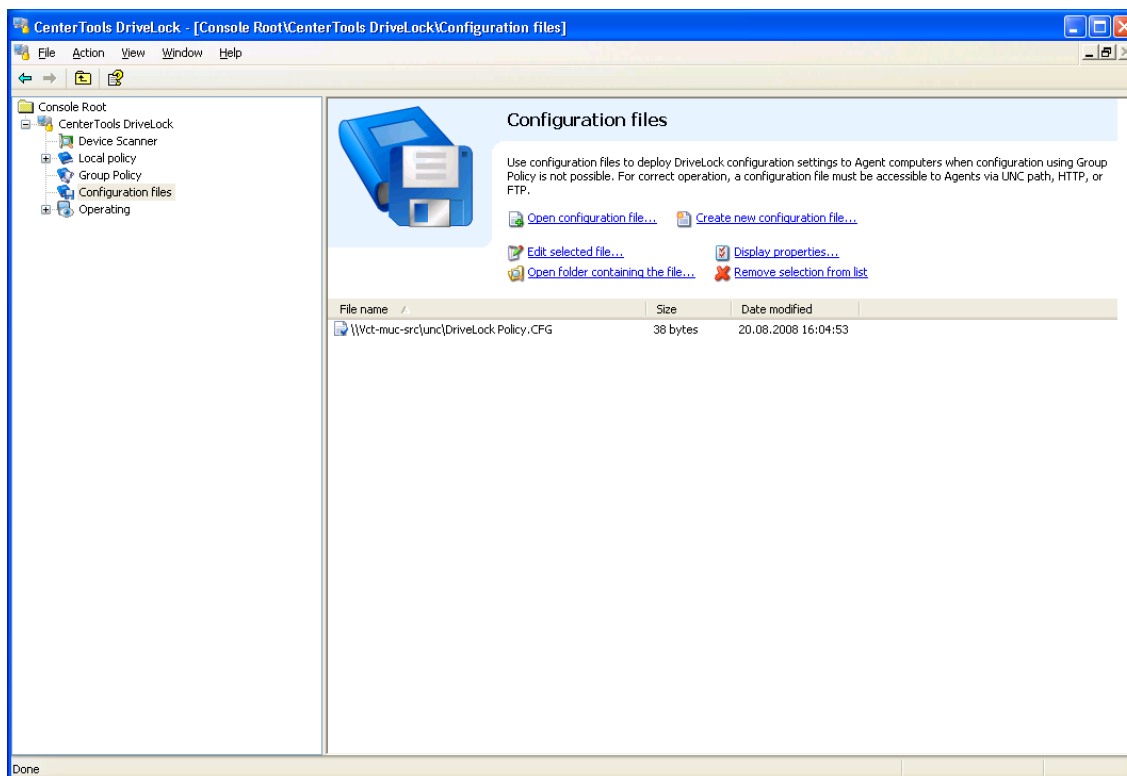
Using configuration files is similar to using Group Policy. However, user-specific configuration options are limited when Active Directory is not available as the central user database. You can still use local users or groups in your configuration settings. Also, you can use Novell eDirectory, if available.

You must configure the DriveLock Agent that you distribute to client computers to obtain its configuration settings from the configuration file. To facilitate this process, DriveLock contains a software distribution assistant that can create a customized MSI or MST file. This procedure is described in the section “Generating installation parameters by using the Deployment Wizard” of this manual.

You can find additional information about using DriveLock in a Novell network in the whitepaper “DriveLock – Interaction with Novell“, which you can download from the DriveLock Web site.

### 4.3.1 Creating a configuration file

Start the DriveLock Management Console (*Start → Programs → CenterTools DriveLock → DriveLock Configuration*).



In the console tree, click “*Configuration files*”, and then in the right pane click **Create new Configuration file**. DriveLock prompts you to provide the name and location of the new configuration file and then opens a new DriveLock Management Console window where you can configure the policy settings.



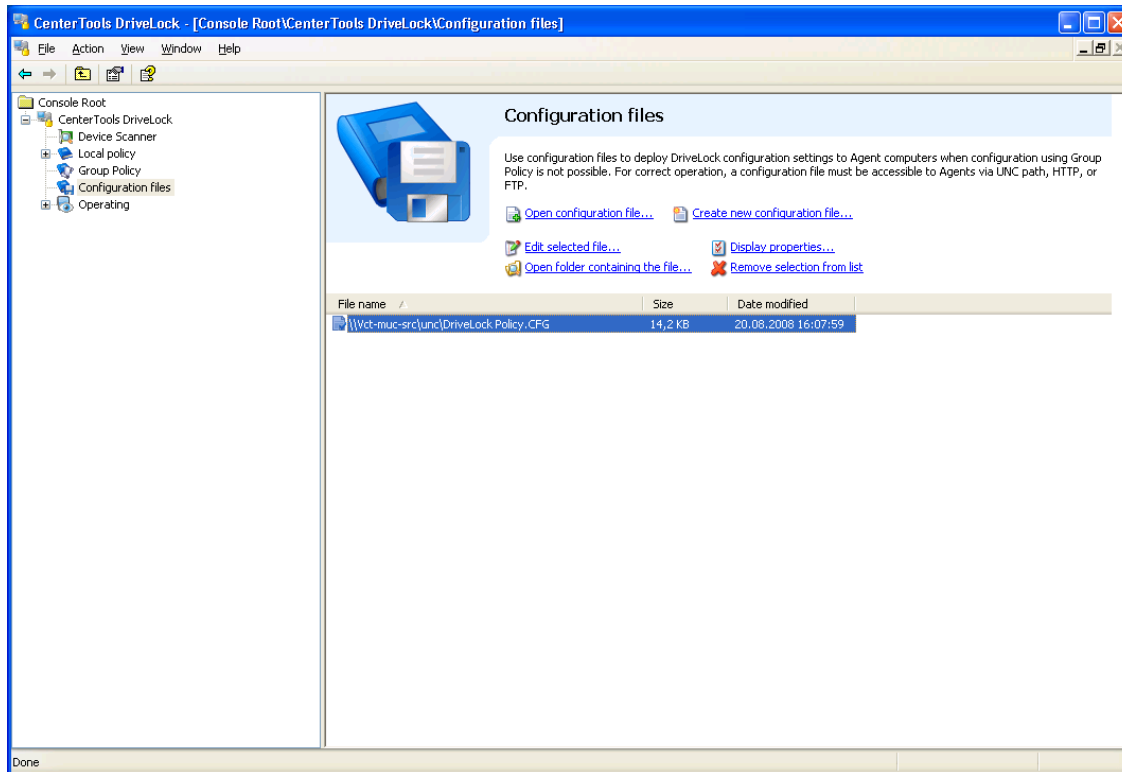
Remember to enter your license information under Global settings (as described in the DriveLock Administration Guide).



You can transfer settings between a Group Policy Object and a local configuration by using the *Import configuration* and *Export configuration* commands.

### 4.3.2 Editing a configuration file

To edit an existing configuration file, select “*Configuration files*” in the console tree, and then in the right pane click **Open Configuration file**. In the dialog box, type the file name and location and then click **Open**. The configuration file will appear in the right pane.



Select the file, and then click **Edit selected file** to open a new DriveLock Management Console window.



The DriveLock Management Console window saves changes you make to a configuration file automatically when you close the window.

When you have finished editing your configuration, close the window. To save the file using a different name, right-click the top node in the console tree, and then click **Save as**.

Once the changes are complete, apply the configuration to client computers by copying the configuration file to the network location from which clients retrieve their policy settings, replacing the old configuration file with the new one.

### 4.3.3 Deploying a configuration manually

The DriveLock Agent can retrieve configuration files using any of the following methods:

- **UNC:** For example “\\myserver\share\$\drivelock\dlconfig.cfg”
- **FTP:** For example “myserver/pub/drivelock/dlconfig.cfg”
- **HTTP:** For example “http://myserver/drivelock/dlconfig.cfg”

In environments without Active Directory (such as Novell NetWare) you must specify the location of the configuration file during the Agent installation (as described in the section “Installing the Agent by using configuration files” in this manual) or by using the DriveLock service command line interface.



You should create an initial configuration file prior to the Agent rollout and then specify the location of the configuration file during setup by using the command line or a modified installation file.

The DriveLock Agent reads the configuration file during installation and then starts enforcing the policies in this file.



When you use configuration files, the Agent only checks for changes to the configuration file when the DriveLock Agent service starts or at an interval that you can configure.

If you can't specify the location of the configuration file during the Agent installation, use the following steps to specify the location after the installation is complete.

- Install the DriveLock Agent on the client computers or deploy the Agent using third-party deployment software, such as Novell Zen Works.
- Switch the Agent mode to use a configuration file instead of a Group Policy, using the method described following this procedure. The configuration file will be loaded by the Agent the next time the service starts.
- Ensure that the Agent can load the configuration file when the service starts. If the Agent encounters errors in loading the configuration file, it records these in the Application Event Log using Event-ID 119.

To configure the location of the configuration file, open a command prompt window, and then run the following command from the directory where you installed DriveLock:

```
drivelock -setconfigfile <file-path>;<protocol>
```

To specify a UNC or local path, use 0 as the value for <protocol>, for an FTP location use 1, for an HTTP location use 2.



Do not use quotes (") around the file path, even when the path includes spaces.

To reset your configuration to the default, use the following command:

```
drivelock -removeconfigfile
```

To change the DriveLock Agent service account, type the following command:

```
drivelock -setserviceaccount <account>;<encrypted-password>
```

The account name must be typed in the format "domain\user" if you specify a domain account. The password is an encrypted password string.



To create the encrypted password, use the DriveLock Deployment Wizard. Specifying an unencrypted password will not work correctly, as the Agent requires that the password is encrypted.

To remove the service account information from the DriveLock configuration, type the following command:

```
drivelock -removeserviceaccount
```

The following commands are examples for configuring DriveLock from the command line:

```
drivelock -setconfigfile c:\program files\myfile\dl.cfg;0
drivelock -setconfigfile \\server\mypath\dl.cfg;0
drivelock -setconfigfile myftpserver/pub/dlconfig/dl.cfg;1
drivelock -setconfigfile http://myserver/dlconfig/dl.cfg;2
drivelock -setserviceaccount mydomain\myuser;"UONESVHZ3LIYXJ3YA
5VJT6E2PCB3RAQOOWRCZRPZSK6OACDEJHDFR72EO4O4GVPCFL5LVUNOTJH5JTI22GU5P6V6TTHQKSKXY7
6LFVYOZFH4GJNA"
```