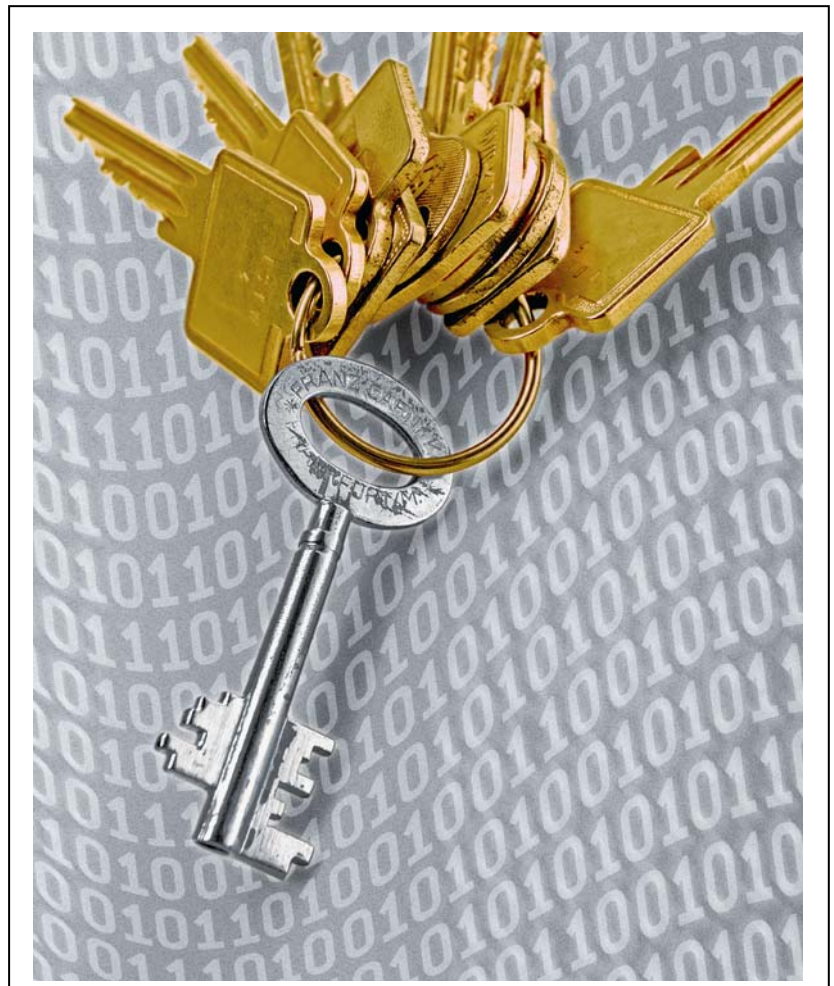




DriveLock 5.5

Encryption Guide



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

0	About This DriveLock Documentation	5
0.1	Content	5
0.2	Document Conventions	6
1	How DriveLock Encryption Works.....	7
1.1	DriveLock Encryption Algorithms.....	7
1.2	DriveLock Encryption Modes	8
2	Configuring DriveLock Encryption	10
2.1	Configuring Global Parameters.....	11
2.1.1	Encryption strength settings.....	12
2.1.2	Encryption end-user appearance	17
2.1.3	Encrypted drive settings.....	21
2.1.4	End-user restrictions	26
2.2	Configuring an Administrative Password	27
2.3	Configuring Encryption Enforcement	30
3	Managing Encrypted Drives	34
3.1	Encrypted Drives History	35
3.2	Creating an Encrypted Drive	36
3.2.1	Using the Create encrypted drive wizard	36
3.3	Connecting Encrypted Drives.....	44
3.3.1	Connecting an encrypted drive that is based on a container file	46
3.3.2	Connecting an encrypted drive that is based on a partition.....	48
3.3.3	Disconnecting an encrypted drive	50
3.4	Changing a Password	53
3.5	Deleting Encrypted Containers.....	57
4	The Mobile Encryption Application.....	59

4.1	Copying the Mobile Encryption Application.....	59
4.2	Using the Mobile Encryption Application.....	61
5	Creating an encrypted CD /DVD.....	65
6	Securely Deleting Data.....	72

0 About This DriveLock Documentation

0.1 Content

This manual contains information about all DriveLock encryption functions, except for the full disk encryption, which is covered in the document “DriveLock Full Disk Encryption”. The first part of this document is intended for administrators who need to configure encryption; the other chapters instruct users how to use encryption.

- Chapter 1 presents an overview on how data encryption works.
- Chapter 2 explains the configuration parameters and is relevant to administrators only.
- Chapter 3 contains information on how to create, maintain and delete encrypted volumes.
- The Mobile Encryption Application is described in Chapter 4
- Chapter 5 describes how to create an encrypted CD or DVD
- Chapter 6 explains how to securely delete data.

Information about how to install DriveLock and how to deploy your configuration settings can be found in the document “DriveLock Planning – Installation – Deployment”.




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”.

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

More information about DriveLock (such as video tutorials, white papers and other documentation) can be found on the DriveLock Web site (www.drivelock.com).

0.2 Document Conventions

Throughout this document the following conventions and symbols are used to emphasis important issues that you should read carefully or menus, items or buttons you have to click on or select.

	<p>Caution: 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>Hint: Useful additional information that might help you save time.</p>
	<p>Information: Additional information about the current topic</p>
<p><i>italics</i></p>	<p>Italics represent fields, menu commands and cross-references.</p>
<pre>C:\>command</pre>	<p>A fixed-width typeface represents messages or commands typed at a command prompt.</p>
<p>Cancel</p>	<p>Bold type 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 How DriveLock Encryption Works

DriveLock has advanced encryption capabilities that allow you to encrypt sensitive information easily, quickly and securely. You can create and manage encrypted drives that consist of container files (encrypted archives) or encrypt an entire disk partition. Access to encrypted drives is secured by passwords. Each encrypted drive has can be accessed by typing a use password that is unique to the drive. In addition, a centrally configured administrative password enables data recovery, providing access to the data when a user's password is not available.

Encryption converts data to a format that makes it appear like random data to anyone who does not have the password that's required to decrypt the data. When you create an encrypted drive, all files and all empty space on that drive is encrypted. The encryption algorithm you select when you create the drive determines how data on it is encrypted.

1.1 DriveLock Encryption Algorithms

DriveLock supports the following encryption algorithms:

- **AES** - The Advanced Encryption Standard (AES) is a symmetric encryption mechanism that was chosen by the National Institute of Standards (NIST) as successor to DES and 3DES in October 2000. It is also called the *Rijndael* algorithm for its developers Joan Daemen and Vincent Rijmen.
- **Triple DES** - Triple DES (3DES) is a symmetric encryption method based on the older DES (Data Encryption Standard) but works with twice the key length (112 bit) of its predecessor. Data is encrypted using three successive DES operations. Because of the key length, 3DES is regarded as a relatively safe method for encrypting most data, unlike DES, which is more susceptible to brute-force attacks.
- **Blowfish** - This is a fast algorithm offering exceptional performance, especially on 32-bit-systems. One advantage of Blowfish is its variable key length (32 to 448 bits). Blowfish was first introduced in 1994 and is considered very secure.
- **Twofish** - Twofish is the entry in the AES competition by Counterpane Systems (the company of renowned cryptography expert Bruce Schneier). This algorithm uses a block size of 128 bits and can utilize key lengths from 128 to 256 bits. Twofish is extremely fast: on a Pentium-class CPU each byte is encrypted using only 18 CPU cycles. Twofish has been tested extensively without finding any weaknesses.

- **CAST 5** - CAST is a symmetric block cipher with a block length of 64 bits and a key length from 40 to 128 bits. The CAST algorithm is named after its developers and a patent application for it was filed in 1996. Because of its higher speed compared to DES, CAST is well-suited for real time applications. When used with key lengths from 80 to 128 bit, the algorithm is referred to as CAST 5.
- **Serpent** - Serpent is a symmetric key block cipher that was a finalist in the Advanced Encryption Standard (AES) contest, where it came in second to Rijndael. Serpent was designed by Ross Anderson, Eli Biham, and Lars Knudsen. Like other AES submissions, Serpent has a block size of 128 bits and supports a key size of 128, 192 or 256 bits. Serpent was widely viewed as taking a more conservative approach to security than the other AES finalists, opting for a larger security margin. The Serpent cipher has not been patented. It is completely in the public domain and can be freely used by anyone without restrictions.

DriveLock doesn't store passwords. Instead it calculates a unique value (hash) that allows it to determine whether the password you type to access an encrypted drive is correct. DriveLock can use the following hash algorithms to perform this calculation:

- **SHA-1** - This algorithm was developed by NIST (*National Institute of Standards and Technology*) in cooperation with the NSA (*National Security Agency*) as the secure signing hash function of the digital signature algorithm (DSA) for the Digital Signature Standard (DSS). Published in 1994, Secure Hash Standard (SHS) specifies a secure hash-algorithm (SHA) with a hash value of 160 bits for messages with a size of up to 2^{64} bits. SHA is similar to the MD4 algorithm developed by Ronald L. Rivest. Initially, SHA existed in two versions, SHA-0 and SHA-1, differing from each other in the number of cycles used for generation of the hash value. Today only SHA-1 is used.
- **RIPEMD-160** - RIPEMD-160 was developed by Hans Dobbertin, Antoon Bosselaers and Bart Preneel and published 1996. It is an improved version of RIPEMD (based on MD4) and comparable to SHA-1 in security and speed. This algorithm is less likely to contain security holes because its development process was more open than that of SHA-1.
- **WHIRLPOOL** - Whirlpool is a cryptographic hash function designed by Vincent Rijmen (co-creator of the Advanced Encryption Standard) and Paulo S. L. M. Barreto. The hash has been recommended by the NESSIE project. It has also been adopted by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as part of the joint ISO/IEC 10118-3 international standard.

1.2 DriveLock Encryption Modes

With DriveLock you can create two types of encrypted drives:

- Drives that are physically represented as a container file.

- Drives that map to an entire existing drive partition.

A DriveLock container file has a DLV extension. You can save a container file on all types of storage devices or on a network share. To use a container, DriveLock mounts it and assigns it a pre-defined or user-selected drive letter, so you can use it like any other drive in Windows.

A DriveLock partition is a normal drive partition that has been completely encrypted by DriveLock. You can encrypt any partition, including floppy disks, ZIP drives, USB or Firewire-connected hard disks, USB flash drives and other mass storage devices.



Certain storage media don't allow the creation of an encrypted partition. If you encounter such a drive, contact the manufacturer for more information.

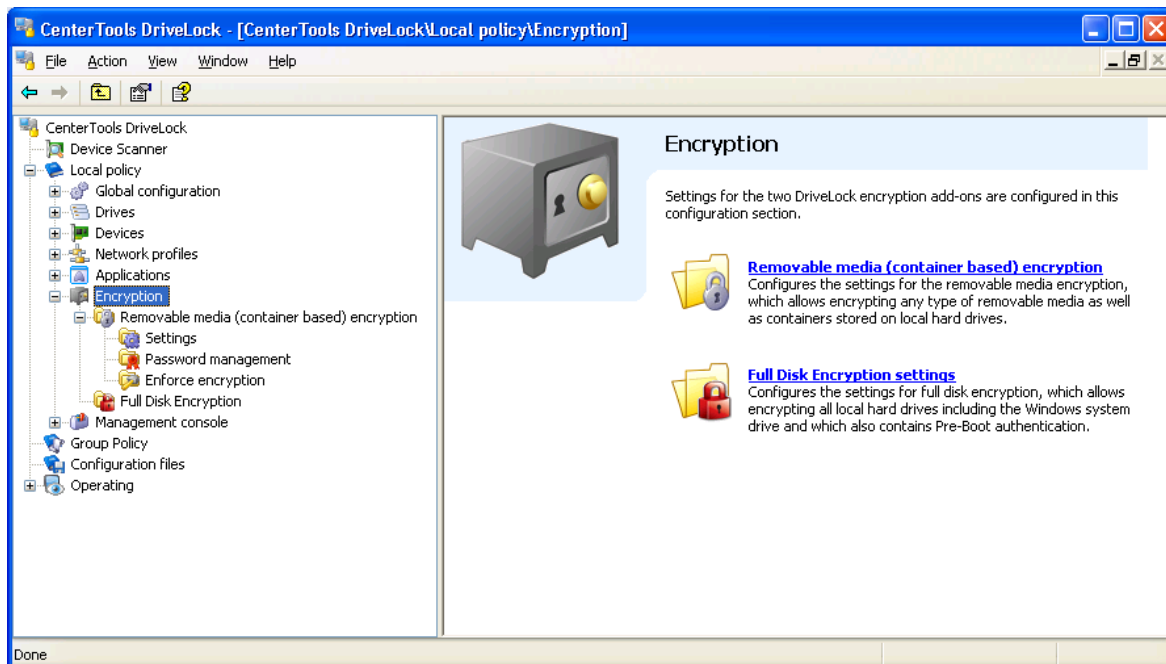


Local drives cannot be encrypted using the methods described here. To encrypt a local drive, use DriveLock Full Disk Encryption instead.

2 Configuring DriveLock Encryption

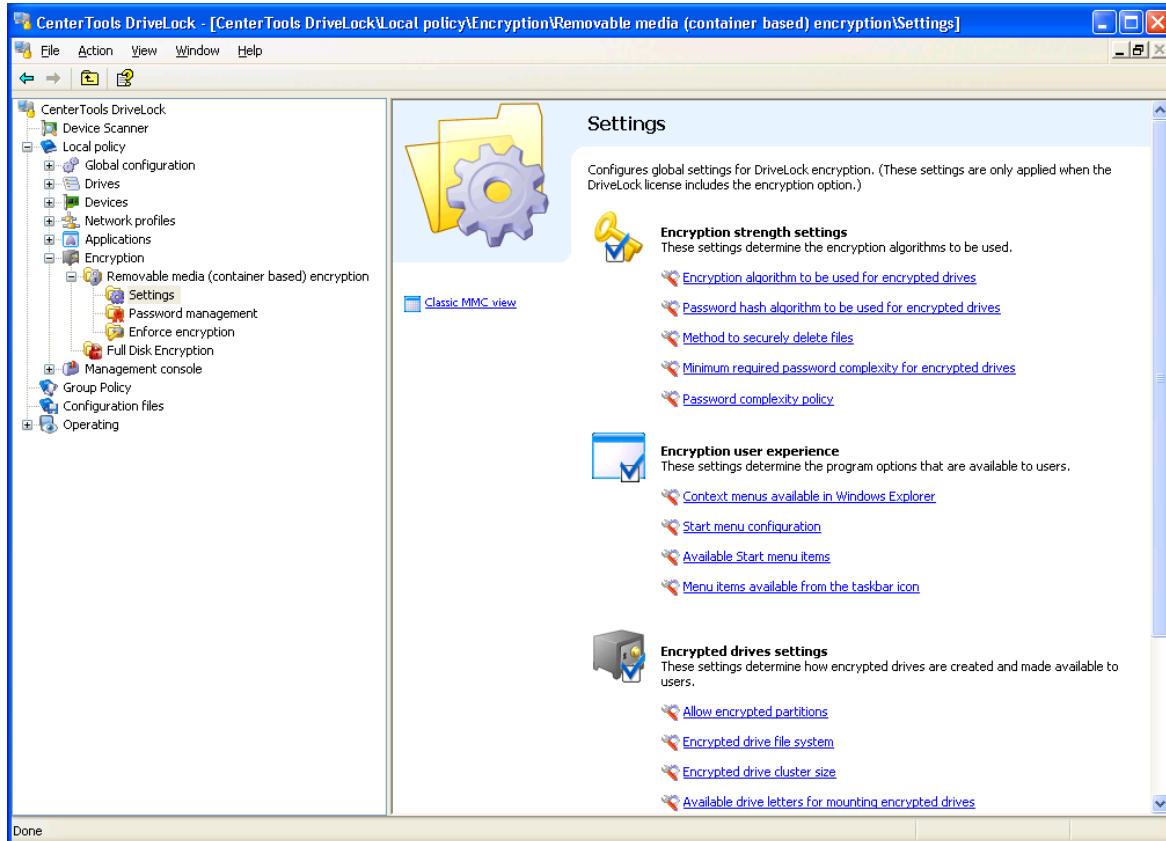
Before you can use DriveLock container-based encryption, an administrator must configure some general encryption parameters.

Click **Encryption** and then **Removable Media Encryption (Container Based)** to display the encryption configuration page.



2.1 Configuring Global Parameters

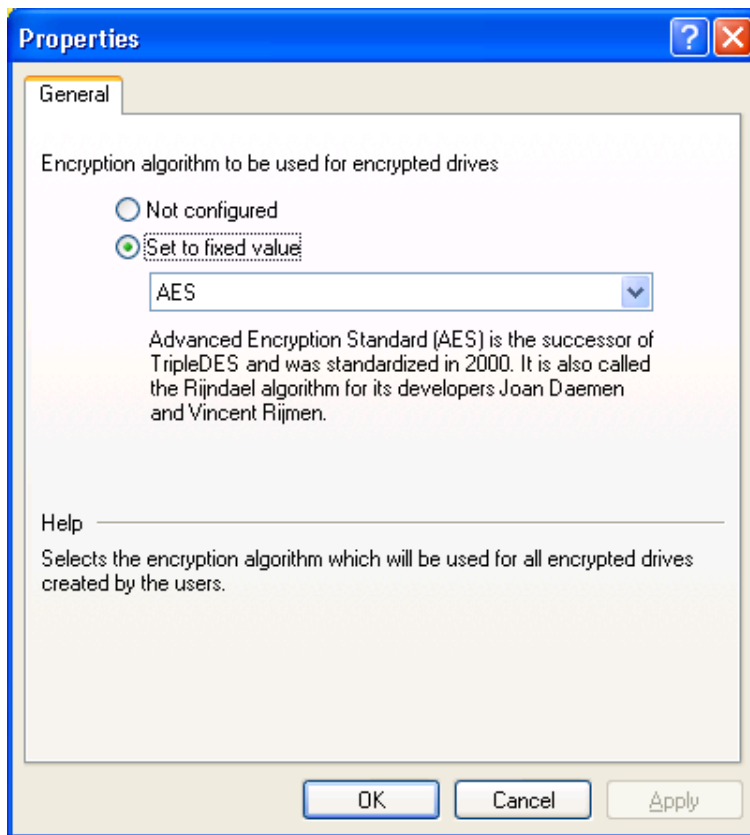
Click Settings to configure global parameters for encryption.



2.1.1 Encryption strength settings

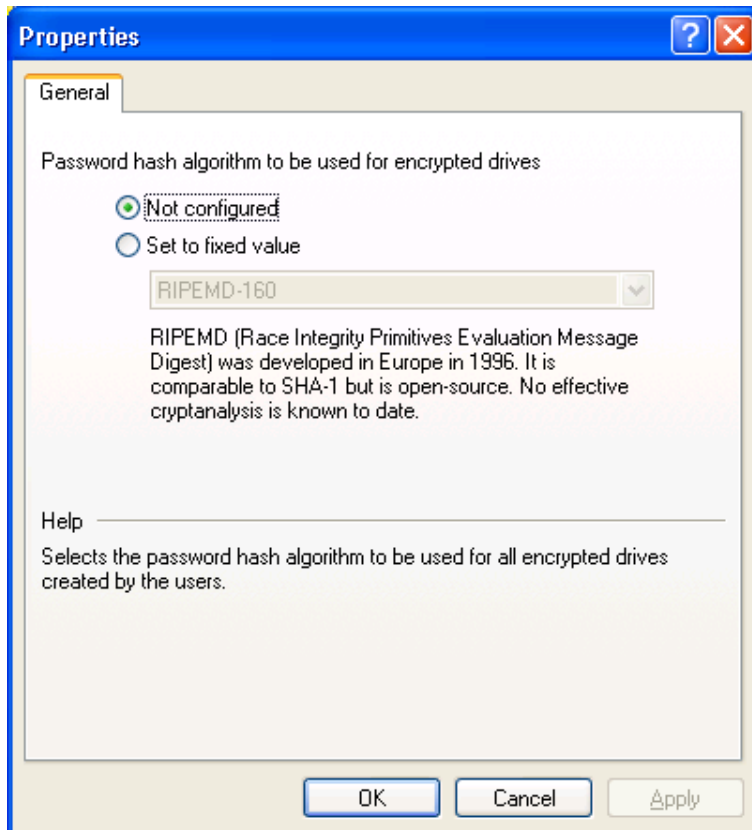
2.1.1.1 Encryption algorithms

Select the encryption algorithm to be used. The available algorithms are described at the beginning of this document.



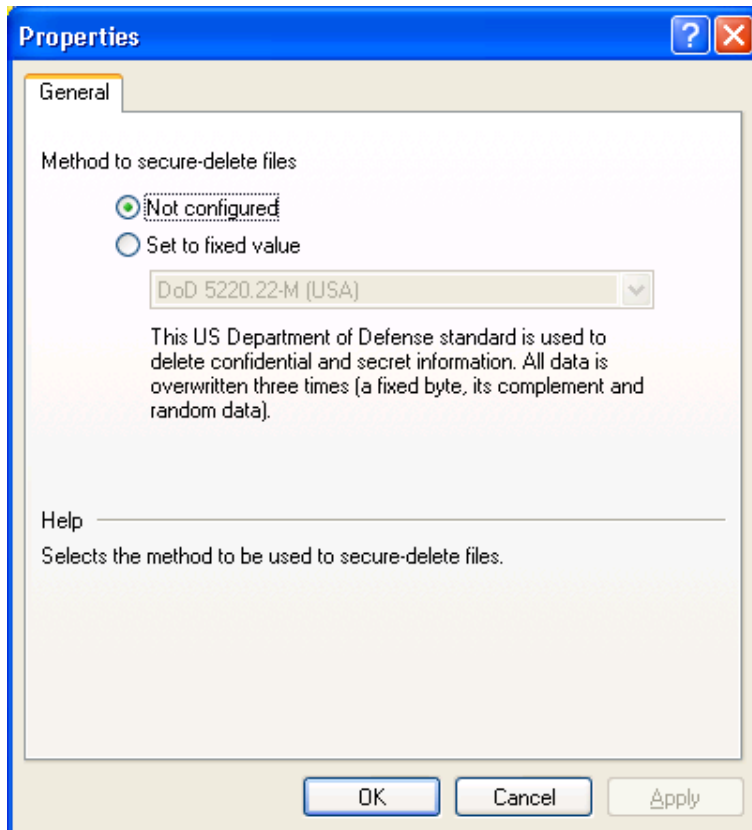
2.1.1.2 Hash algorithms

Select the hashing algorithm to be used. The available algorithms are described at the beginning of this document.



2.1.1.3 Method to secure-delete files

Select the algorithm to be used for securely deleting files. The available algorithms are described in the chapter “Securely Deleting Data”.



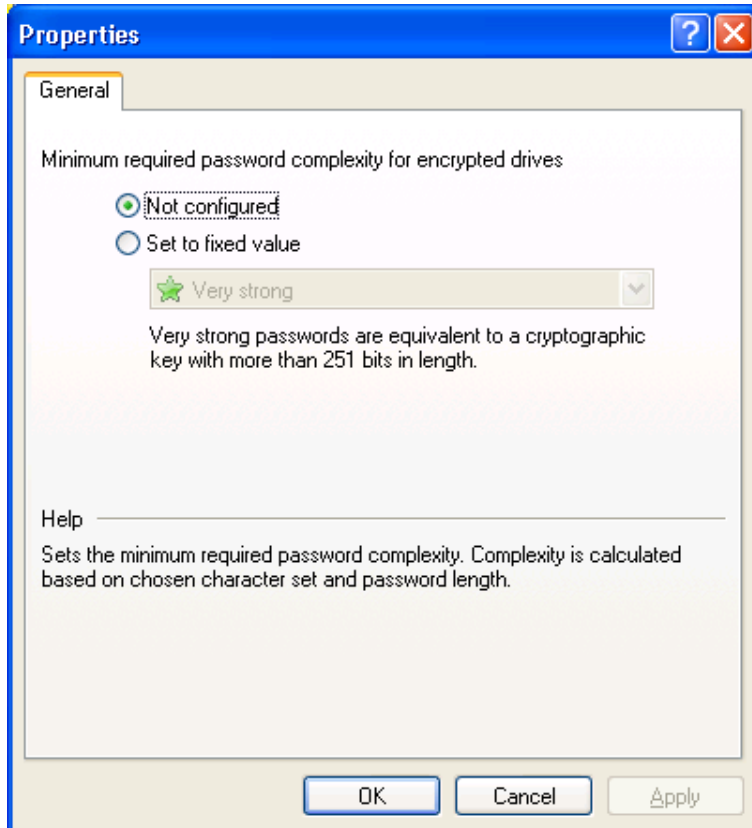
2.1.1.4 Minimum required password complexity for encrypted drives

To ensure that users select secure passwords, you should define the minimum complexity that is required for these passwords. This complexity requirement should match your organization’s guidelines for data security. The password complexity is dynamically calculated based on the characters used in the password and the password length.

If you want to configure your own password complexity policy, select “*Use password policy*” and then configure a custom policy (see the section “Password complexity policy” for more information).

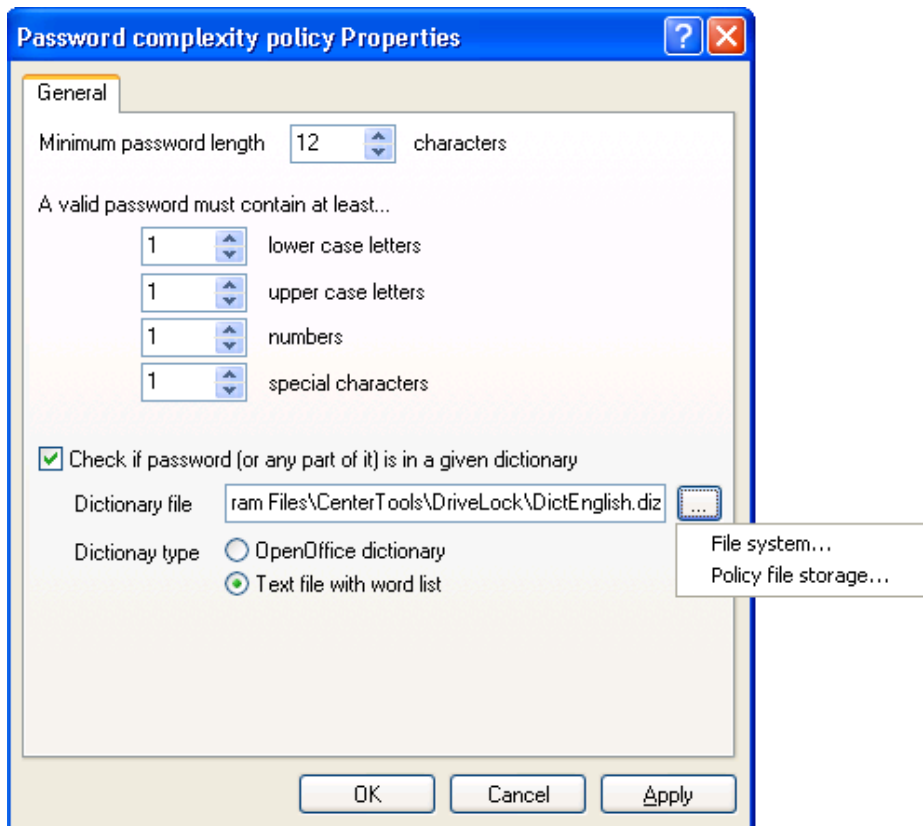


Password complexity policy can only be enforced by Agents Version 5.5 or higher !



2.1.1.5 Password complexity policy

A password complexity policy contains all requirements that a user password must meet when it is created. This includes the minimum number of characters and the number of special characters or numbers it must contain. DriveLock can also prevent users from creating a password that exists in a dictionary you specify (password dictionary validation).



A dictionary can be a dictionary file in the OpenOffice format or a text file that contains one single word on each line. DriveLock includes OpenOffice dictionaries for English, German, Dutch and French. You can find these .diz-files in the DriveLock installation folder on the administration computer where you installed the DriveLock Management Console (for example “*DictEnglish.diz*”).



If you specify a custom file, ensure that this file exists on all Agent computers in exactly the same location, as the Agents looks for this file in the location you specify.

You can also place dictionary files into the policy file storage and select “*Policy file storage...*” as the dictionary location. Files located in the policy file storage are identified by an asterisk (“*”) in front of the file name and are copied to the client automatically. For more information about the policy file storage, see the corresponding chapter in the document “DriveLock Administration Guide”

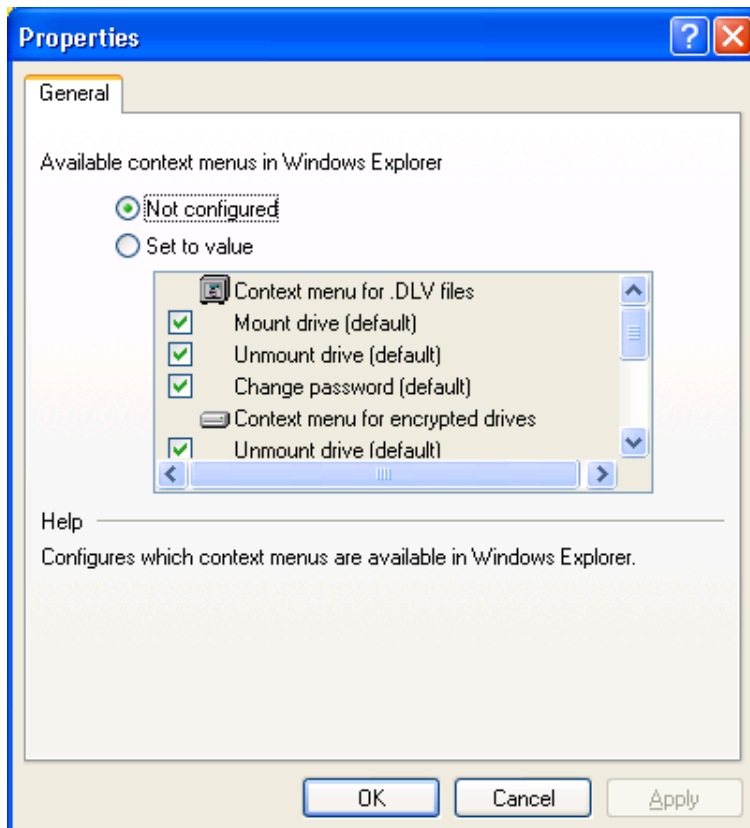


When you use a dictionary to validate your passwords, keep in mind that passwords containing any part of a word contained in the dictionary are not allowed (for example if the dictionary contains “it”, passwords such as “hit”, “with” or “glitter” are not allowed).

2.1.2 Encryption end-user appearance

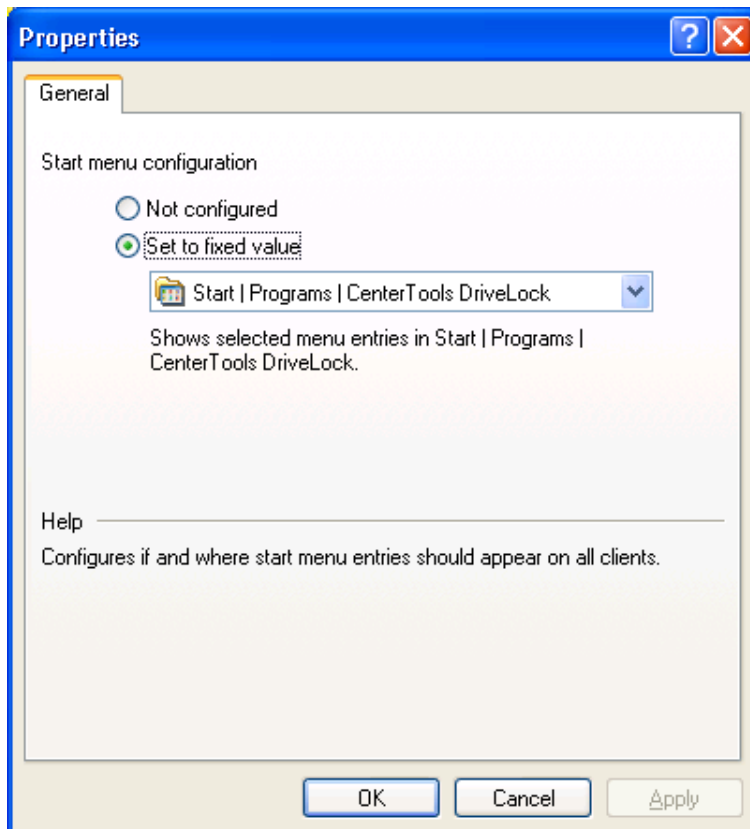
2.1.2.1 Context menus available in Windows Explorer

These settings determine which commands are displayed to users in the context menus that appear when a user right-clicks an encrypted drive or container file in Windows Explorer. When this option is set to “Not configured”, all available commands are displayed.



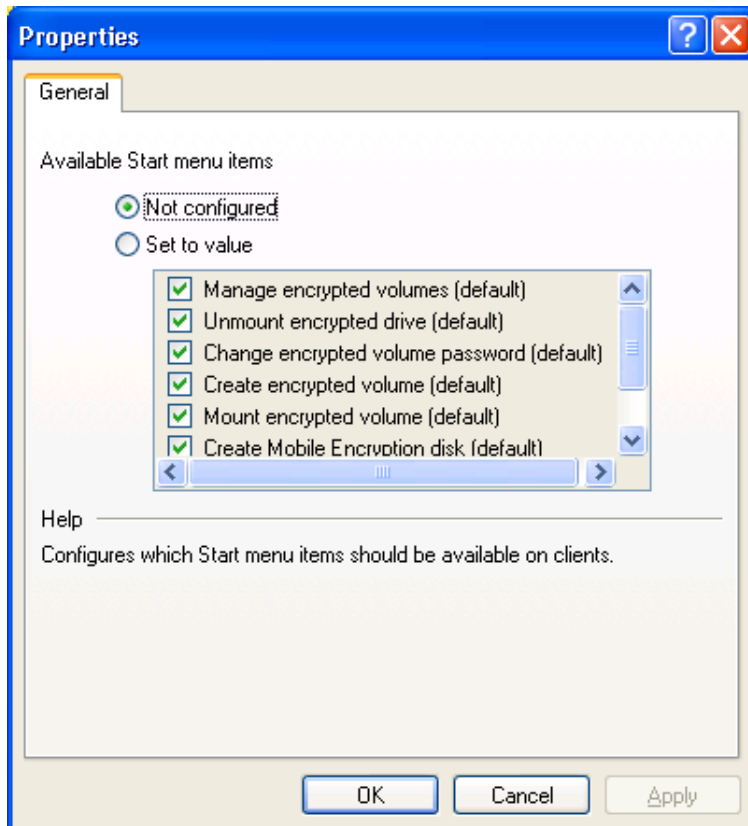
2.1.2.2 Start menu configuration

You can configure whether DriveLock commands are available from the Start menu and how they are arranged. When this option is set to “Not configured”, the commands can be accessed from the default location “Start – Programs – CenterTools DriveLock”.



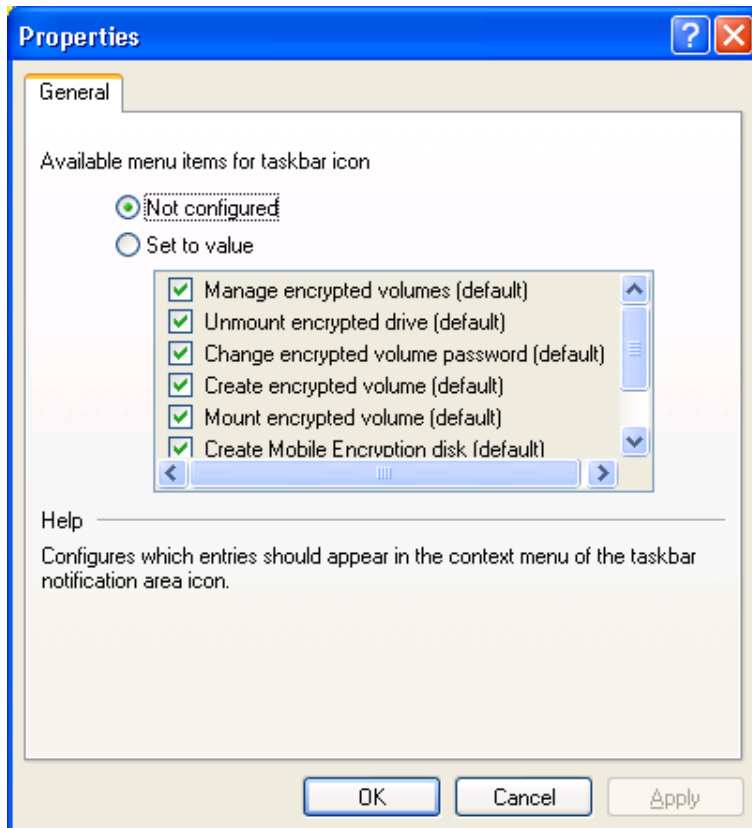
2.1.2.3 Available Start menu items

This option defines which commands are available from the Start menu. When this option is set to “Not configured”, all commands appear in the Start menu.



2.1.2.4 Menu items available from the taskbar icon

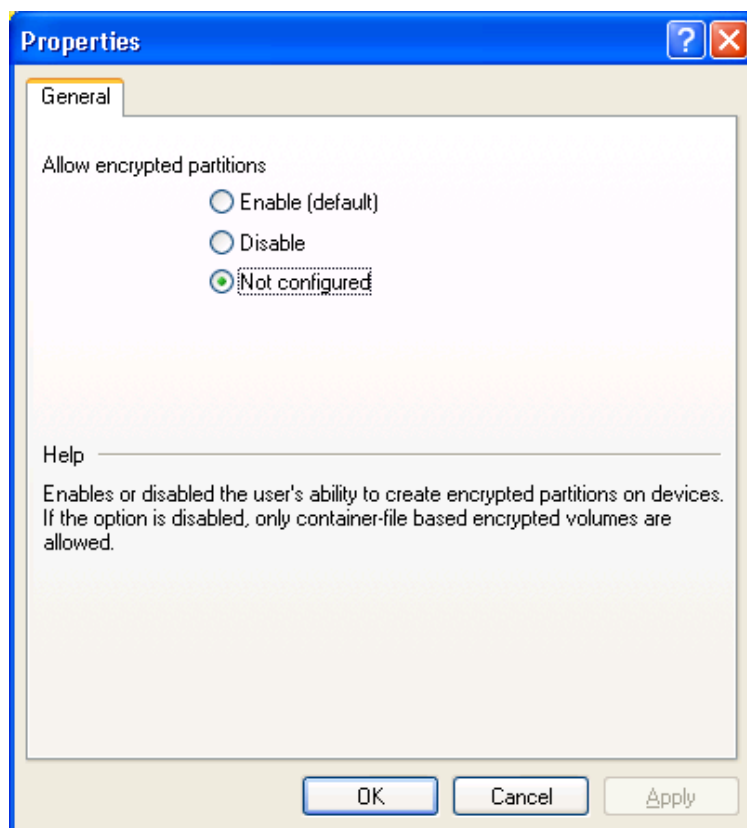
This option defines which commands are available when right-clicking the DriveLock taskbar icon. When this option is set to “Not configured”, all commands can be accessed from the taskbar icon.



2.1.3 Encrypted drive settings

2.1.3.1 Allowing encrypted partitions

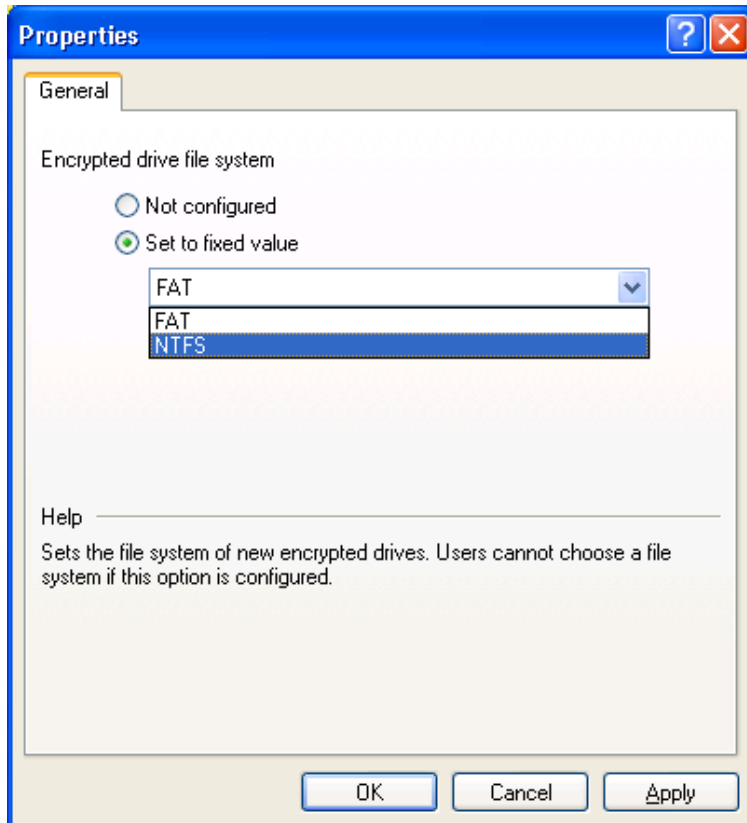
Configure whether users are allowed to encrypt entire partitions. This setting does not affect the creation of encrypted container files.



2.1.3.2 Encrypted drive file system

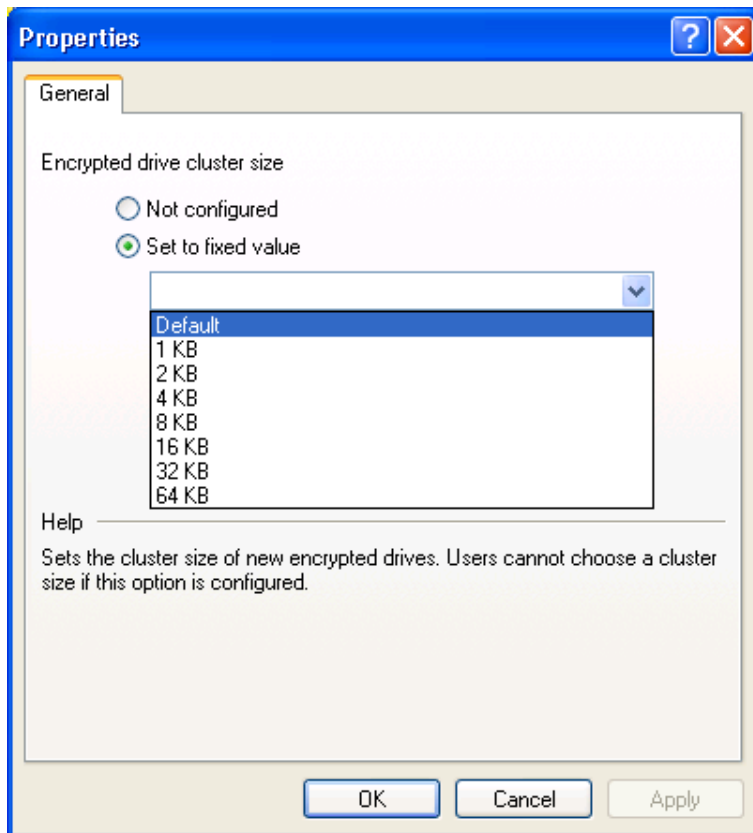
Configure this option to set the file system that is used for new encrypted drives to FAT or NTFS.

When you select FAT, DriveLock automatically uses FAT32 when the size of the drive is larger than 40 MB. For smaller drives DriveLock uses FAT.



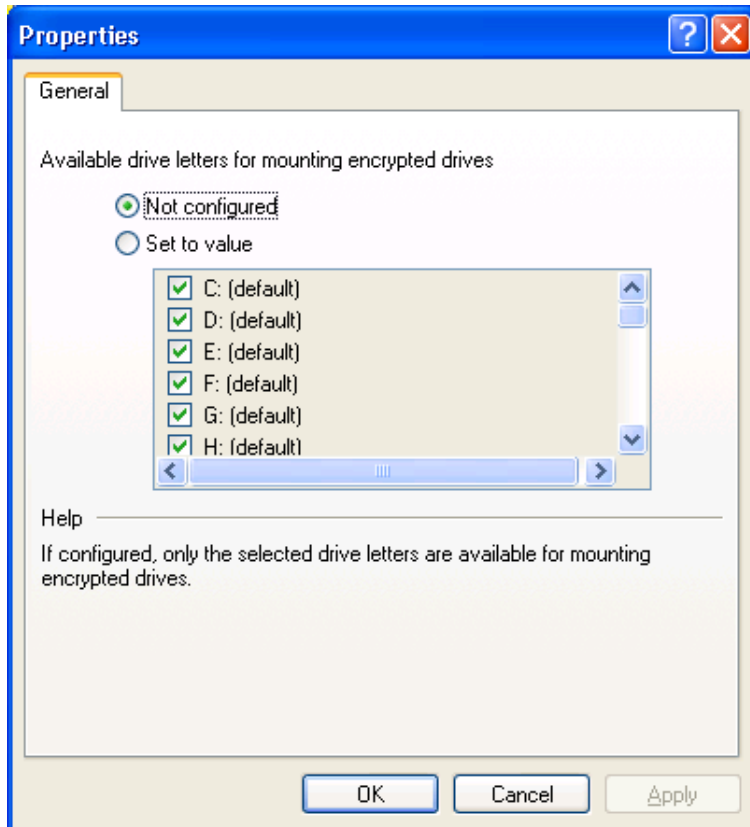
2.1.3.3 Encrypted drive cluster size

Configure this option to set the cluster size that is used for new encrypted drives.



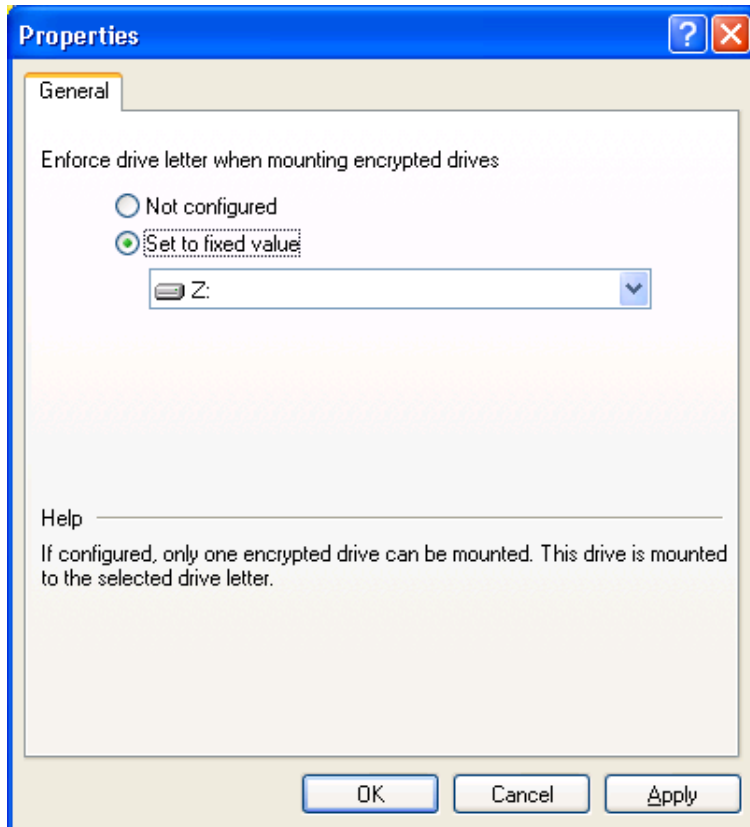
2.1.3.4 Available drive letters for mounting encrypted drives

Configure this option to select the drive letters that can be assigned to encrypted volumes when they are mounted on a computer. If you don't configure this option, a user can assign any available drive letter to an encrypted volume and DriveLock offers the next available drive letter as the default choice.



2.1.3.5 Enforce drive letter when mounting encrypted drives

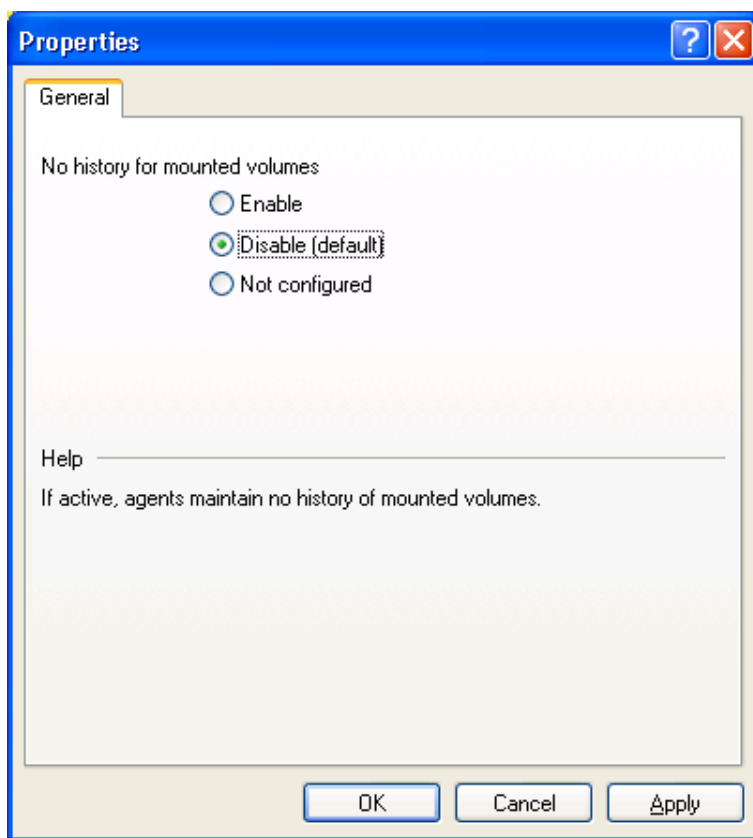
Configure this option to always assign a single drive letter to encrypted volumes when they are mounted on a computer. When you configure this option, only one encrypted drive can be connected at a time and the drive letter you selected is assigned.



2.1.4 End-user restrictions

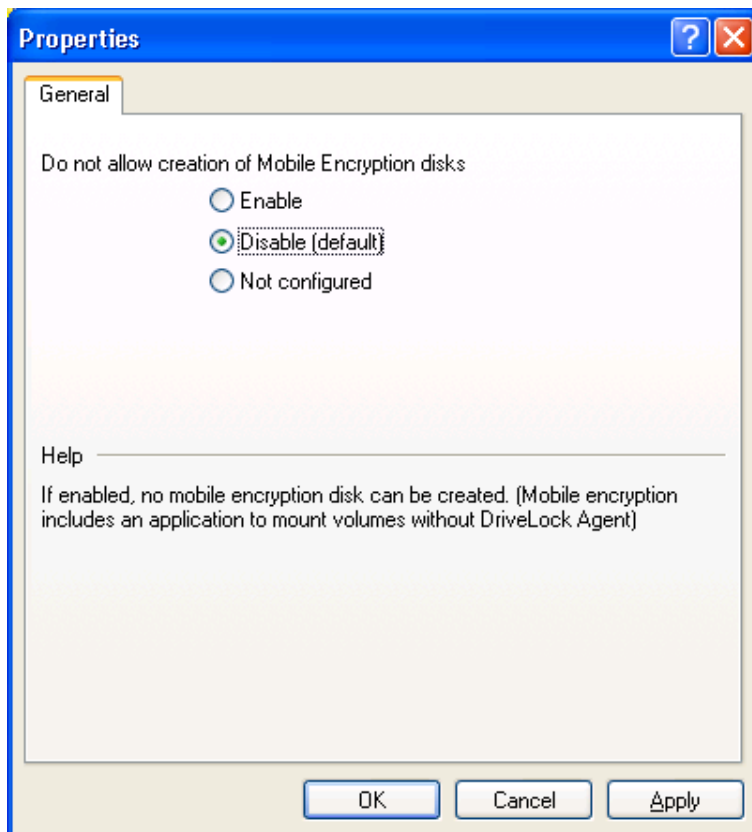
2.1.4.1 No history for mounted volumes

Configure this option to prevent client computers from storing information about which encrypted volumes users mount.



2.1.4.2 Do not allow creation of Mobile Encryption disks

The Mobile Encryption Application (MEA) is a standalone program that lets you access encrypted drives on a computer without the DriveLock Agent. When a user creates a Mobile Encryption disk by selecting the corresponding option on the DriveLock menu, DriveLock copies the MEA and an auto-start file (Autorun.inf) to the drive. Enable this option to prevent the copying of the MEA and Autorun.inf to drives.



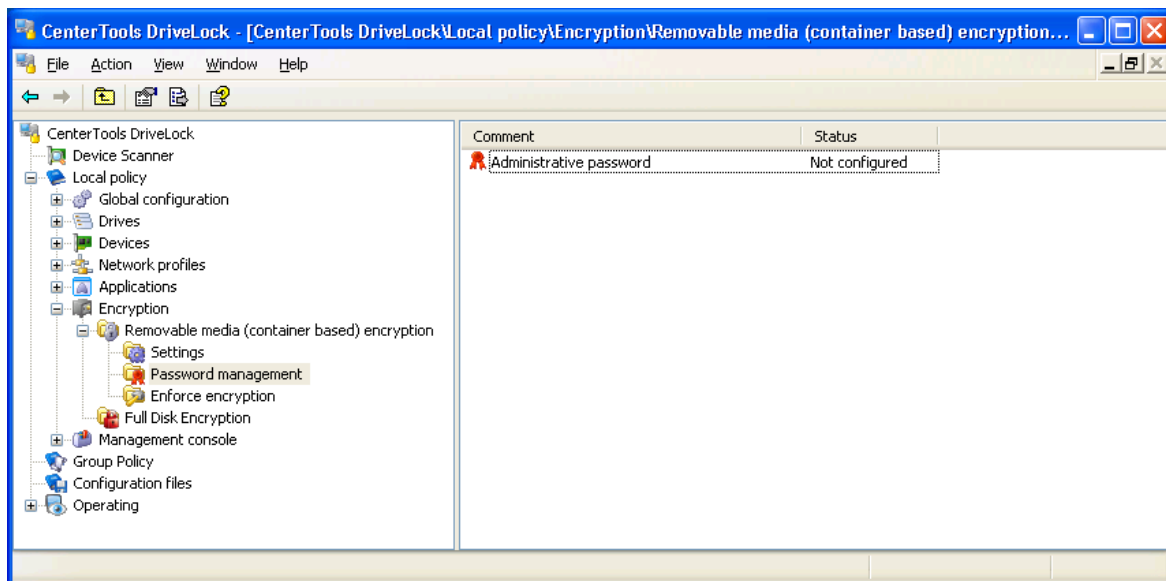
If you disable the Mobile Encryption disk DriveLock will prevent execution of the Mobile Encryption Application on removable drives also.

2.2 Configuring an Administrative Password

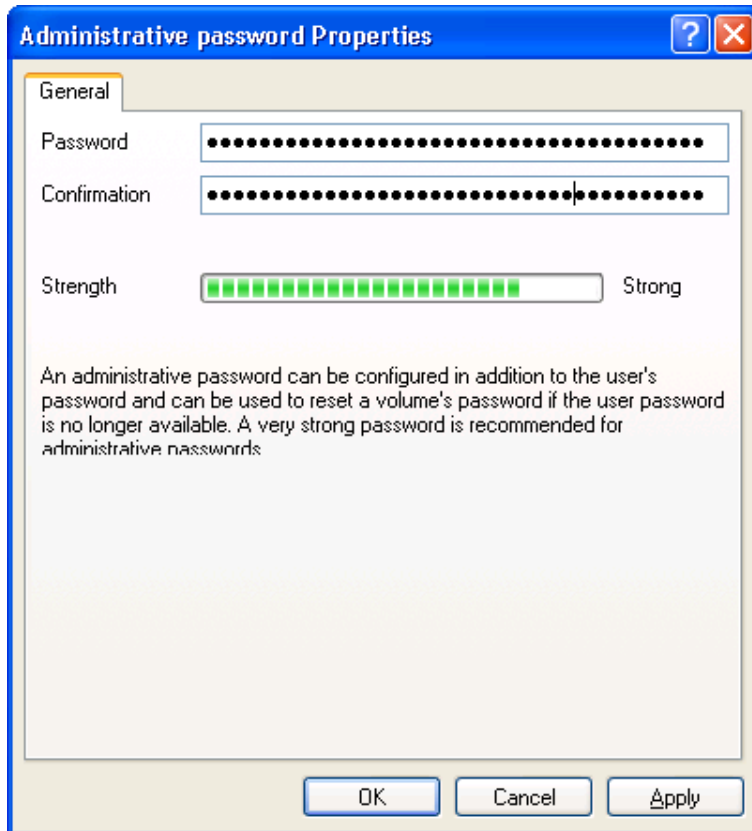
In addition to the user password that is unique to each encrypted volume, you can configure a central administrative password. Use the administrative password to access an encrypted drive if a user cannot remember his or her password or if the password is not available for any other reason. You can use the administrative password to access the encrypted drive or reset the existing user password. CenterTools recommends that you use a very strong password or passphrase as the administrative password.



If you don't create an administrative password (the option is set to "Not configured"), you must know the user password to access and encrypted drive or to reset its password. This may be a desired configuration in certain high-security environments, but using encryption without enabling the password recovery mechanism provided by the administrative password significantly increases the risk of losing access to the data due to a forgotten password.



For maximum security it is strongly recommended that you use a very strong password or passphrase as the administrative password. Use the strength indicator in the password dialog box to determine whether the password is strong enough to meet your requirements.



Consider using the following guidelines when choosing an administrative password:

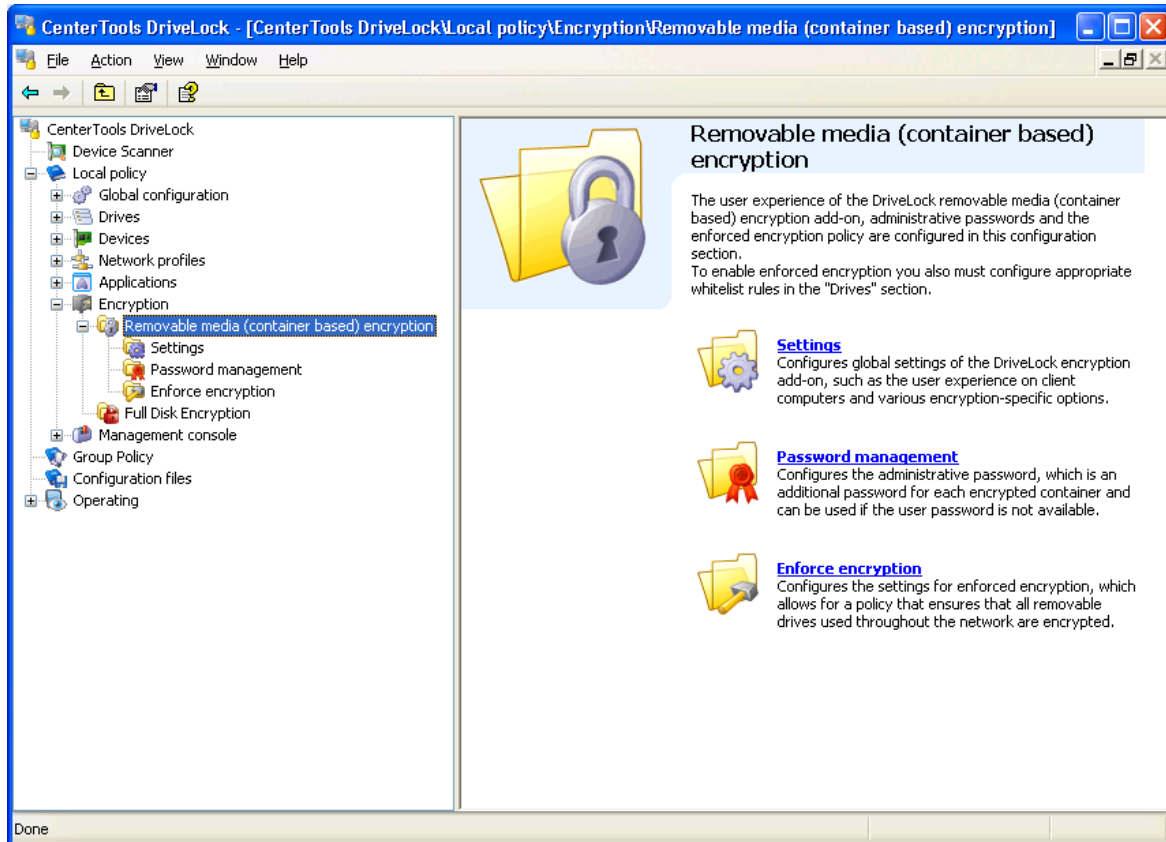
Use a combination of characters from the at least three of the following categories: Numbers (0 to 9), uppercase letters (A to Z), lowercase letters (a to z) and special characters (+"*ç%&/()=?è!éà£;:_.-öä\$ü``^# etc.)

- The password cannot be guessed by anyone.
- The password or parts of it don't appear in any dictionary
- The password should be as long as feasible. Passwords that are shorter than 15 characters generally don't provide sufficient long-term protection for stored data. If you find it too difficult to remember a long, complex password, consider using a phrase instead.
- Consider storing a copy of the administrative password in a secure location, such as a safe.

Do not write down a password unless you can store it in a secure location, such as a safe.

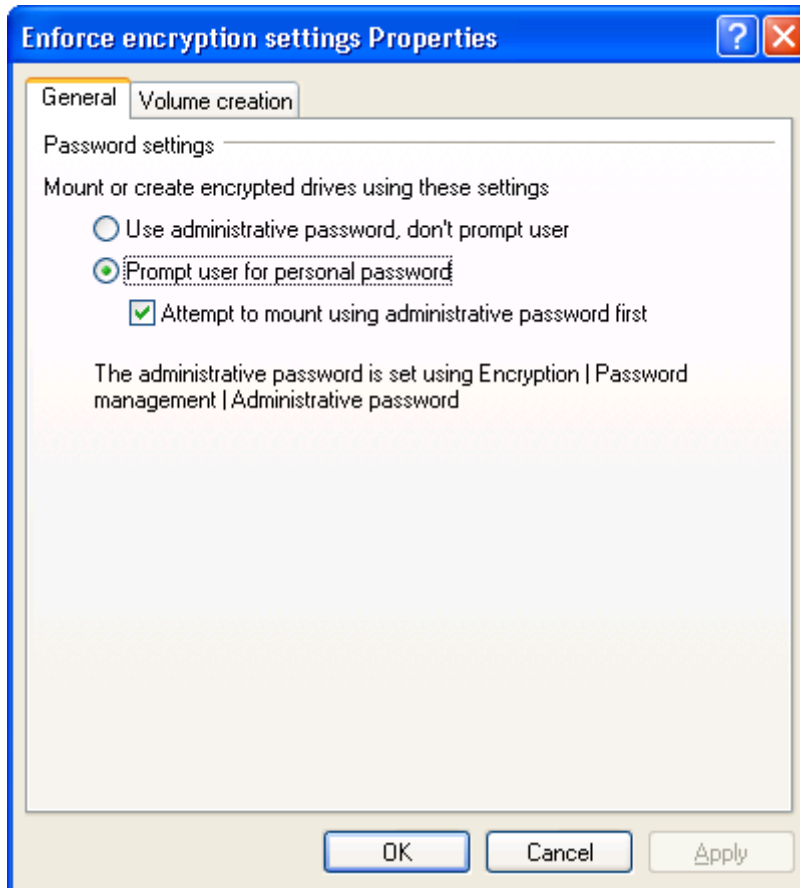
2.3 Configuring Encryption Enforcement

To enable automatic encryption of removable drives you must configure the settings that are used to automatically encrypt removable drives that you connect to the computer.



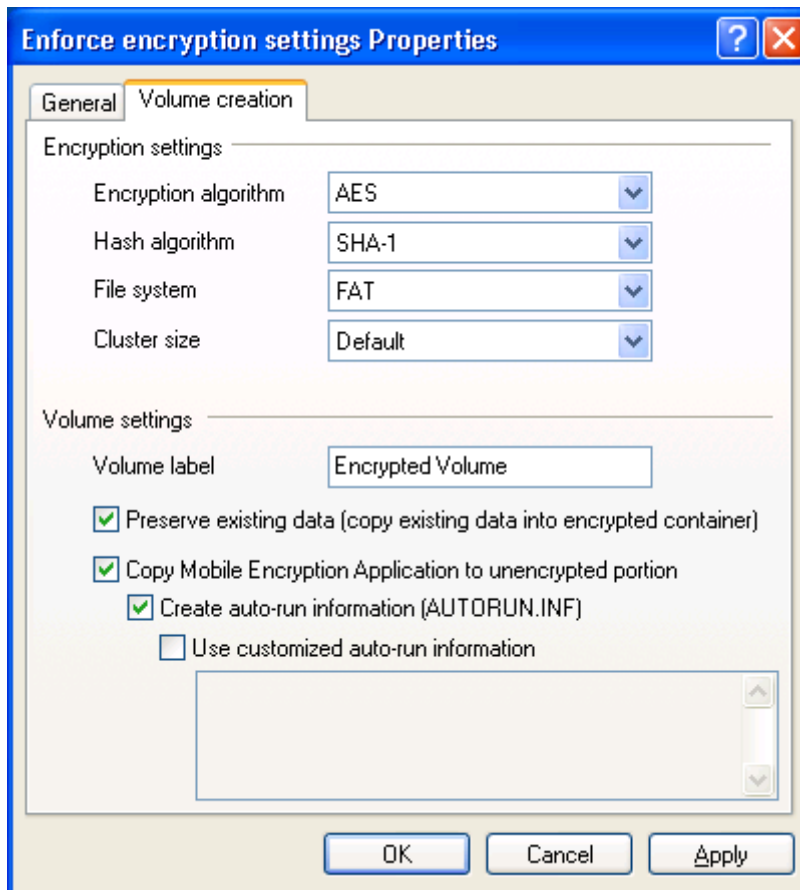
Double-click Enforce encryption.

Configure the encryption settings that DriveLock will use when automatically encrypting a removable drive.



The following general settings are available:

- *Use administrative password, do not ask user*
Select this option if you want DriveLock to mount and create encrypted drives without prompting users for a password. To use this setting, you must first configure an administrative password, as described in the section "Configuring an Administrative Password". Users do not have the option to specify their own password. If you select this option, you can use encrypted drives on all computers that are configured with the same administrative password, but you are not able to access any encrypted drive using the Mobile Encryption Application.
- *Ask user for personal password*
Select this option if you want DriveLock to prompt for the password of the encrypted drive when the computer detects an encrypted drive or when initially encrypting a drive. If you select this option, you can use encrypted drives using the Mobile Encryption Application. If you have configured an administrative password, you can also select the option to try mounting drives using the administrative password first. If you select this option, users are not prompted for a password when using an encrypted drive on any computer that is configured with the same administrative password. Users are still prompted for the password when accessing an encrypted drive by using the Mobile Encryption Application.



The following settings for volume creation are available:

- **Encryption algorithm**
Select the encryption algorithm that is used to encrypt drives when your policy enforces media encryption.
- **Hash algorithm**
Select the password hash algorithm that is used to encrypt drives when your policy enforces media encryption.
- **File system**
Select NTFS or FAT as the file system that is used on encrypted drives when your policy enforces media encryption.
- **Cluster size**
Select the cluster size that is used for the file system on encrypted drives when your policy enforces media encryption.
- **Volume label**
Type a volume label that is assigned to encrypted drives when your policy enforces media encryption.
- **Preserve existing data**

Select this checkbox to create an encrypted removable drive without deleting the data that's currently stored on it. Instead, DriveLock creates a temporary container on the computer's hard drive, copies all files from the drive to this container and then moves this container to the removable drive.



When a drive contains data, DriveLock needs to estimate how much space will be available for the encrypted container when it will be copied to the removable drive.

To ensure that the container size doesn't exceed the available space, some unencrypted space will remain available on the drive after the process complete. To ensure that the container uses all the available disk space, disable the option to preserve existing data, allowing DriveLock to delete any existing files before creating the encrypted container.

- ***Copy Mobile Encryption Application***

You can select to have DriveLock copy the Mobile Encryption Application to removable drives when a drive is encrypted and your policy enforces media encryption. You use the Mobile Encryption Application to access encrypted removable media on computers where DriveLock is not installed, such as an employee's home computer. You can find additional information about the Mobile Encryption Application in the section "The Mobile Encryption Application".

- ***Create auto-run information***

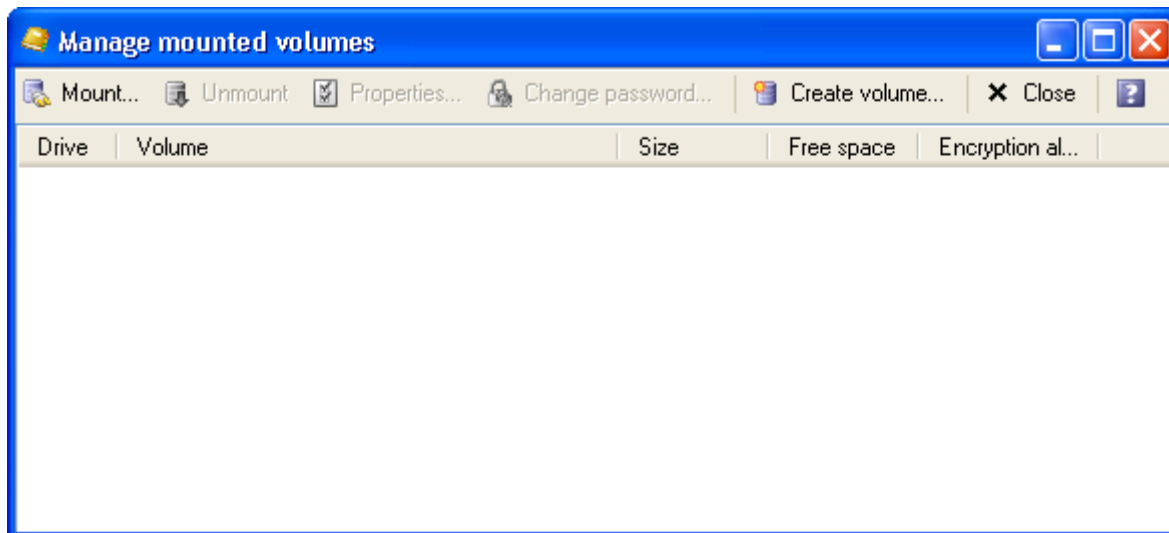
Check this to automatically copy the default *autorun.inf* to the removable drive.

- ***Create custom auto-run information***

You can also define the content of the *autorun.inf* file by entering the lines of code in the text box and activate "Create custom auto-run information".

3 Managing Encrypted Drives

DriveLock includes an application that you can use to manage encrypted drives. The Manage mounted volumes program lists all mounted encrypted drives and the drive letters assigned to them.



Access the Manage mounted volumes program from the Start menu (“Start → Programs → CenterTools DriveLock → Manage mounted volumes”) or right-click the DriveLock icon in the taskbar notification area.



The Start menu shortcut and taskbar icon command may not be available because they were disabled using a central policy. Contact your system administrator if you need to manage encrypted volumes and cannot access the program.

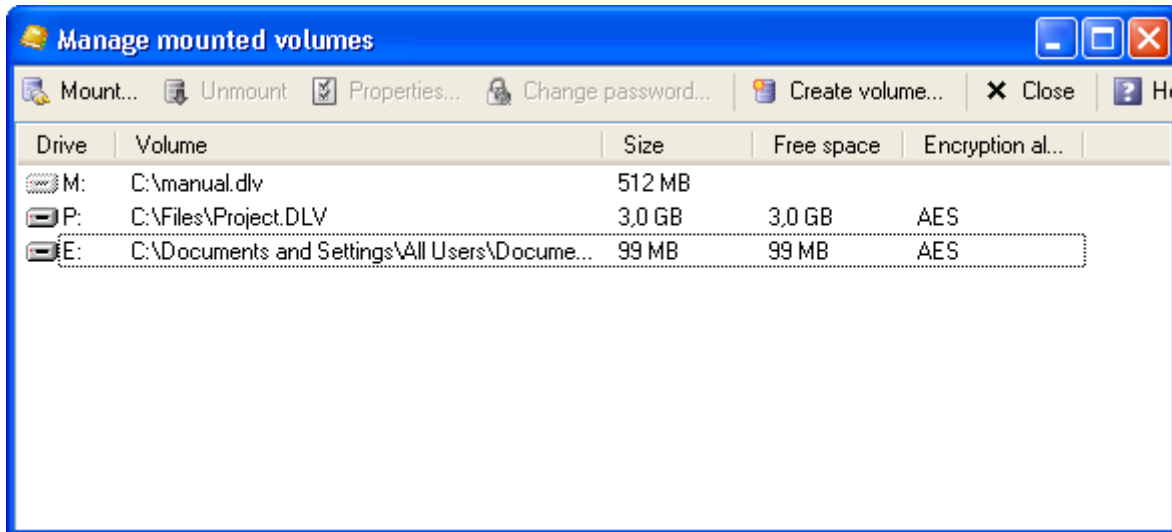
You can use all DriveLock encryption functions and manage encrypted drives by using the buttons and menu items in the program. Clicking the buttons starts wizards that guide you through the encryption tasks.



Partitions on storage devices that have been encrypted by DriveLock appear as “Not formatted” when connected to the computer. To mount such an encrypted partition, connect the device as described in the section “Connecting an encrypted drive that is based on a partition”. If you format the storage device (as suggested by Windows), you will permanently lose access to all data on the drive.

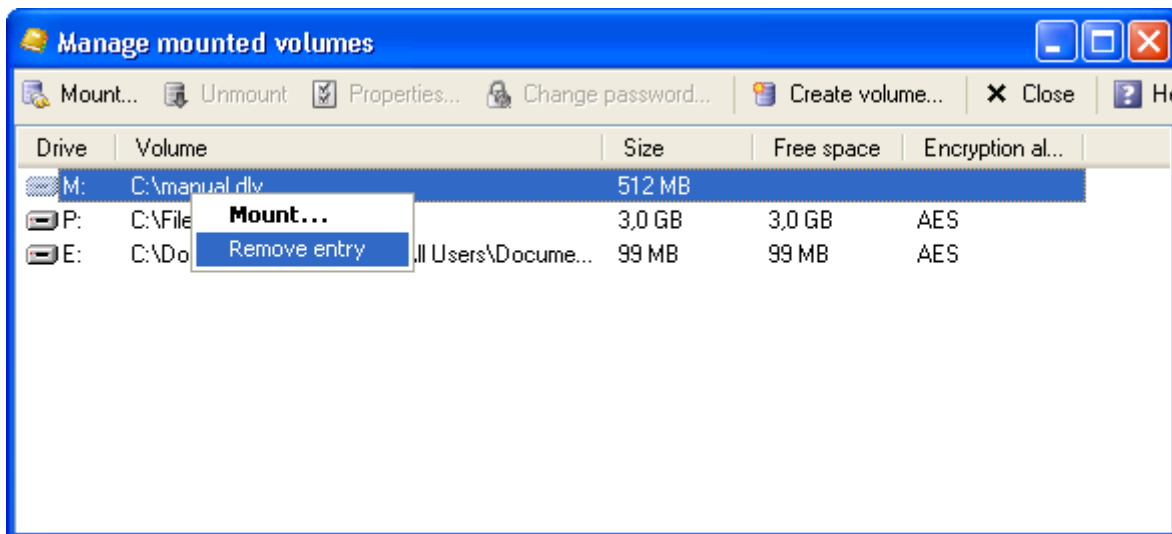
3.1 Encrypted Drives History

The encrypted drive history consists of a list of all currently and previously connected drives. Drives that are currently connected to the computer are displayed with a dark gray icon. Drives that are not currently connected are displayed with a light gray icon.



To mount a previously attached drive, double-click it. The mounting wizard starts, as described in the section “Connecting Encrypted Drives”.

To remove a drive from the list, right-click the drive and then click *Remove entry*.





Depending on your company-wide DriveLock configuration, the history function may not be available. If you need to use the history and it is not available, contact your system administrator.

3.2 Creating an Encrypted Drive

DriveLock includes an integrated wizard for creating an encrypted drive. To start the wizard, click *Start → Programs → CenterTools DriveLock → Create encrypted drive*, or use the *“Manage encrypted drives”*-menu. If the DriveLock task bar icon is available, you can also right-click it and then click *“Create encrypted drive”*.

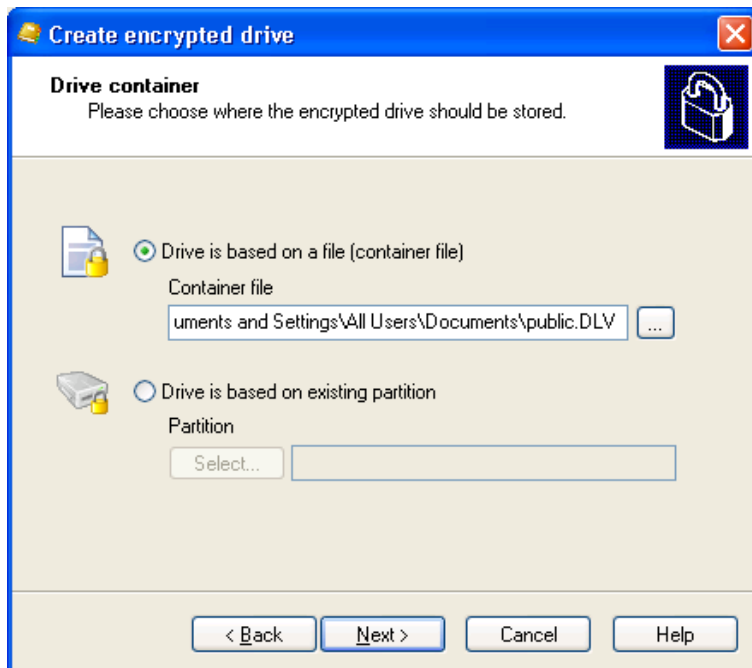
3.2.1 Using the Create encrypted drive wizard

Use the wizard to create encrypted drives that are stored as a container file or that occupy an entire existing disk partition.

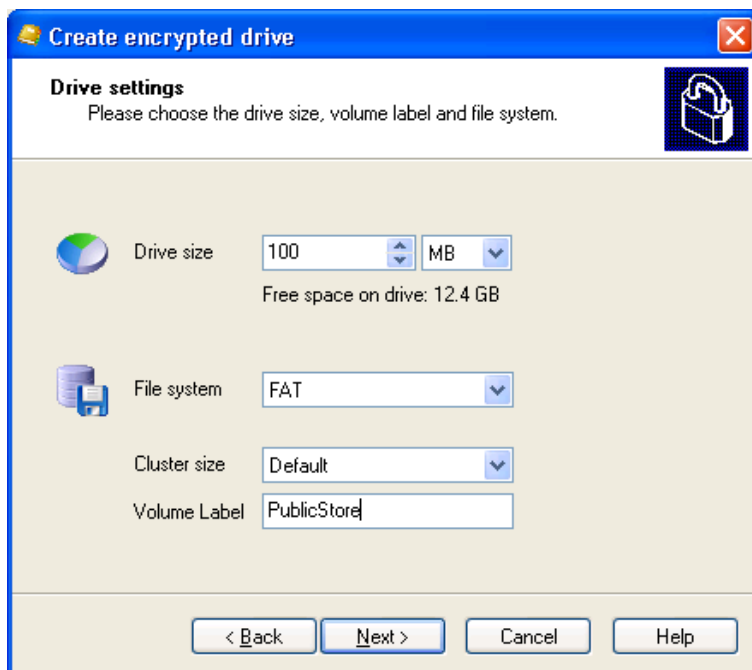
3.2.1.1 Create an encrypted drive based on a container file



Click Next.



To create an encrypted drive as a container file, select or type the name and path for the new container. You can click “...” to open a file selection dialog box.



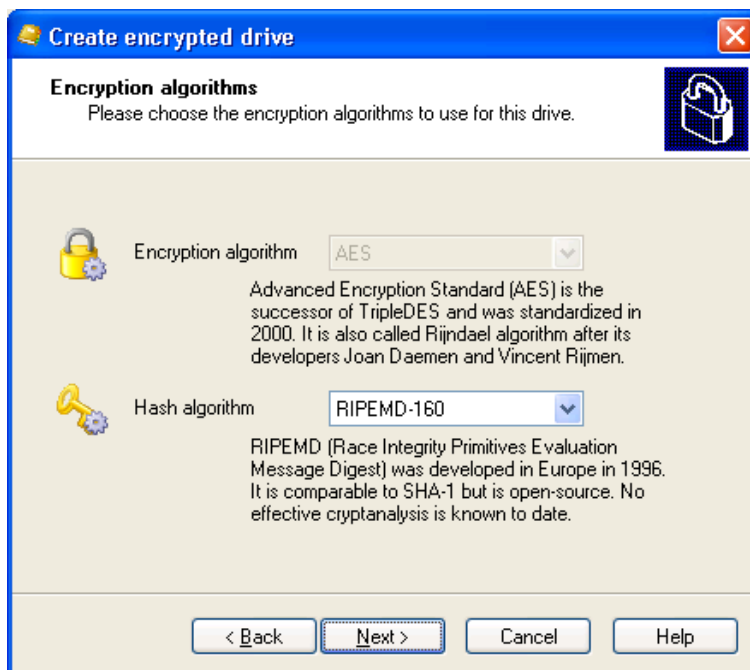
Specify the size of the container file. This will also be the size of the encrypted drive you are creating. A certain minimum size is necessary to support the file system you select (FAT: 100 KB; NTFS: 3072 KB). Add this minimum to the desired drive size, and then select the cluster size for the drive. Finally, type an optional volume label, and then click Next.



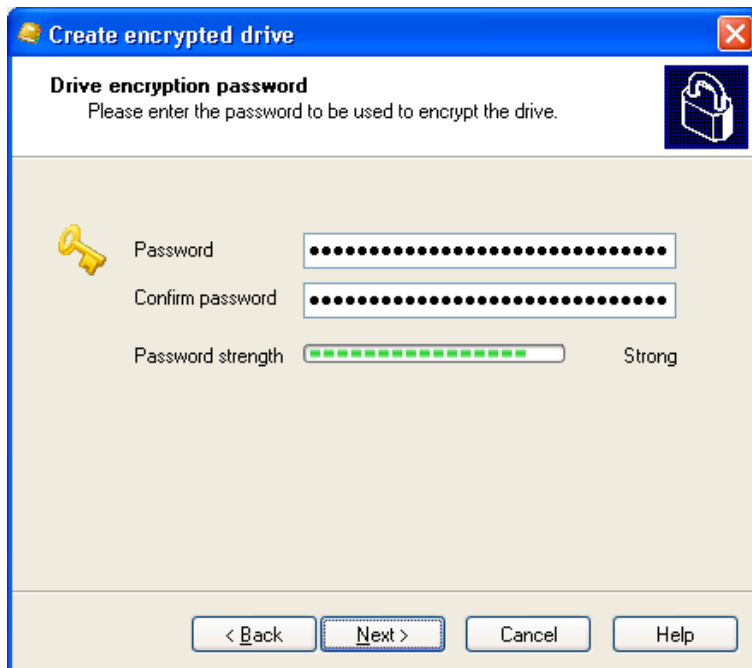
You may not be able to change some of the fields if your system administrator has centrally configured these settings.



A cluster is a logical unit of blocks on a disk. Normally the file system reads and writes files by accessing entire clusters, and can't address single blocks or bytes contained within a cluster. Therefore files always use space in multiples of the cluster size. On drives with large clusters the operating system can access large files more efficiently and creates less fragmentation. However, using a large cluster size on drives that store many smaller files can result in wasted storage space.



Select the encryption and hash algorithms to use for the encrypted drive and then click Next.



Type the password to be used for the encrypted drive, and then confirm the password by typing it again. If both entries are identical and meet your organization's password strength requirements, the "Next"-button becomes available.

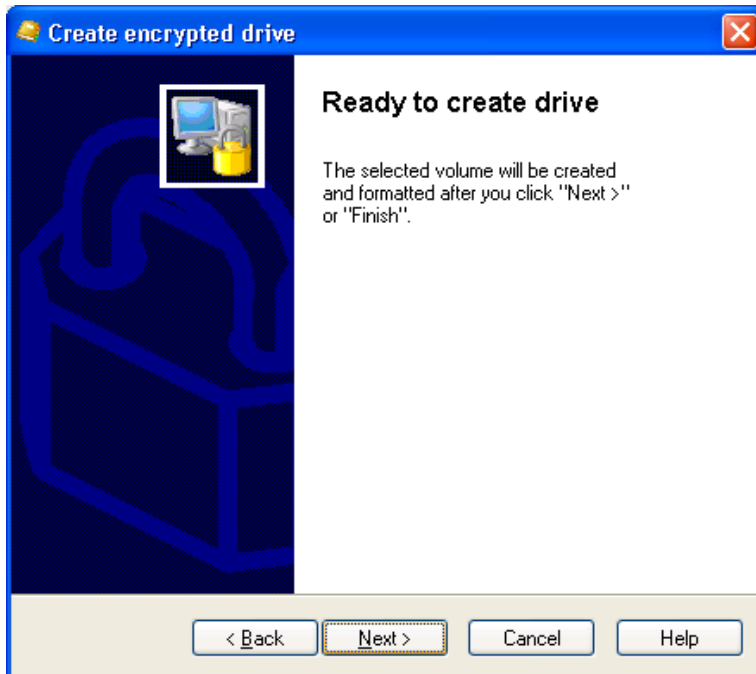
The strength of a password is determined both by its length and its complexity. DriveLock analyzes both of these factors and displays an estimate of the password strength.

Password may include the following characters:

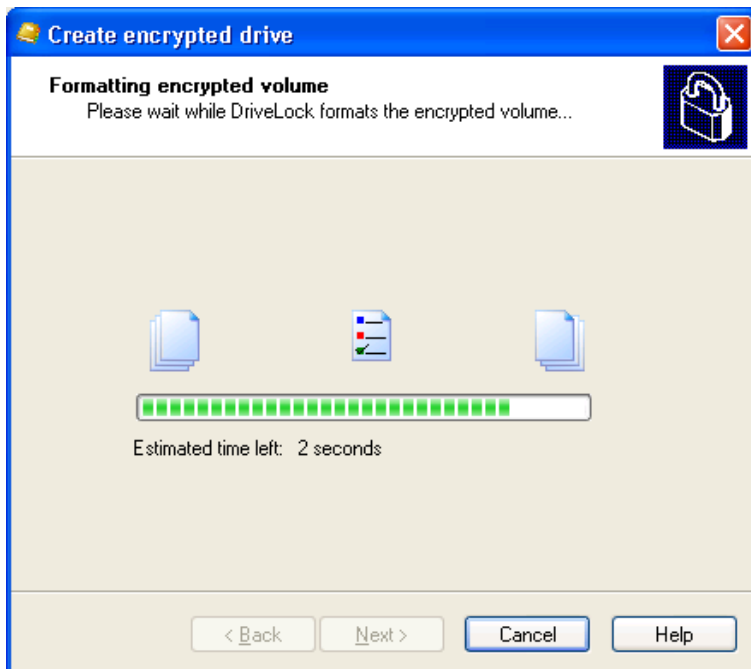
- Capitals (A-Z)
- Lower case letters (a-z)
- Arabic numerals (0-9)
- Non-alphanumeric characters (e.g. !, \$, #, \ or &)

You can also use a passphrase that consists of multiple words and punctuation instead of a password. Passphrases are typically easier to remember than long complex passwords. If your system administrator configured a requirement for minimum password strength or defined a password complexity policy, DriveLock notifies you of this requirement on this wizard page.

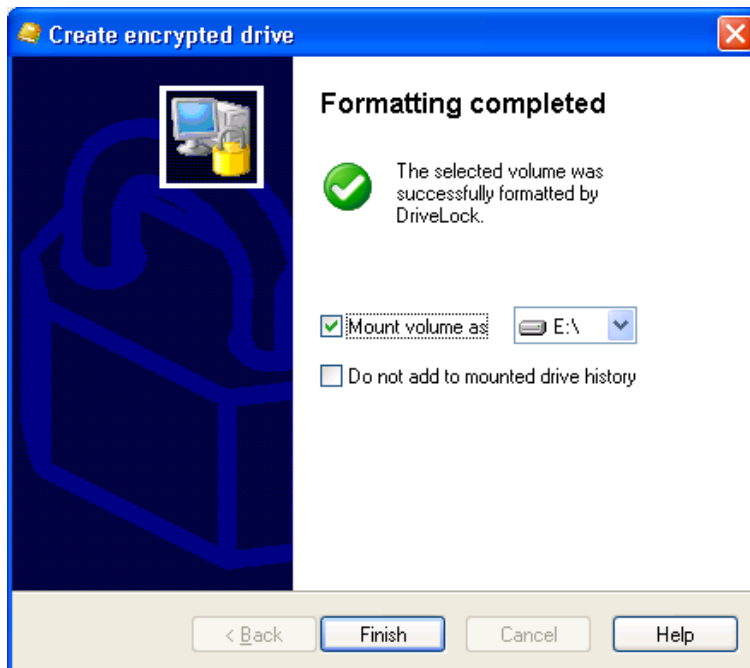
Click Next to continue.



Click Next to start creating the encrypted drive.



Depending on drive size and encryption algorithm used, creation of a new encrypted drive may take several minutes.



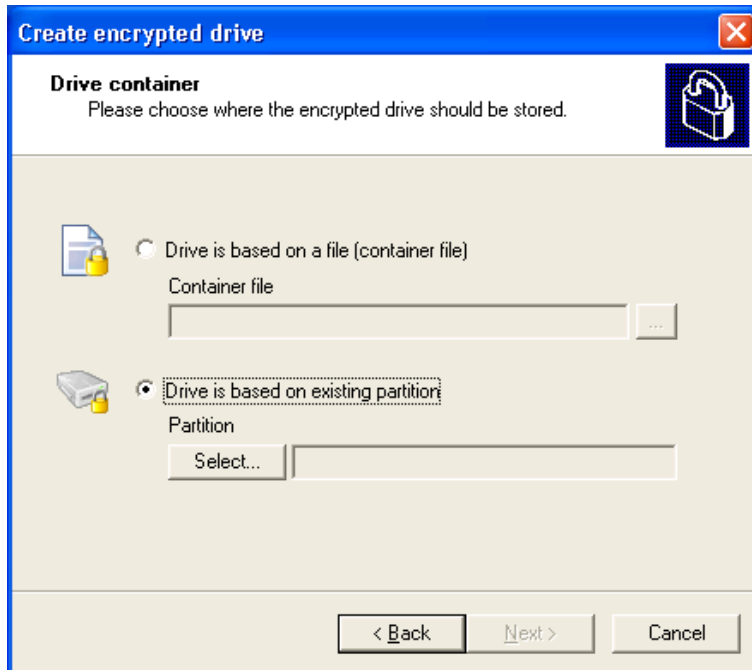
When DriveLock has finished formatting the volume, you can mount it and assign it a Windows drive letter. To mount the volume and make it available in Windows, select a drive letter and then click Finish.

If you don't want DriveLock to add the drive to the drive history in the encrypted drive management program, select the "Do not add to mounted drive history" checkbox.

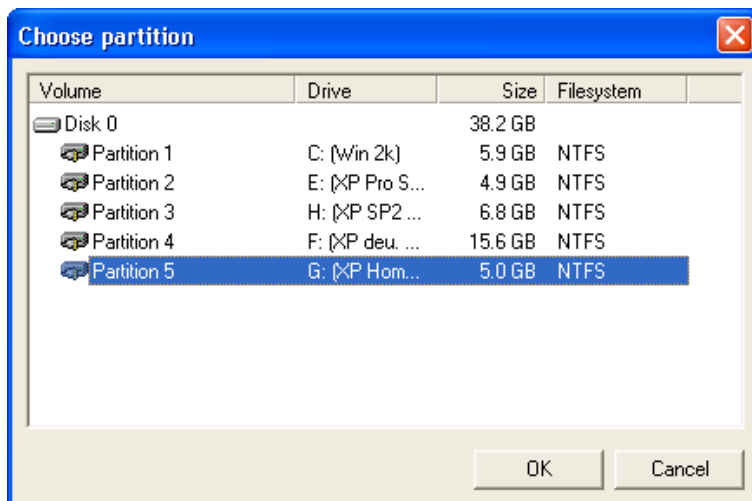
3.2.1.2 Creating encrypted drive based on existing partition

Creating an encrypted drive that occupies an entire existing partition is almost identical to creating an encrypted drive based on a container file. The only difference is that you must select a partition instead of a container file. This section describes the steps that are different when creating a drive that is based on a partition.

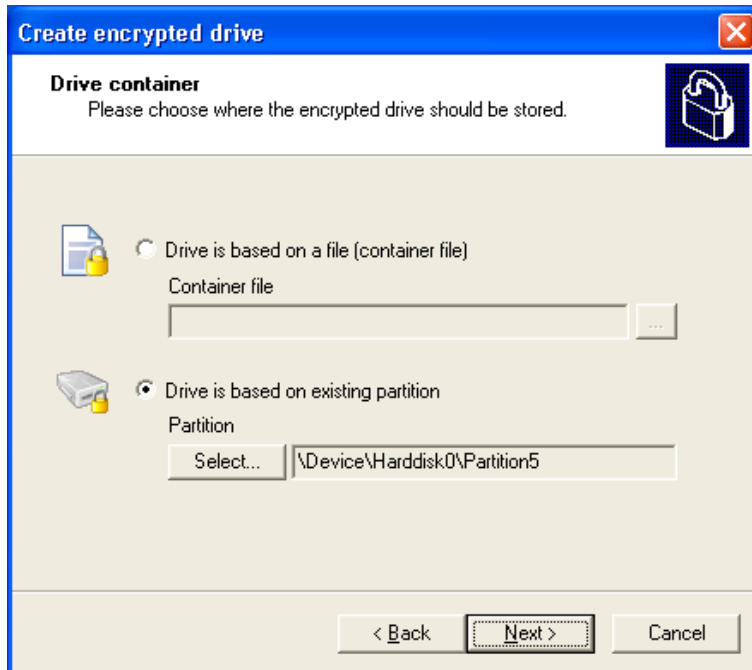
After starting the wizard, select "Drive is based on existing partition".



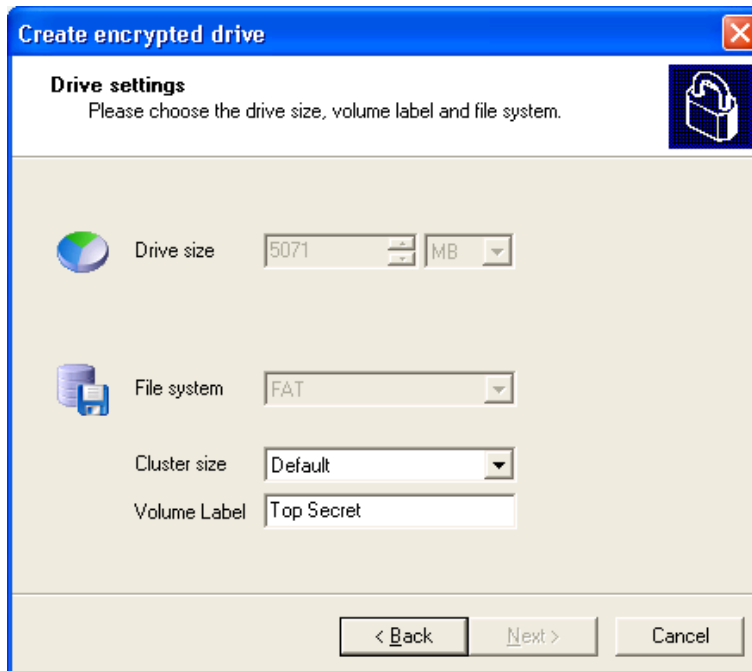
Click **Select** and then select the partition to encrypt from the list of all partitions on the computer.



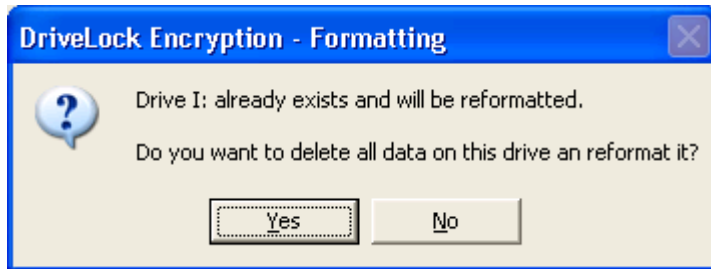
Select the partition to encrypt, and then click **OK**.



Click Next to continue.



You can't change the drive size for a partition-based encrypted volume. Complete all other settings, click Next, and then confirm that the drive will be formatted and that all existing data on the drive will be permanently deleted.



The remaining steps of creating a partition-based encrypted volume are described in the section “Using the Create encrypted drive wizard”.



Partitions encrypted by DriveLock appear in Windows as “*Not formatted*”. Be careful to not encrypt partitions that are already encrypted or partitions that contain the operating system files. Don’t format such partitions using Windows. Formatting a partition overwrites all existing data and you will permanently lose the ability to access the information on it. Also, don’t create an encrypted drive based on the partition that contains the operating system or any other important files as encrypting a partition permanently erases all data on it

The remaining steps of creating a partition-based encrypted volume are described in the section “Using the Create encrypted drive wizard”.

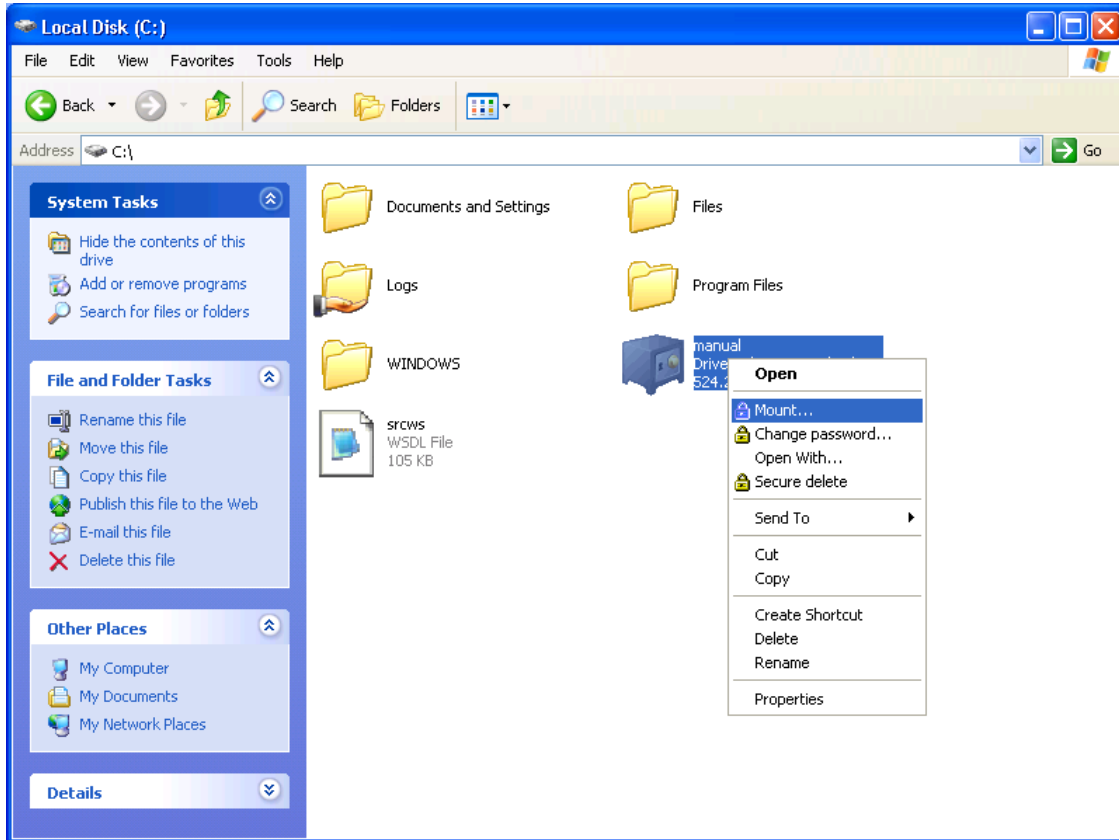
3.3 Connecting Encrypted Drives

To connect (mount) an encrypted drive, use the Mount encrypted volume wizard. Start the wizard by performing one of the following steps:

- Click “*Start → Programs → CenterTools DriveLock → Mount encrypted volume*”.
- If the DriveLock taskbar icon is available, right-click the icon, and then click “*Mount encrypted volume*”.
- In the Manage encrypted volumes program, click the drive, and then click Mount.
- In the Manage encrypted volumes program, double-click a previously connected drive.
- In Windows Explorer, double-click a *.dlv file.
- In Windows Explorer, right-click a *.dlv file and then click “*Mount*”.



If a volume has been already mounted, only the option “*Unmount*” will be available.



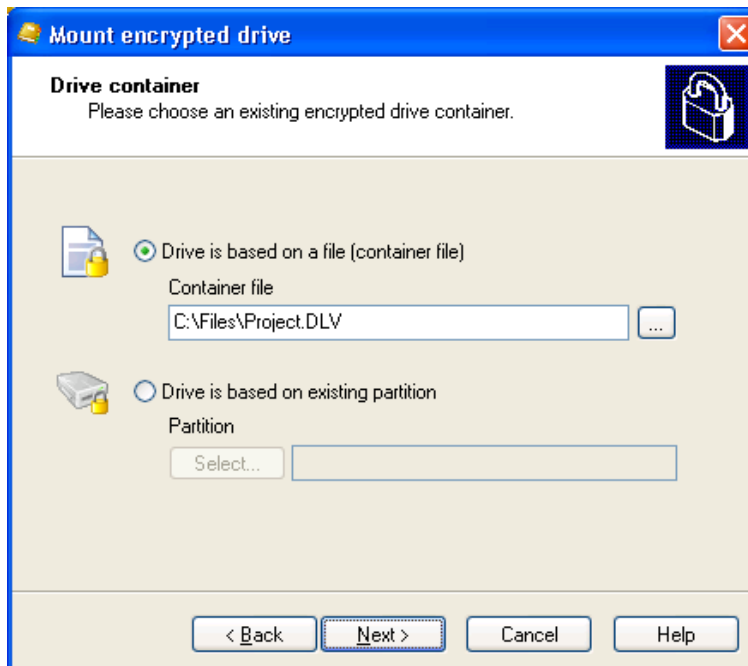
Availability of Start menu entries can vary, depending on your central configuration settings. If an item does not appear, your system administrator may have disabled it.

Use the wizard to connect encrypted drives that are based on a container file or an existing partition.

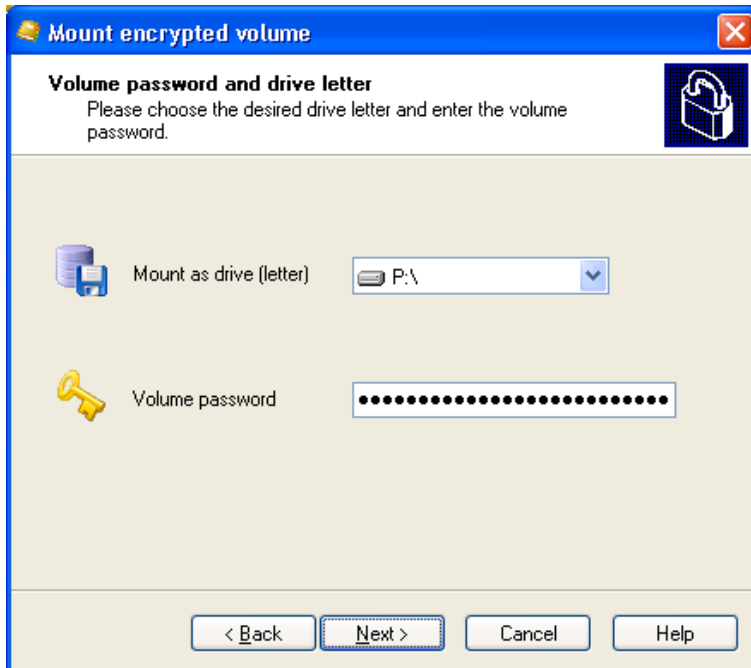
3.3.1 Connecting an encrypted drive that is based on a container file



Click Next.



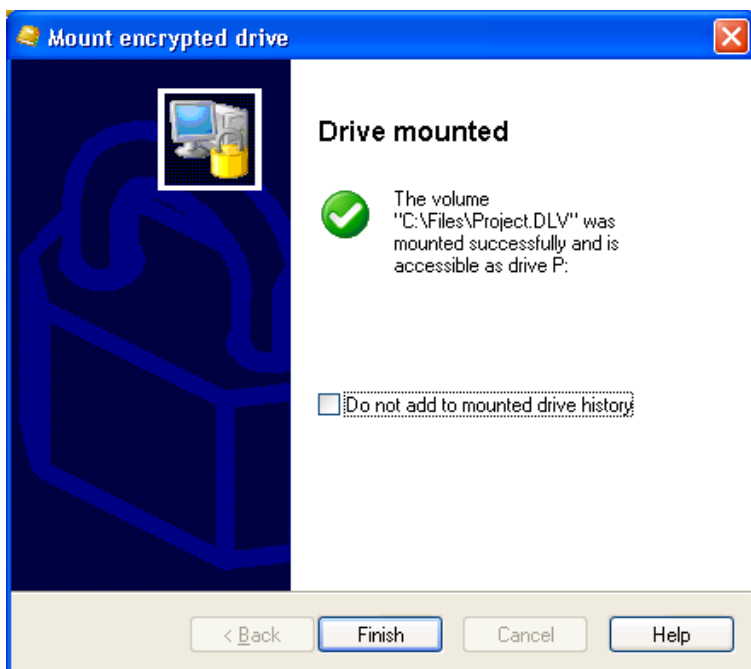
Select “Drive is based on a file (container file)” and then type the path and name of the *.dlv file, or click the “...”-button and then select the file. Click Next.



Select the drive letter to use for the encrypted drive, type the password you specified when you encrypted the drive, and then click Next.



If the wizard does not let you change some items, your system administrator has preconfigured these items.

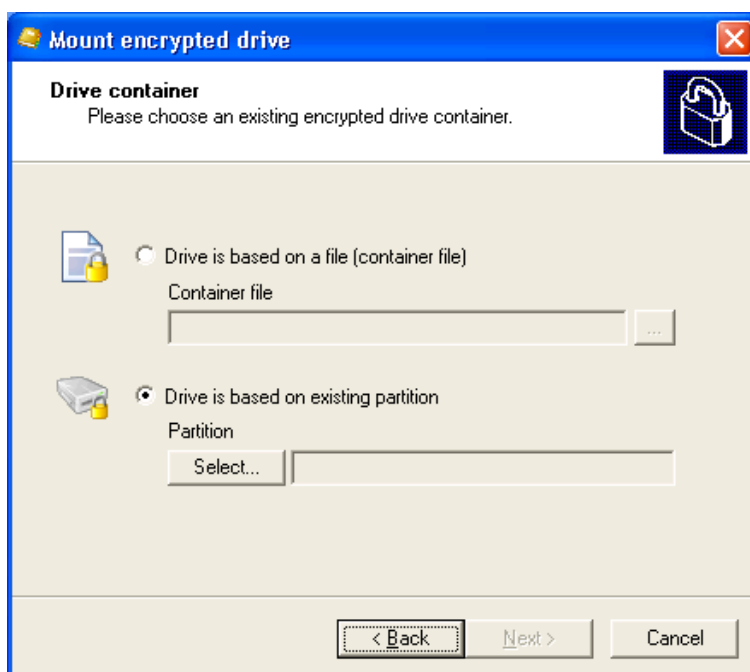


To not add the drive to the mounted drives history, select the *“Do not add to mounted drive history”* checkbox. Click Finish to close the wizard.

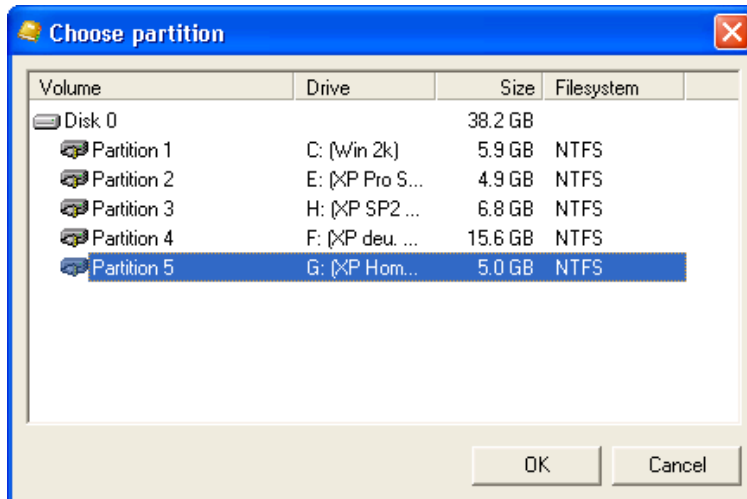
3.3.2 Connecting an encrypted drive that is based on a partition

Connecting (mounting) an encrypted drive that is based on a partition is almost identical to connecting an encrypted drive that is based on a container file. The only difference is that you must select a partition instead of a file. For all other steps, refer to the section *“Create encrypted drive based on a container file”*.

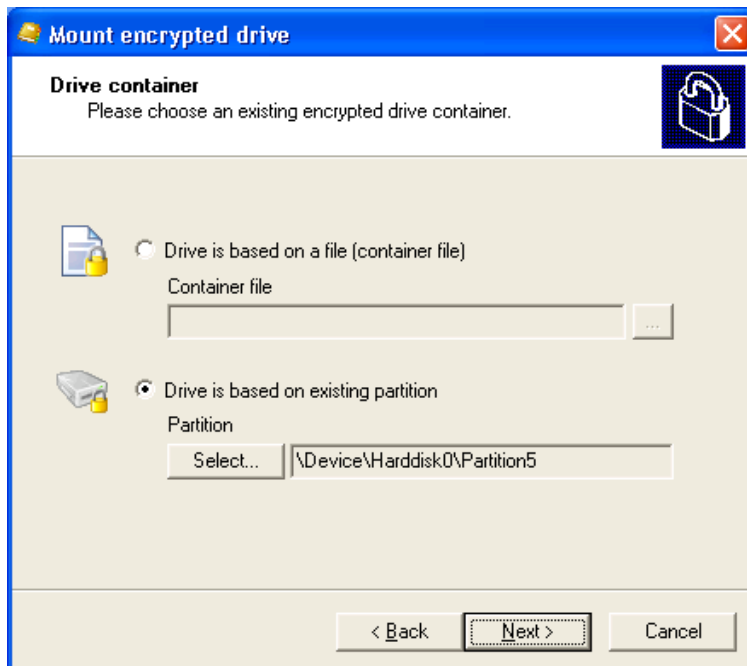
After starting the wizard, select *“Drive is based on existing partition”*.



Click Select to select the encrypted partition.



Click the encrypted partition to mount, and then click OK.

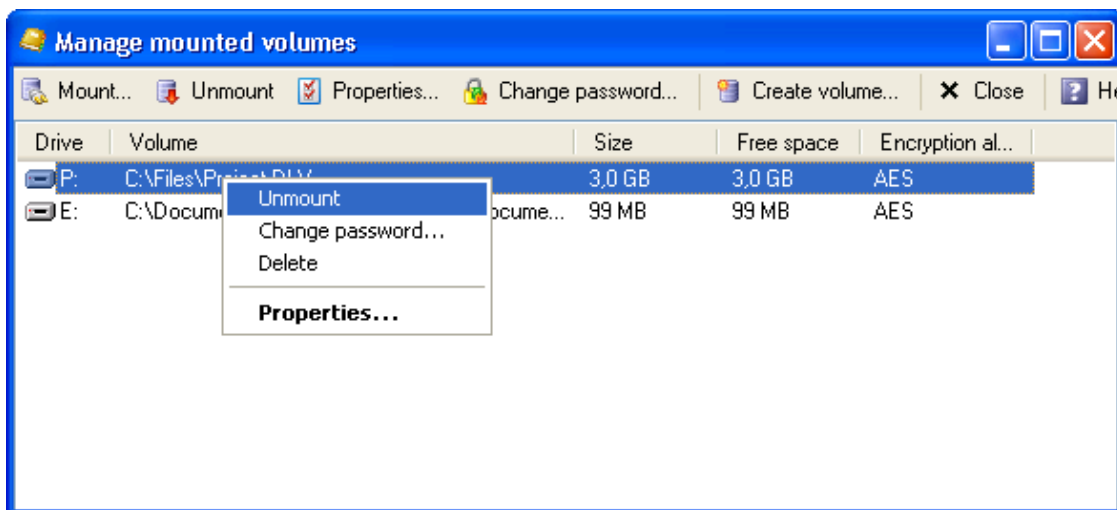


Click Next to continue.

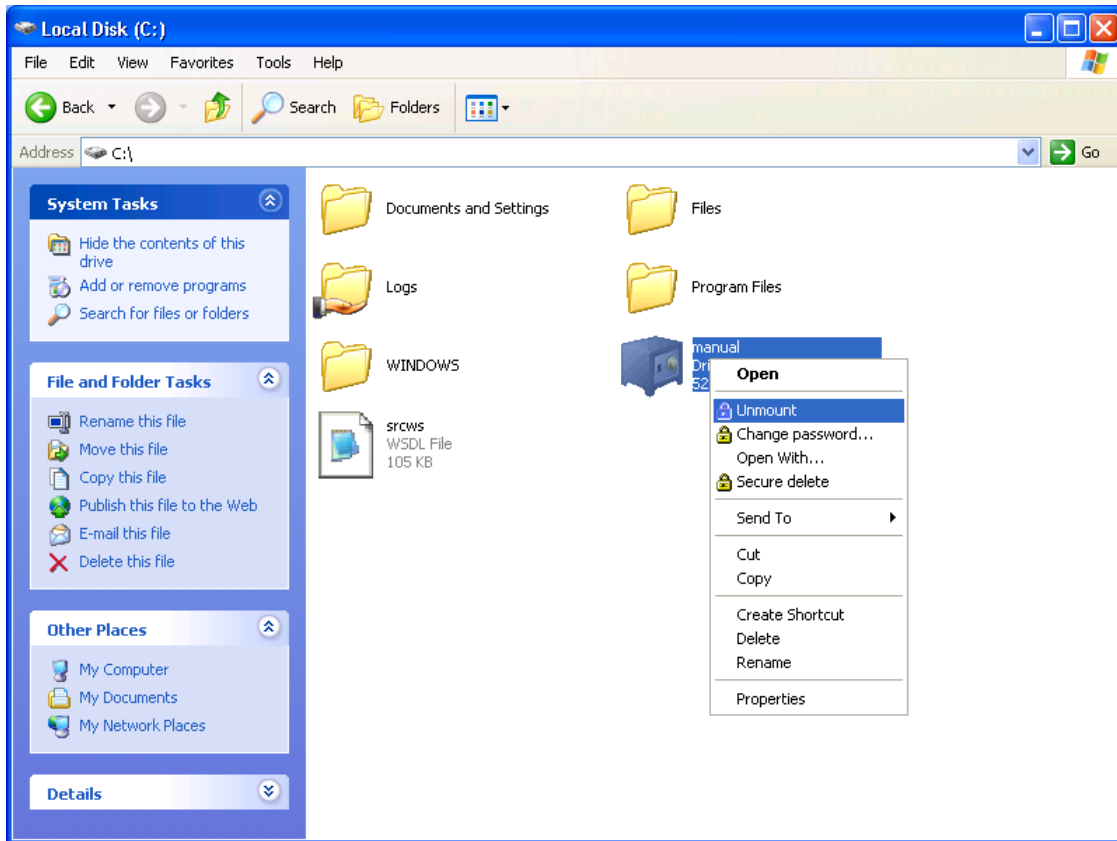
3.3.3 Disconnecting an encrypted drive

To disconnect (unmount) an encrypted drive, use the Unmount encrypted volume wizard. Start the wizard by performing one of the following steps:

- Click “*Start → Programs → CenterTools DriveLock → Unmount encrypted drive*”
- If the DriveLock taskbar icon is available, right-click the icon, and then click “*Unmount encrypted volume*”.
- In the Manage encrypted volumes program, click the drive, and then click Unmount.
- In the Manage encrypted volumes program, right-click the drive, and then click “*Unmount*”.



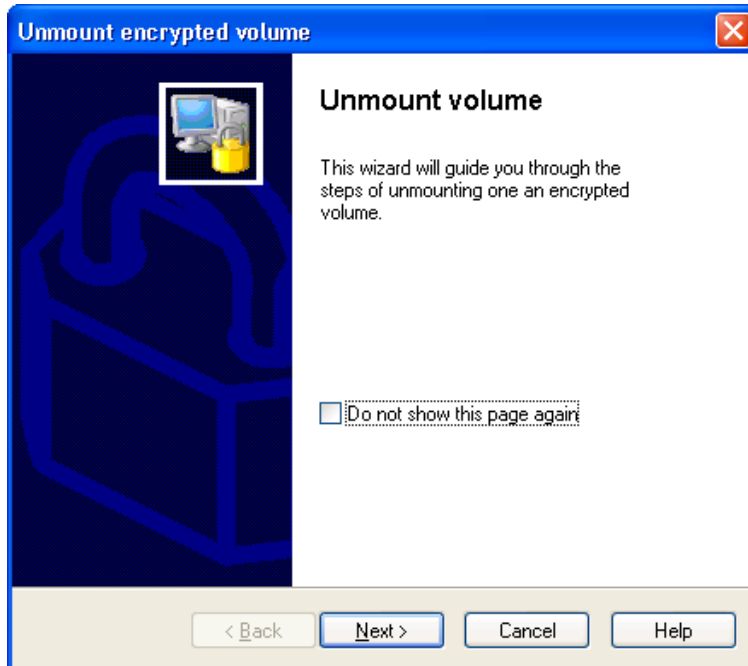
- In Windows Explorer, right-click an encrypted volume, and then click “*Unmount*”.
- In Windows Explorer, right-click a *.dlv file, and then click “*Unmount*”.



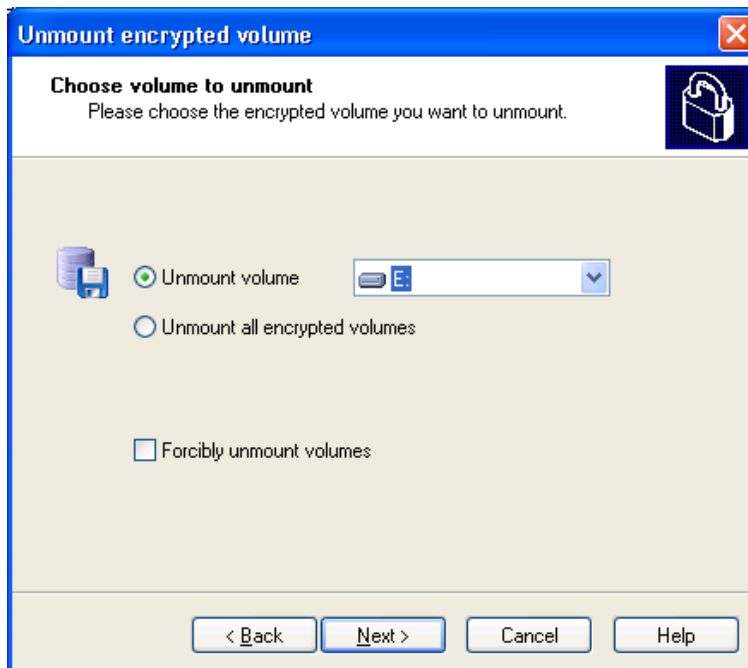
The Unmount-Wizard starts.



Availability of Start menu entries can vary, depending on your central configuration settings. If an item does not appear, your system administrator may have disabled it.



Click Next.

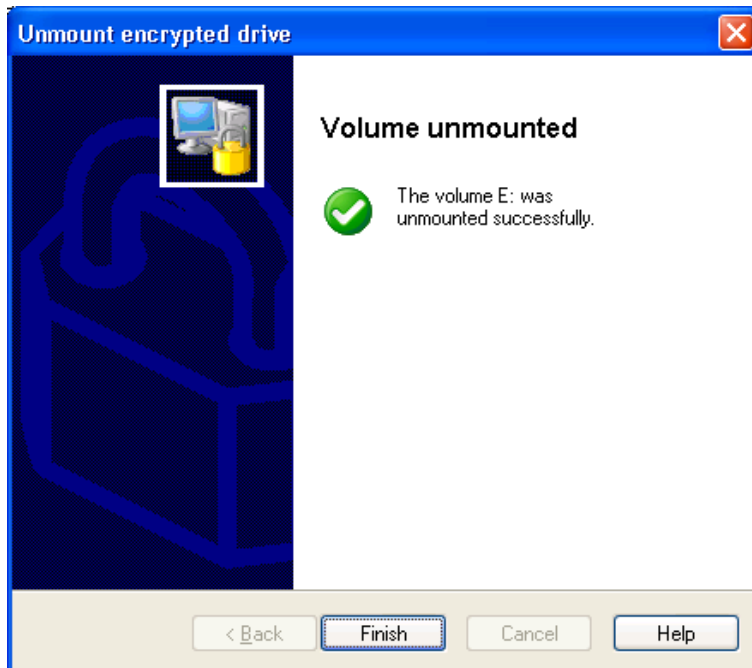


Select the volume to unmount, or to disconnect all currently attached volumes, select “*Unmount all encrypted volumes*”.

Select the “*Forcibly unmount volumes*” check box to unmount the volume even if files on it are still in use by a program running on your computer.



Always close all files that are in use before disconnecting an encrypting drive. Unmounting or removing an encrypted drive while files on it are opened may result in damaged files and loss of your data. CenterTools is not responsible for any data loss.

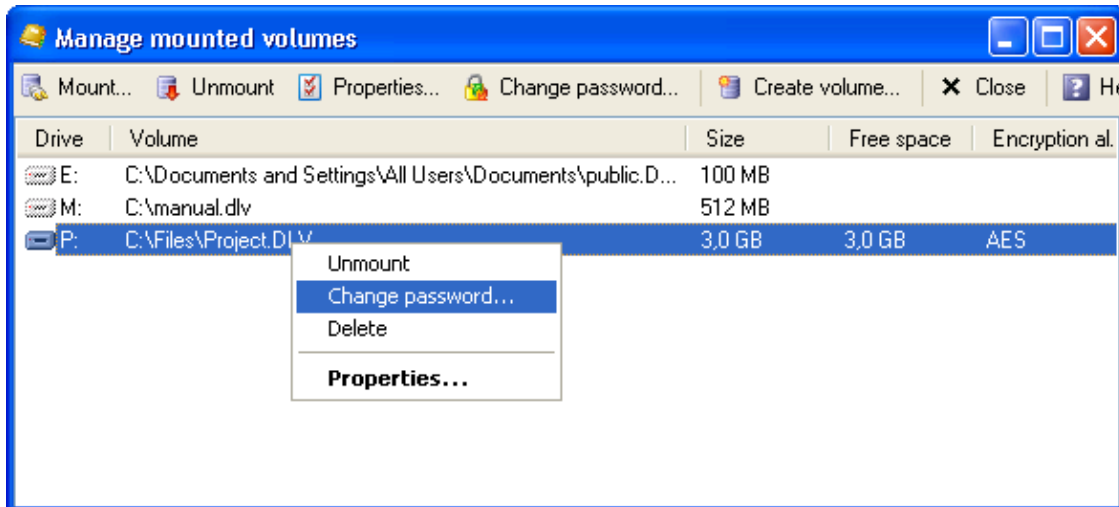


After the volume has been disconnected, click Finish to close the wizard.

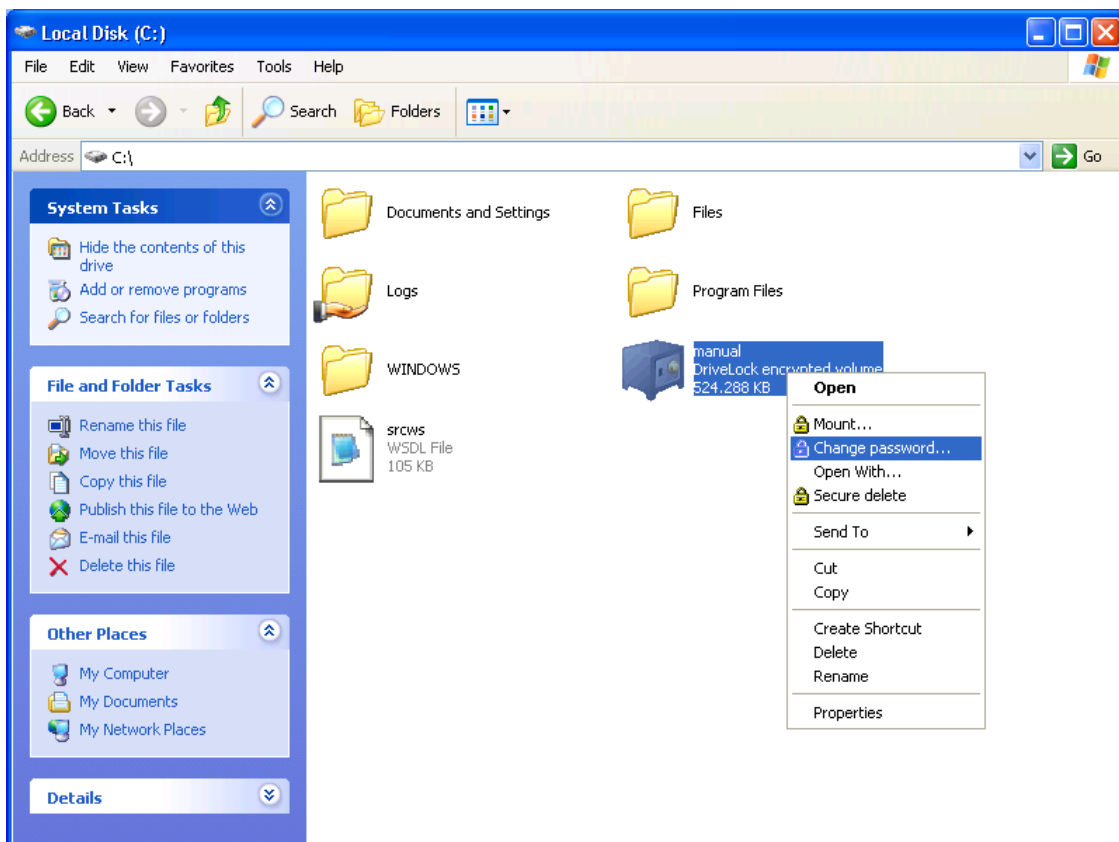
3.4 Changing a Password

To change the password of an encrypted drive, use the Change volume password wizard. Start the wizard by performing one of the following steps:

- Click *Start → Programs → CenterTools DriveLock → Change password*
- If the DriveLock taskbar icon is available, right-click the icon, and then click *Change password*.
- In the Manage encrypted volumes program, click the drive, and then click Change password.
- In the Manage encrypted volumes program, right-click the drive, and then click *Change password*.



- In Windows Explorer, right-click an encrypted volume, and then click “*Change password*”.
- In Windows Explorer, right-click a *.dlv file, and then click “*Change password*”.



The Change volume password Wizard starts.

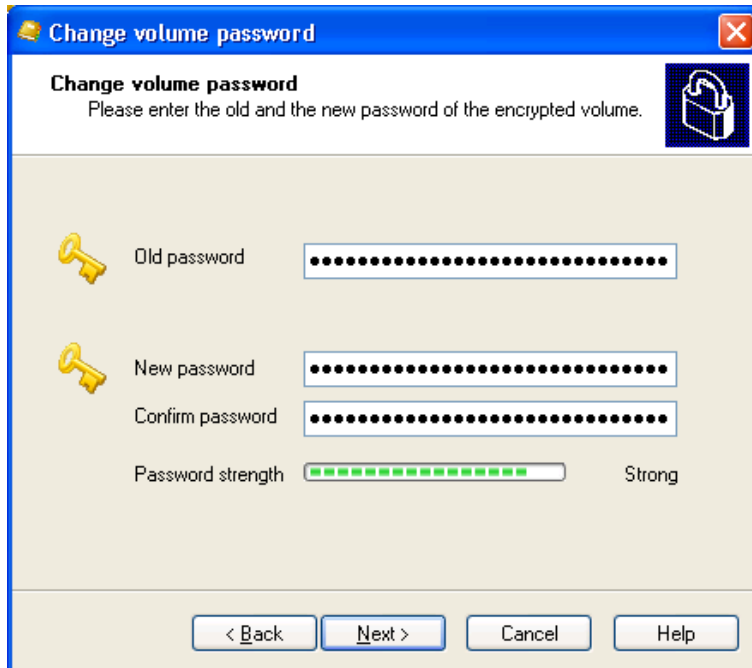


Availability of Start menu entries can vary, depending on your central configuration settings. If an item does not appear, your system administrator may have disabled it.

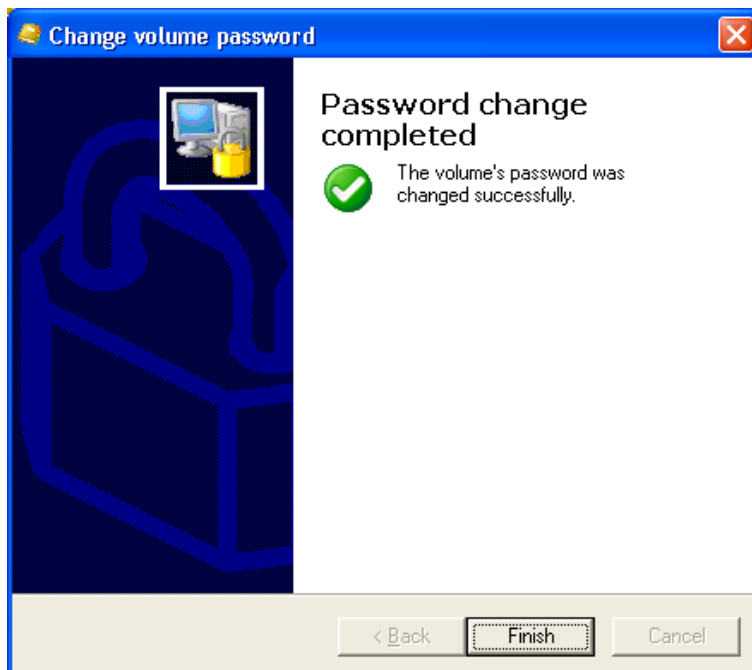


To change a password used to access an encrypted drive, you must know the current password. If you don't know the current password, contact your system administrator.

Click Next.



Type the current password, the new password, and then confirm the new password. If the new password and confirmation are identical and meet your organization's password strength requirements, the "Next"-button becomes available. Click Next.



Click Finish to close the wizard.

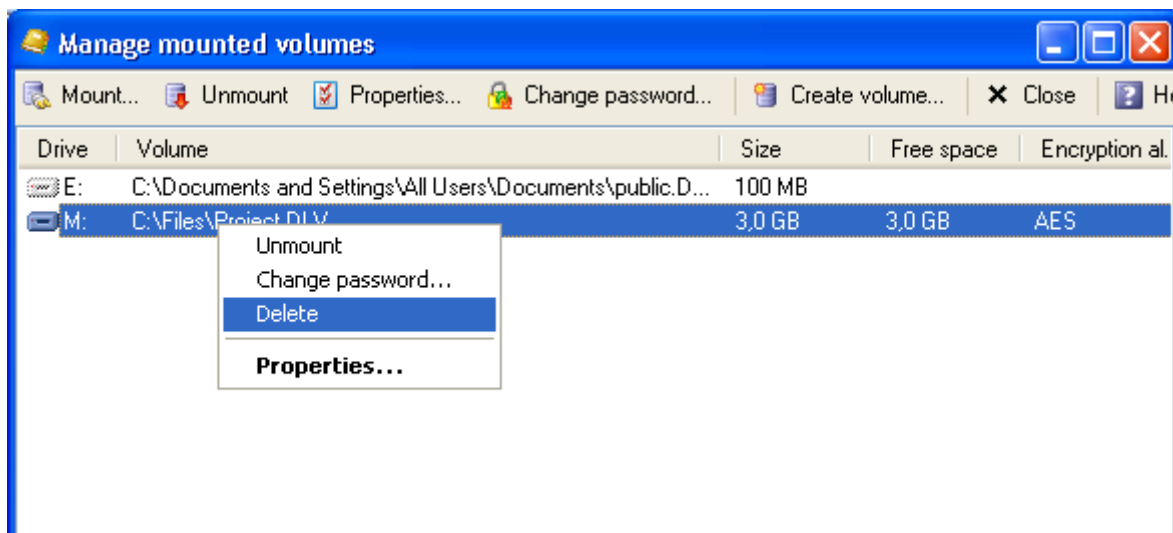
3.5 Deleting Encrypted Containers

You can delete encrypted containers by using the Manage mounted volumes program or by using Windows Explorer.

To open the Manage mounted volumes program, click *Start → Programs → CenterTools DriveLock → Manage mounted volumes*. If the DriveLock taskbar icon is available, you can also right-click it and then click *Manage mounted volumes*.

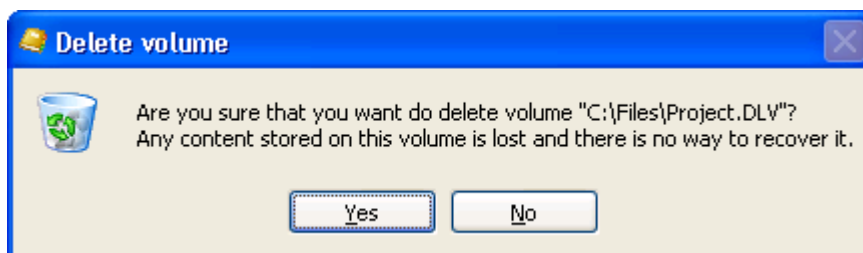


Availability of Start menu entries can vary, depending on your central configuration settings. If an item does not appear, your system administrator may have disabled it.



Right-click a currently connected container and then click *Delete*.

DriveLock prompts you to confirm the deletion.



Click **Yes** to permanently delete the selected container.

You can also delete the *.DLV file by using Windows Explorer after disconnecting the encrypted drive, or by using the secure deletion function of DriveLock. (For more information about secure deletion, see the section “Securely Deleting Data”.)



Secure deletion of an encrypted partition is not possible. Instead use the Windows Drive Manager console to format the partition, or contact your system administrator.

4 The Mobile Encryption Application

To access and use a DriveLock-encrypted drive that is based on a container file on a computer that does not have DriveLock installed, use the Mobile Encryption Application (MEA). The MEA is a small program (DLMobile.exe) that doesn't require any installation steps and puts no files on the computer you run it on.

Use the MEA to mount and unmount encrypted containers and access them in Windows using drive letters. If you run MEA using an account that does not have local administrative rights, you can't access the encrypted drive using a drive letter. Instead, you can view the contents of a container in a window and export or import files and folders.

4.1 Copying the Mobile Encryption Application

To copy MEA to removable media or another location, use the Create Mobile encryption disk wizard. To start the wizard, click “*Start → Programs → CenterTools DriveLock → Create Mobile Encryption Application*”. If the DriveLock taskbar icon is available, you can also right-click it and then click “Create Mobile Encryption Application”.



Availability of Start menu entries can vary, depending on your central configuration settings. If an item does not appear, your system administrator may have disabled it.



Click Next.



Type the location to store the Mobile Encryption Application, or to select a location, click "...".

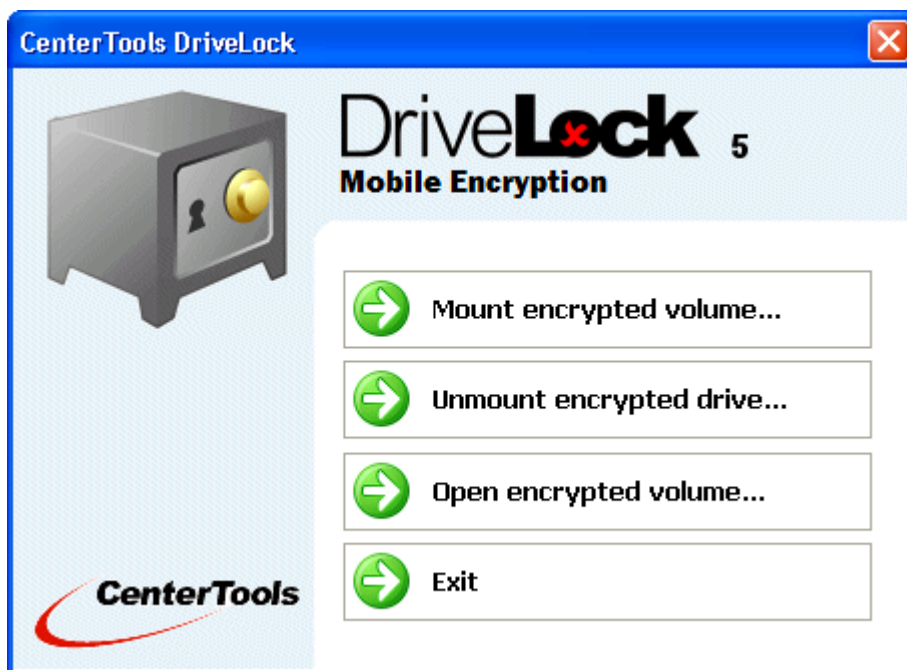
Click Next.



Click Finish to close the wizard.

4.2 Using the Mobile Encryption Application

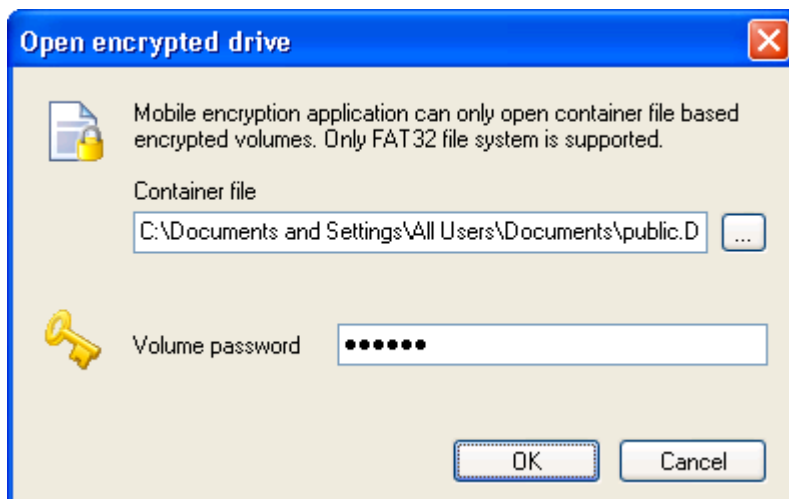
To start the Mobile Encryption Application, double-click the program file (DLMobile.exe).



Click **Mount encrypted volume** to mount a drive by using the wizard described in the section “Connecting an encrypted drive that is based on a container file”.

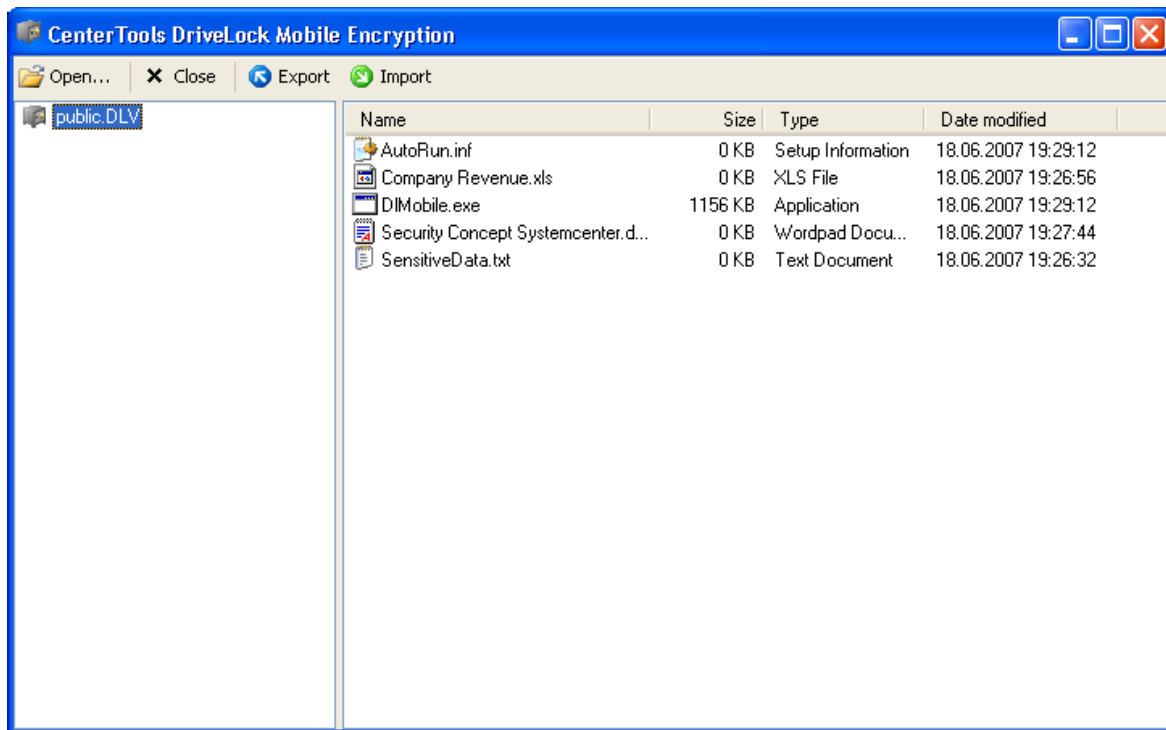
Click **Unmount encrypted drive** to disconnect an encrypted drive by using the wizard described in the section “Disconnecting an encrypted drive”.

Click **Open encrypted volume** to open a container file and view its contents. Use this button to access files on an encrypted drive when you don’t have administrative rights on the local computer. The following steps describe the procedure for accessing an encrypted drive using this method.

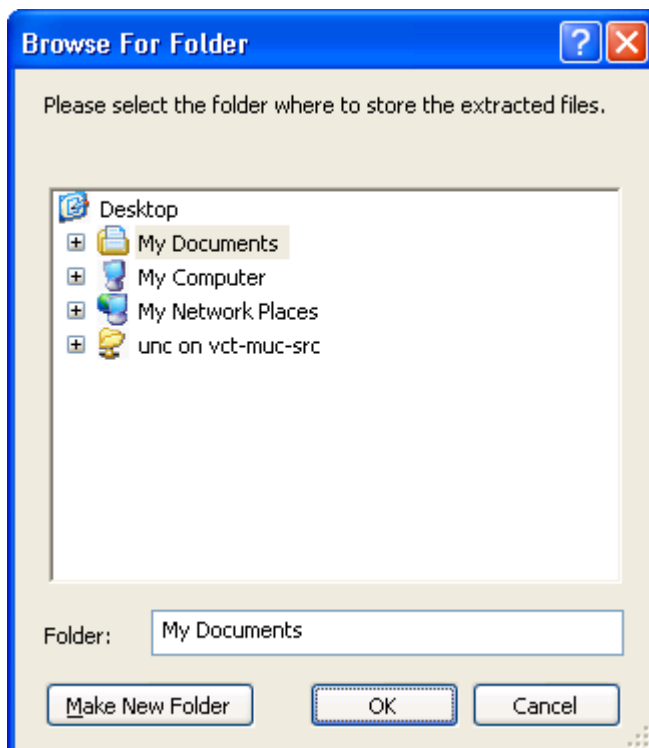


Type or select the name of the encrypted container file, type the encrypted drive password, and then click **OK**.

The MEA Import/Export window opens.



To copy files or directories to a local disk, select one or more items, click **Export**, and then select the folder where you want to store the files.



Click **Import** to copy files from a local disk or network location to the encrypted container.

Click Exit to close “Mobile Encryption Application”.



If the MEA is started from a location that also contains a file with a DLV extension, it automatically prompts you for a password. After you provide the password, MEA mounts or opens the volume, depending on whether you have local administrative rights.

If you detach the removable drive from your computer, DriveLock MEA will automatically unmount the volume.

5 Creating an encrypted CD /DVD

DriveLock's encryption features can be used to store sensitive information in an encrypted container, either on a removable drive or the local hard disk. You can also copy such container files to a recordable CD or DVD by using third-party products or native Windows functionality.

Starting with Version 5.5, DriveLock includes a wizard that lets you to create an encrypted recordable CD or DVD automatically. Use this wizard to select the files to be encrypted and to specify an encryption password. DriveLock then creates an encrypted container, copies the files to it and burns this container to the media. You can also specify whether DriveLock adds the Mobile Encryption Application to the CD or DVD to allow easy access to the data on a computer where DriveLock is not installed.

To start the wizard, click *Start → Programs → CenterTools DriveLock → Record encrypted media*. If the DriveLock taskbar icon is available, you can also right-click it and then click Record encrypted media.



Click Next.

If your computer doesn't meet the prerequisites for recording a disk, the wizard alerts you of the problem:

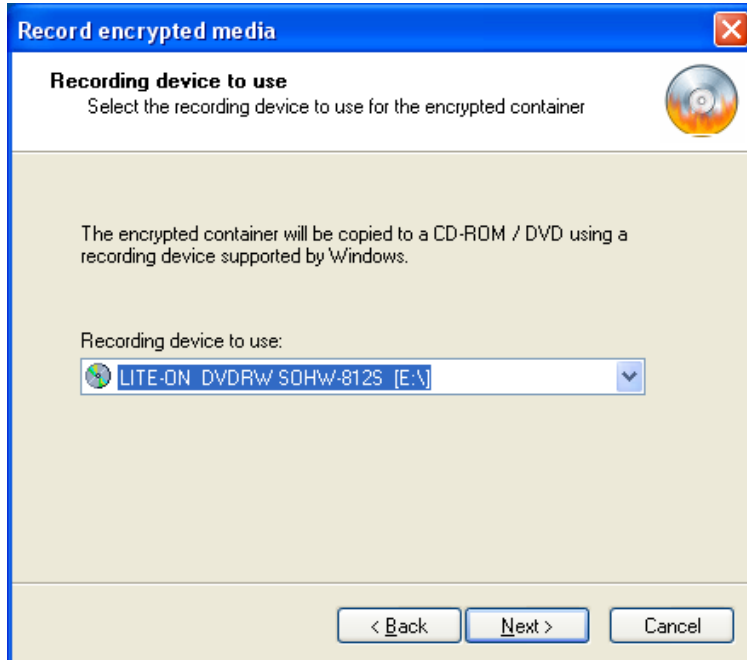


The CD/DVD recording wizard requires that the Image Mastering API (IMAPI v2.0) is installed on your computer. See <http://support.microsoft.com/kb/KB932716> for information on how to obtain this system component for Windows XP. Windows Vista already includes this component.

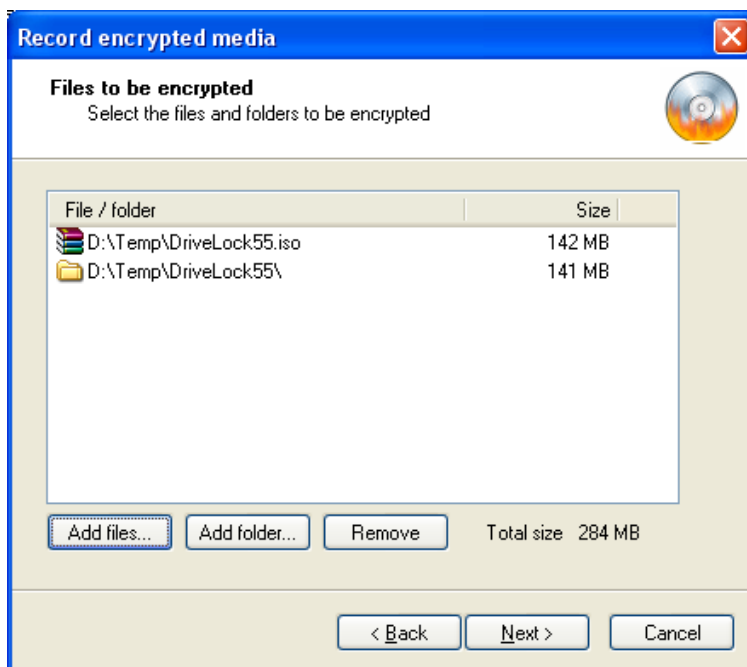
If your computer doesn't contain a drive capable of burning CDs or DVDs the following message appears:



Select a recording device from the list and then click Next.

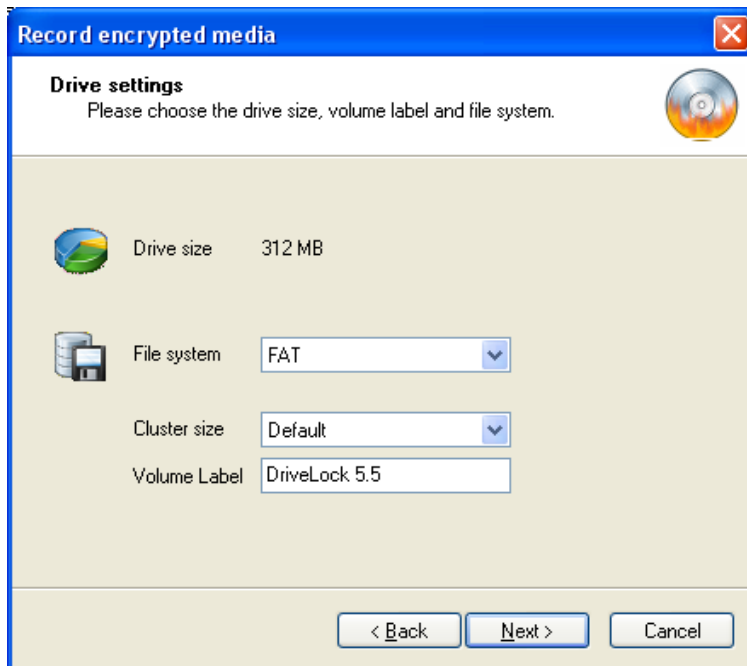


Use the available buttons to add files or folders to the list of items you want to encrypt.

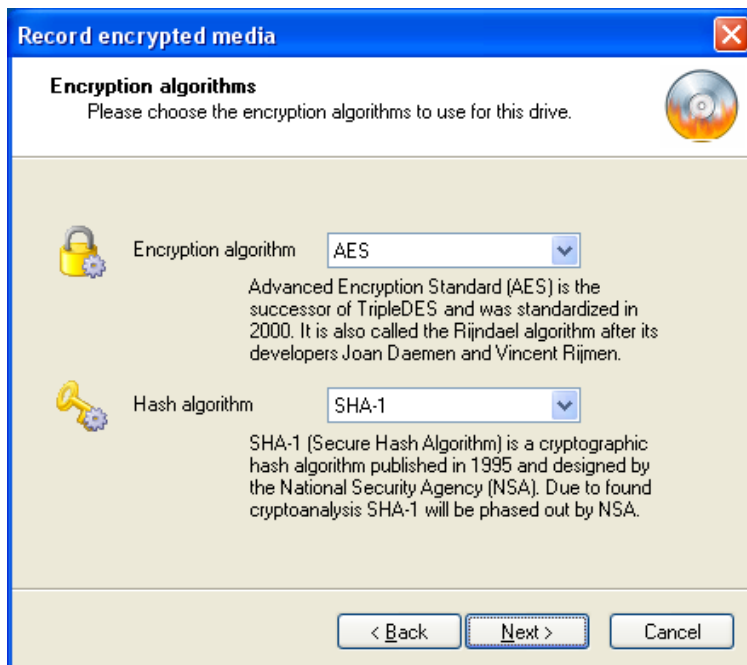


When you select a folder, all files and folders in it will also be copied and encrypted.

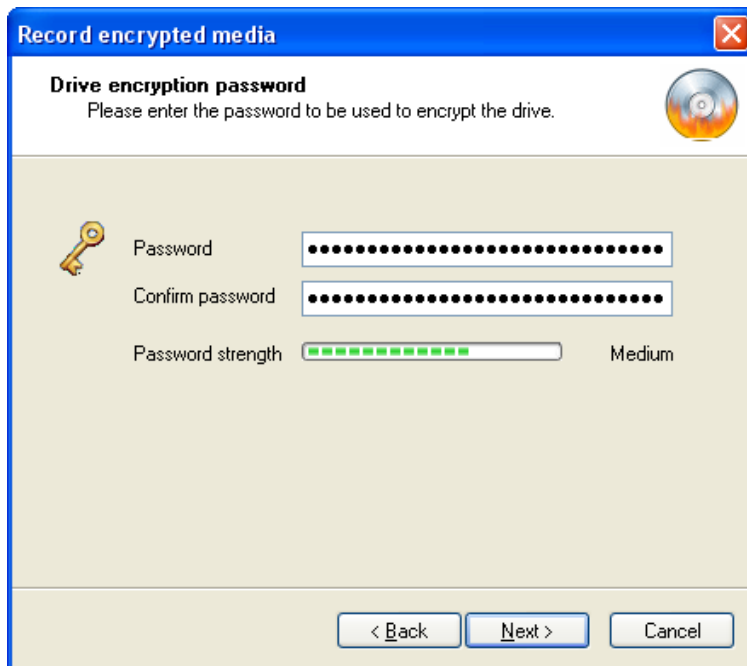
Click Next after you have finished adding files.



Select the file system, cluster size and the volume label for the encrypted volume and then click Next.



Select the encryption and hash algorithms to be used for encryption and then click Next.



Type the password to be used for the encrypted drive, and then confirm the password by typing it again. If both entries are identical and meet your organization's password strength requirements, the "Next"-button becomes available.

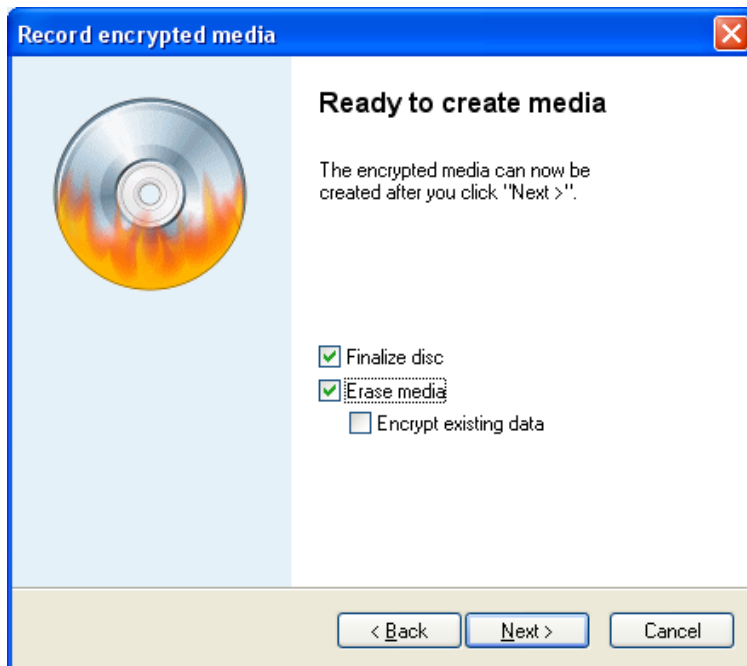
The strength of a password is determined both by its length and the number of unique characters it contains (complexity). As you type the password, DriveLock analyzes both and displays an estimate of the password strength.

Password may include the following characters:

- Upper-case (A-Z)
- Lower case letters (a-z)
- Arabic numerals (0-9)
- Non-alphanumeric characters (e.g. !, \$, #, \ or &)

You can also use a passphrase that consists of multiple words and punctuation instead of a password. Passphrases are typically easier to remember than long complex passwords. If your system administrator configured a requirement for minimum password strength or defined a password complexity policy, DriveLock notifies you of this requirement on this wizard page.

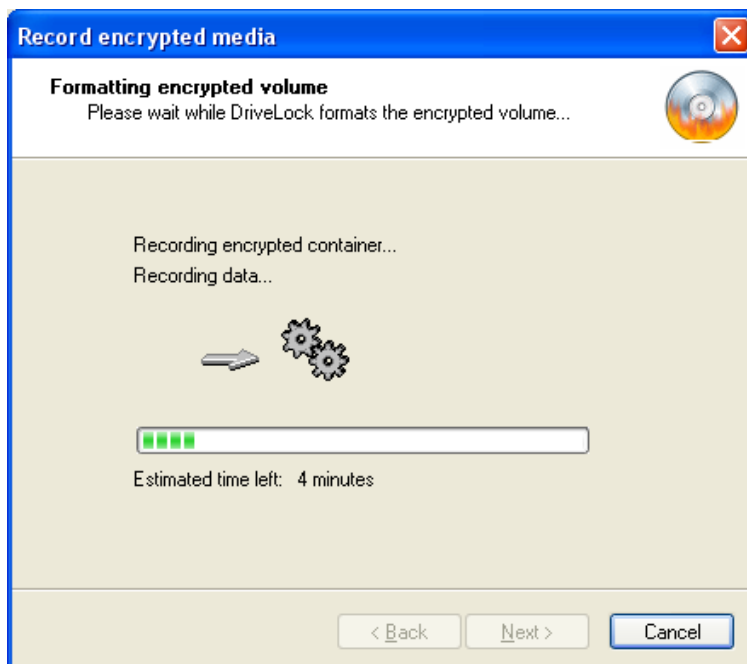
Click Next to continue.



If you want the disc to be finalized check „*Finalize disc*”. Once a disc has been finalized you can no longer add data to it. Finalizing a disc may be required to enable certain disk drives to read it.

When you use a re-writeable disk you can select to erase data from the media first. If you want to keep existing files but encrypt these files in addition to files you added, select the “*Encrypt existing data*” checkbox.

Click Next to continue.



DriveLock creates the encrypted disk.



When the wizard has finished writing to the disk, click Finish to close the wizard.

6 Securely Deleting Data

When you delete files or folders by using Windows Explorer, the data contained in them is not destroyed; but Windows only deletes the corresponding entries in the file system. Many programs exist to recover such deleted files and make the data accessible again.

Erasing sensitive or confidential files normally requires that the data is made permanently inaccessible. To prevent recovery of the data DriveLock can delete files and folders securely. To prevent recovery of the data DriveLock overwrites the files with random data. The deletion algorithm you select determines how many times the data is overwritten and how the random data is generated.

DriveLock can use the following algorithms to securely delete data:

- **DoD 5220.22-M (USA)** – Standard 5220.22-M of the US Department of Defense. Regulations for deleting confidential, secret or top-secret classified data securely are defined in the "National Industrial Security Program Operating Manual". Use of the regulations in this manual is mandatory for the US military and most other government agencies. According to these regulations, data can be deleted by first overwriting it with an arbitrary pattern. Subsequently the data must be overwritten three times, using a different pattern each time. Hard disks containing top-secret information are not allowed to be erased using this method. Instead; they must be physically destroyed or demagnetized. Demagnetizing destroys all magnetic patterns on a disk to make it unusable.
- **Peter Gutmann Algorithm** – Peter Gutmann of the Department of Computer Science at the University of Auckland specializes in the design and analysis of encryption methods. His research results about data deletion on magnetic media are considered leading in this field. The deletion method he developed based on his research results overwrites existing data using several passes. The data patterns used for this operation reduce the risk that any existing data patterns remain on the disk and applies to all known methods for writing to disks. The algorithm consists of 35 overwrite passes and is considered the most secure method to destroy data that doesn't use magnets or physical destruction. This high level of security increases the time required to erase data. Overwriting a hard disk with the Peter Gutmann algorithm takes about seven times as long as using the Bruce Schneider algorithm and about 15 times as long as using the DoD 5220.22-M standard.
- **Bruce Schneider Algorithm** – Bruce Schneider, a well-known security specialist and author, recommends overwriting a hard disk seven times. During the first pass the hard disk is overwritten with the pattern "00"; the second pass uses "11", and the following five passes apply random patterns. The result of this method is similar to the VSITR-standard. However, the randomness of the last five passes adds security by making it extremely difficult to determine whether data patterns on track borders and bit transitions on the hard disk were produced by overwriting the data, or whether

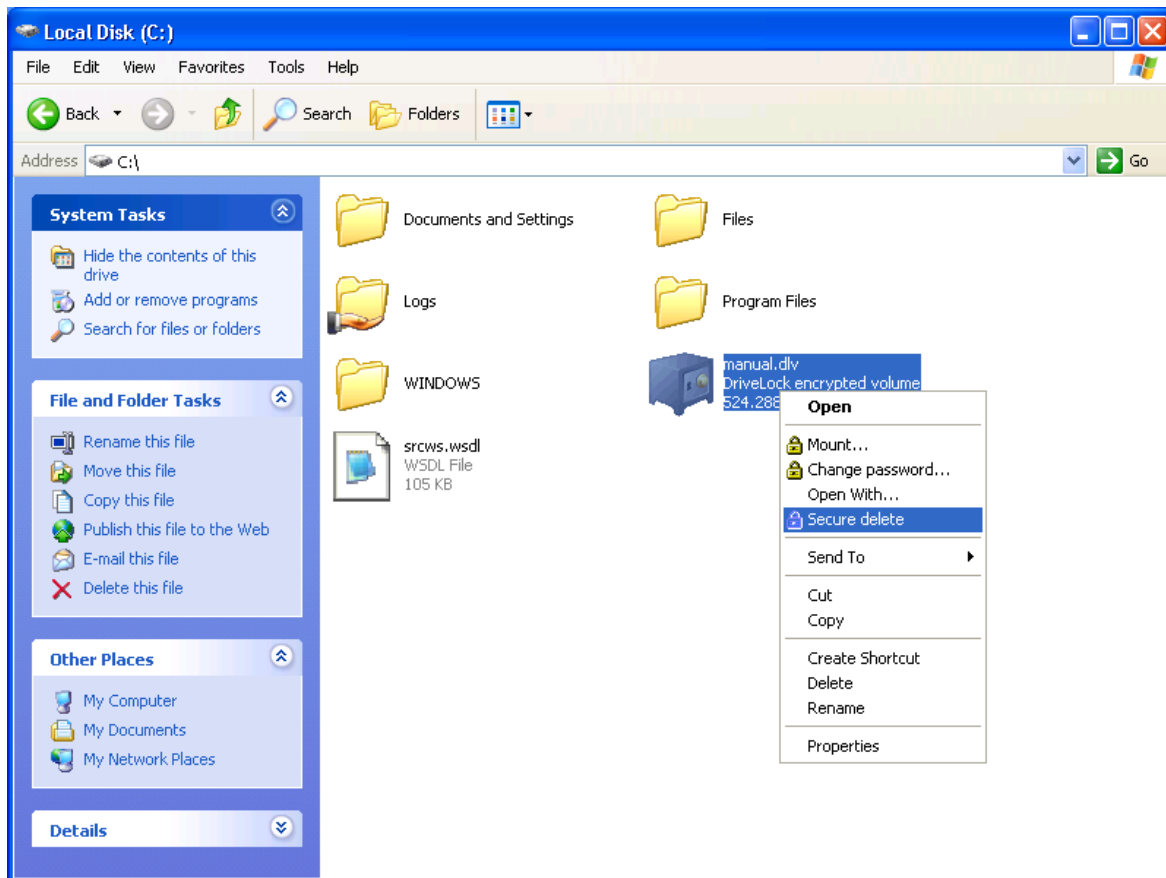
they are remnants of the original data. This method is generally considered more secure than the VSITR standard but takes longer because of the time required to create the random patterns.

- **BSI VSITR (Germany)** – Guidelines of the BSI (German Federal Office for Information Security) for securing confidential data using information technology. The VSITR-standard requires that a hard disk must be overwritten seven times. During each of the first six passes the pattern is inverted from the previous one. This method is designed to “destabilize” data remaining on the track borders. To further decrease the chance of successful data recovery, a final pass is performed, overwriting the data on the hard disk with the pattern „01010101“. This method is generally considered sufficient to securely delete data.
- **Royal Canadian Mounted Police DSX** – The Disk Overwrite utility (DSX) uses a triple pass (“0”, “1” and ASCII pattern generated from the DSX version number and the system time) to overwrite data. DSX was developed by the Royal Canadian Mounted Police (RCMP).
- **DoD 5220.22-M ECE (USA)** – This method is an extension of the DoD 5220.22-M standard. This version of the DoD Standard uses seven passes for overwriting the data. The data is first overwritten twice according to the DoD 5220.22-M (E) standard and then once with random data according to DoD 5220.22-M (C).
- **Random data** – This method uses random data to overwrite the data once. This method is the quickest but has the highest likelihood that some of the data can get recovered

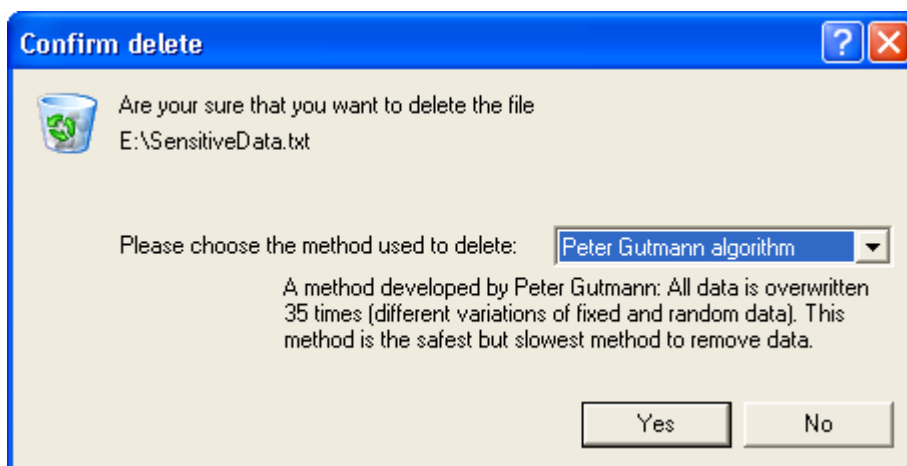


Securely deleting files by overwriting the data multiple times can take a long to complete, especially if files are located in a network location.

To securely delete a file or folder, in Windows Explorer right-click it, and then click Secure delete.



Availability of context menu entries in Windows Explorer can vary, depending on your central configuration settings. If an item does not appear, your system administrator may have disabled it.



Select the algorithm to use for erasing the data and then click Yes.



If you can't select the deletion method, your system administrator has pre-selected it.