cededrive

User Guide

Version 2.7

CEDESOFT

CEDESOFT

For more information or contact details please visit our website:

www.cedesoft.com

Introduction

CedeDrive offers complete data security without changing the way you work. Whether we are aware of it or not, all our data is stored on drives, whether it is hard drives, external drives, flash drives, or network drives. One of the main concerns today is what happens to this data when a drive is lost or stolen.

CedeDrive eliminates this concern by providing a military strength encryption layer between your valuable data and the drive it is stored on. CedeDrive does not alter the way you work, and no additional steps are required to ensure your data is encrypted. One of the best features of CedeDrive is that you will forget it is there, while it silently secures your data as you work.

CedeDrive not only protects the data on your laptop or desktop, it will also secure the data on all of your portable storage devices with one click, turning them into encrypted drives. These include external hard drives, USB flash drives and even network drives.

Features

- **Complete transparency**

  CedeDrive uses on-the-fly virtual drive technology. A virtual drive acts exactly like a normal drive such as your C:\ drive, except it is actually writing and reading from a protected file on any location you choose. CedeDrive uses AES 256-bit military grade encryption technology to secure your valuable data.

- **Robust Security**

  Once secured by CedeDrive's powerful encryption standard, sensitive files and folders are stored safely on your laptop, desktop and all of your portable devices. Working on encrypted files is as easy as entering one single password, and all of your encrypted drives will be mounted automatically ready for you to use just as you would use any USB flash drive or external hard drive.

- **One Click conversion of Flash Drives**

  Convert any Flash Drive or portable hard disk to an encrypted removable drive. CedeDrive will secure any standard Flash Drive with existing data, backup your data, and then convert the drive to an encrypted device. It will then restore your data on the encrypted drive. You can then use this removable drive on any windows computer without installing any additional software.

- **Easy to use and deploy**

  There are no additional steps necessary to encrypt or decrypt your data. It's so easy you'll forget you have CedeDrive installed. Only one password is necessary to mount all of your encrypted drives. CedeDrive also installs in seconds and can be deployed easily across a large network.

Further technical support is available from techsupport@cedesoft.com.

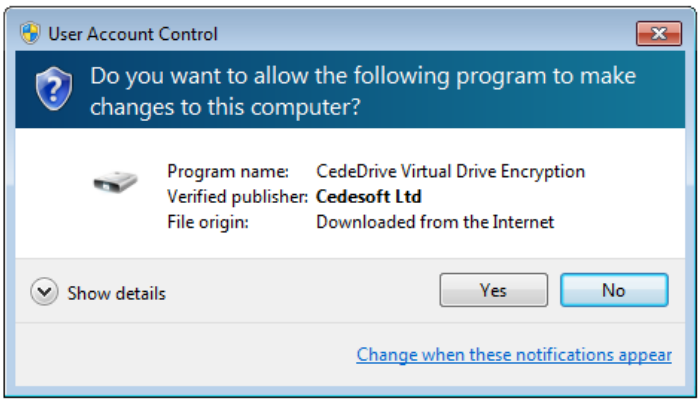
Compatibility

CedeDrive is compatible with all supported Microsoft operating systems. This includes Windows XP (SP2 or later), Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008. 32-bit and 64-bit operating systems are both supported.

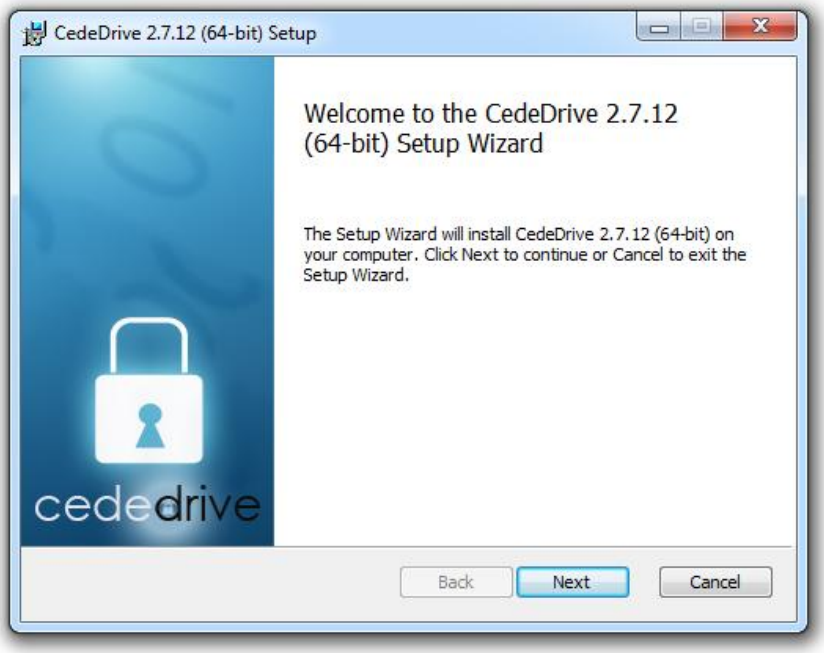
Installing CedeDrive

The CedeDrive installation file is provided in a single setup file. The Setup program will automatically determine whether to install the 32-bit version or the 64-bit version of CedeDrive depending on your current operating system.

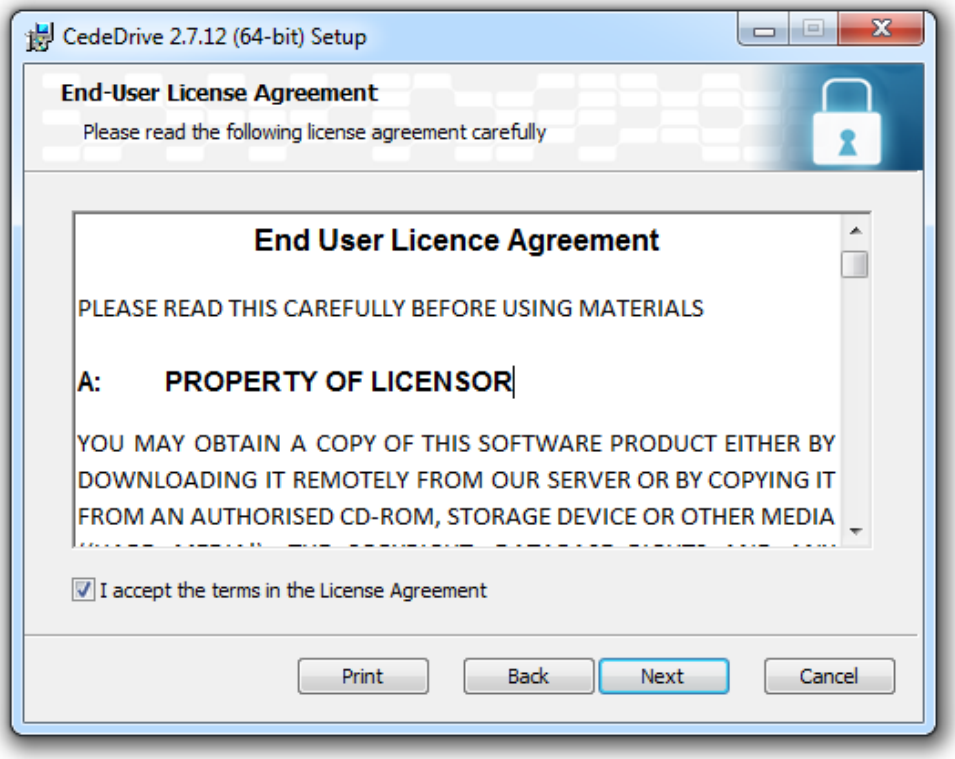
1) Double click the setup file to begin the installation process, and click **Yes** to the User Account Control prompt.



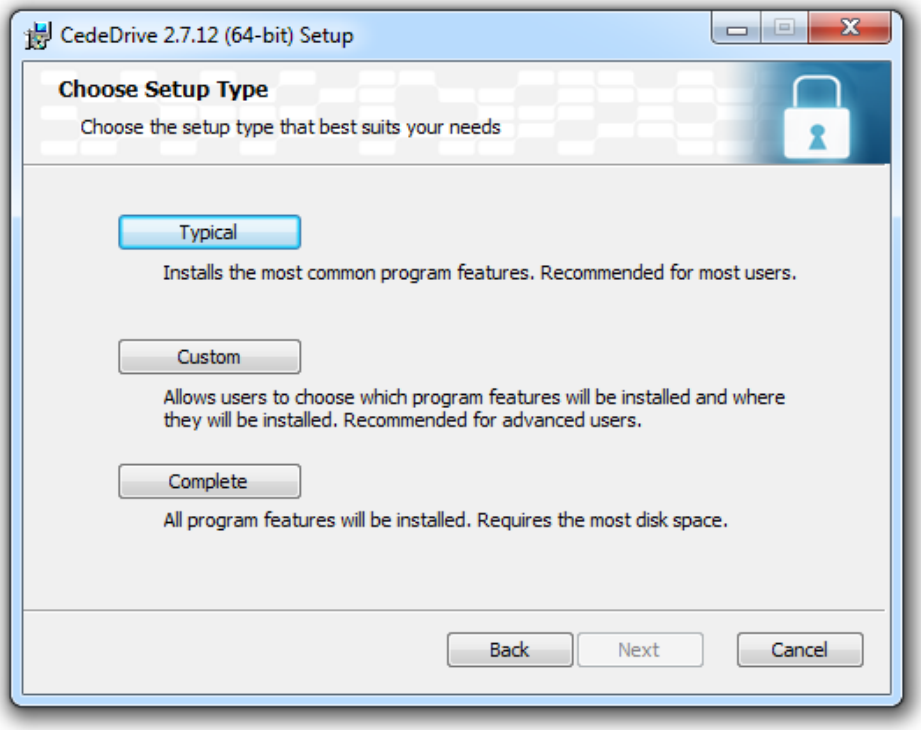
2) Click **Next** to proceed to the license agreement.



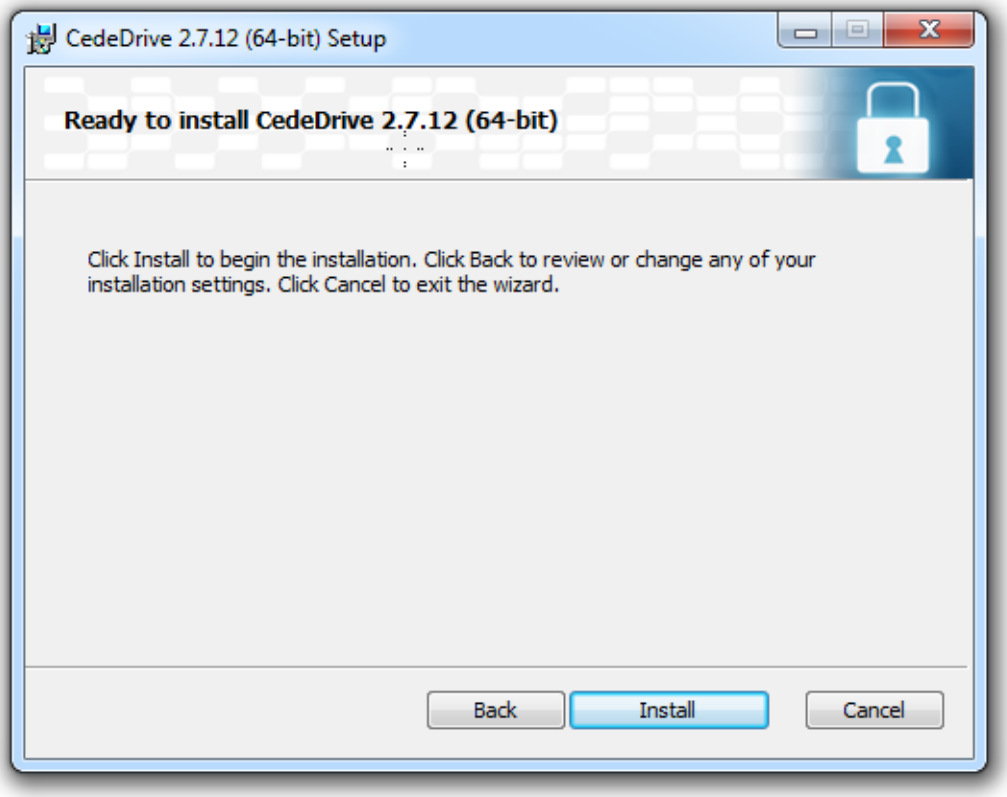
Please read the license agreement provided. Click **I accept the terms in the License Agreement** to continue and click **Next** to accept the license agreement.



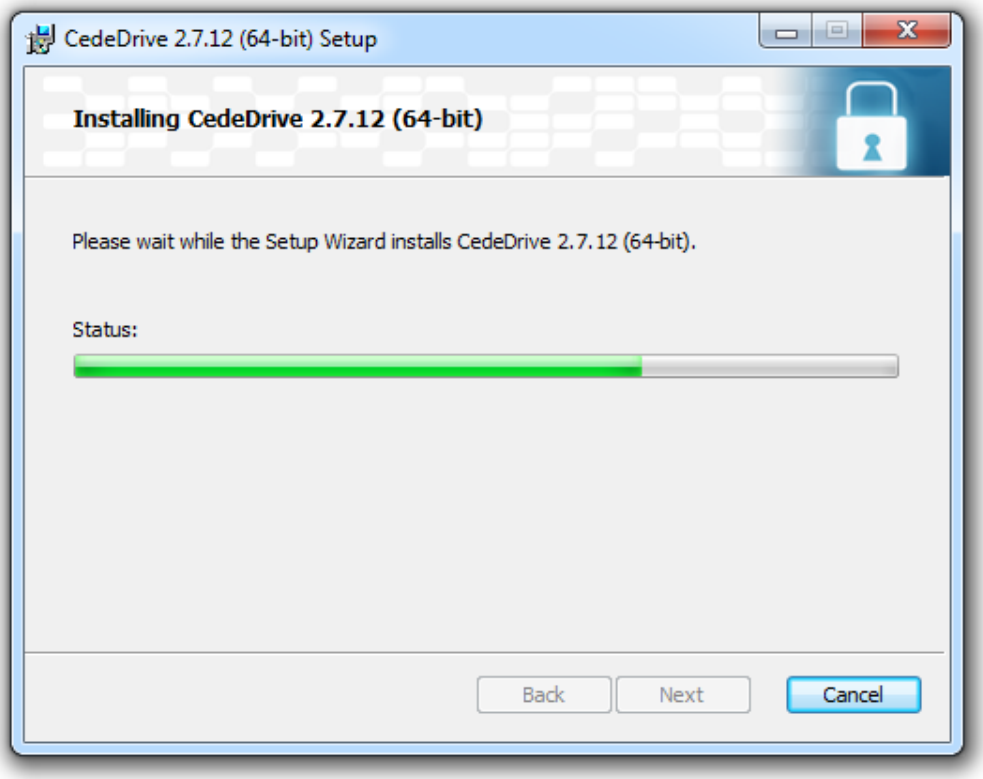
Choose the installation type that best suits your requirements. **Typical** is the recommended installation.



Click **Install** to begin the installation process**.** By default, CedeDrive will install to your Program Files directory on your hard drive.



CedeDrive will install shortcuts by default. These shortcuts will appear on your desktop in addition to your Start Menu in a folder named **CedeDrive.**

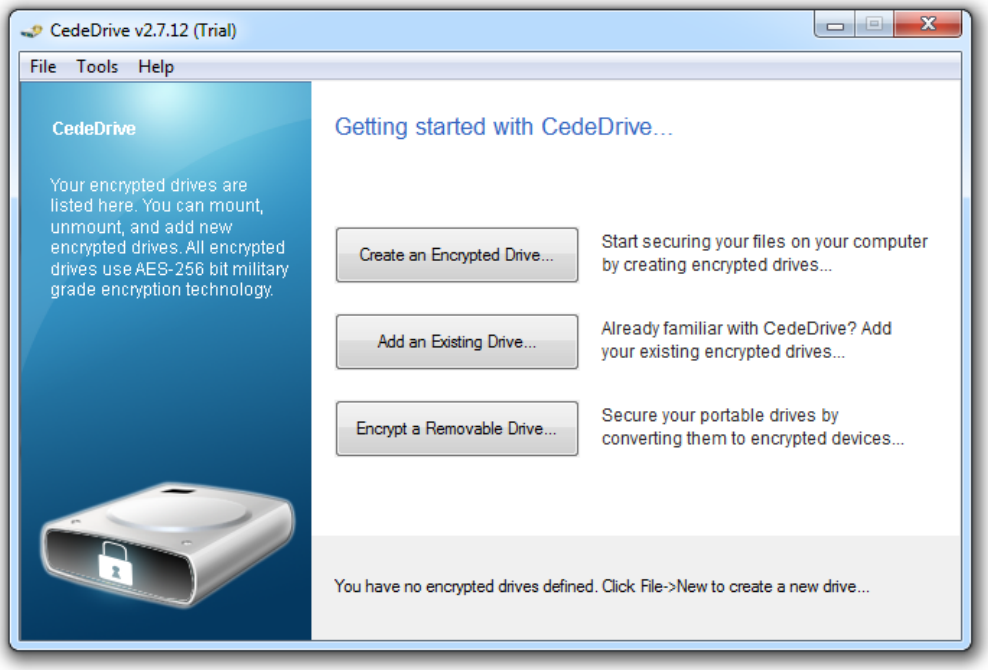


Running CedeDrive for the first time

Once CedeDrive has been installed on your computer, you will have a CedeDrive icon on your desktop. Double Click this icon to run CedeDrive for the first time.

When CedeDrive runs for the first time you will be required to set up a password. This password must then be entered whenever you run CedeDrive in order to mount your encrypted virtual drives. Enter a password in this dialog twice and click **Ok** to complete the first run setup. Once CedeDrive has been setup with a password you will have an additional icon in your system tray.

You can Double Click this icon to access the CedeDrive console. However if this is the first time you are running CedeDrive you will be presented with the Getting started window:



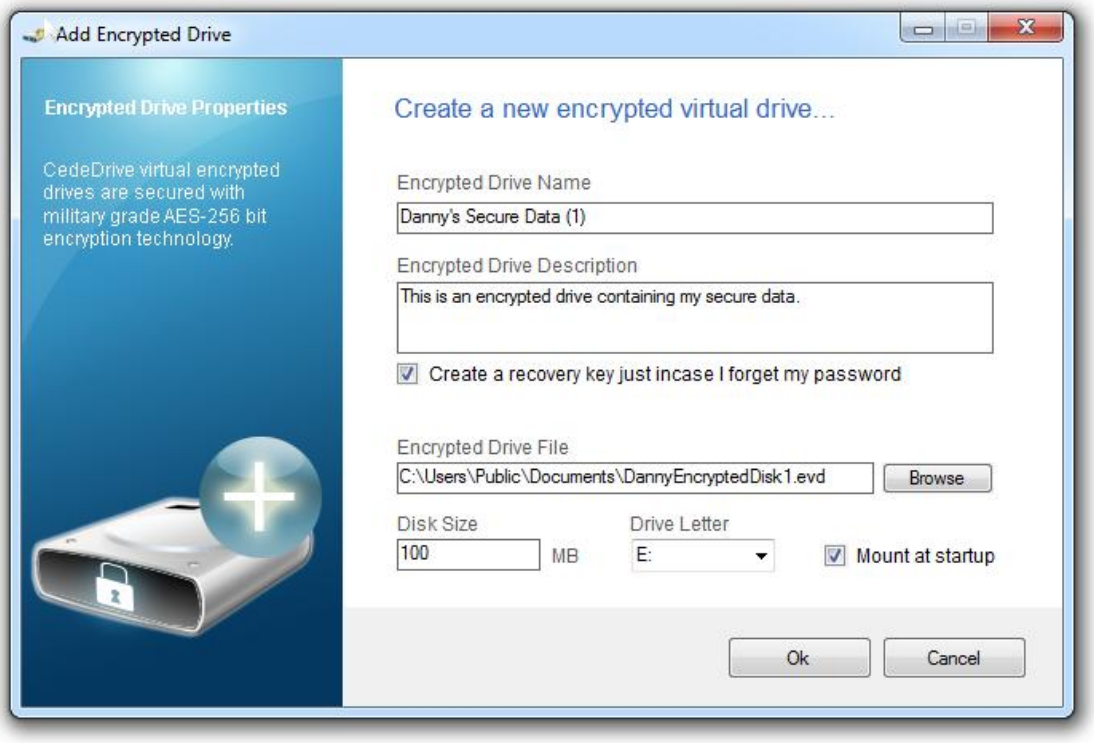
The CedeDrive Getting Started window

Creating an encrypted drive

To begin creating encrypted virtual drives, click the 

button.

The following dialog will be displayed:



CedeDrive will automatically fill in the required information in this dialog, however if you wish to change any of the properties you can do so in this dialog. To accept the default values and create the encrypted drive, click **Ok**.

Encrypted Drive Name

This is the name of your new encrypted drive. E.g. this might be “Work” or “My Personal Data”. The purpose of the encrypted drive name is to help you to distinguish multiple virtual drives in the list if you have created more than one.

Encrypted Drive Description

You can enter a description of your virtual drive here which might describe the data that it contains. This is helpful if multiple virtual drives are created on the computer.

Encrypted Drive File

Click **Browse** to choose a location to store the encrypted drive file. When your encrypted drive has been mounted, all of the data stored on the drive will be encrypted and written to this file. It is important to choose a location on your computer where you have full write access. CedeDrive will automatically place your new encrypted drive under your Documents folder, and will automatically number the files.

Disk Size

Specify the size **in Megabytes (MB)** of the encrypted virtual drive. To create a drive of 2GB in size, enter 2000. To create a drive of 500GB enter 500000. There are 1024 megabytes in 1 gigabyte. It is important to ensure you have enough disk space on your computer in the target location before continuing. CedeDrive will default to a value of 100MB.

Drive Letter

When your virtual drive is mounted it will appear as any other hard drive on your computer. You can choose the drive letter which will always be assigned to this virtual drive. CedeDrive will automatically pick an appropriate drive letter, however if you wish to choose another drive letter you can click the Drop Down list to view available drive letters you can use.

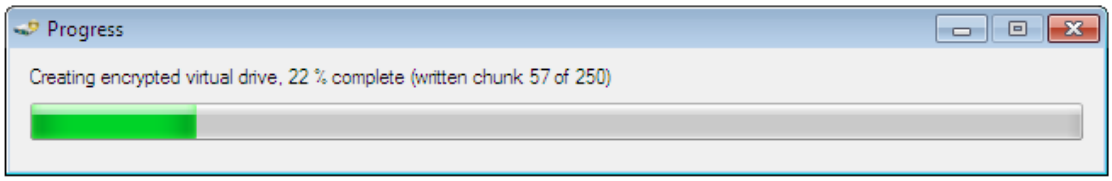
Mount on start-up

If you would like this virtual drive to be mounted automatically every time CedeDrive starts, then ensure this box is checked. If not, leave this box unchecked and you can mount this drive manually by using the CedeDrive console.

Create a recovery key just in case I forget my password

If you would like the ability to recover the password you used to create your encrypted drives, then ensure this option is ticked. If you have chosen to create a recovery key you will be prompted to save this recovery key. NOTE: It is strongly recommended to store your recovery key separate from the computer on which you have CedeDrive installed, and to absolutely not disclose this key. Recovery keys are created using RSA 4096 bit Certified Encryption.

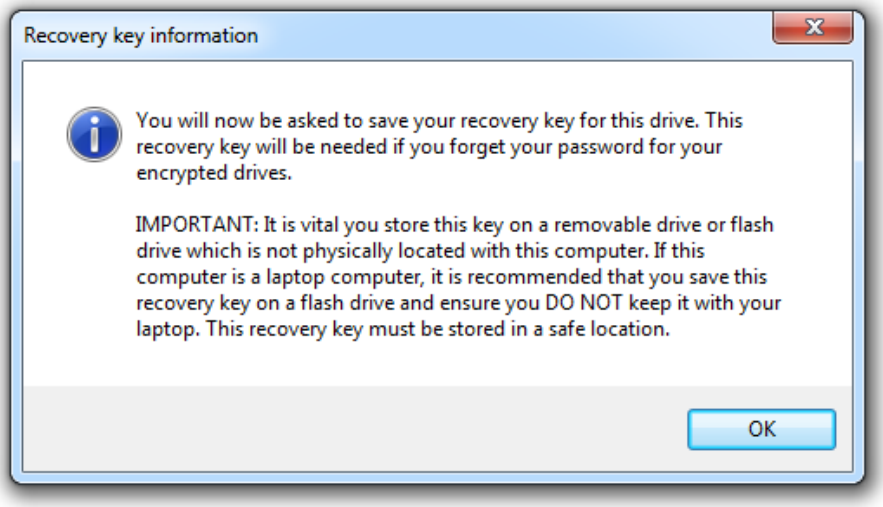
Once you are happy with all of the virtual drive details, click **Ok.** The virtual drive will then be created, and a progress bar will be displayed indicating the progress of the virtual drive creation.



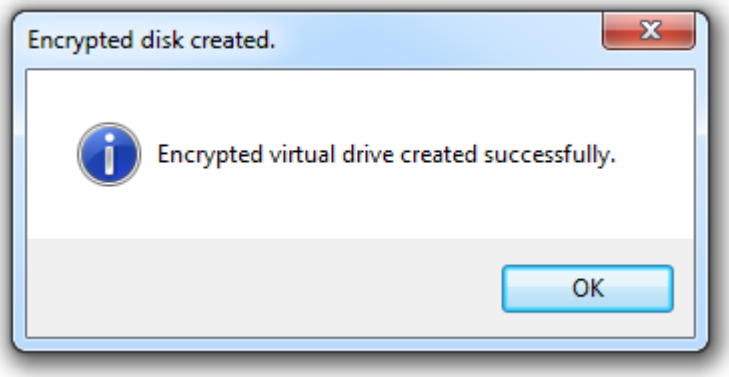
NOTE: The amount of time this takes depends on the size of the virtual drive you have created. E.g a virtual drive size of 250MB may take several seconds to create, whereas a virtual drive size of 80GB may take several minutes to create.

If you have chosen to create a recovery key for your encrypted drive, you will be prompted to save this recovery key. We recommend using a Flash Drive,

and storing the Flash Drive in a physically secure location, as this recovery key will enable recovery of your password.

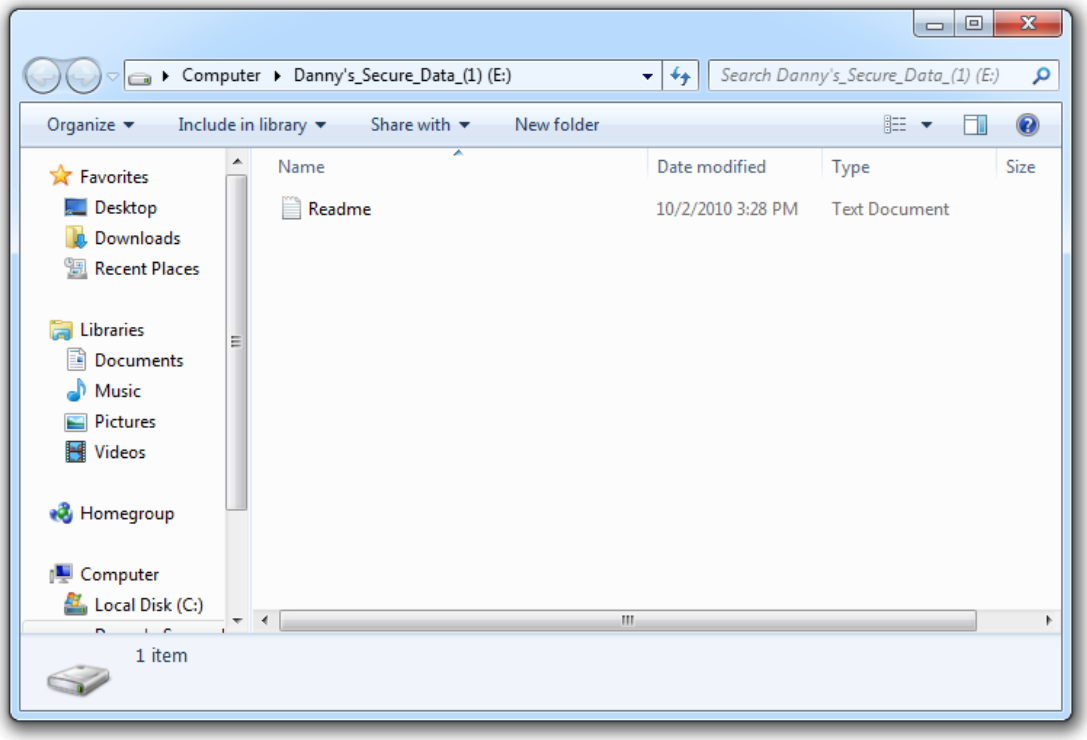


Once the virtual drive has been created, you will be presented with the following dialog:



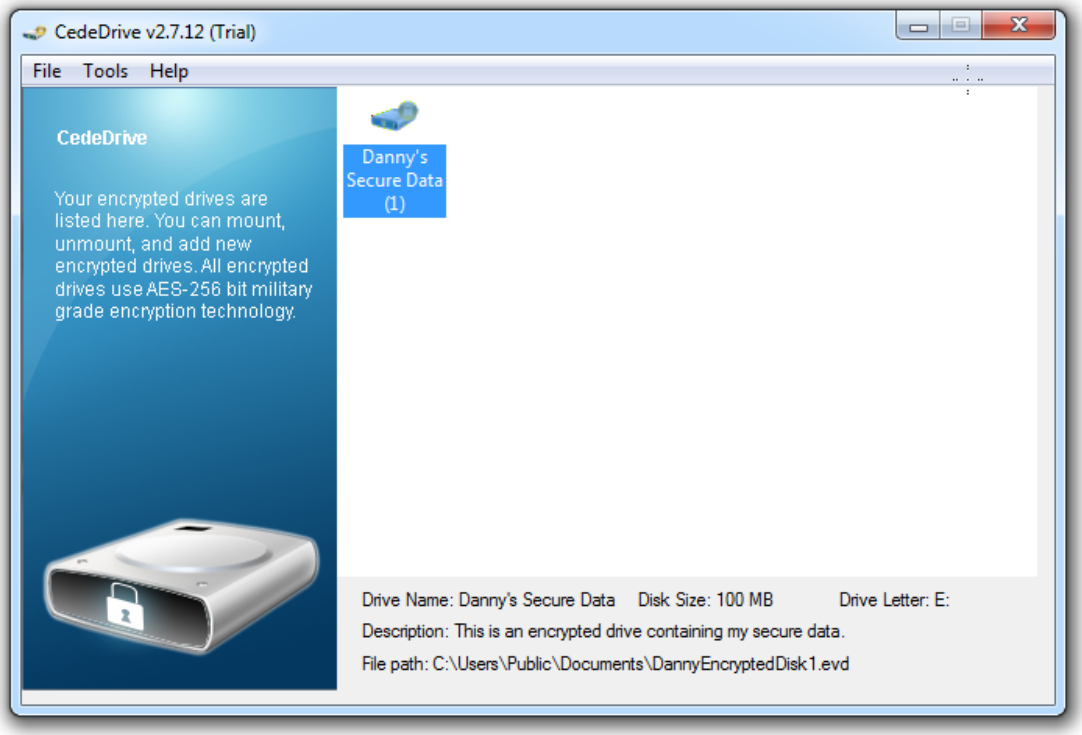
Using your new encrypted drive

Once you have created your new encrypted drive, you will have a new icon in the CedeDrive console with the name of your new drive. Your new encrypted drive will automatically be formatted and ready for you to use immediately. Once your encrypted drive has been created, CedeDrive will display the drive using Windows Explorer, as shown below:



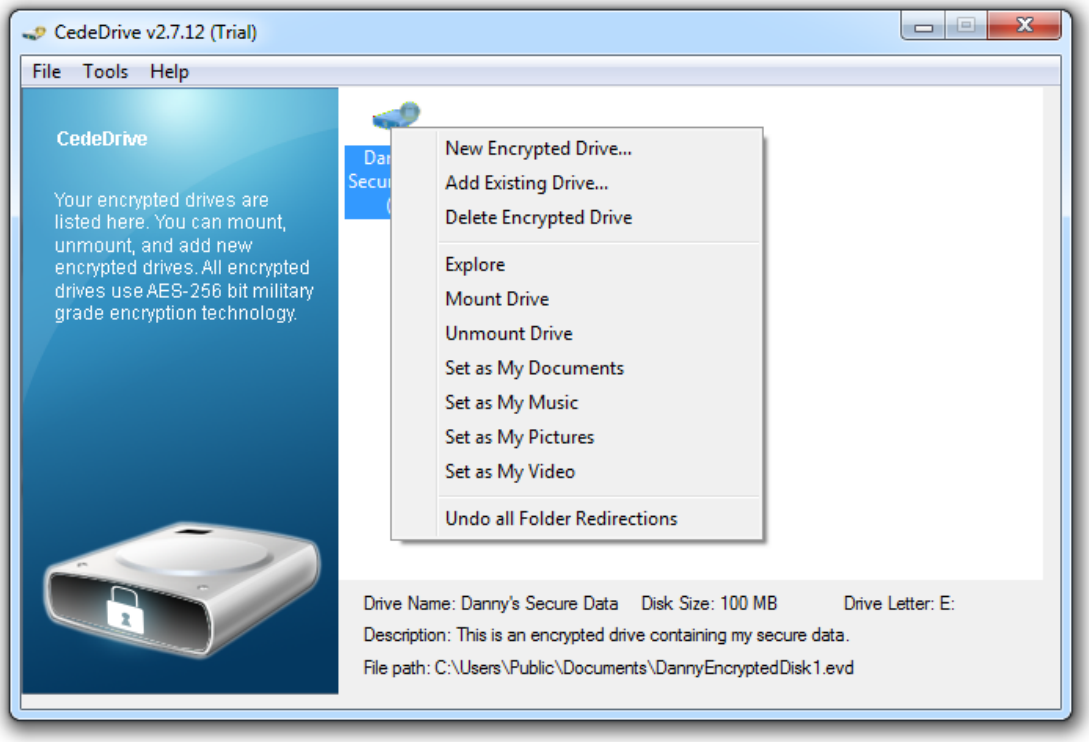
You will notice a Readme.txt file on your new Encrypted Drive which contains a brief description of your new encrypted drive.

To manage your encrypted drives, you can use the console window:

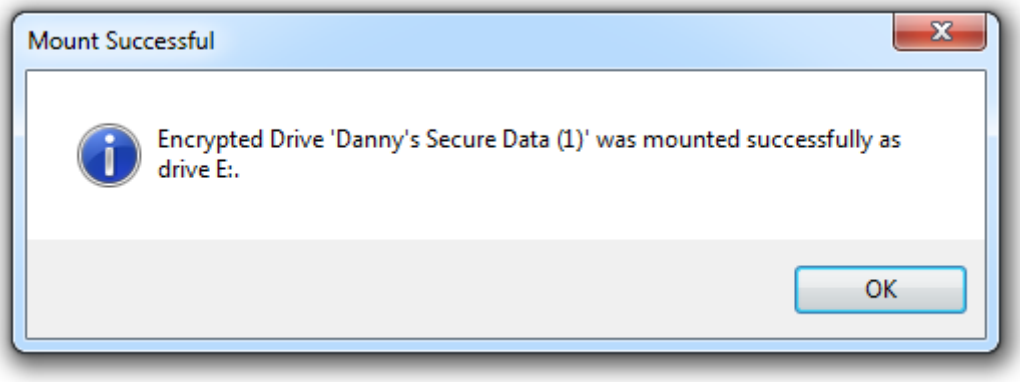


In this example, we have created a new drive named “Danny’s Secure Data”. To manage this drive, right click on the drive icon in the console window and

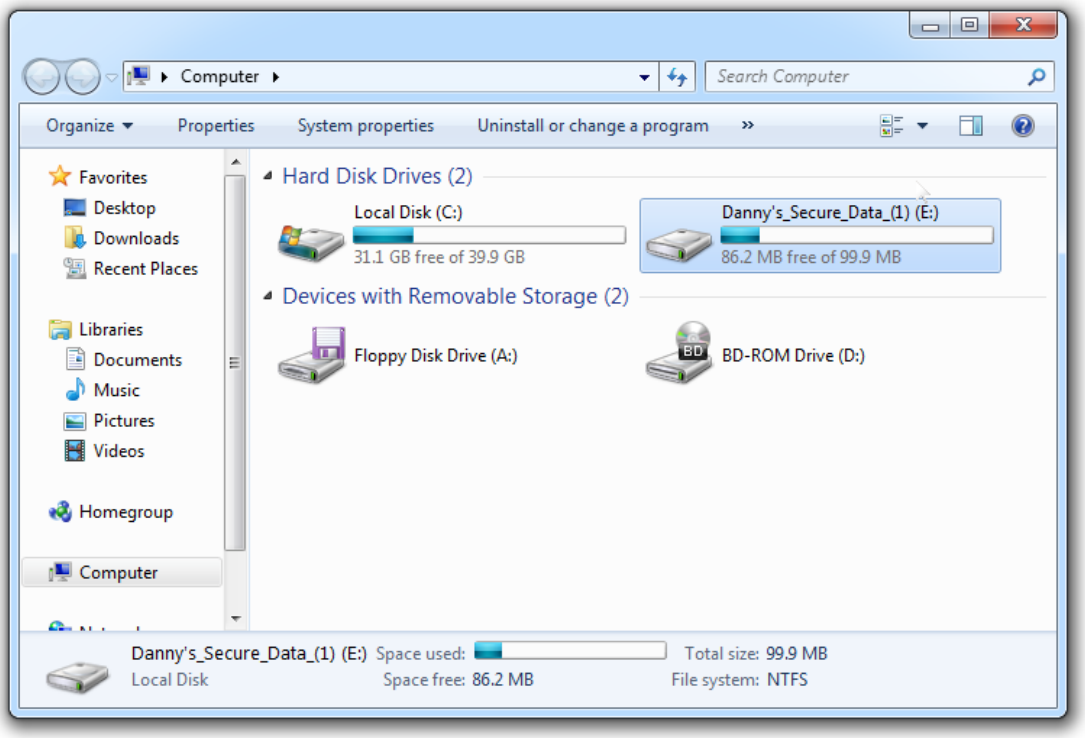
you will have the option to Mount, Unmount, Delete the drive or Create a new drive. By Default, CedeDrive will mount new encrypted drives for you automatically.



If you choose to mount the drive, you will see the following dialog.



All Encrypted Drives can be shown by clicking **Start -> My Computer.**

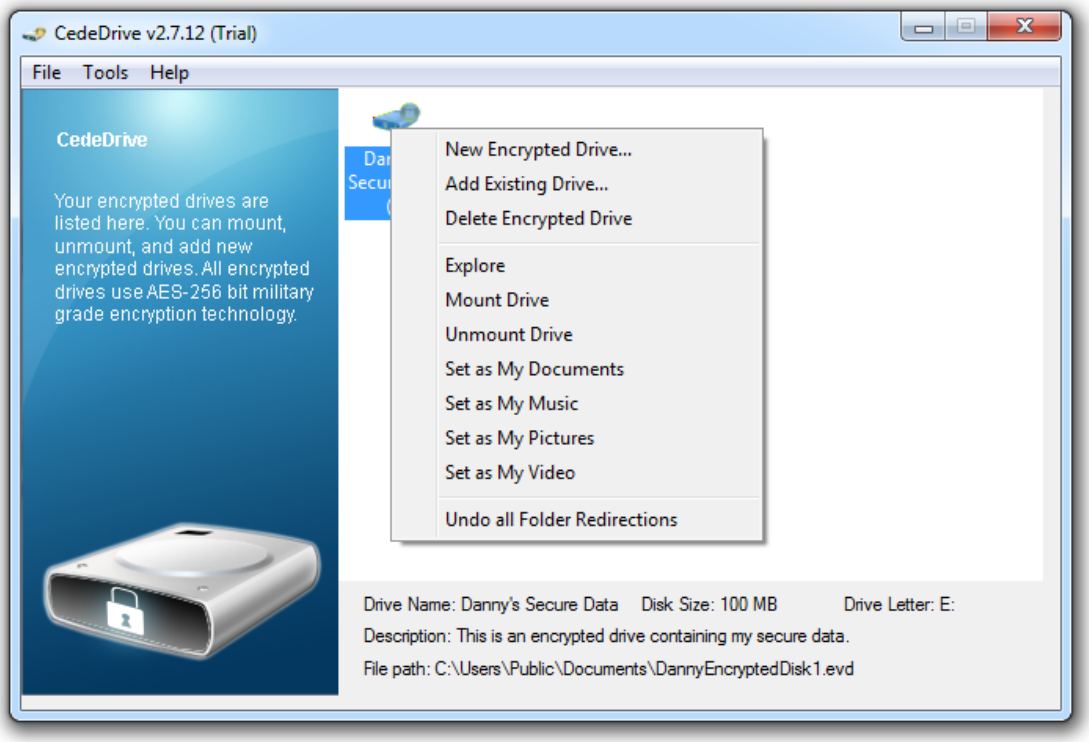


New encrypted drive ready for use

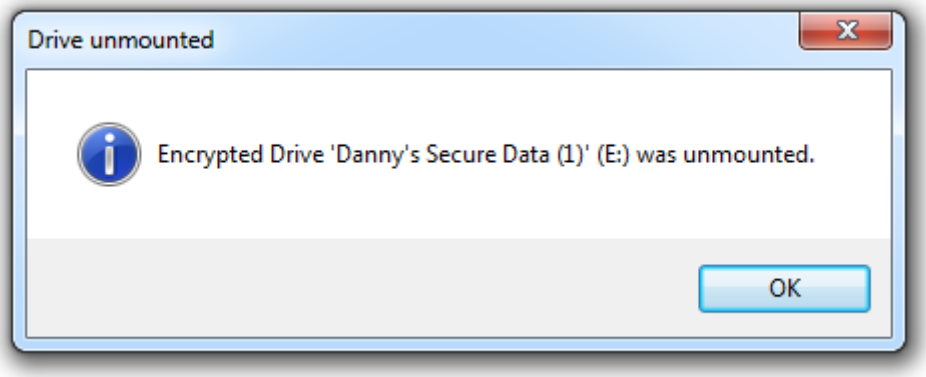
As shown above, Windows will display your new encrypted virtual drive just like any other hard disk in your computer. The only difference is, under the hood all of the read and write requests are being encrypted and stored in the **EncryptedDisk.evd** file you specified when creating your new virtual drive.

Unmounting encrypted drives

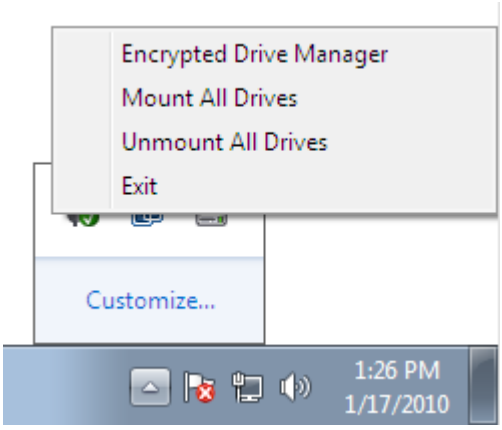
There are two ways to unmount virtual drives when you no longer wish to use them. You can either use the console window and unmount the drive by right clicking on the drive icon and selecting **Unmount drive**...



Once the drive has been unmounted, you will see the following dialog:



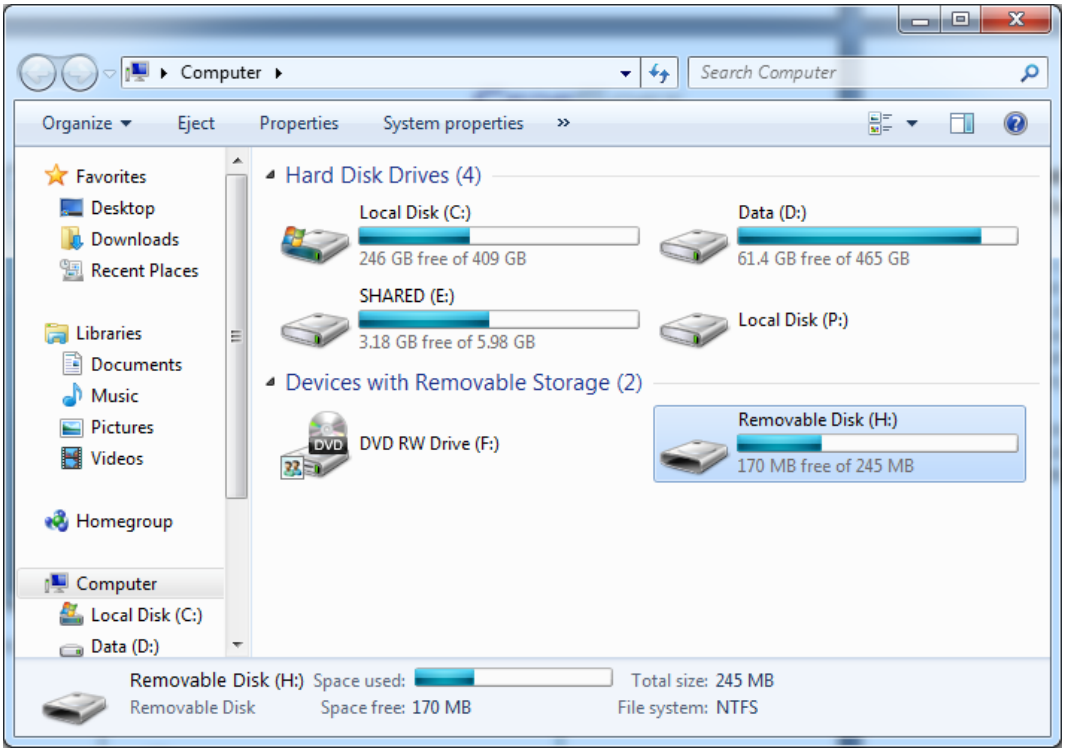
The alternative way, and possibly the quickest way to unmount an encrypted drive is to right click on the icon in the system tray and select **Unmount All Drives.**



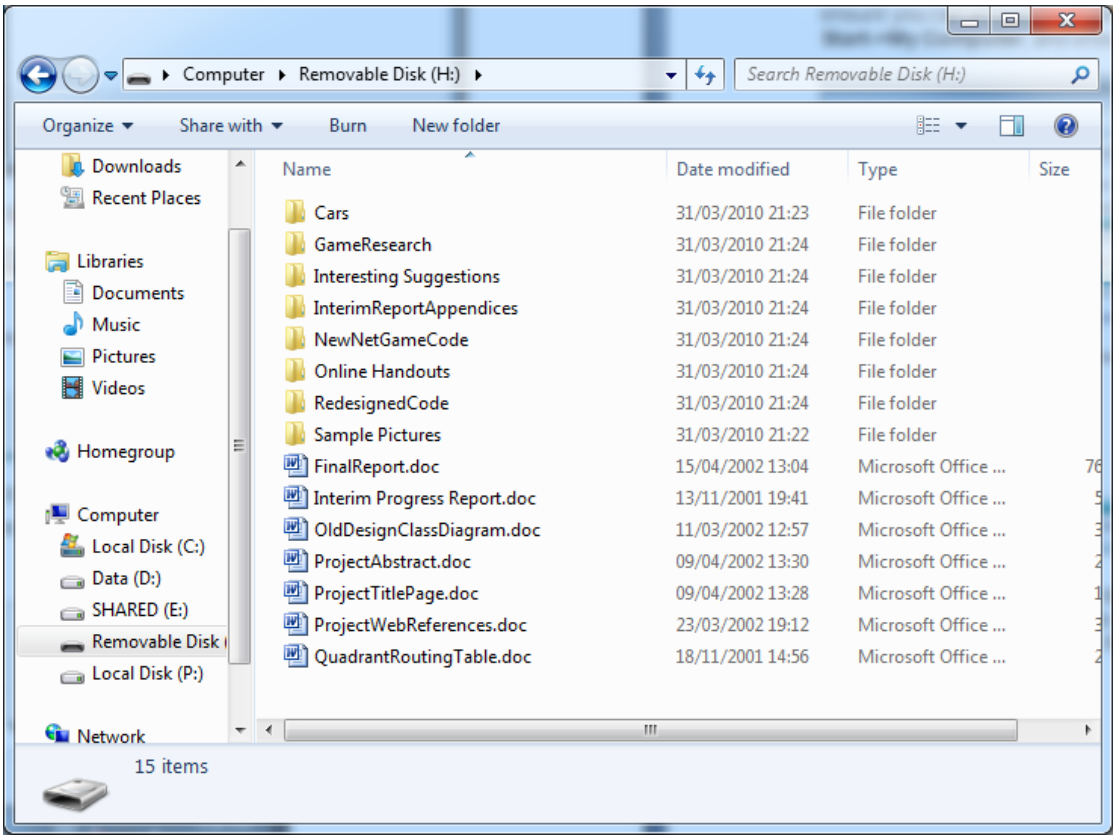
One Click Conversion of Flash Drives / Removable Drives

One of the unique features of CedeDrive is to convert any standard Flash Drive with existing data to a fully encrypted drive so that you can use it in any other windows computer without having to install additional software. The converted drive functions **exactly** like a hardware encrypted flash drive. The advantage with CedeDrive is that you can also convert removable hard disks of any size to encrypted devices.

To begin, first plug your Flash Drive into your Computer's USB port, and ensure you can access the Flash Drive. The best way to check this is to click **Start->My Computer**, and ensure you can see your Flash Drive:



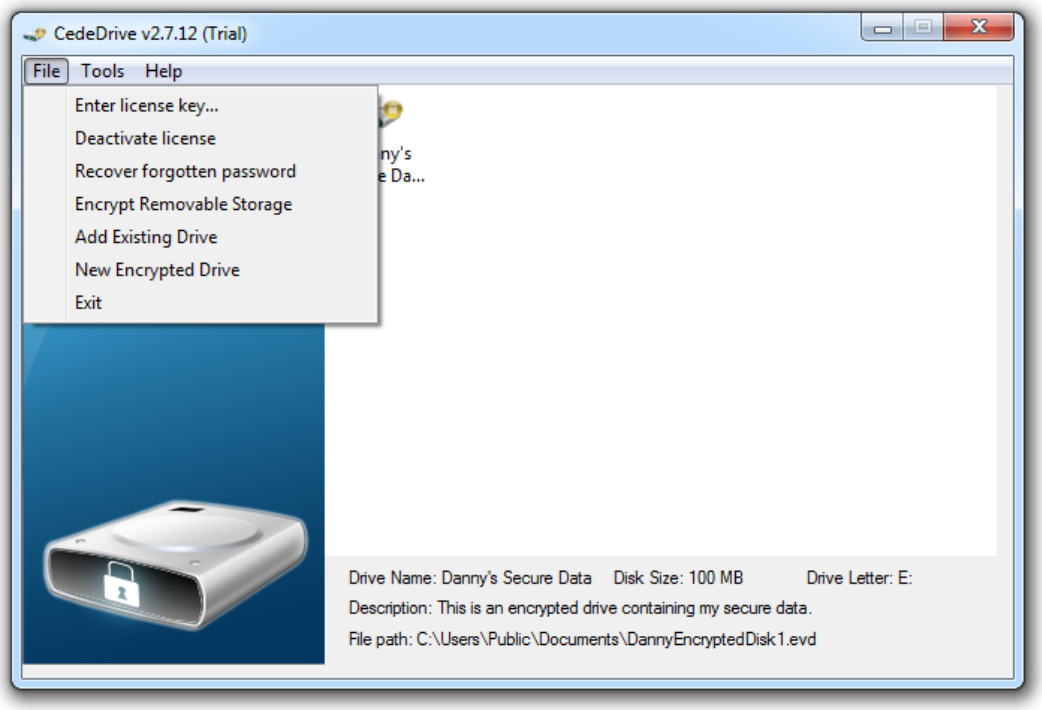
In this example, drive H: is the flash drive which will be converted to an encrypted drive. If we open this drive we can see that there are some images and documents already on the flash drive.



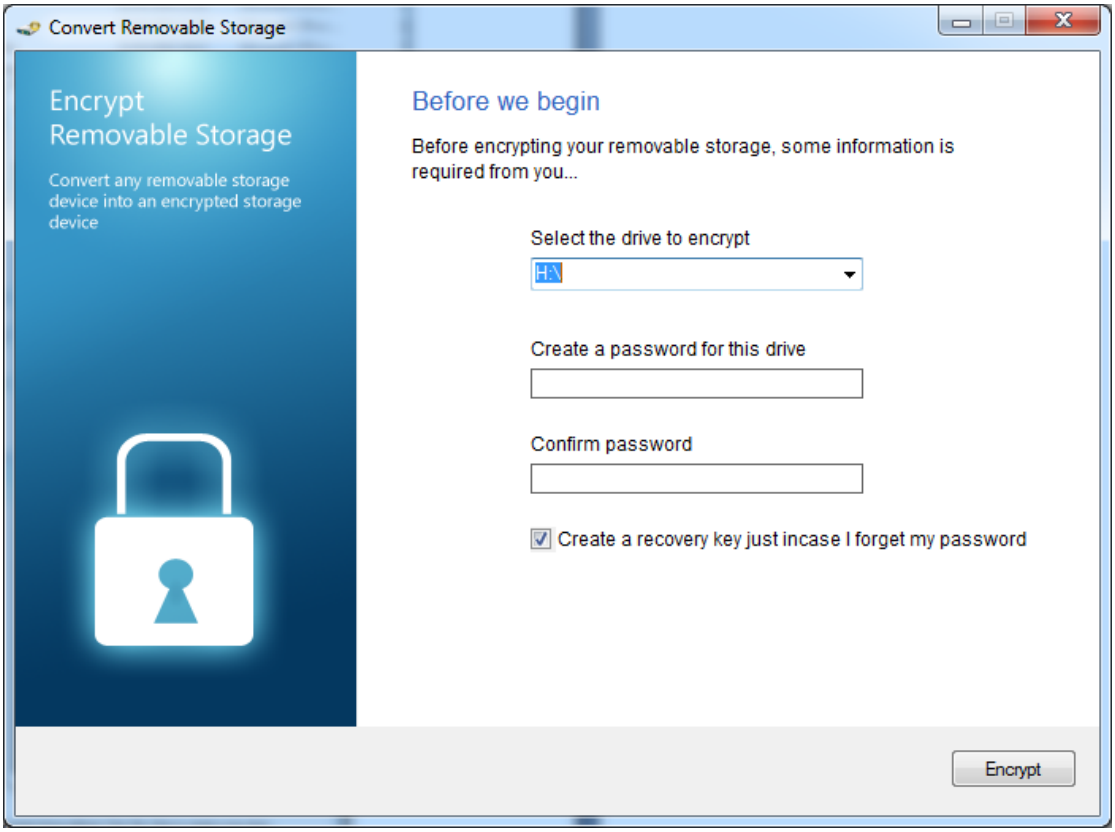
Flash Drive with existing data ready to be encrypted

Once you've confirmed the Flash drive is accessible, open the CedeDrive Console window by double clicking the icon in your system tray.

To start the one-click conversion process, click **File->Encrypt Removable Storage:**



You will then be presented with the Convert Removable Storage Dialog. CedeDrive will automatically try to detect your Flash Drive, however if you have more than one Flash drive connected to your computer you can select the drive you wish to convert from the drop down list.

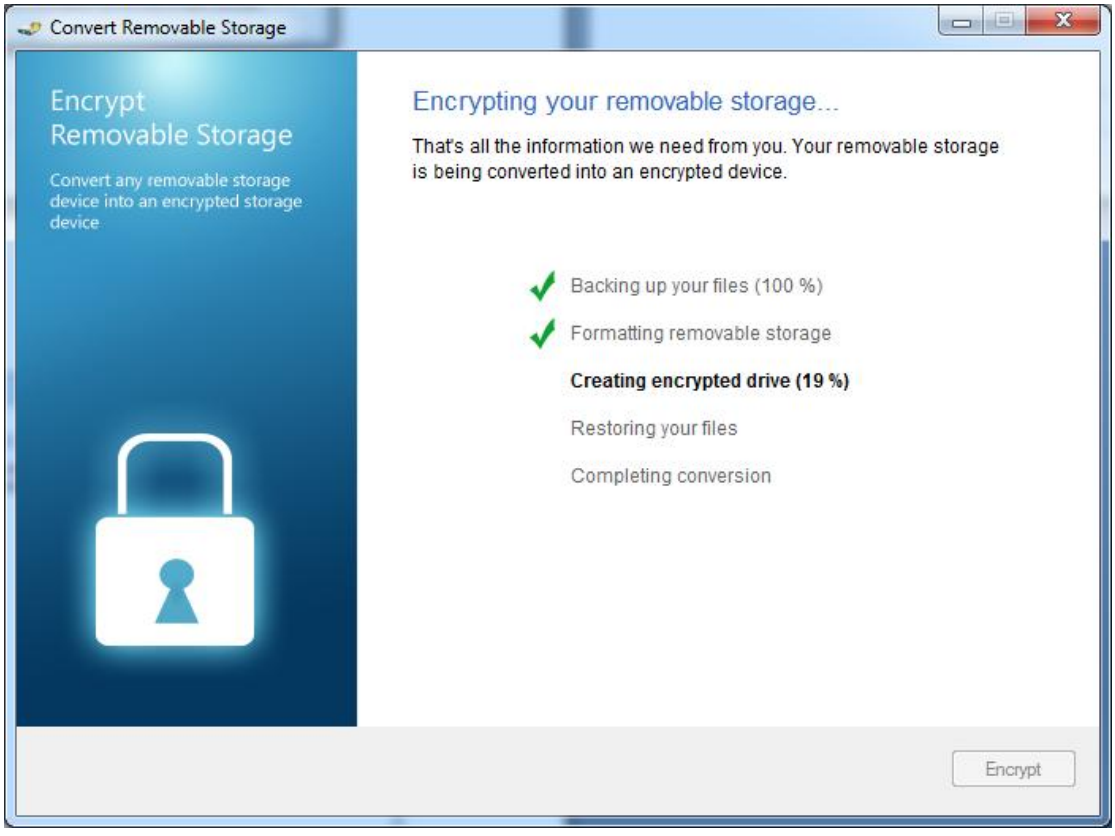


In this example we will be converting drive H:\. You will be required to enter a password for your removable drive. This password will be required whenever you wish to use your encrypted flash drive in any computer.

You can also create a recovery key much like with standard encrypted drives, just in case you forget your password. If this option is selected you will be asked to save the recovery key. It is important to save this recovery key in a location that will not be physically located with your Encrypted Flash Drive, as this will enable recovery of your password.

Once you have entered a password, and selected the correct drive you wish to convert, click **Encrypt.** This will begin the conversion of your Flash Drive to an Encrypted device.

The conversion process consists of 5 stages as shown below.

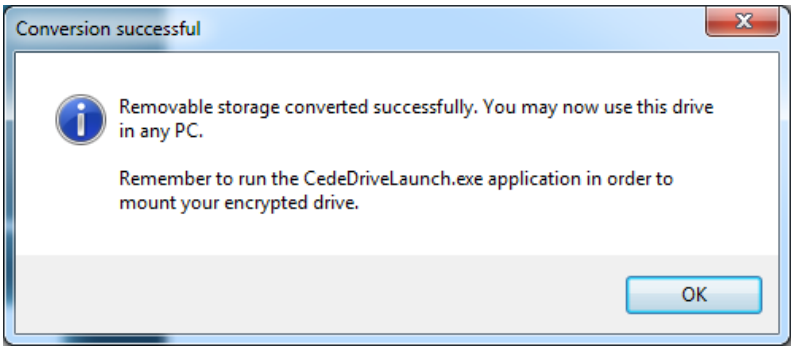


All of the data on your Flash Drive will automatically be backed up. Once the backup process has completed successfully, the Flash Drive will then be formatted and converted to an NTFS drive.

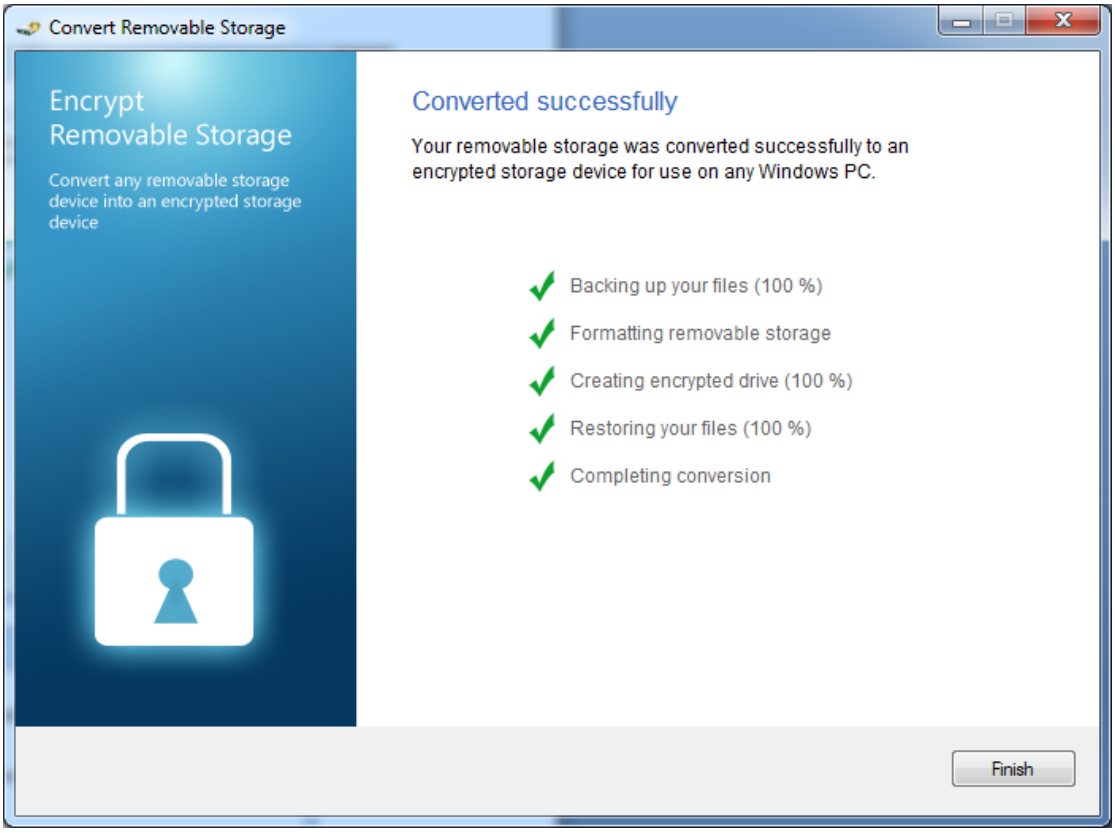
The encrypted drive will then be created, and verified using the password you specified. Once the verification of your encrypted drive is complete, CedeDrive will restore all of your data to the encrypted drive.

The process is then completed by creating a CedeDrive Launcher application which enables you to use your newly converted encrypted Flash Drive on any Windows computer.

Once the process has completed you will receive the following message:

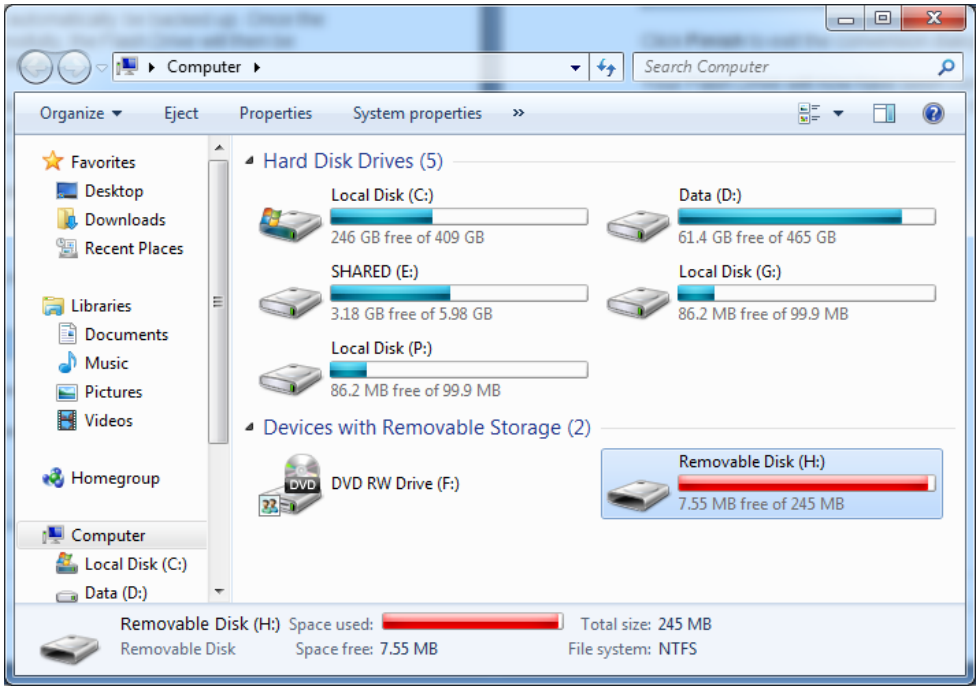


The following dialog will also be displayed indicating a successful conversion of your Flash Drive to an encrypted drive.



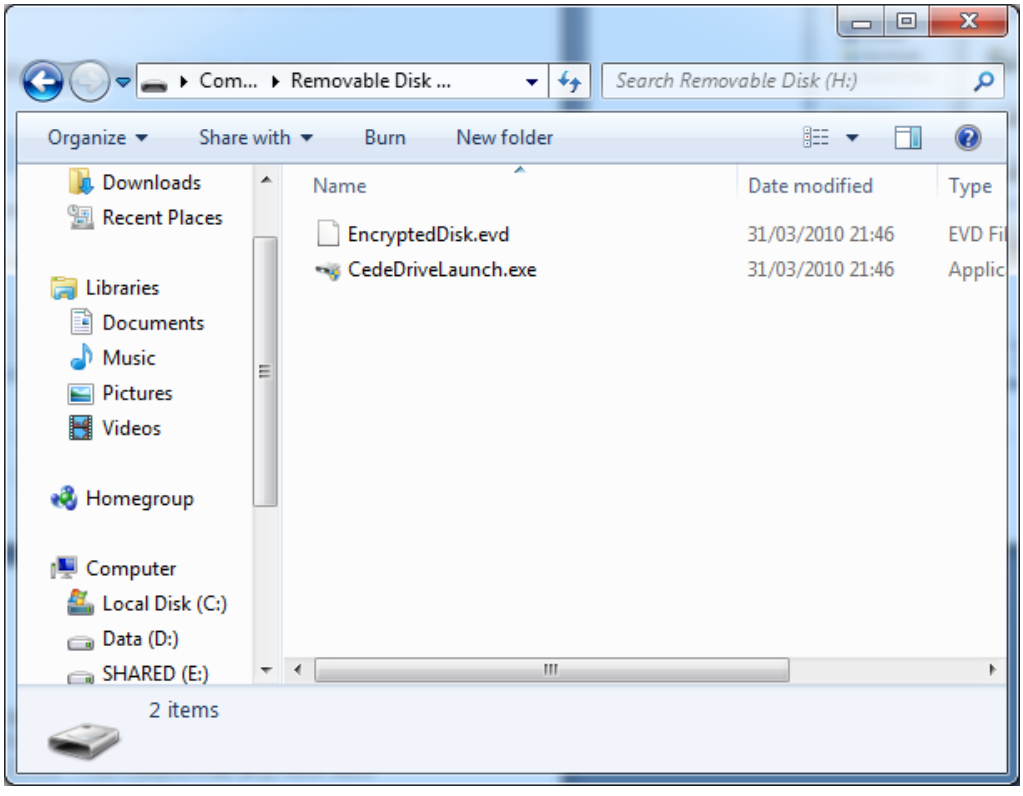
Click **Finish** to exit the conversion dialog.

Your Flash Drive has now have been converted to an encrypted device. To see the changes made to your Flash Drive, click **Start->My Computer.**



You will notice that your Flash Drive will appear completely full, without any free disk space. This is perfectly normal because CedeDrive has also encrypted the free space on your Flash Drive. This means that any new files added to your flash drive from now on, will be encrypted.

If you now open your Flash Drive from Windows Explorer, you will notice just two files, as shown below:



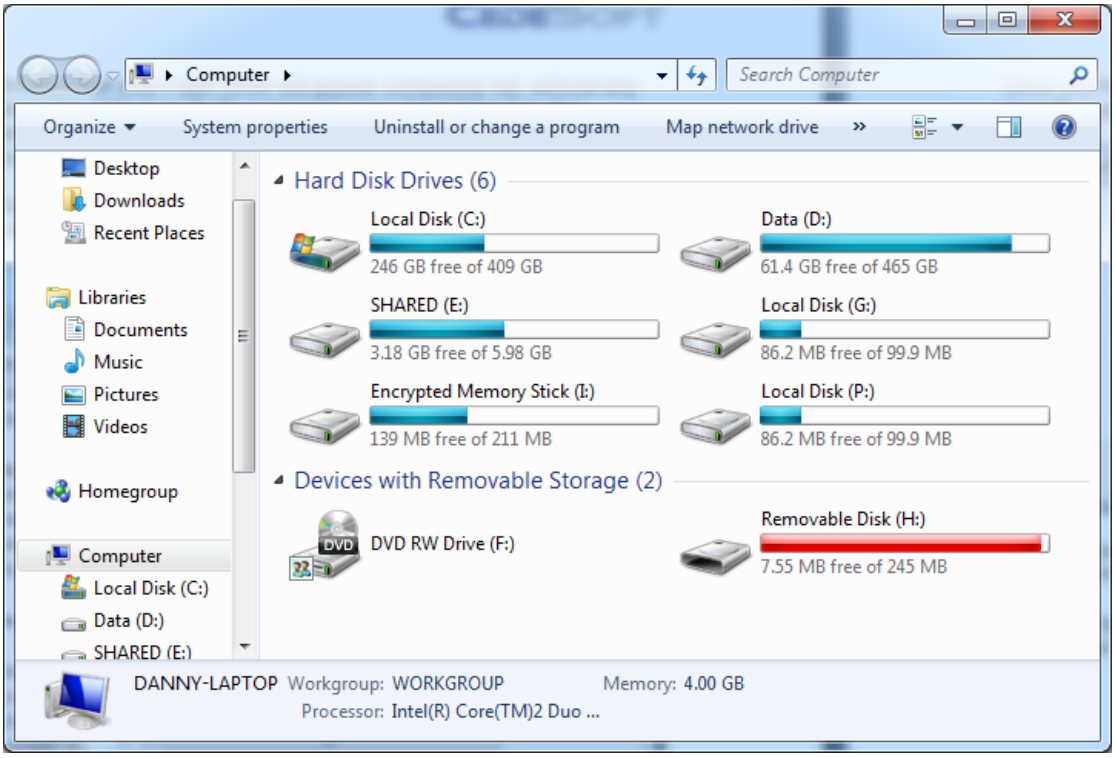
All of your data and free space is now contained within the Encrypted File **EncryptedDisk.evd.** Also, a portable version of CedeDrive has been created. This portable version will allow you to mount the encrypted drive for use in any Windows computer.

To start using your Encrypted Flash Drive, double click **CedeDriveLaunch.exe**.

Once you have launched **CedeDriveLaunch.exe** you will be prompted for your Encrypted Drive Password, as shown below:

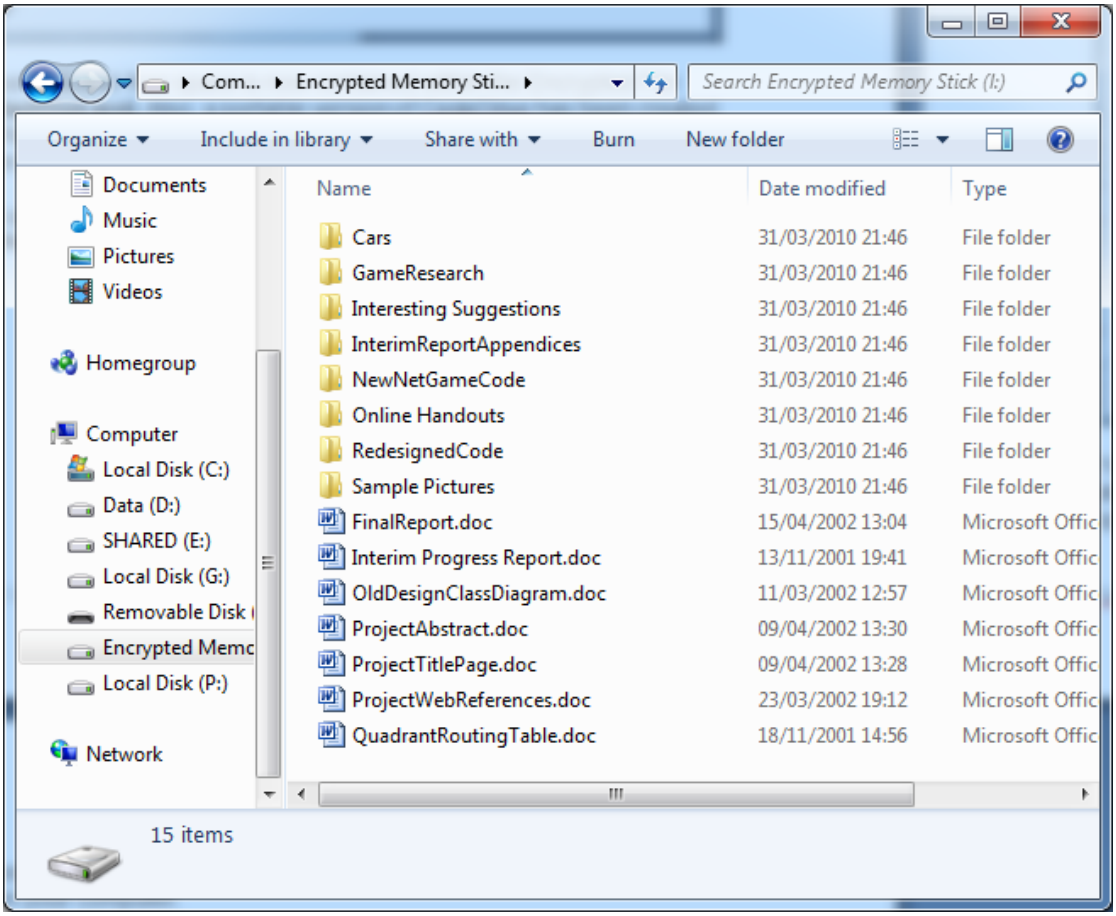
Enter the password you chose when converting the Flash Drive. Once you have entered the password, click **Ok** or press **Enter.**

Your Encrypted Flash Drive will then be mounted. To view your Encrypted Flash Drive, click **Start->My Computer.**



You will notice an additional drive named **Encrypted Memory Stick.** You will also notice that this encrypted memory stick has the same amount of free disk space as your Flash Drive previously had before it was converted. CedeDrive will automatically choose and assign a drive letter based on the available drive letters on your computer.

If you open the **Encrypted Memory Stick** drive, you will notice all of your data is now contained within this encrypted drive.



You can now start using the **Encrypted Memory Stick** drive as you would any normal drive. All of the data will be encrypted and stored on your Flash Drive.

Unplugging Converted Flash Drives

If you have finished using your Encrypted Flash Drive, and wish to disconnect it from your computer, it is strongly recommended to unmount the encrypted drive before disconnecting your flash drive. To do this right click the  icon in your system tray and click **Unmount All Drives.** You can then **Exit** CedeDrive, allowing you to disconnect your flash drive from your computer.

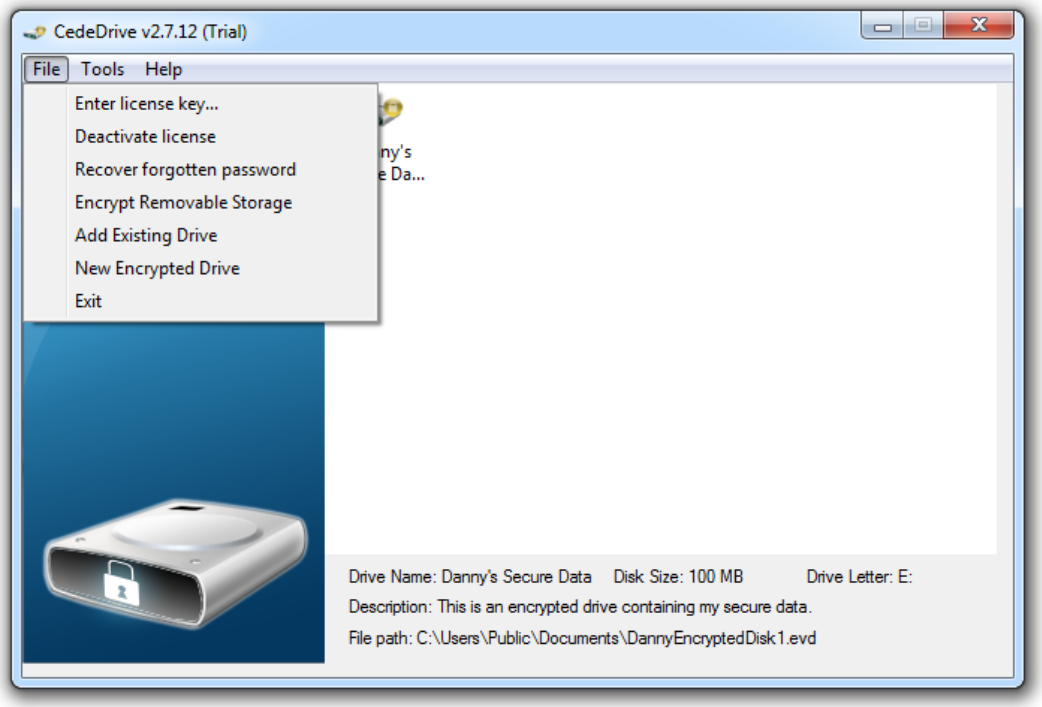
Licensing CedeDrive

CedeDrive initially ships as a feature limited trial version allowing you to mount 1 drive of 100MB for trial purposes.

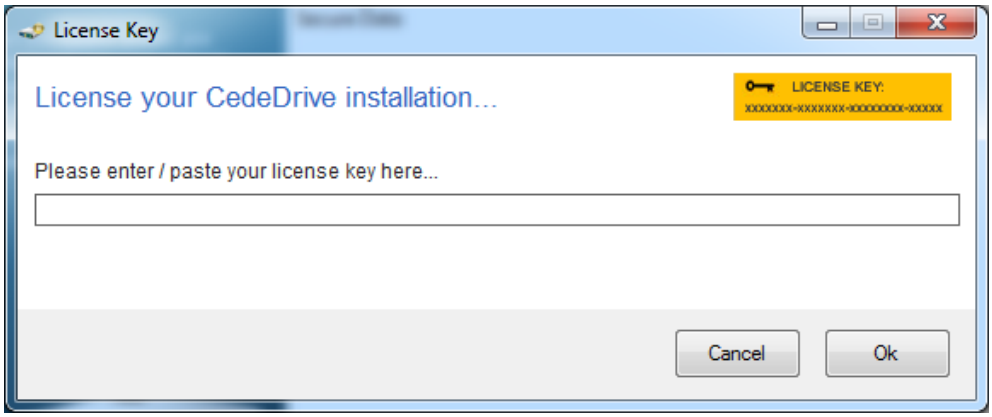
Once you have purchased the full version of CedeDrive you will be sent a License Key contains many numbers and letters.

To apply this license key to your installation of CedeDrive, open the CedeDrive Console Window by double clicking the icon in your system tray.

Once the console window is opened, click **File->Enter license key...**



You will then be prompted to paste your license key into the following dialog:



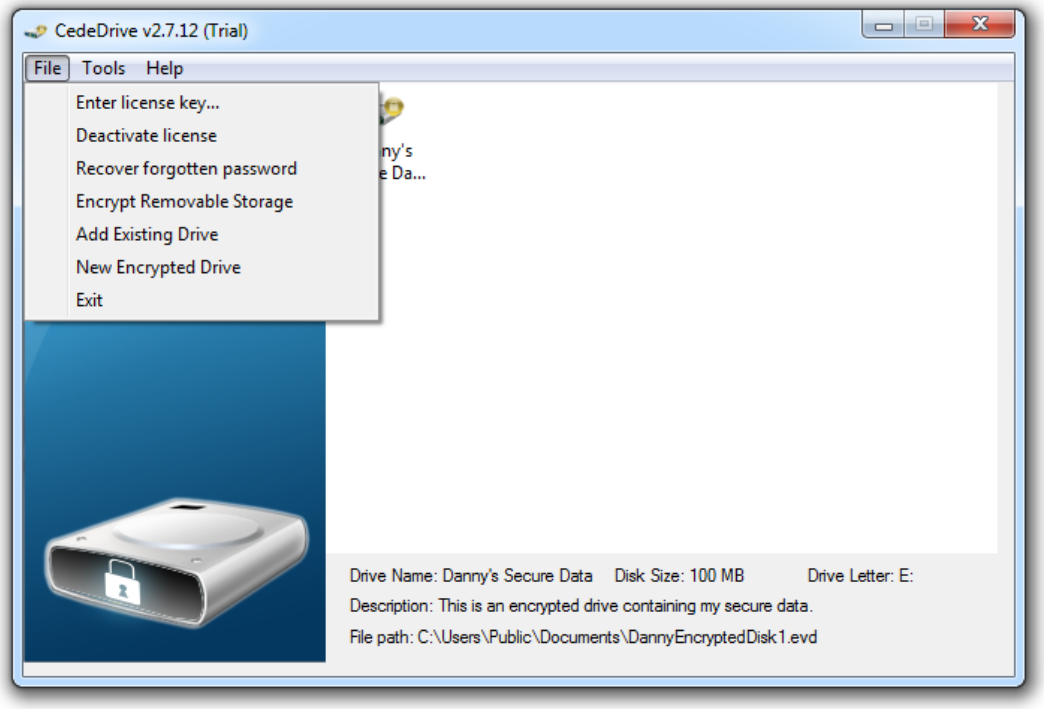
Your license key will then be verified online by our CedeSoft activation servers, and when successful your installation of CedeDrive will be fully licensed.

Recovering forgotten passwords

CedeDrive allows you to recover forgotten passwords provided you have created a recovery key when you created your encrypted drive.

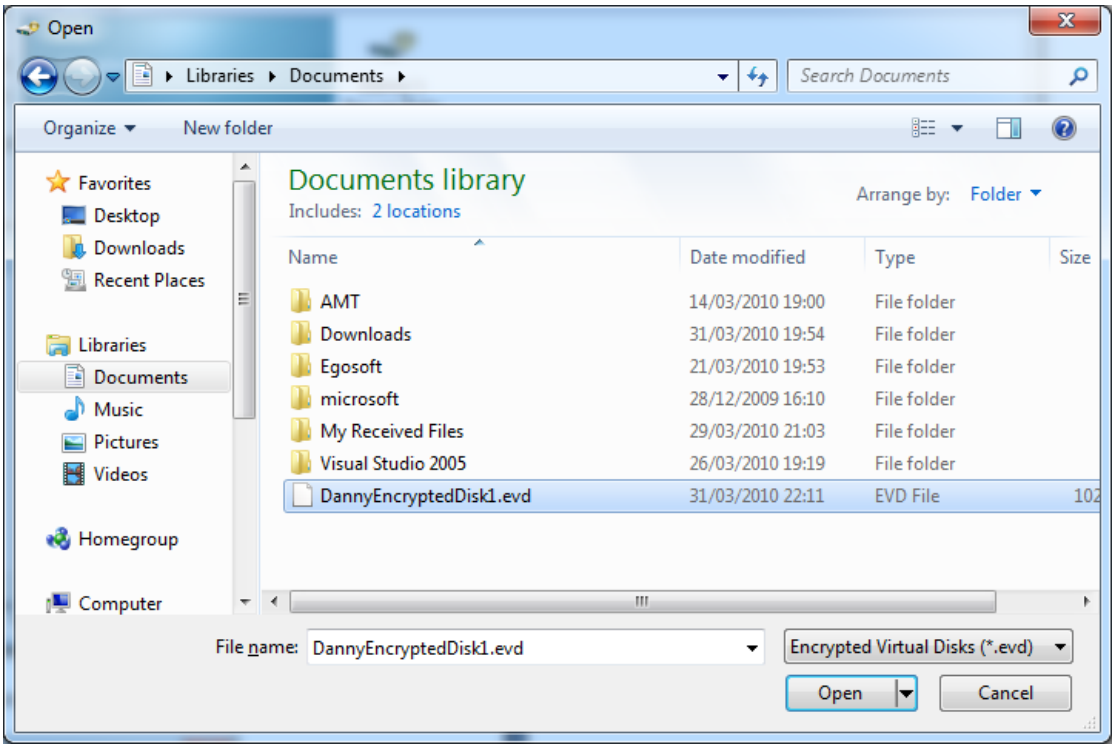
Once you have located your recovery key, open the CedeDrive Console Window by double clicking the  icon in your system tray.

Once the console window is visible, click **File->Recover forgotten password**

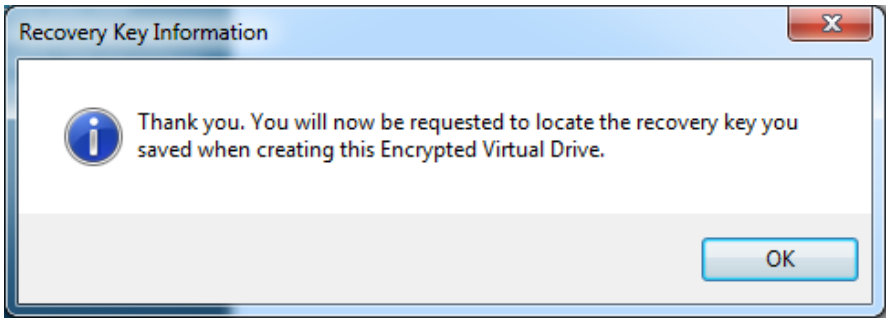


You will then be prompted with the following dialog:

Click **Ok,** and you will be prompted for the location of the Encrypted Drive file you wish to recover as shown below:

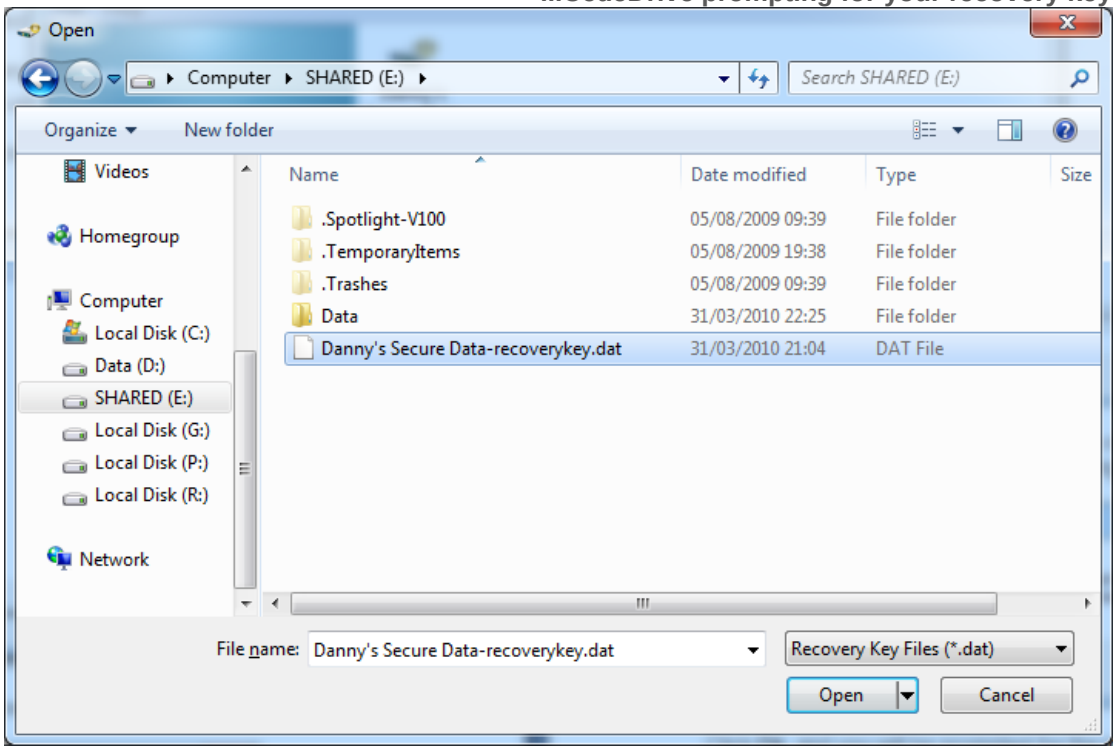


Locate the encrypted EVD file you wish to recover, and then click **Open.** You will then be prompted with the following message:

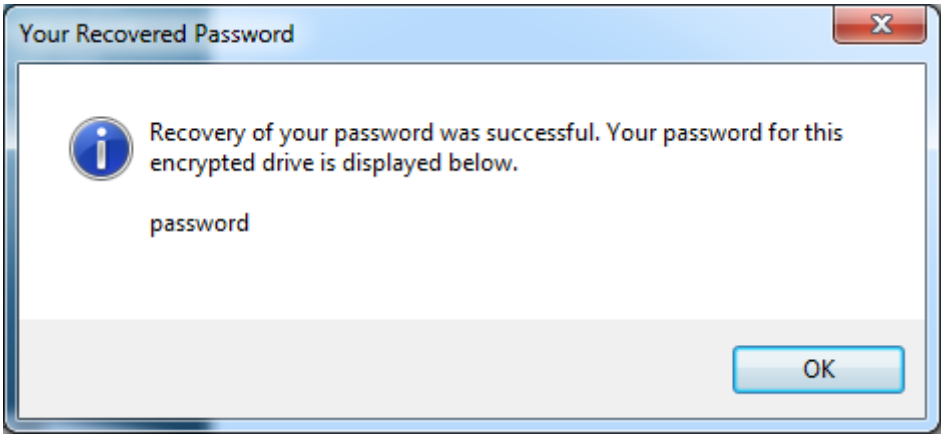


Click **Ok,** and you will be prompted for the location of your recovery key for this drive, as shown...

...CedeDrive prompting for your recovery key



Locate the recovery key you initially saved when creating this drive and click **Open.** You will then be shown the recovered password as shown below:



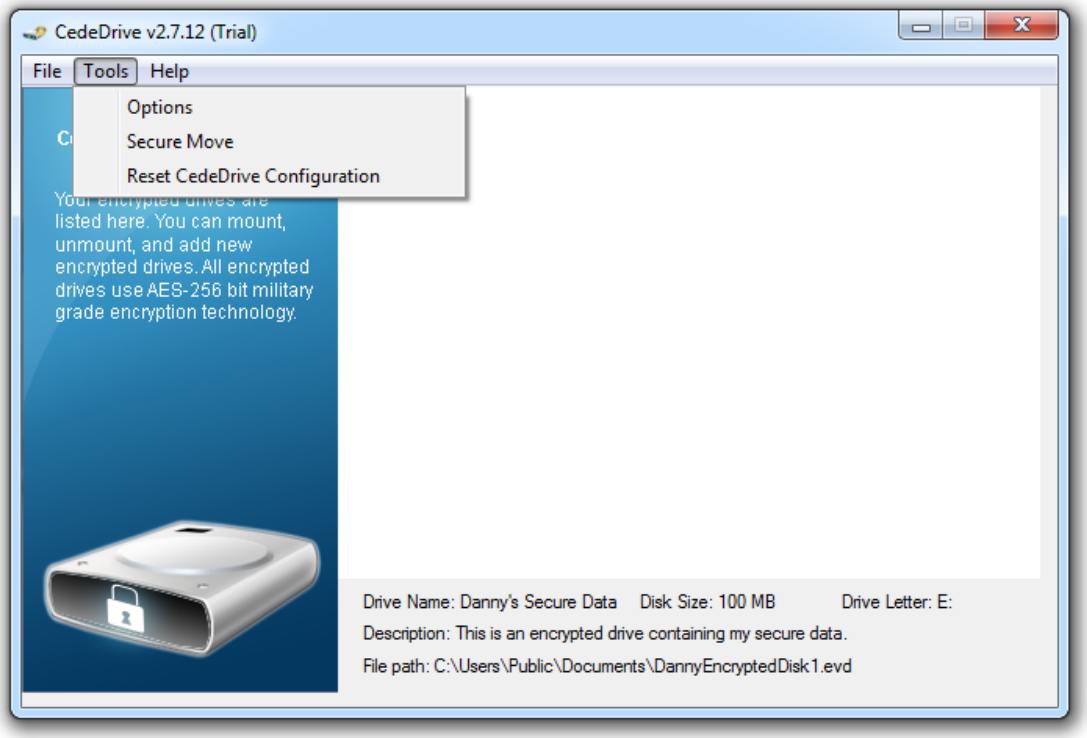
Securely moving files to your Encrypted Drives

CedeDrive ensures that all data that is saved to an Encrypted Drive is securely encrypted. However when you have initially set up your encrypted drives and would like to move your data, you can do this using Windows Explorer and the files will be copied as they would be for any standard drive.

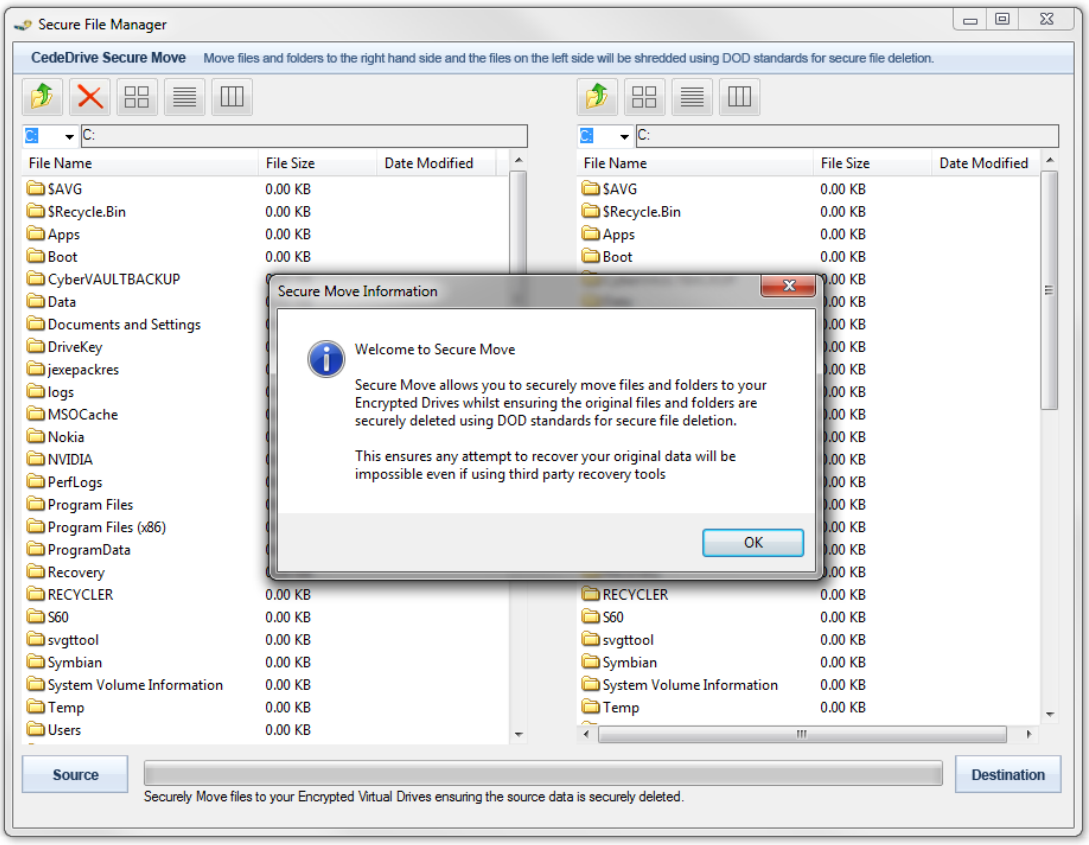
However using Windows Explorer to move your files and folders will still make it possible to recover your original data using any third party recovery tool as Windows does not permanently erase the data from your hard disk when deleting or moving files.

For this reason, CedeDrive provides a **Secure Move** feature. This feature will copy selected files and folders you choose to your Encrypted Drives (or any other drive), but it will ensure that the original data is permanently erased from the source hard disk. CedeDrive contains a built-in File Shredder which uses the Department of Defense standard DOD 5220.22-M to permanently and securely erase the source data from your hard disk. Therefore any attempt to recover the source data will be made impossible.

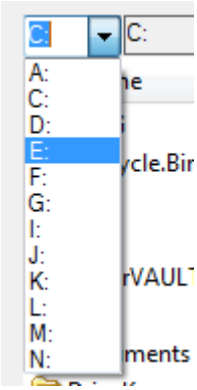
To access the Secure Move feature, click **Tools->Secure Move** from the CedeDrive console window.



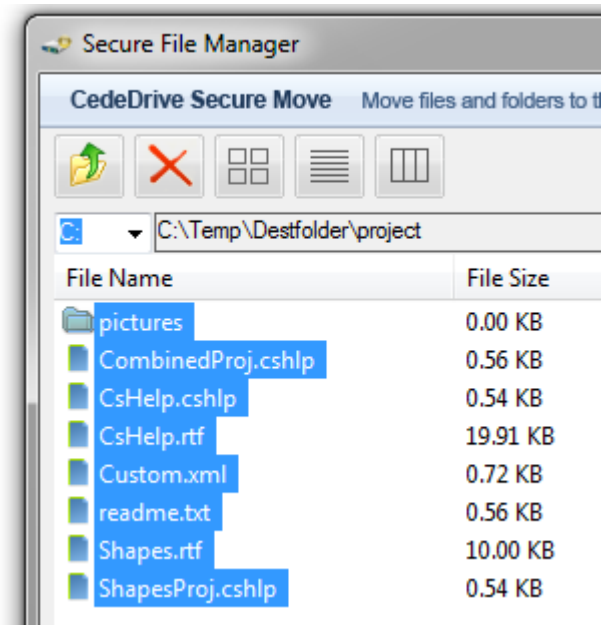
This will launch the Secure Move file manager...



To begin securely moving files to your Encrypted Drive, first use the Drive Selection Drop Down list on the right hand side to navigate to your Encrypted Drive.

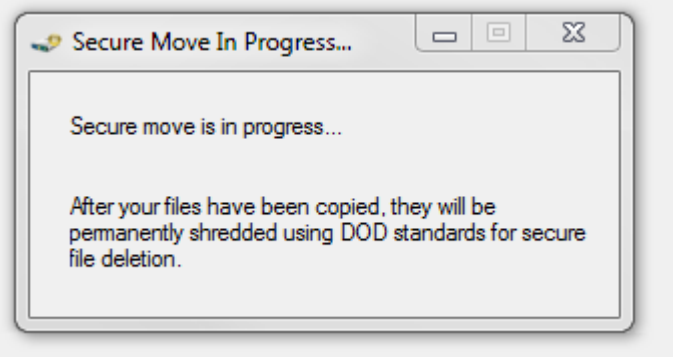


Once you have selected your Target Drive, you can then select multiple files and folders from the left hand side to specify the files and folders you wish to move securely.



Once you have specified the source files, click the  button in the centre of the window to begin the secure moving of your files and folders.

A window will appear indicating that a secure move is now in progress.



The progress of the secure move will also be shown at the bottom of the window.

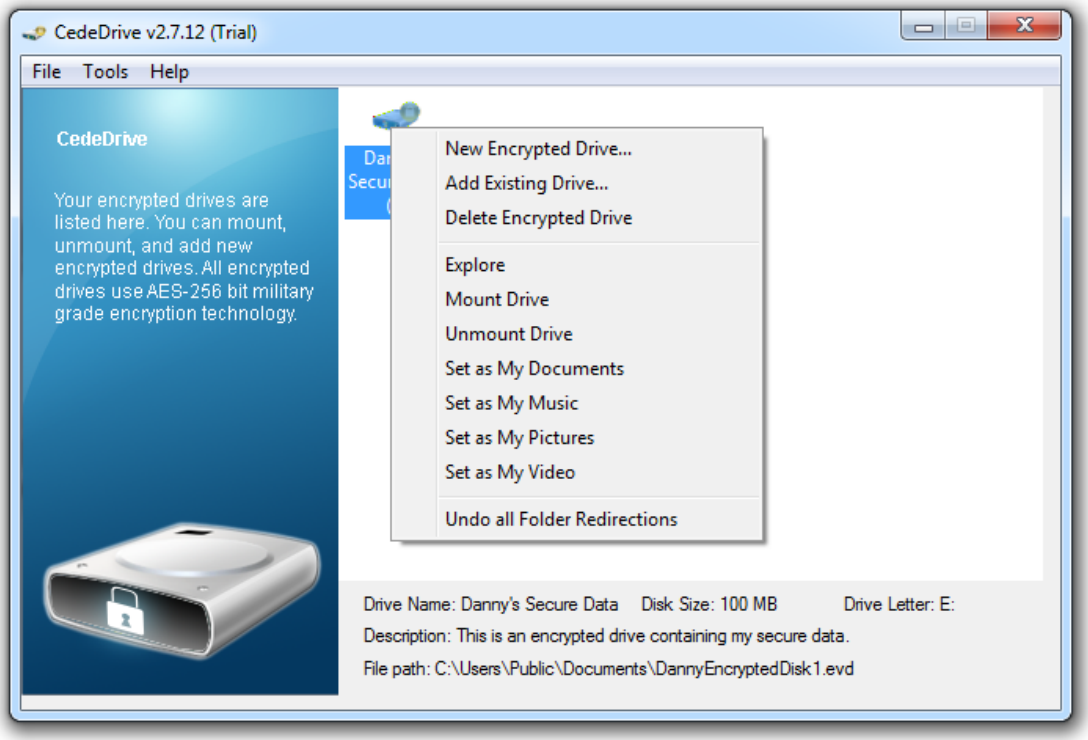
Redirecting Windows folders to Encrypted Drives

CedeDrive allows you to safely redirect any of your standard Windows folders to an encrypted drive you have created with CedeDrive. These folders include My Documents, My Pictures, My Music and My Video.

Once a folder has been redirected to an encrypted drive, all windows applications that use My Documents as a default saving location will instead be redirected to your encrypted drive. Clicking Start->My Documents within Windows will also open your encrypted drive.

This feature is very useful if you regularly access your documents and pictures using Windows shortcuts and office applications that open and save documents directly to these locations.

To enable this feature, open the CedeDrive console window by double clicking on the  in the system tray.



You can then right click on any of your drives in the console window and click **Set as My Documents, Set as My Pictures** etc.

Once you have enabled this feature you will need to restart your computer for the changes to take effect.

To disable this feature click **Undo all Folder redirections.** This will set all of your Windows folders back to Microsoft defaults.

Standby / Hibernation protection

CedeDrive is also designed to protect your encrypted data when your computer is put into Standby or Hibernation. When your computer is put into Standby or Hibernation, all of your encrypted drives will automatically be unmounted to protect your data. When your computer is resumed from Standby or Hibernation you will be presented with a secure password screen as shown below:

You will be required to enter your CedeDrive password here to regain control of your computer. This secure password screen is designed to protect Laptop computers should they be compromised whilst they are in a hibernated state or in standby.

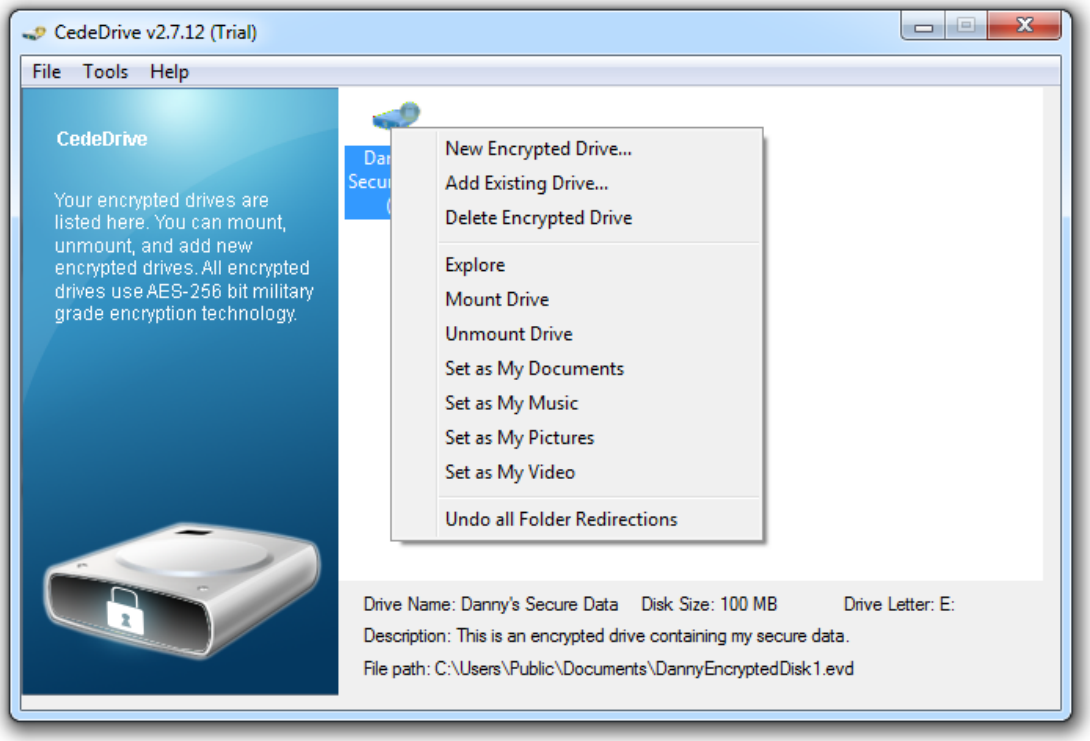
Any unauthorised person attempting to gain access to your computer whilst it is in standby will be forced to restart your computer as they will not know the password. Your encrypted data and any applications you had open at the time (and the data contained) will not be disclosed to the unauthorised person, and your data will remain encrypted once the unauthorised person has restarted your computer.

Adding existing encrypted drives

CedeDrive allows you to add any previously encrypted drives you may have created perhaps on another computer, or if your computer has had a hard drive failure and you have had to re-install the operating system. In this scenario, you will require the EVD files and you will be able to add these drives so you can access the data contained in the EVD files.

IMPORTANT: When adding existing EVD files back into CedeDrive it is very important that the password used to setup CedeDrive is the same password that was used to create the EVD files you are adding. If the passwords do not match then Windows will not recognise the drive and will believe it is a new drive that needs to be formatted.

To add an existing drive, right click on the CedeDrive console window and click **Add Existing Drive.**



You will then be prompted to locate the EVD file you wish to add back into CedeDrive. Once you have located this file you will be able to mount it normally just like a newly created drive.

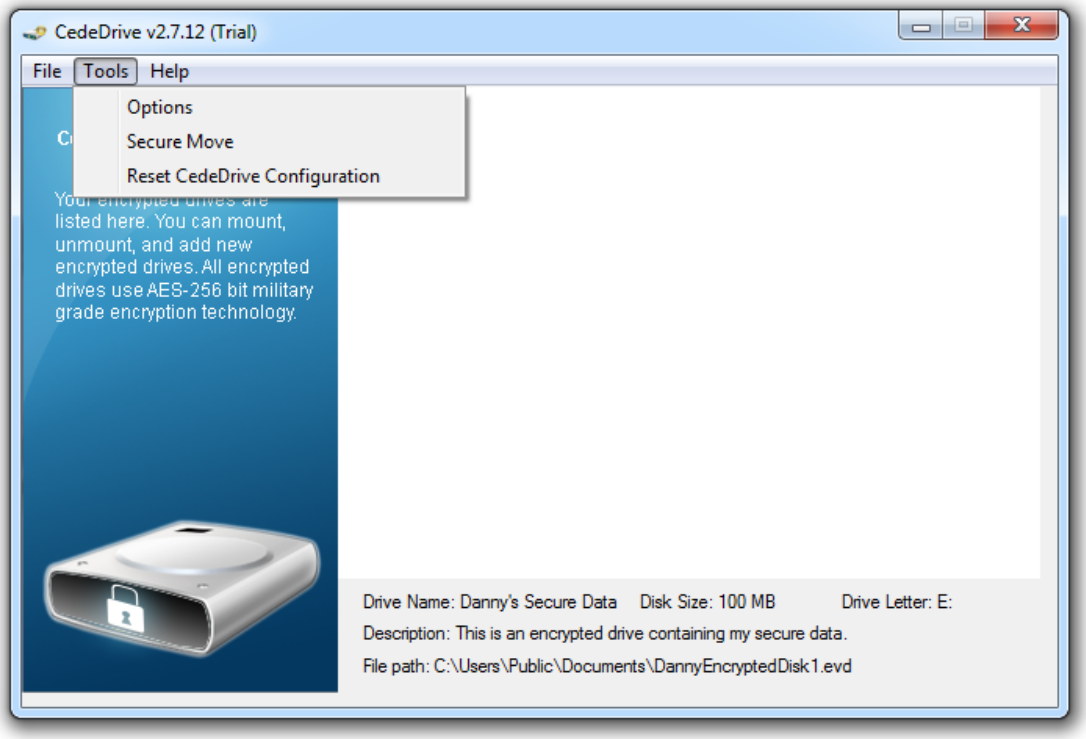
Resetting CedeDrive configuration

It may be necessary to reset the CedeDrive configuration under the following circumstances:

- You wish to setup CedeDrive for a different user.
- You wish to change the CedeDrive password used to create and mount existing drives.
- You wish to restore CedeDrive back to manufacturer defaults.

The CedeDrive configuration stores details of the drives that are added to the CedeDrive console. Resetting the CedeDrive configuration does not modify or delete any EVD files associated with the encrypted drives, it is purely configuration data that is affected. Once you have reset the CedeDrive configuration you will have to add your EVD files back into CedeDrive as described in the previous section.

To reset the CedeDrive configuration, click **Tools->Reset CedeDrive Configuration.**



Once the configuration has been reset you will be required to exit CedeDrive and relaunch the application. You will then be required to set up a new password.

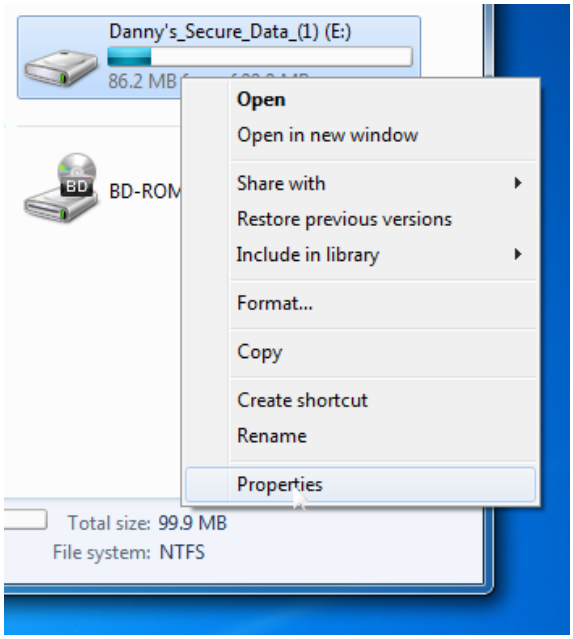
Converting Removable Drives using Windows XP

IMPORTANT: Once you have converted a removable drive using Windows XP, and then wish to use that removable drive in Windows Vista or Windows 7 the removable drive will by default have Read only permissions on the encrypted drive.

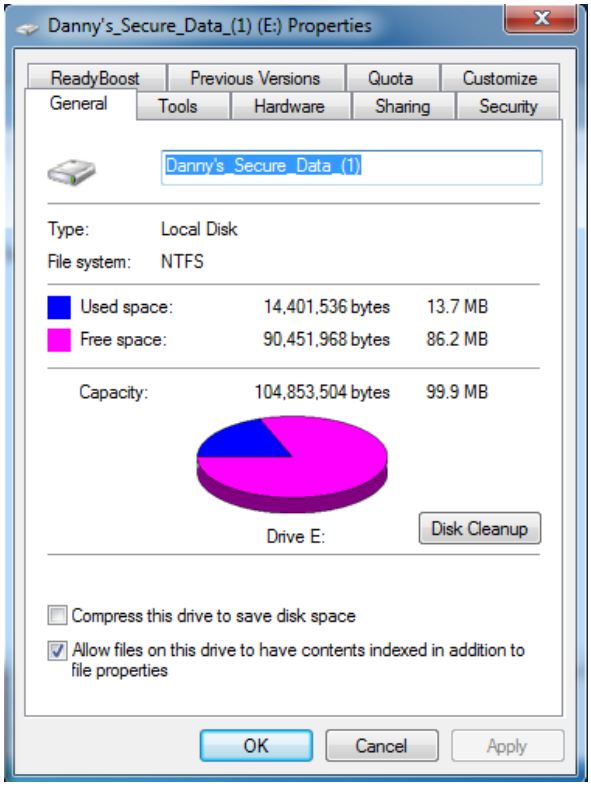
This is due to the enhanced security provided by Windows Vista & Windows 7. In order to make changes to a removable encrypted drive in Windows Vista/7 that has been converted in Windows XP, you must make the following permission changes.

Mount the Removable Encrypted Drive by running the CedeDriveLaunch.exe application

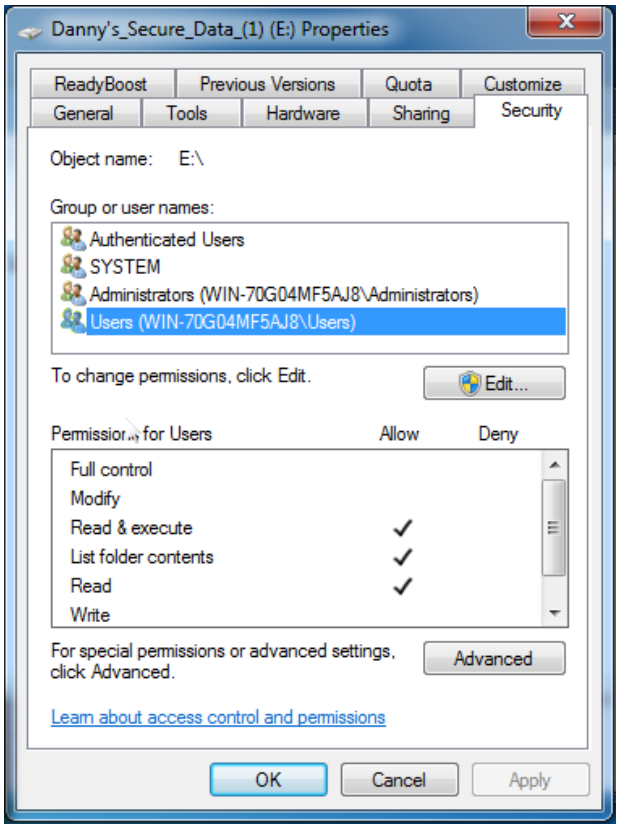
Once the drive has mounted, right click on the Encrypted Drive from Windows Explorer, and click **Properties.**



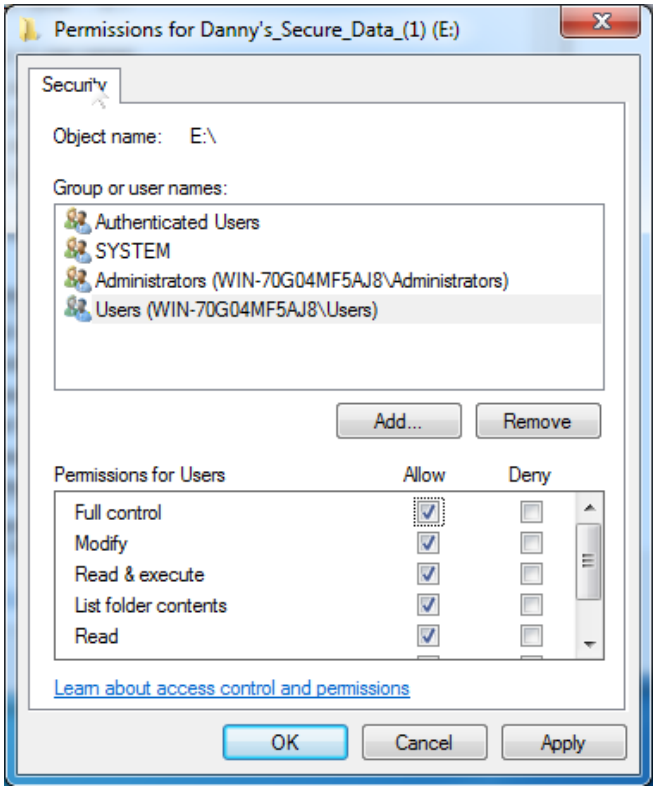
The following dialog will appear...



Click on the **Security** tab.



Click on **Users** under Groups or user names, then click the **Edit** button.



Click on **Users** in the list, and then ensure that Full control, Modify, Read & Execute, list folder contents and Read are all checked in the Permissions for Users section.

Once that is completed, click **Apply**, and then click **Apply** and then **Ok** to each of the previous dialogs.

If you have converted a removable drive using Windows Vista or Windows 7 then this step is unnecessary, and the removable drive will operate normally in Windows XP.

CEDESOFT

For more information or contact details please visit our website:

www.cedesoft.com