

Install and setup TrueCrypt

This guide is for organisations and individuals who wish to use TrueCrypt to secure their computer(s) and/or portable USB drives.

It explains how to:

- install and setup TrueCrypt (version 5.1a Windows Vista/XP/2000)
- encrypt portable USB drives using TrueCrypt

Finally we include some extra notes on using TrueCrypt.

This guide is suitable for users with computers running Windows Vista/XP/2000 with a single operating system installed. It is not suitable for computers running more than one operating system. For example, dual boot computers running Windows and Linux.

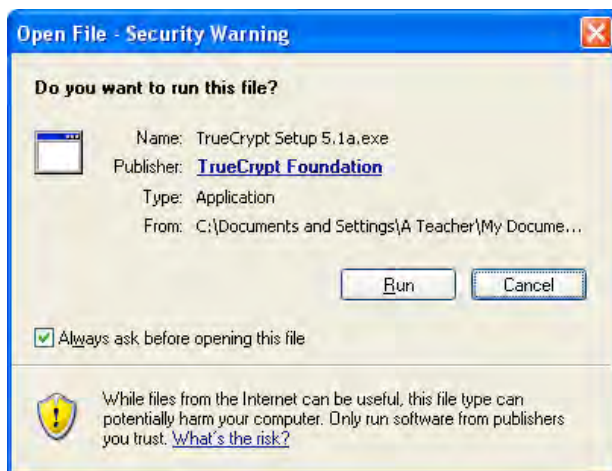
TrueCrypt is a free and open source encryption software for Windows Vista/XP, Mac OS X, and Linux. You must install and set it up with care. If you set it up incorrectly, you may loss important data **permanently**.

1. Applying whole disk encryption with TrueCrypt

1.1. Installing TrueCrypt

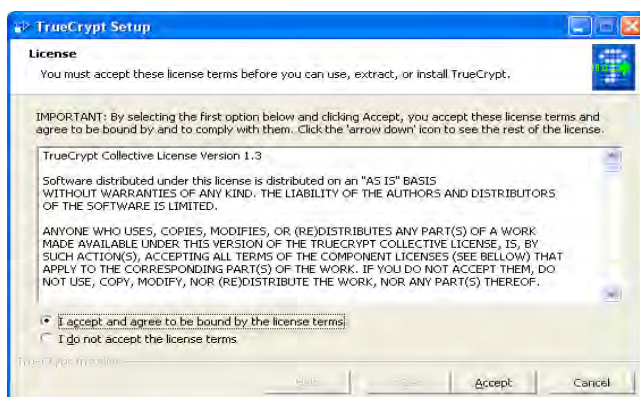
First, obtain the correct installer file from TrueCrypt.

- Download the Windows installer file from TrueCrypt [<http://www.truecrypt.org/downloads>].
- Run the file.



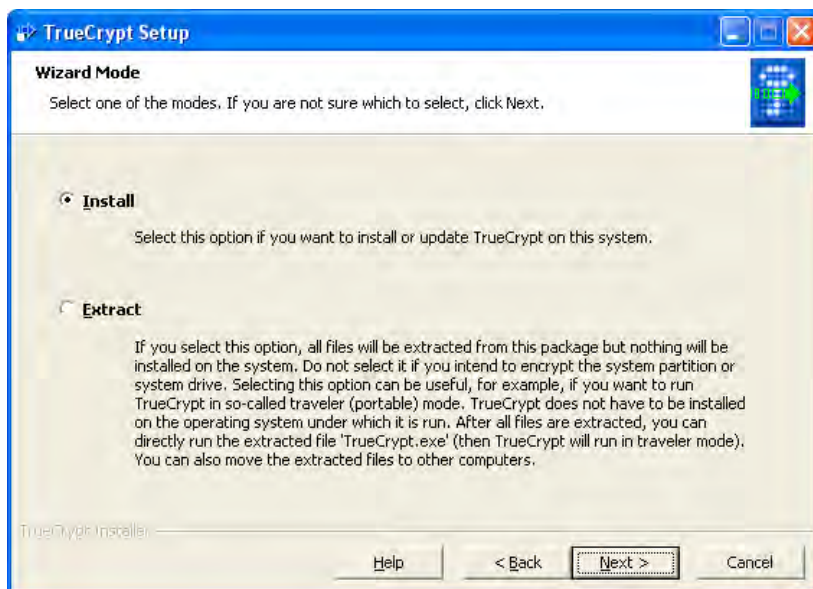
The installer will show you a License window.

- Read, then Accept and agree to the Licence.



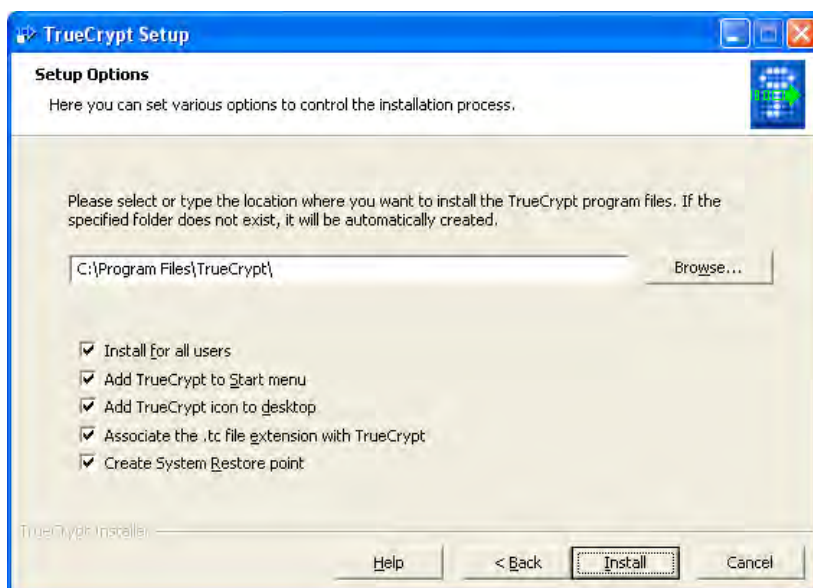
You will see a Wizard Mode window.

- Select the Install option.

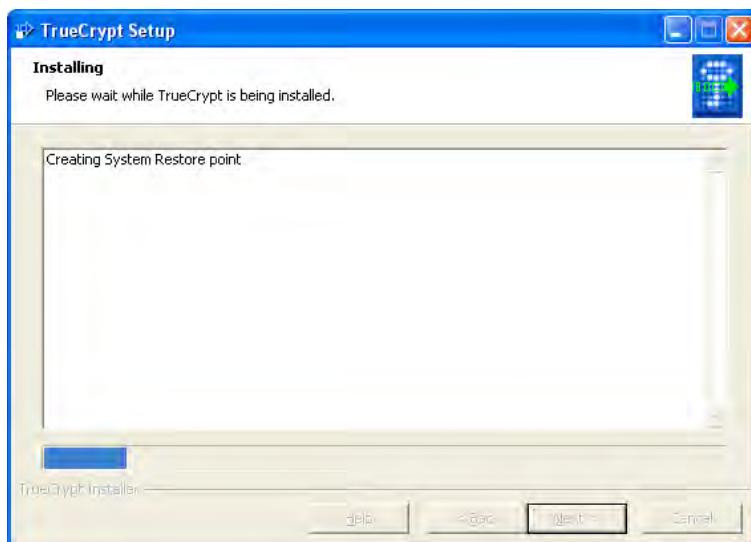


You will see a Select Options window.

- Accept all the default options. Click Install.

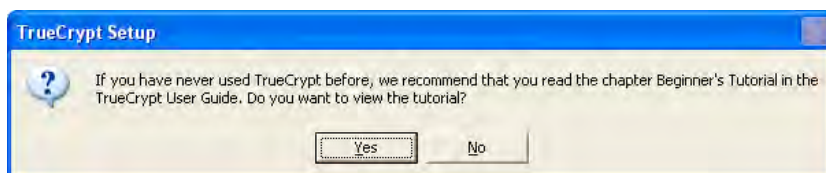


TrueCrypt will create a System Restore point and install the software.



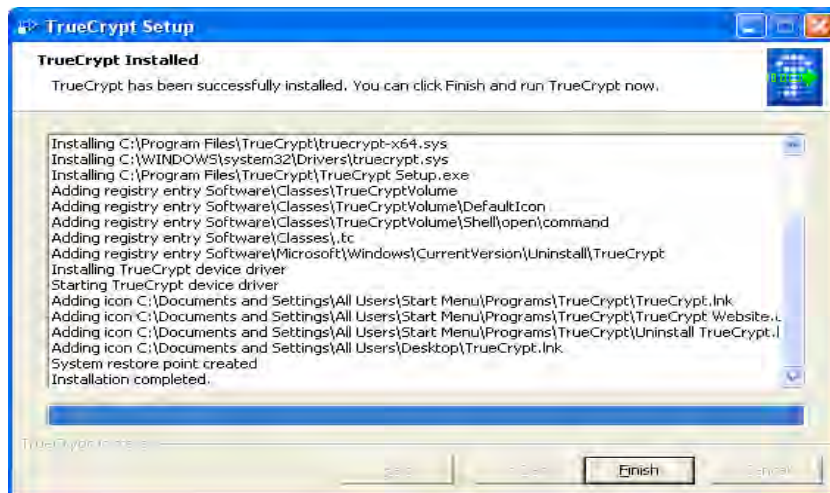
When the installer finishes you will see the Setup dialog box below. The 'Beginner's Tutorial' is not suitable for educational users.

- Click No.



You will see a TrueCrypt Installed window.

- Click Finish.



Congratulations! You have installed TrueCrypt.

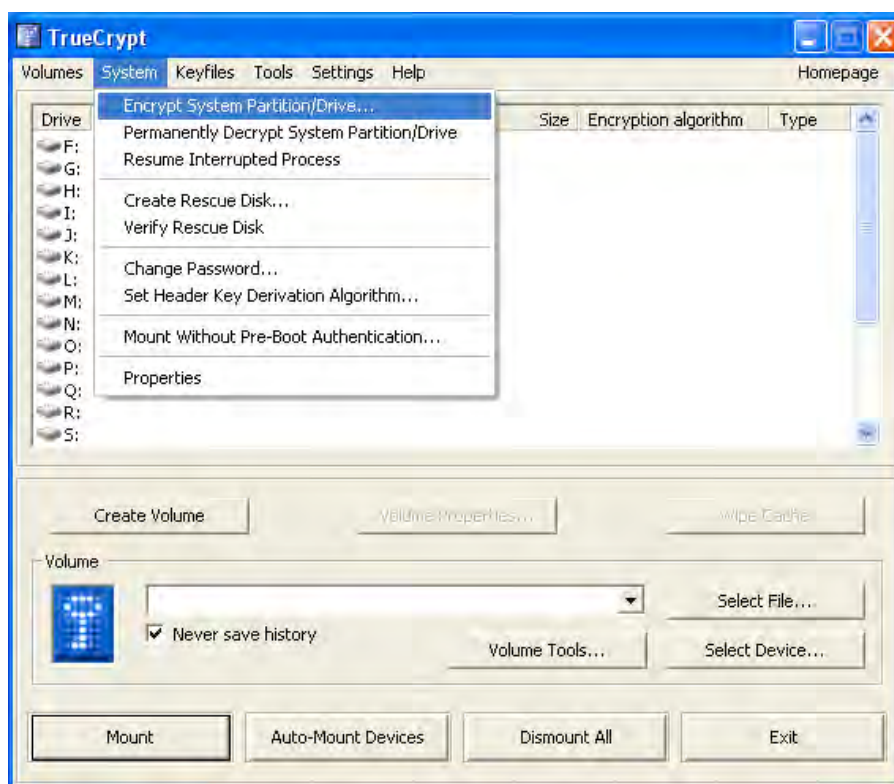
1.2. Setting up TrueCrypt

You will see a TrueCrypt icon on your desktop.

- Double-click it to launch TrueCrypt.

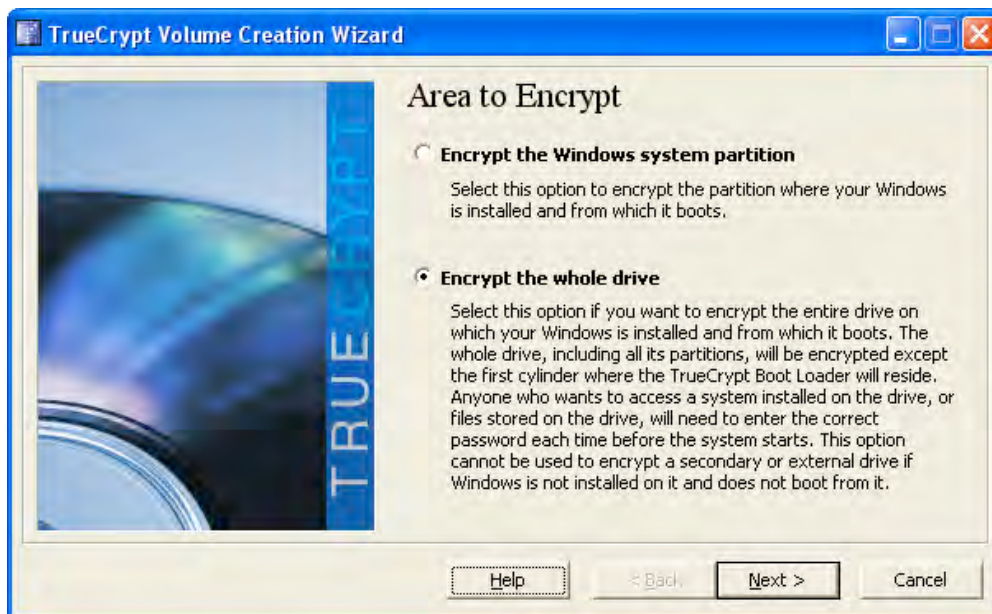
Wait for TrueCrypt to start.

- Select Encrypt Systems Partition/Drive... from the System menu.

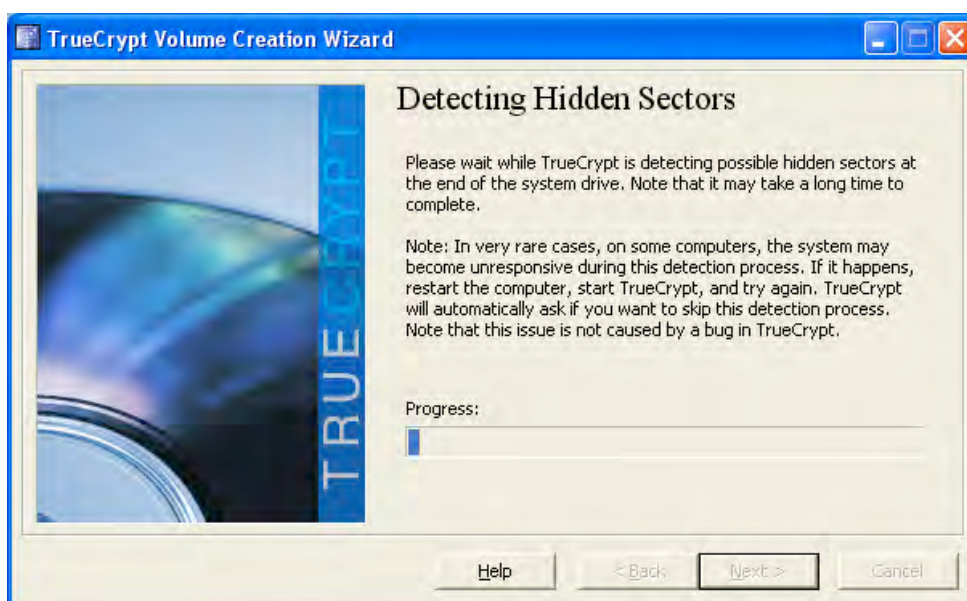


You will see an Area to Encrypt window.

- Select Encrypt the whole drive.
- Click Next.

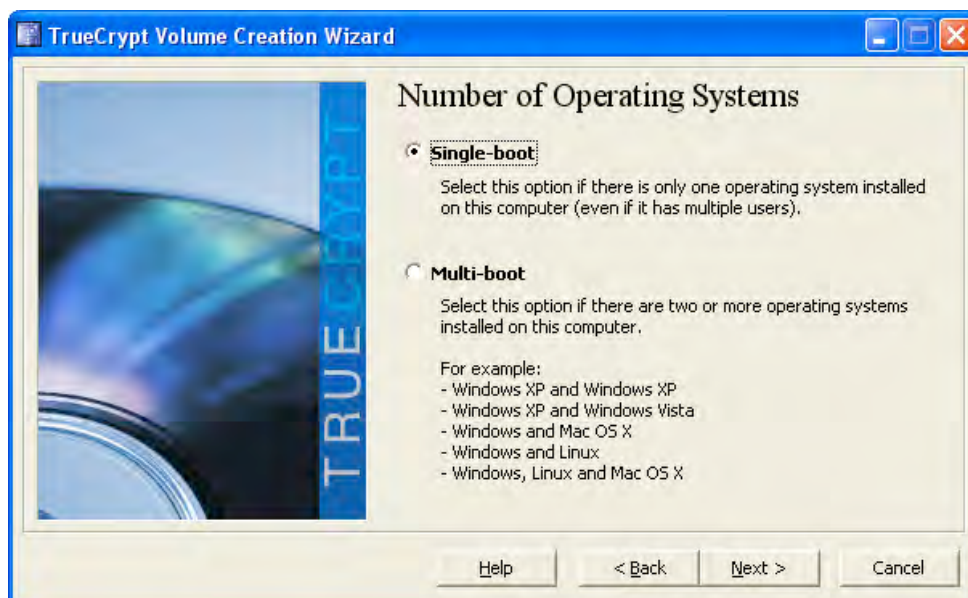


The TrueCrypt Volume Creation Wizard will start and TrueCrypt will try to detect hidden sectors on your hard drive. This may take a long time.



You will see a Number of Operating Systems window.

- Select the Single-boot option (If your computer has more than one operating system installed you will need to select Cancel at this point).



Next, you will see an Encryption Options window.

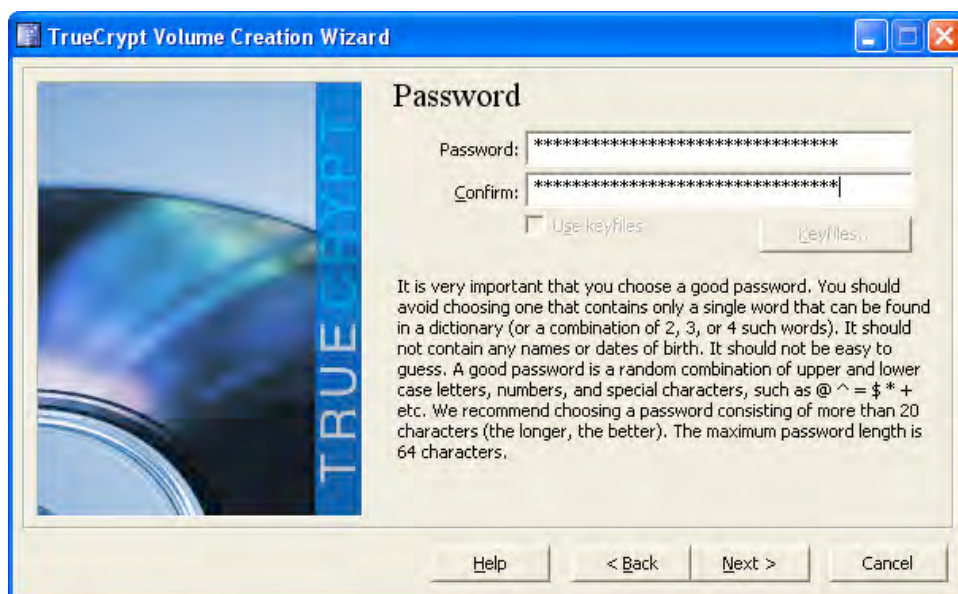
- Accept the default selections for Encryption and Hash algorithms. (We recommend the AES-256 Encryption Algorithm and the RIPEMD-160 Hash Algorithm.)



You will see a Password window.

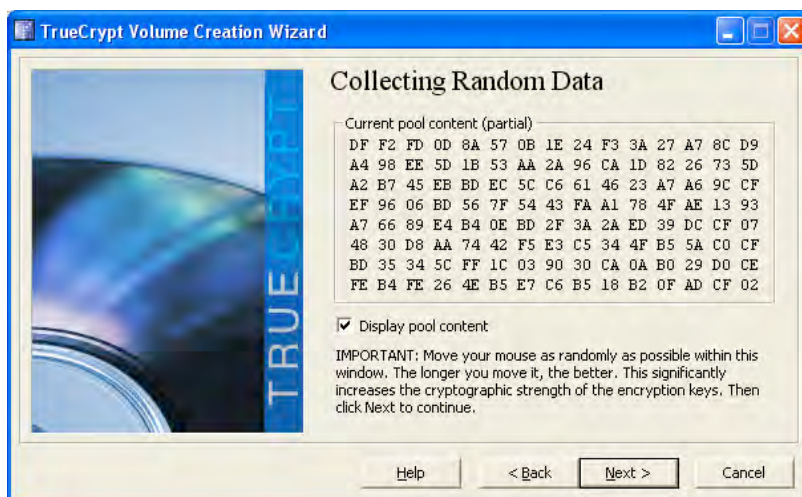
- Choose a strong password. (A strong password is at least 10 characters long and contains letters and numbers.)

Warning! You must remember this password! If you forget it, you will not be able to access any the data on your computer again! You will loss the data permanently.



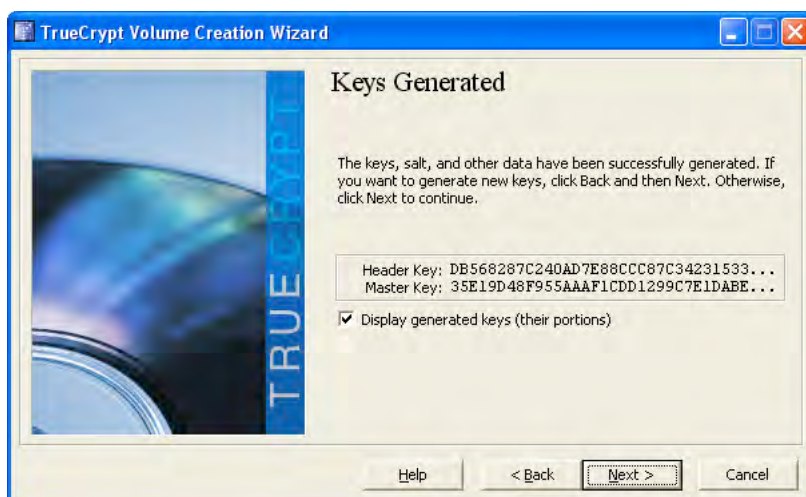
Next, you will see a Collecting Random Data window.

- Randomly move your mouse for at least a minute.
- Click Next. (You do not need to wait for the characters in the box to stop changing.)



You will see a Keys Generated window.

- Click Next.



You will see a Rescue Disk window. TrueCrypt will ask you to create a rescue disk.

- Choose (and make a note of) the location to save the TrueCrypt Rescue Disk (TRD) image.
- Click Next.



You will see a Rescue Disk Recording window.

- **DO NOT** click Next.



If you have CD/DVD recording software that will burn the TrueCrypt Rescue Disk ISO image.

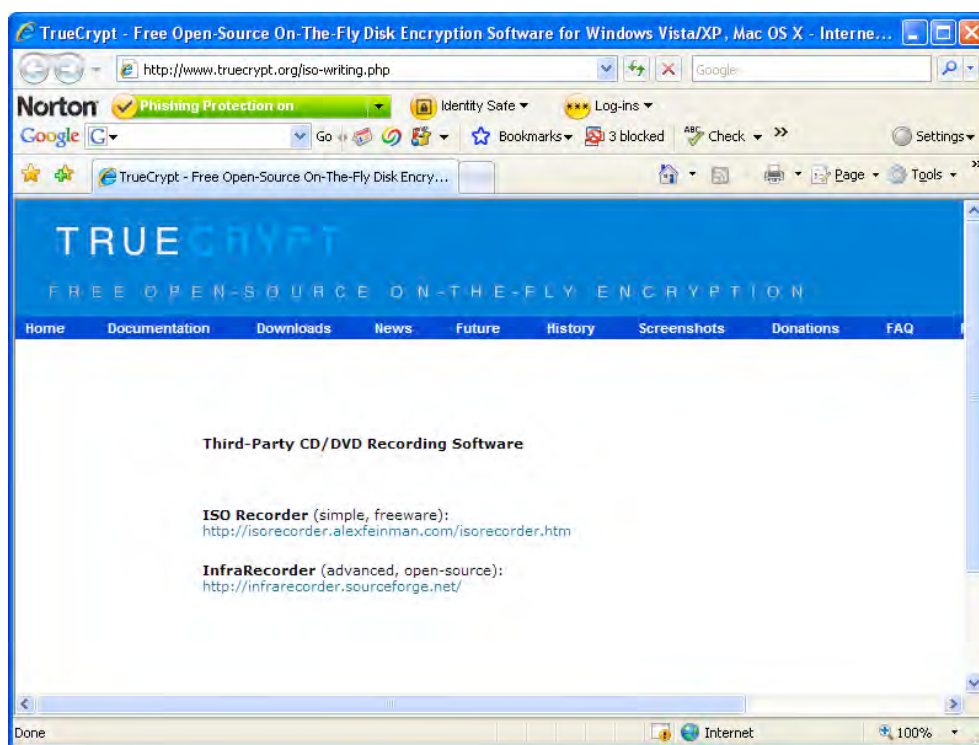
- Use it now.

If you do not have CD/DVD recording software.

- Follow the Download CD/DVD recording software link to download free software [<http://www.truecrypt.org/iso-writing>].

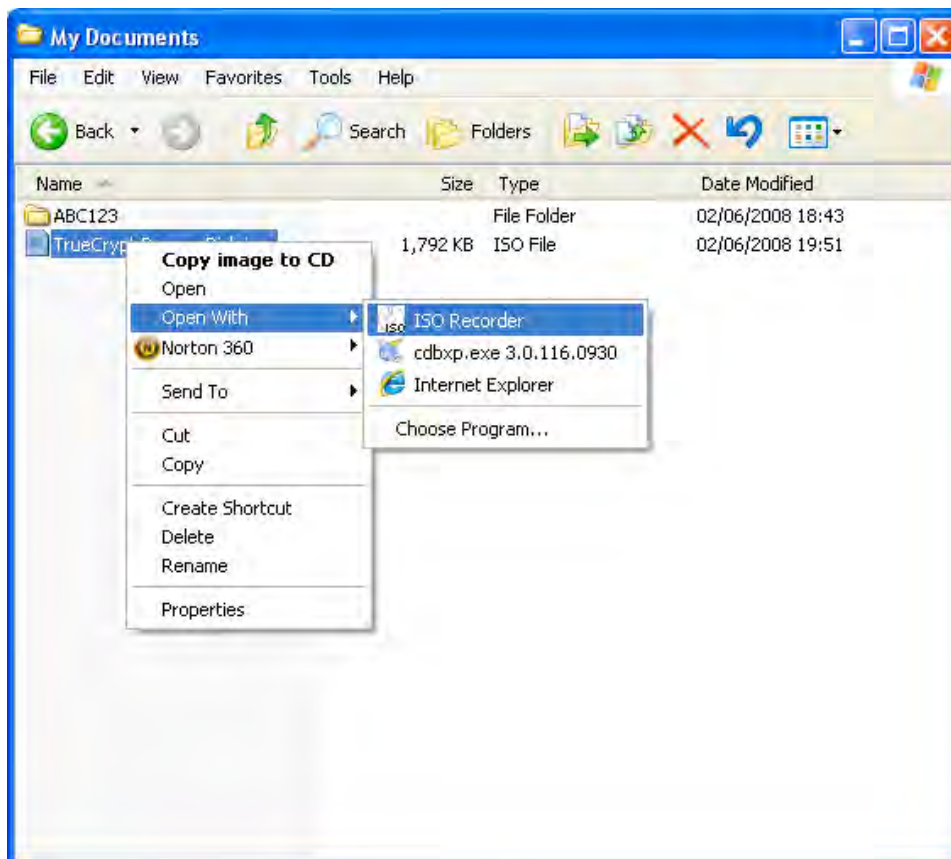
You will see a page on the TrueCrypt website with links to CD/DVD Recording Software.

- ISO Recorder will only burn to a CD. If you need to burn the image to a DVD, select InfraRecorder.



If you selected ISO Recorder.

- Download the version for your operating system and install.
- Right-click the TrueCrypt Rescue Disk ISO image and select Open With ISO Recorder.
- Follow the onscreen instructions.



- Burn two copies of the rescue disk and store them in different (secure) locations.

Warning! Your rescue disks are the only way to recover your data if there is a problem with TrueCrypt on your computer. You can only use these disks if you have the password you chose earlier.

Finish burning the two disks and return to the TrueCrypt Rescue Disk Recording window.

- Click Next.



You may see the error message box below.

- Reinsert one of the rescue disks you have just burned.



TrueCrypt will now verify the disk and show a Rescue Disk Verified window.

- Remove the disk. Store it safely.
- Click Next.



You will see a Wipe Mode window.

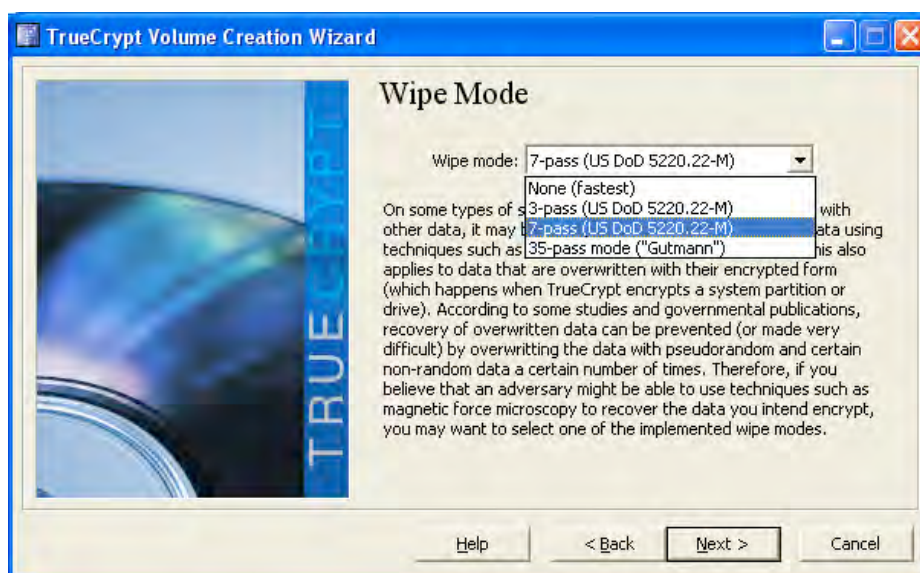
If you have data on your computer that needs to be secured.

- Select 7-pass (US DoD 5220.22-M) from the drop down menu.

If your computer has a freshly installed operating system or has no existing data that needs to be secured.

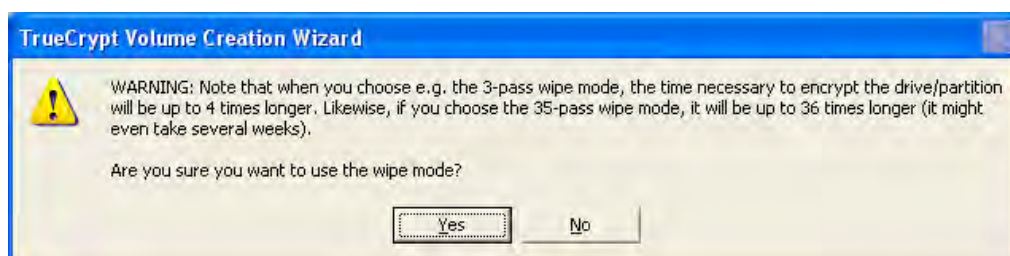
- Select None (fastest) from the drop down menu.

Warning! Do not select 35-pass mode ("Gutmann"). You will wait several weeks for TrueCrypt to encrypt your computer!



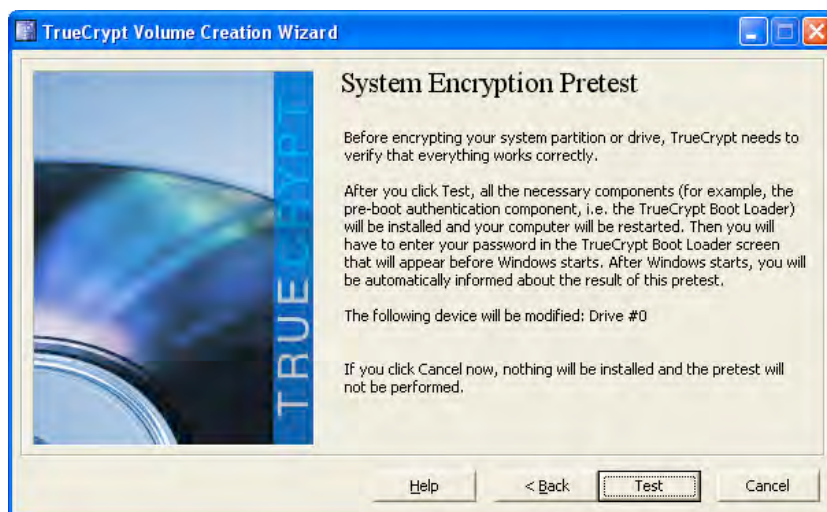
You will see a warning window.

- Click Yes.



Finally, TrueCrypt will test the install and reboot your computer.

- Select Test.



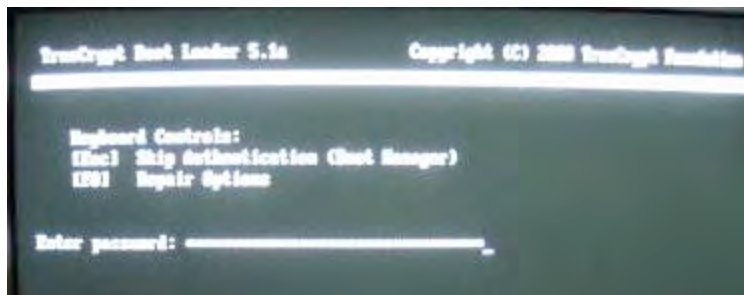
You will see a window containing important notes.

- Click Print.
- Click OK.



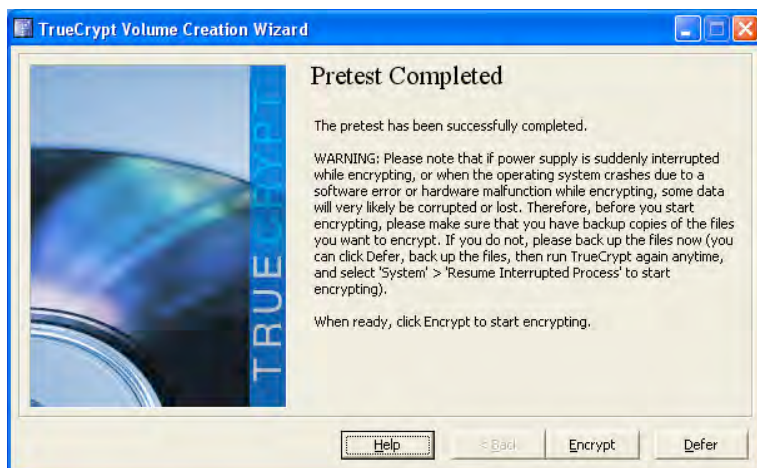
Your computer will now reboot. Before Windows loads, you will now see a password prompt.

- Enter the password you chose earlier.



If the test completed successfully you will see a Pretest Completed window.

- Click on Encrypt.



You will see important instructions on using the Rescue Disk.

- Click Print.
- Click OK.



You will see an Encryption progress window. Encryption can take a several hours (or longer).

- Do not use the computer during this process. It will slow down the encryption.

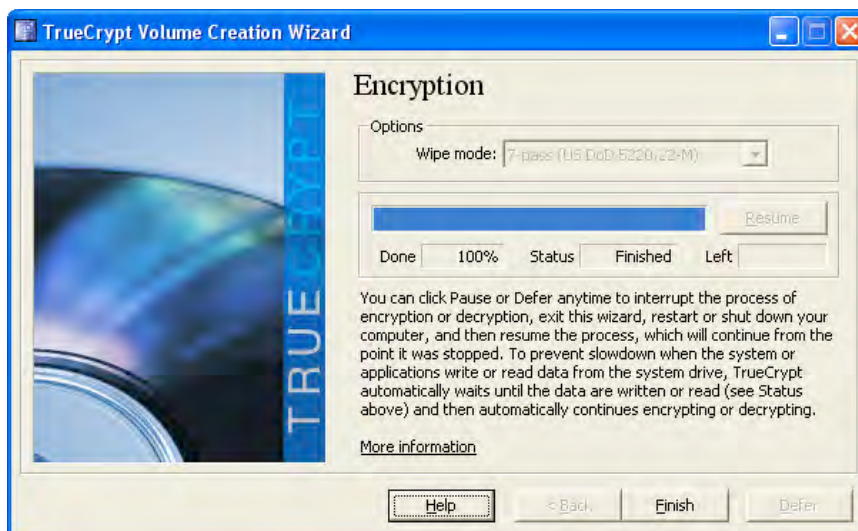


Once encryption has finished you will see a success message box.

- Click OK.



- Click Finish.



Congratulations! You have setup TrueCrypt.

2. How to encrypt portable USB drives with TrueCrypt

Warning! This process will destroy any data already on the portable drive.

Using a computer with TrueCrypt installed.

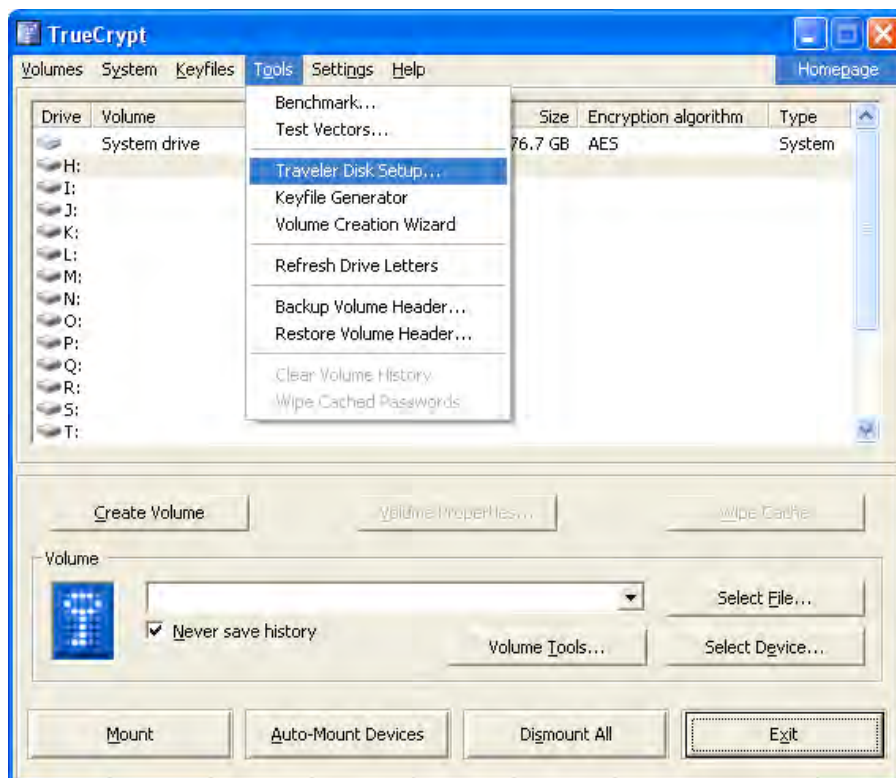
- Insert the portable USB drive.
- Delete any data on the portable drive.

Many portable USB drives come with two partitions (a small partition containing software, and a primary partition for data storage).

- Ignore the small partition.

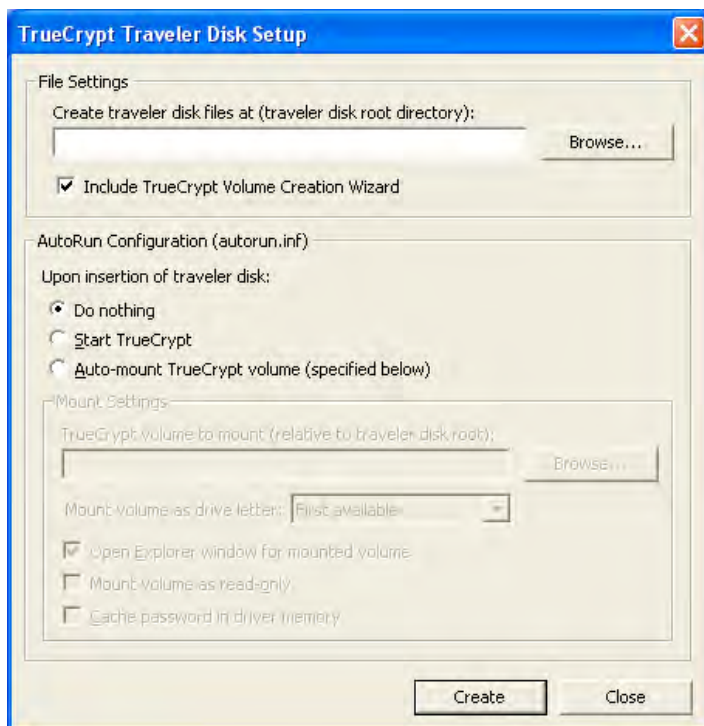
Find and start TrueCrypt.

- Select Traveler Disk Setup...from the Tools menu.



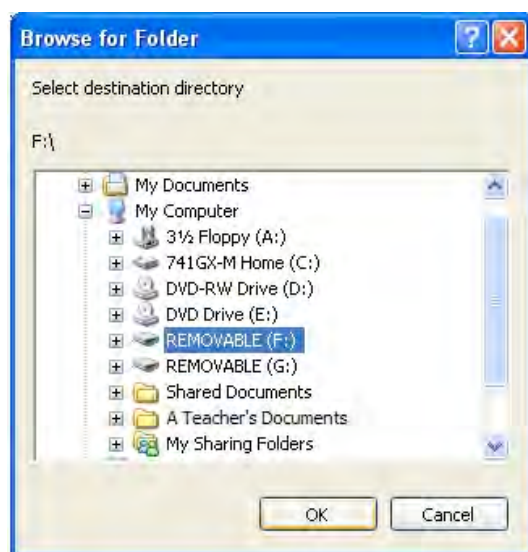
You will see a TrueCrypt Traveler Disk Setup window.

- Click Browse to select the drive you want to encrypt.



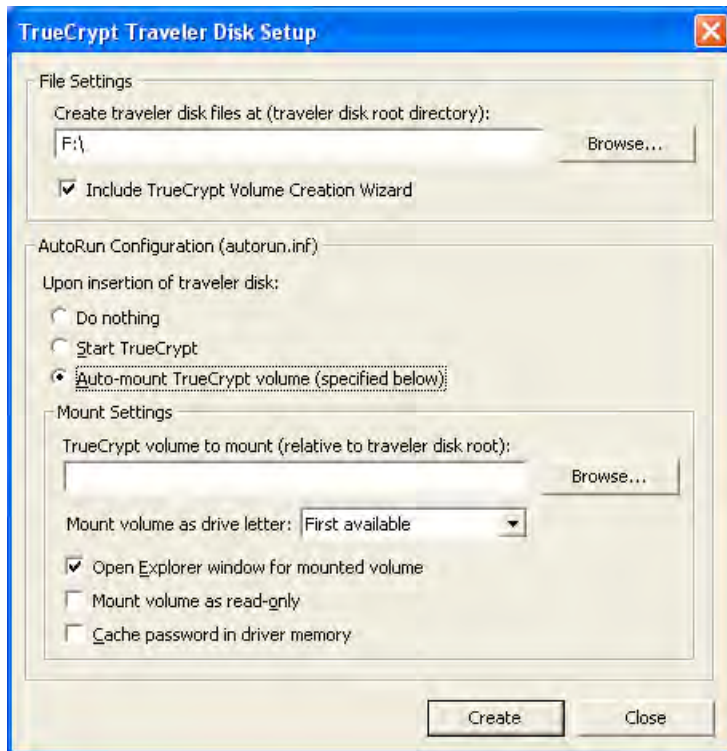
Find the portable drive you want to encrypt. Take care to select the correct drive.

- Click OK.



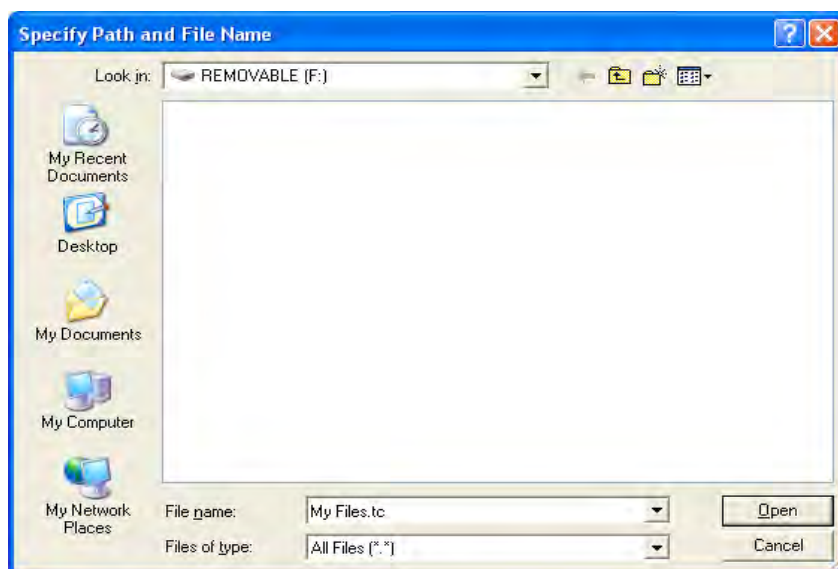
Back at the TrueCrypt Traveler Disk Setup window.

- Select the Auto-mount TrueCrypt volume (specified below) AutoRun Configuration option.



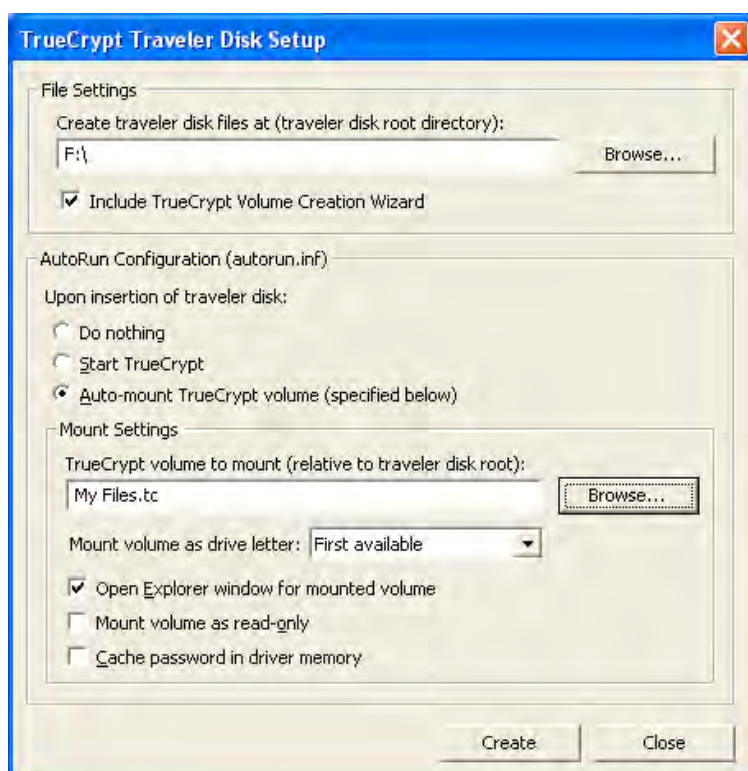
- Click Browse.
- Create a file with a .tc extension. (For example, 'My Files.tc').
- Click Open.

Important! Remember the name of the file. You will need this later.



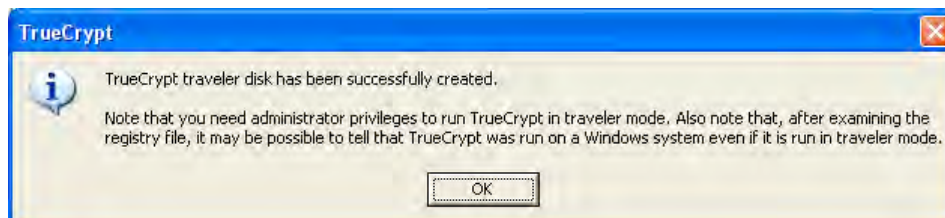
Return to the TrueCrypt Traveler Disk Setup window.

- Click Create.



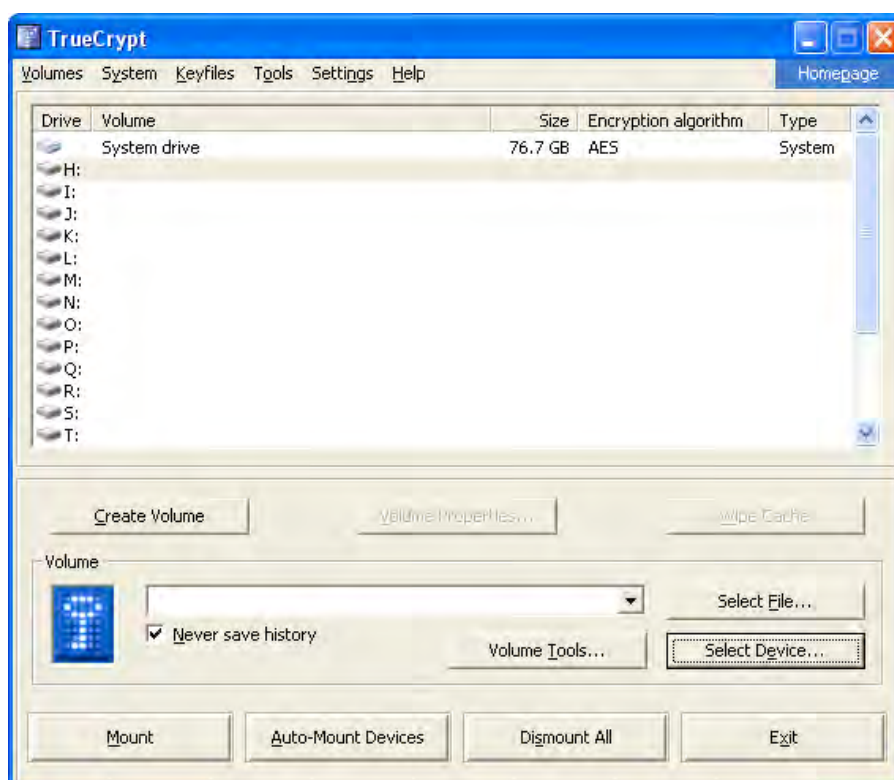
If the process finishes successfully, you will see a dialog box.

- Click OK.
- Click Close to return to the main TrueCrypt application window.



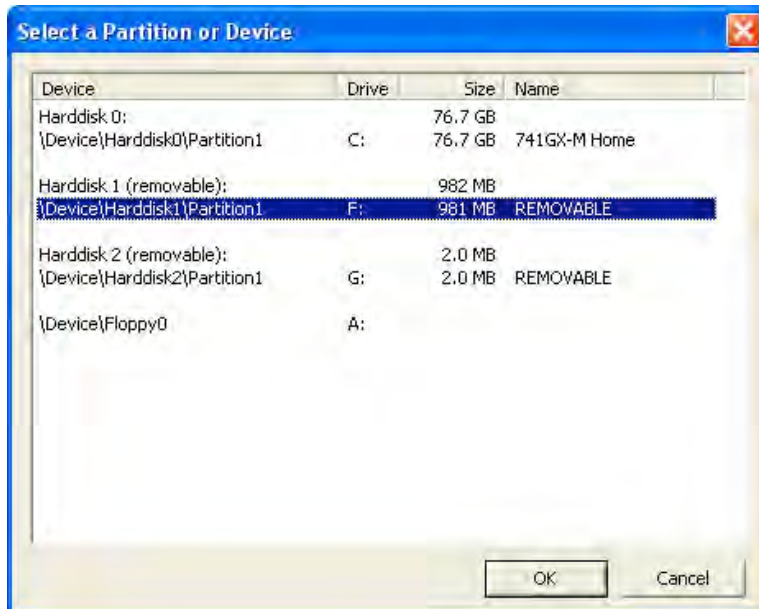
At the main TrueCrypt application window.

- Click Select Device.



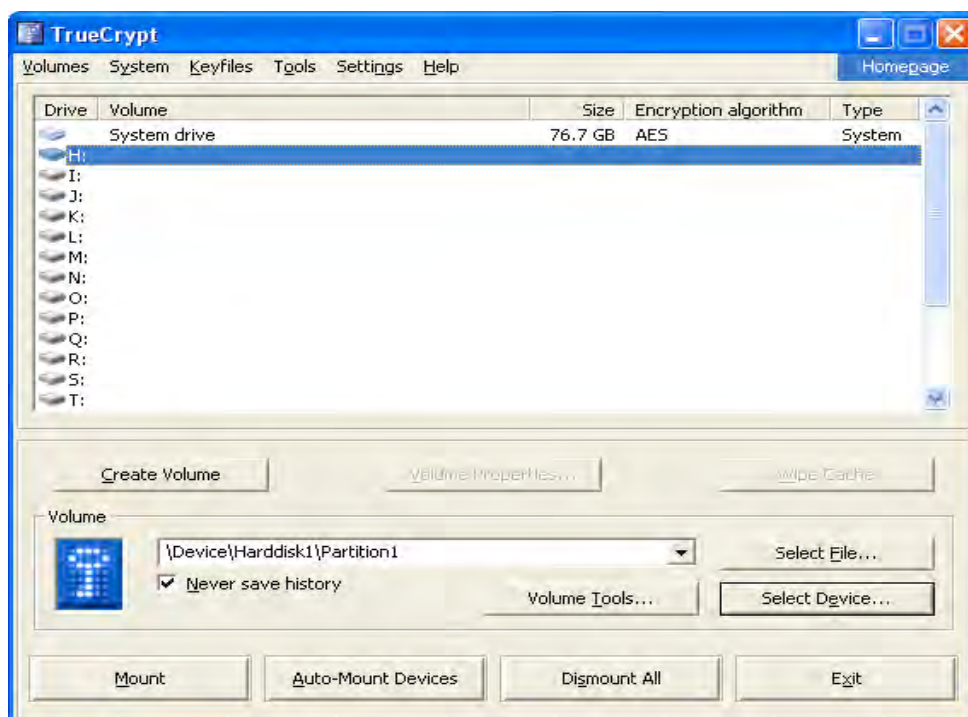
Select the USB portable drive's partition that you wish encrypt. Take care to select the correct drive and partition.

- Click OK.



At the main TrueCrypt application window.

- Click Create Volume.



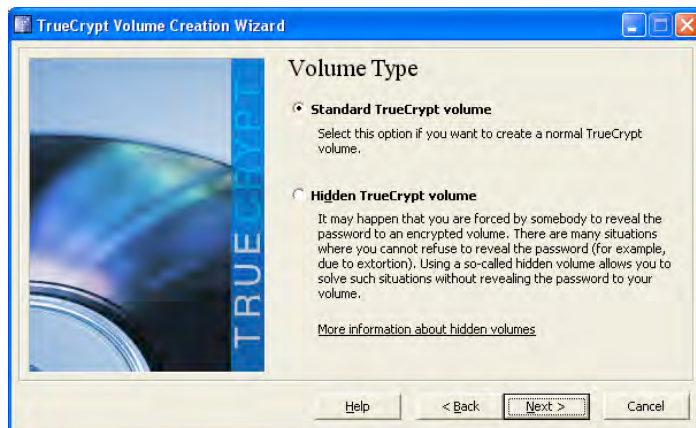
The TrueCrypt Volume Creation Wizard will start.

- Accept the default options.
- Click Next.



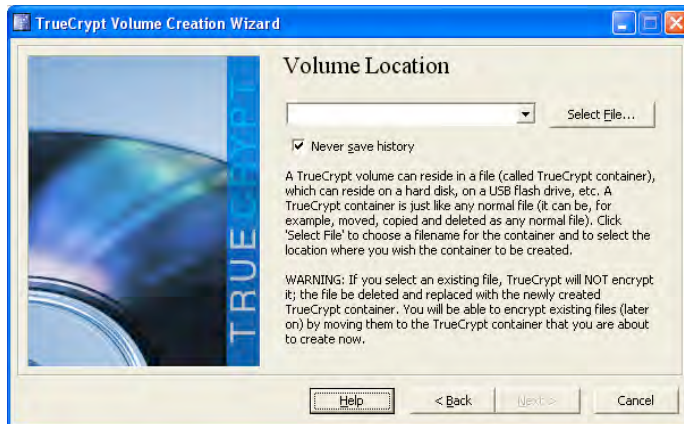
You will see a Volume Type window.

- Accept the default option.
- Click Next.



Next, you will see a Volume Location window.

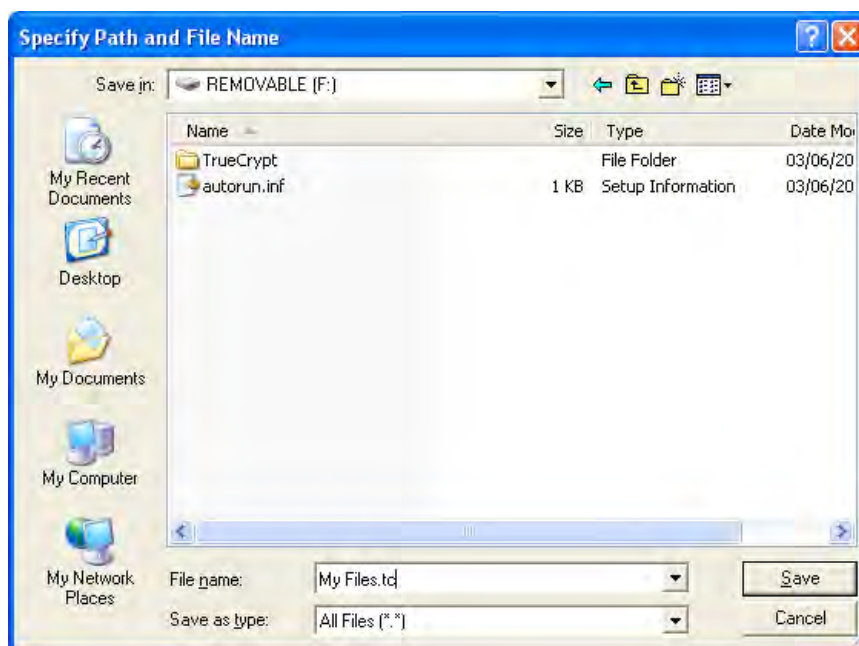
- Click Select File.



You will see a Specify Path and File Name box.

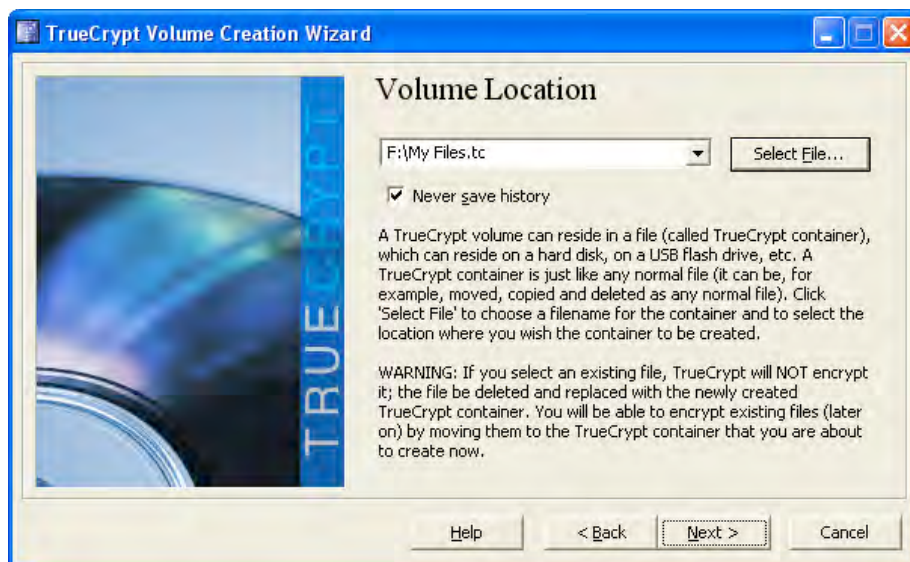
- Type the name of the file you created earlier (in this example My Files.tc)
- Click Save

Despite creating this file earlier, it will not show up in this directory browse so you have to type it in by hand!



Back at the Volume Location window.

- Click Next.



You will see an Encryption Options window.

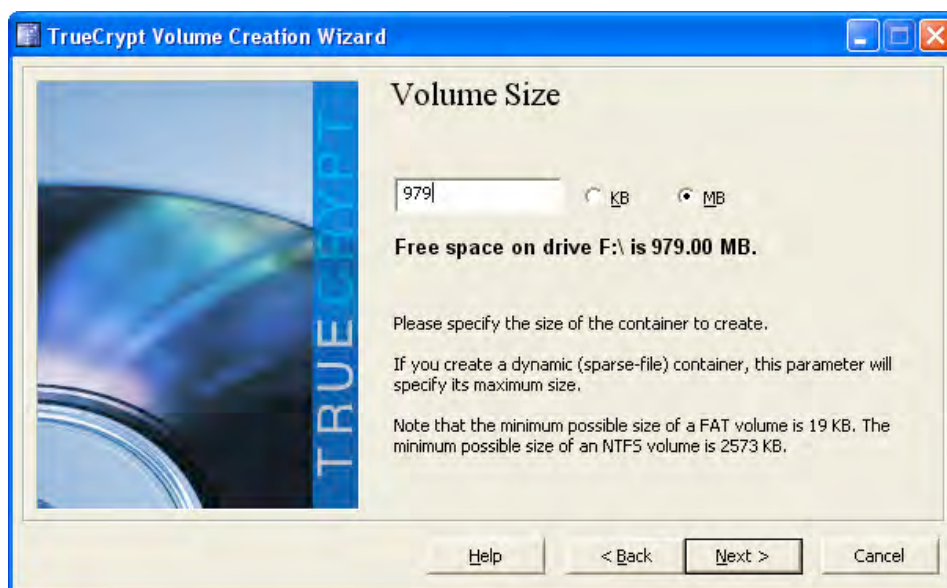
- Select the AES Encryption Algorithm.
- Select the RIPEMD-160 Hash Algorithm
- Click Next.



Next, you see a Volume Size window.

- In the box, type in the value shown as free space on your drive (in our example, 979).
- Click Next.

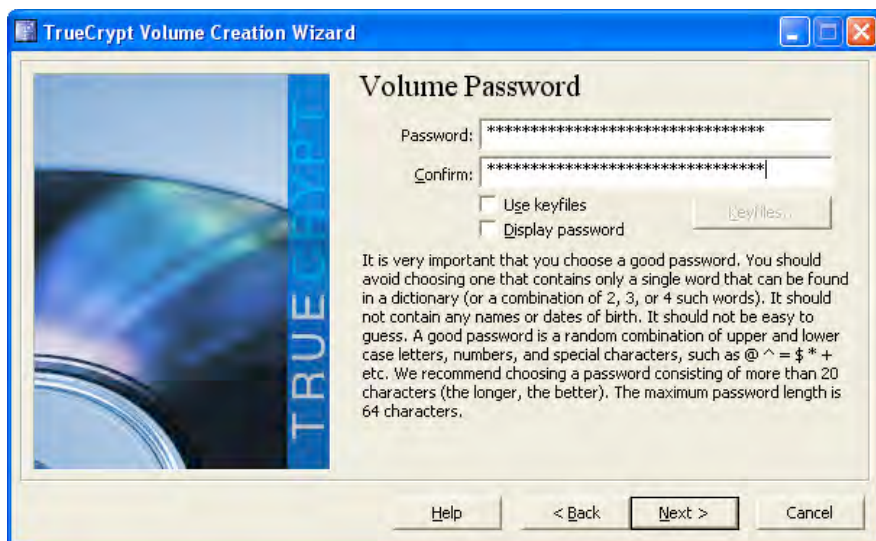
The largest value you can enter is 4000 MB (4GB).



You will see a Password window.

- Choose a strong password. (A strong password is at least 10 characters long and contains letters and numbers.)

Warning! You must remember this password! If you forget it, you will not be able to access any the secured data on your portable drive again! You will loss the data permanently.



Next, you will see a Volume Format window.

- Randomly move your mouse for at least a minute.
- Click Format. (You do not need to wait for the characters in the box to stop changing.)

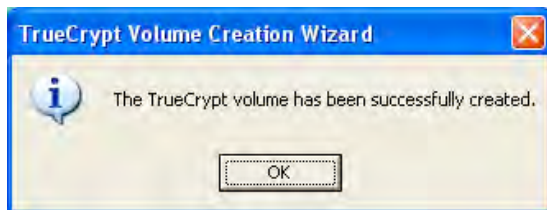


You will see Volume Format progress.



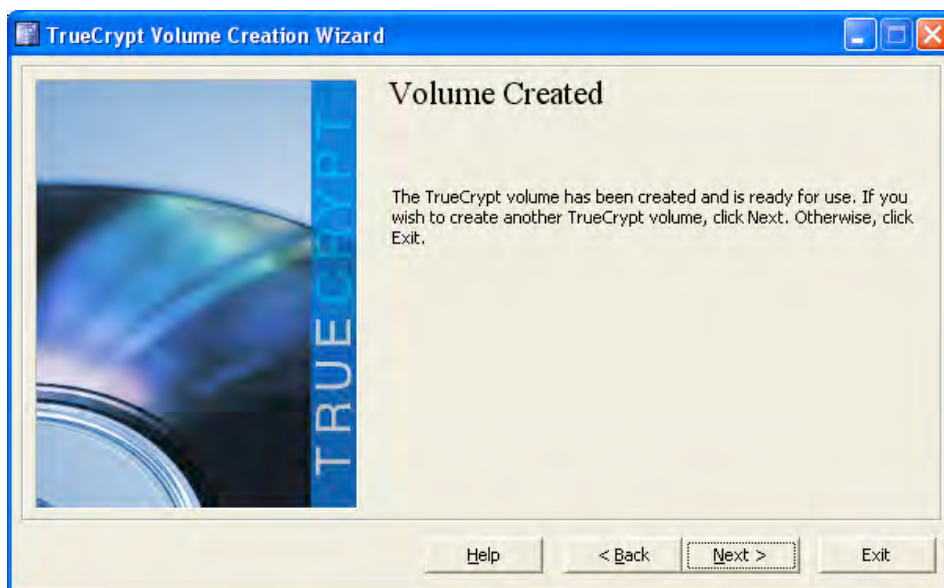
Then a success message box.

- Click OK.



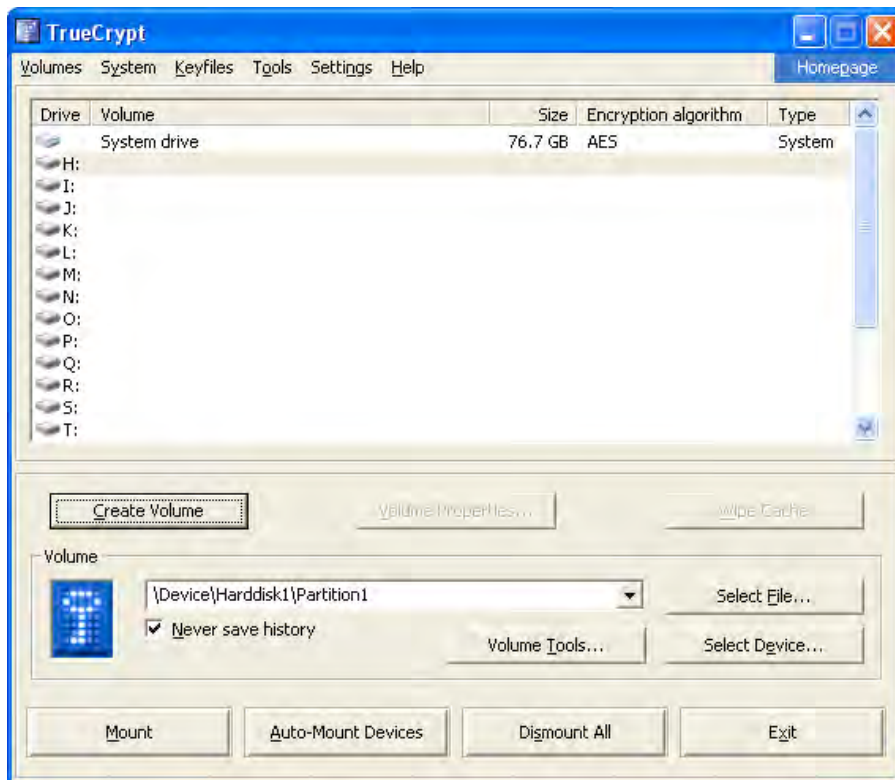
You will see a Volume Created window.

- Click Exit.



You will return to the TrueCrypt main application window.

- Click Exit.



Congratulations! You have now encrypted your USB portable drive and it is ready to use.

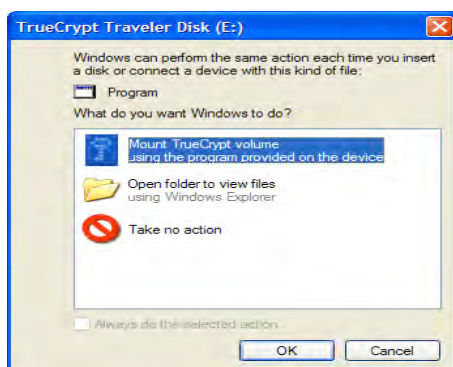
- Select Safely Remove Hardware to eject the device.

2.1. Issues with TrueCrypt encrypted portable USB drives

You must be logged into your computer with administrator privileges to use TrueCrypt encrypted USB portable drives.

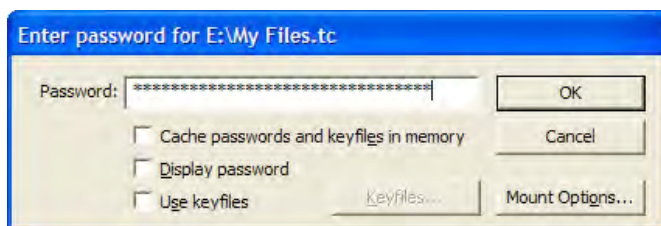
When you insert the portable drive into your computer, the following dialogue will appear.

- Select Mount TrueCrypt Volume.
- Click on OK.



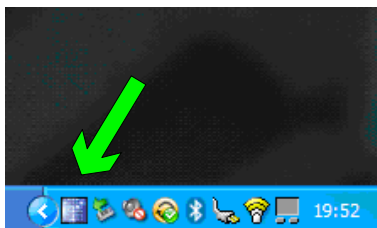
TrueCrypt will ask for your Password.

- Enter your password.



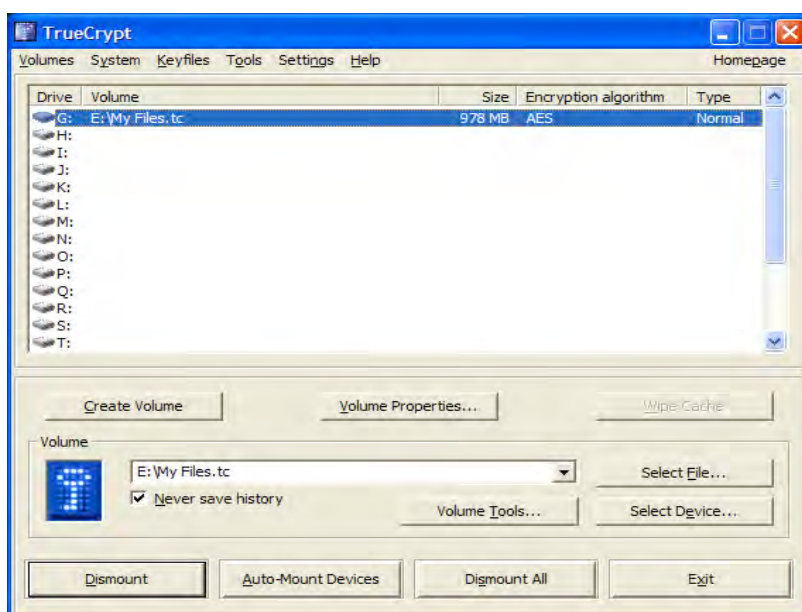
The disk is now open and you can use it like any other portable drive.

Warning! A TrueCrypt encrypted portable drive must not be 'stopped' with Safely Remove Hardware. You must use TrueCrypt to 'dismount' it. You will find a TrueCrypt icon in your computer's system tray.

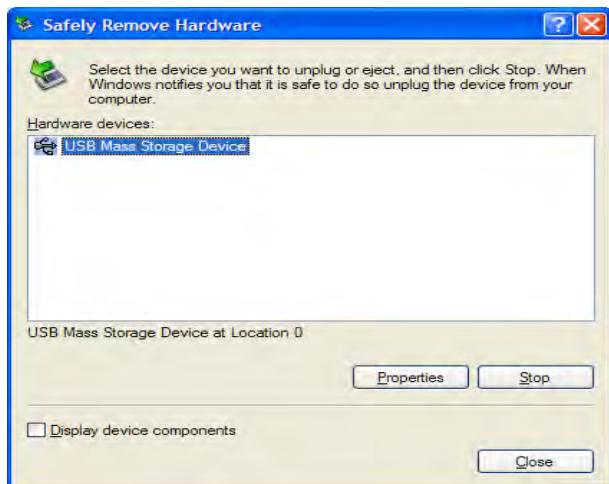


Clicking on this icon to bring up a TrueCrypt window.

- Select the portable USB drive.
- Click Dismount.
- Click Exit.



You can then use Safely Remove Hardware to remove it from your computer.



3. Extra notes on using TrueCrypt

TrueCrypt is free and open source software. This means that different developers have independently checked its source code and so it should be secure.

Provided you have installed and setup TrueCrypt correctly, it will meet the needs of our good practice for encryption. However, its effectiveness depends on the strength of passwords you have chosen.

Becta strongly recommend that you only use TrueCrypt if you have suitable technical help and support available locally.

Becta strongly recommend that you store your two TrueCrypt Rescue Disks in two separate physically secure locations, along with the printouts you made during the install and setup. You should also make sure that you do not forget your TrueCrypt passwords. You cannot recover your encrypted data without these.

Becta do not recommend TrueCrypt over other encryption products available. Other products may be more suited to you or your organisation's needs.