Instructions for Computer Use

1) Turn on machine pressing the power button on the unit on the floor

2) On the home screen choose “SSW User”

3) Create a folder for your data on either the E: or D: drives. DO NOT use the C: drive. The C: drive is for programs only.

4) It is YOUR responsibility to password protect and encrypt your data! Please follow the steps below.

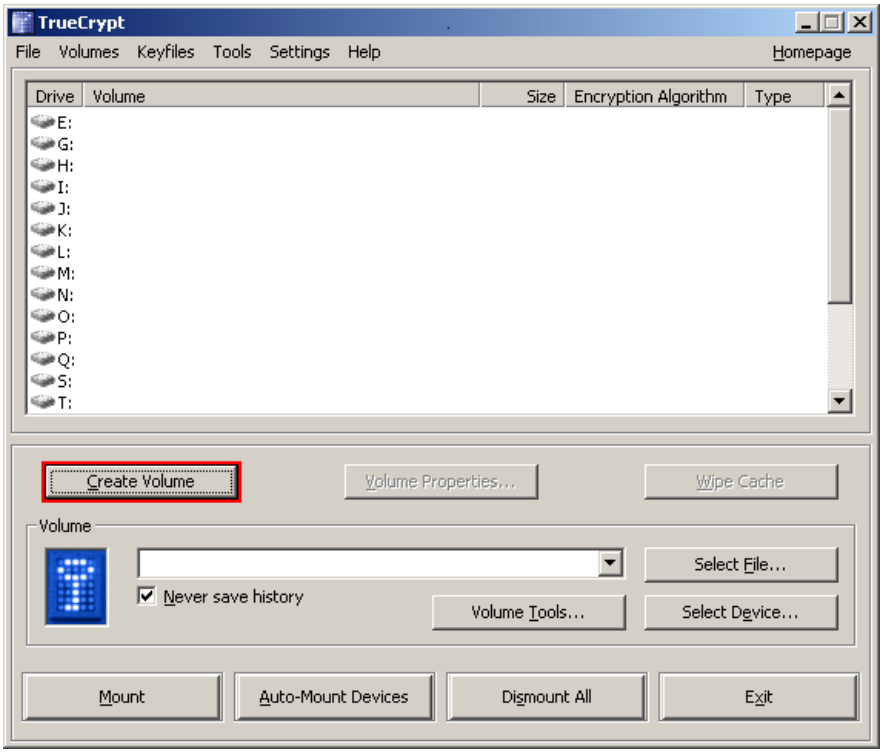
Instructions for setting up encryption and password protection with TrueCrypt

How to Create and Use a TrueCrypt Container in 18 SMALL steps

Step 1:

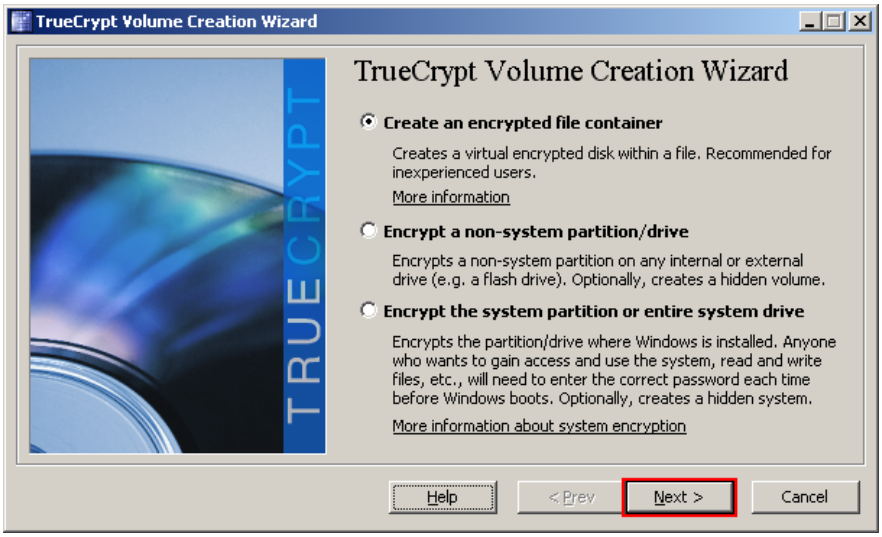
Launch TrueCrypt by double-clicking the file *TrueCrypt.exe* or by clicking the TrueCrypt shortcut in your Windows Start menu.

Step 2:



The main TrueCrypt window should appear. Click **Create Volume** (marked with a red rectangle for clarity).

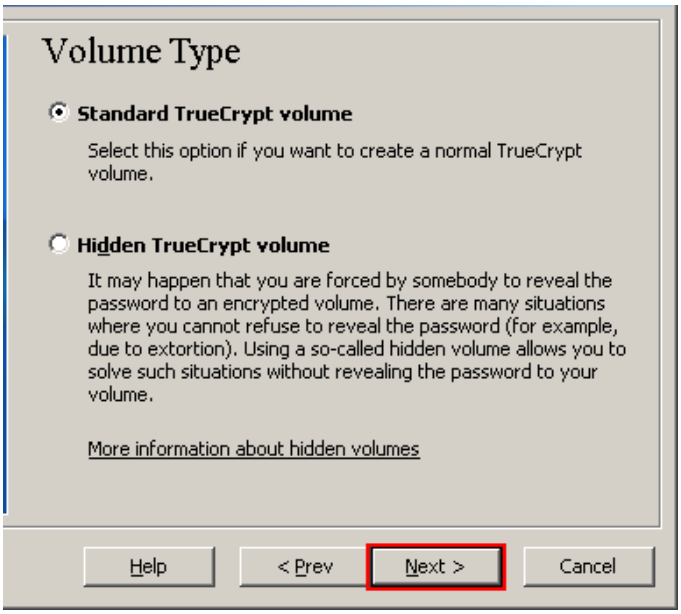
Step 3:



The TrueCrypt Volume Creation Wizard window should appear.

In this step you need to choose where you wish the TrueCrypt volume to be created. A TrueCrypt volume can reside in a file, which is also called container, in a partition or drive. In this tutorial, we will choose the first option and create a TrueCrypt volume within a file. Choose one of the three, then click **Next**.

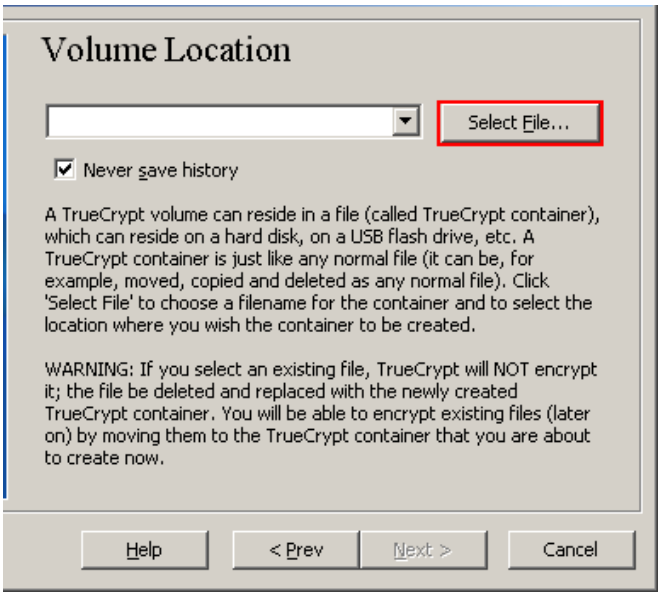
Step 4:



In this step you need to choose whether to create a standard or hidden TrueCrypt volume. Choose the standard option and create a standard TrueCrypt volume.

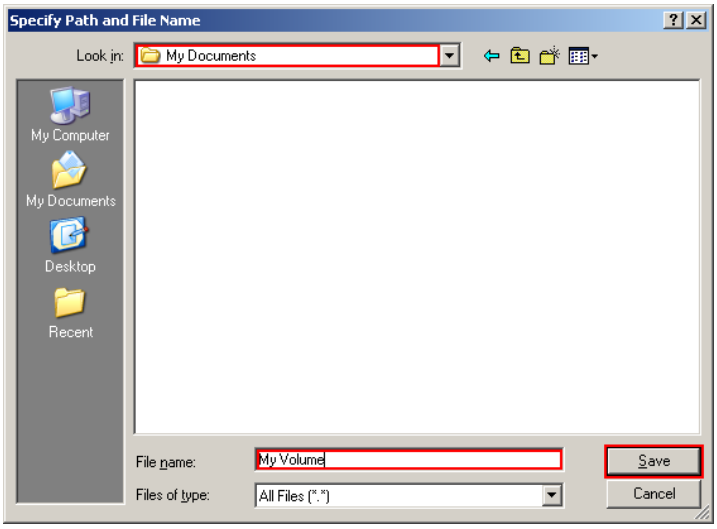
As the option is selected by default, you can just click **Next**.

Step 5:



In this step you have to specify where you wish the TrueCrypt volume (file container) to be created. Note that a TrueCrypt container is just like any normal file. It can be, for example, moved or deleted as any normal file. It also needs a filename, which you will choose in the next step. Click **Select File**. The standard Windows file selector should appear (while the window of the TrueCrypt Volume Creation Wizard remains open in the background).

Step 6:

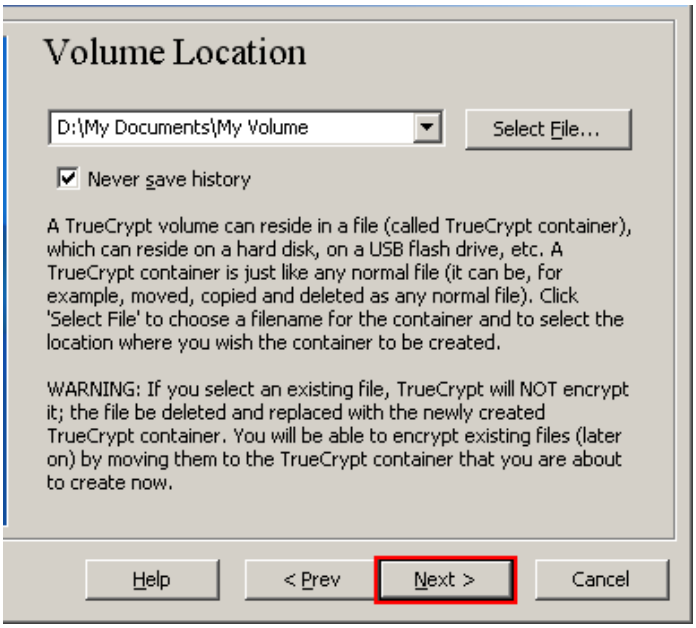


You may choose any filename and either the D: or E: drives.

IMPORTANT: **Note that TrueCrypt will *not* encrypt any existing files (when creating a TrueCrypt file container). If you select an existing file in this step, it will be overwritten and replaced by the newly created volume (so the overwritten file will be *lost*, *not* encrypted). You will be able to encrypt existing files (later on) by moving them to the TrueCrypt volume that we are creating now.***

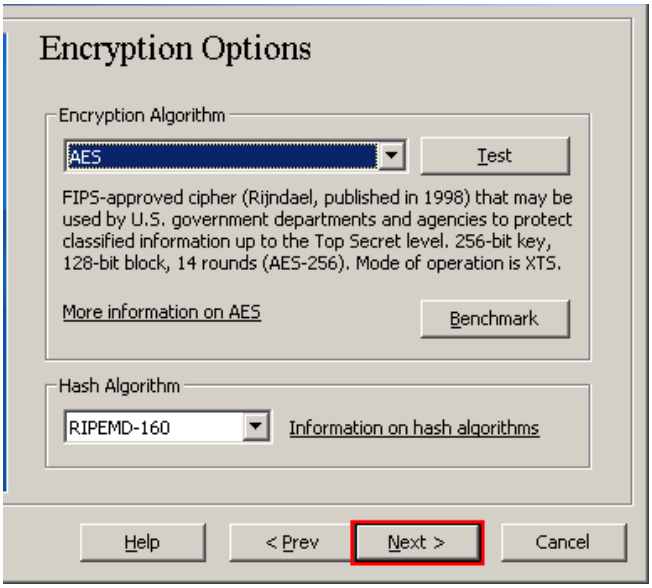
Select the desired path (where you wish the container to be created) in the file selector. Type the desired container filename in the **File name** box. Click **Save**. The file selector window should disappear.

Step 7:



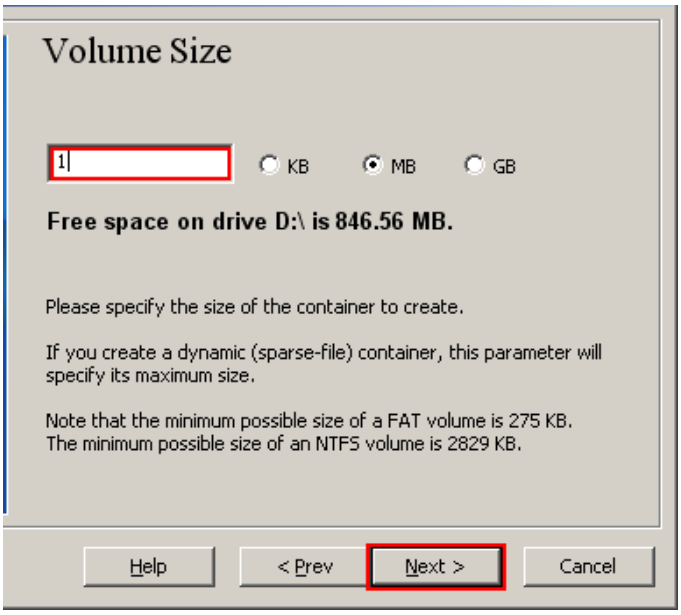
In the Volume Creation Wizard window, click **Next**.

Step 8:



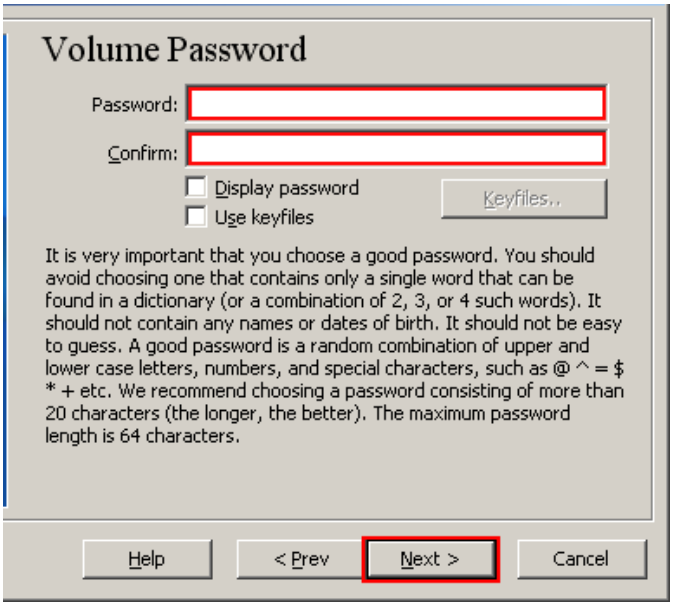
Here you the default choose an encryption algorithm and a hash algorithm for the volume and click **Next**.

Step 9:



Here we specify that we wish the size of our TrueCrypt container to be 1 megabyte. You may, of course, specify a different size. After you type the desired size in the input field (marked with a red rectangle), click **Next**.

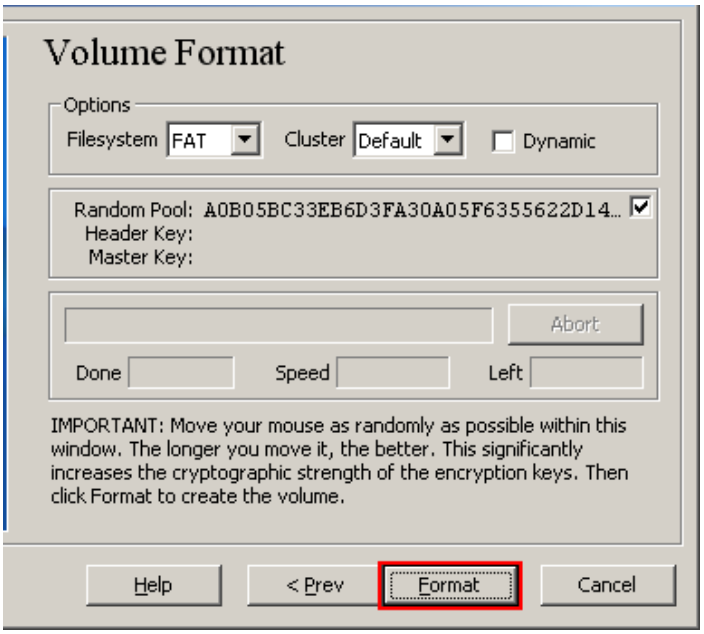
Step 10:



Read carefully the information displayed in the Wizard window about what is considered a good password. After you choose a good password, type it in the first input field. Then re-type it in the input field below the first one and click **Next**.

Note: The button **Next** will be disabled until passwords in both input fields are the same.

Step 11:



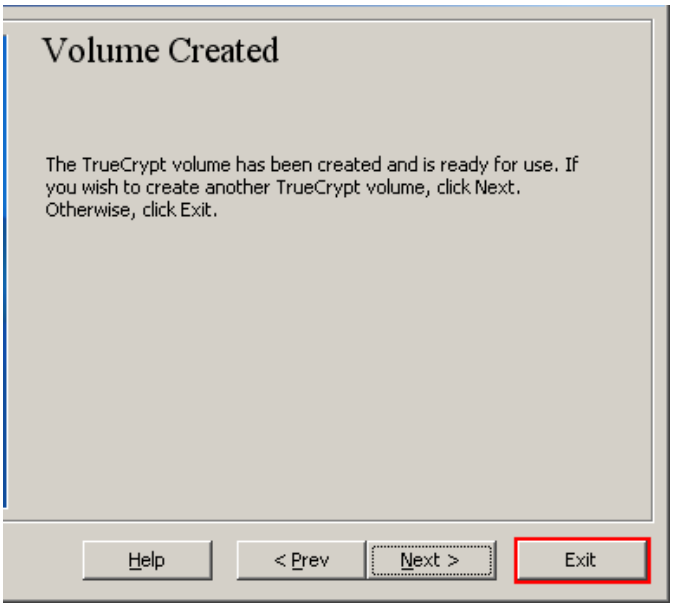
Move your mouse as randomly as possible within the Volume Creation Wizard window **at least** for 30 seconds. The longer you move the mouse, the better. This significantly increases the cryptographic strength of the encryption keys (which increases security).

Click **Format**.

Volume creation should begin. After it finishes, the following dialog box will appear:

Click **OK** to close the dialog box.

Step 12:



We have just successfully created a TrueCrypt volume (file container).

In the TrueCrypt Volume Creation Wizard window, click **Exit**.

The Wizard window should disappear.

The main TrueCrypt window should now be open, but if it is not, repeat Step 1 to launch TrueCrypt and then continue from Step 13.

Step 13:

Select any drive from the list. This will be the drive letter to which the TrueCrypt container will be mounted.

Step 14:

Click **Select File**.

Step 15:

In the file selector, browse to the container file (which we created in Steps 6-11) and select it.

Click **Open** (in the file selector window).

The file selector window should disappear.

Step 16:

In the main TrueCrypt window, click **Mount**.

Password prompt dialog window should appear.

Step 17:

Type the password which you specified.

Step 18:

Click **OK** in the password prompt window.

TrueCrypt will now attempt to mount the volume. If the password is incorrect (for example, if you typed it incorrectly), TrueCrypt will notify you and you will need to repeat the previous step (type the password again and click **OK**). If the password is correct, the volume will be mounted.

And you’re done!

Operating TrueCrypt

Copying Files into your Volume

You can copy files (or folders) to and from the TrueCrypt volume just as you would copy them to any normal disk (for example, by simple drag-and-drop operations). Files that are being read or copied from the encrypted TrueCrypt volume are automatically decrypted on the fly in RAM (memory). Similarly, files that are being written or copied to the TrueCrypt volume are automatically encrypted on the fly in RAM (right before they are written to the disk).

Note that TrueCrypt never saves any decrypted data to a disk – it only stores them temporarily in RAM (memory). Even when the volume is mounted, data stored in the volume is still encrypted. When you restart Windows or turn off your computer, the volume will be dismounted and all files stored on it will be inaccessible (and encrypted). Even when power supply is suddenly interrupted (without proper system shut down), all files stored on the volume will be inaccessible (and encrypted). To make them accessible again, you have to mount the volume. To do so, repeat Steps 13-18.

Closing Out TrueCrypt

If you want to close the volume and make files stored on it inaccessible, either restart your operating system or dismount the volume. To do so, follow these steps:

Select the volume from the list of mounted volumes in the main TrueCrypt window (marked with a red rectangle in the screenshot above) and then click **Dismount** (also marked with a red rectangle in the screenshot above). To make files stored on the volume accessible again, you will have to mount the volume. To do so, repeat Steps 13-18.

Main Program Window

Select File

Allows you to select a file-hosted TrueCrypt volume. After you select it, you can perform various operations on it (e.g., mount it by clicking 'Mount'). It is also possible to select a volume by dragging its icon to the 'TrueCrypt.exe' icon (TrueCrypt will be automatically launched then) or to the main program window.

Select Device

Allows you to select a TrueCrypt partition or a storage device (such as a USB memory stick). After it is selected, you can perform various operations with it (e.g., mount it by clicking 'Mount').

Note: There is a more comfortable way of mounting TrueCrypt partitions/devices – see the section *Auto-Mount Devices* below for more information.

Mount

After you click 'Mount', TrueCrypt will try to mount the selected volume using cached passwords (if there are any) and if none of them works, it prompts you for a password. If you enter the correct password (and/or provide correct keyfiles), the volume will be mounted.

Important: Note that when you exit the TrueCrypt application, the TrueCrypt driver continues working and no TrueCrypt volume is dismounted.

Auto-Mount Devices

This function allows you to mount TrueCrypt partitions/devices without having to select them manually (by clicking 'Select Device'). TrueCrypt scans headers of all available partitions/devices on your system (except DVD drives and similar devices) one by one and tries to mount each of them as a TrueCrypt volume. Note that a TrueCrypt partition/device cannot be identified, nor the cipher it has been encrypted with. Therefore, the program cannot directly "find" TrueCrypt partitions. Instead, it has to try mounting each (even unencrypted) partition/device using all encryption algorithms and all cached passwords (if there are any). Therefore, be prepared that this process may take a long time on slow computers.

If the password you enter is wrong, mounting is attempted using cached passwords (if there are any). If you enter an empty password and if *Use keyfiles* is unchecked, only the cached passwords will be used when attempting to auto-mount partitions/devices. If you do not need to set mount options, you can bypass the password prompt by holding down the *Shift* key when clicking *Auto-Mount Devices* (only cached passwords will be used, if there are any).

Drive letters will be assigned starting from the one that is selected in the drive list in the main window.

Dismount

This function allows you to dismount the TrueCrypt volume selected in the drive list in the main window. To dismount a TrueCrypt volume means to close it and make it impossible to read/write from/to the volume.

Dismount All

Note: The information in this section applies to all menu items and buttons with the same or similar caption (for example, it also applies to the system tray menu item Dismount All).

This function allows you to dismount multiple TrueCrypt volumes. To dismount a TrueCrypt volume means to close it and make it impossible to read/write from/to the volume. This function dismounts all mounted TrueCrypt volumes except the following:

- Partitions/drives within the key scope of active system encryption (e.g., a system partition encrypted by TrueCrypt, or a non-system partition located on a system drive encrypted by TrueCrypt, mounted when the encrypted operating system is running).
- TrueCrypt volumes that are not fully accessible to the user account (e.g. a volume mounted from within another user account).
- TrueCrypt volumes that are not displayed in the TrueCrypt application window. For example,system favorite volumes attempted to be dismounted by an instance of TrueCrypt without administrator privileges when the option '*Allow only administrators to view and dismount system favorite volumes in TrueCrypt*' is enabled.

Wipe Cache

Clears all passwords (which may also contain processed keyfile contents) cached in driver memory. When there are no passwords in the cache, this button is disabled. For information on password cache, see the subsection *Cache Password in Driver Memory* in the section Mounting TrueCrypt Volumes.

Never Save History

If this option disabled, the file names and/or paths of the last twenty files/devices that were attempted to be mounted as TrueCrypt volumes will be saved in the History file (whose content can be displayed by clicking on the Volume combo-box in the main window).

When this option is enabled, TrueCrypt clears the registry entries created by the Windows file selector for TrueCrypt, and sets the "current directory" to the user's home directory (in portable mode, to the directory from which TrueCrypt was launched) whenever a container or keyfile is selected via the Windows file selector. Therefore, the Windows file selector will not remember the path of the last mounted container (or the last selected keyfile). However, note that the operations described in this paragraph are not guaranteed to be performed reliably and securely (see e.g. Security Requirements and Precautions) so we strongly recommend that you encrypt the system partition/drive instead of relying on them (seeSystem Encryption).

Furthermore, if this option is enabled, the volume path input field in the main TrueCrypt window is cleared whenever you hide TrueCrypt.

Note: You can clear the volume history by selecting *Tools -> Clear Volume History*.

Exit

Terminates the TrueCrypt application. The driver continues working and no TrueCrypt volumes are dismounted. When running in portable mode, the TrueCrypt driver is unloaded when it is no longer needed (e.g., when all instances of the main application and/or of the Volume Creation Wizard are closed and no TrueCrypt volumes are mounted). However, if you force dismount on a TrueCrypt volume when TrueCrypt runs in portable mode, or mount a writable NTFS-formatted volume on Windows Vista or later, the TrueCrypt driver may *not* be unloaded when you exit TrueCrypt (it will be unloaded only when you shut down or restart the system). This prevents various problems caused by a bug in Windows (for instance, it would be impossible to start TrueCrypt again as long as there are applications using the dismounted volume).

How to Back Up Securely

Due to hardware or software errors/malfunctions, files stored on a TrueCrypt volume may become corrupted. Therefore, we strongly recommend that you backup all your important files regularly (this, of course, applies to any important data, not just to encrypted data stored on TrueCrypt volumes).

Non-System Volumes

To back up a non-system TrueCrypt volume securely, it is recommended to follow these steps:

1. Create a new TrueCrypt volume using the TrueCrypt Volume Creation Wizard (do not enable the*Quick Format* option or the *Dynamic* option). It will be your *backup* volume so its size should match (or be greater than) the size of your *main* volume.

2. Mount the newly created *backup* volume.

3. Mount the *main* volume.

4. Copy all files from the mounted *main* volume directly to the mounted *backup* volume.

Note: Never create a new TrueCrypt volume by cloning an existing TrueCrypt volume. Always use the TrueCrypt Volume Creation Wizard to create a new TrueCrypt volume.

How to Remove Encryption

Please note that TrueCrypt can in-place decrypt only **system partitions and system drives** (select*System* > *Permanently Decrypt System Partition/Drive*). If you need to remove encryption (e.g., if you no longer need encryption) from a **non-system volume**, please follow these steps:

1. Mount your TrueCrypt volume.
2. Move all files from the TrueCrypt volume to any location outside the TrueCrypt volume (note that the files will be decrypted on the fly).
3. Dismount the TrueCrypt volume.
4. **If the TrueCrypt volume is file-hosted**, delete it (the container) just like you delete any other file.