Beginner's Tutorial

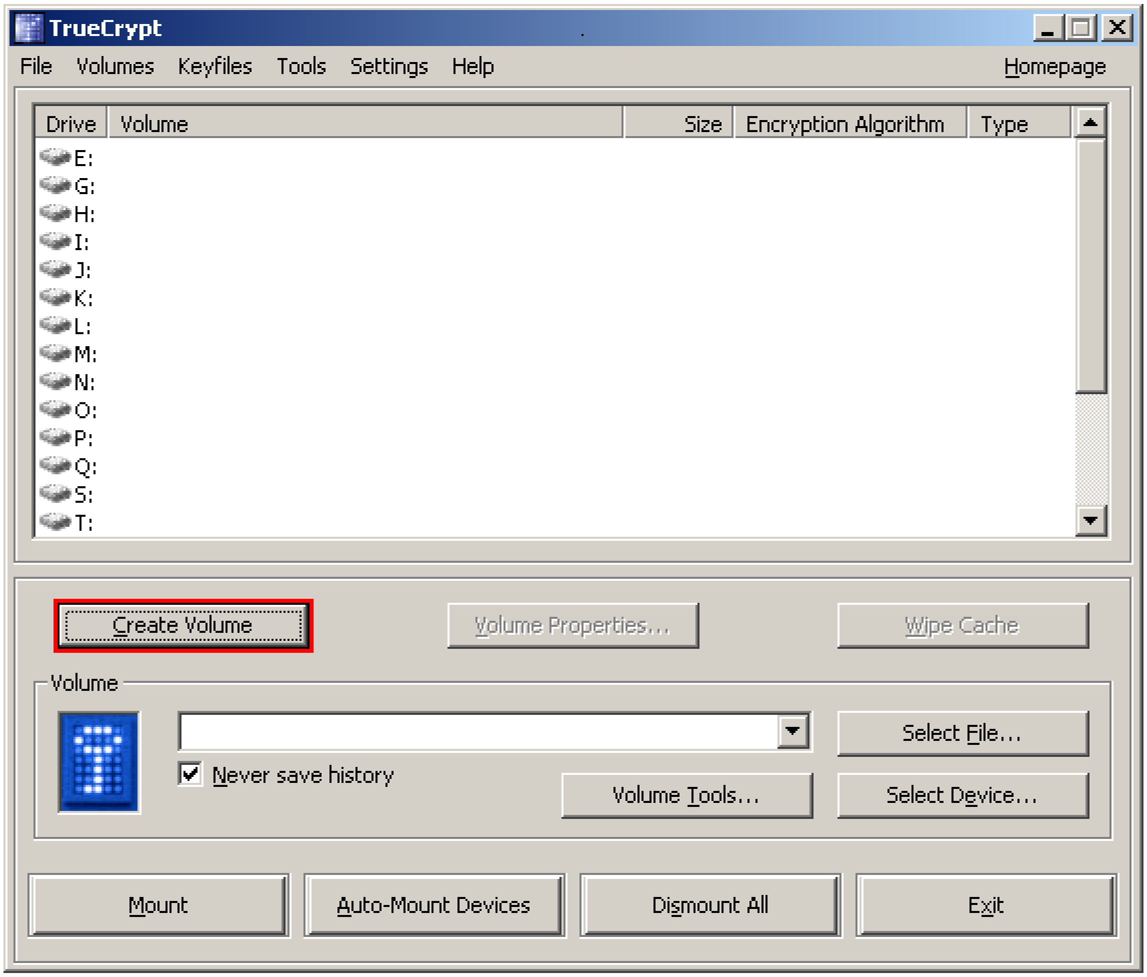
How to Create and Use a TrueCrypt Container

This chapter contains step-by-step instructions on how to create, mount, and use a TrueCrypt volume. We strongly recommend that you also read the other sections of this manual, as they contain important information.

Step 1:

If you have not done so, download and install TrueCrypt. Then launch TrueCrypt by double-clicking the file *TrueCrypt.exe* or by clicking the TrueCrypt shortcut in your Windows Start menu.

Step 2:

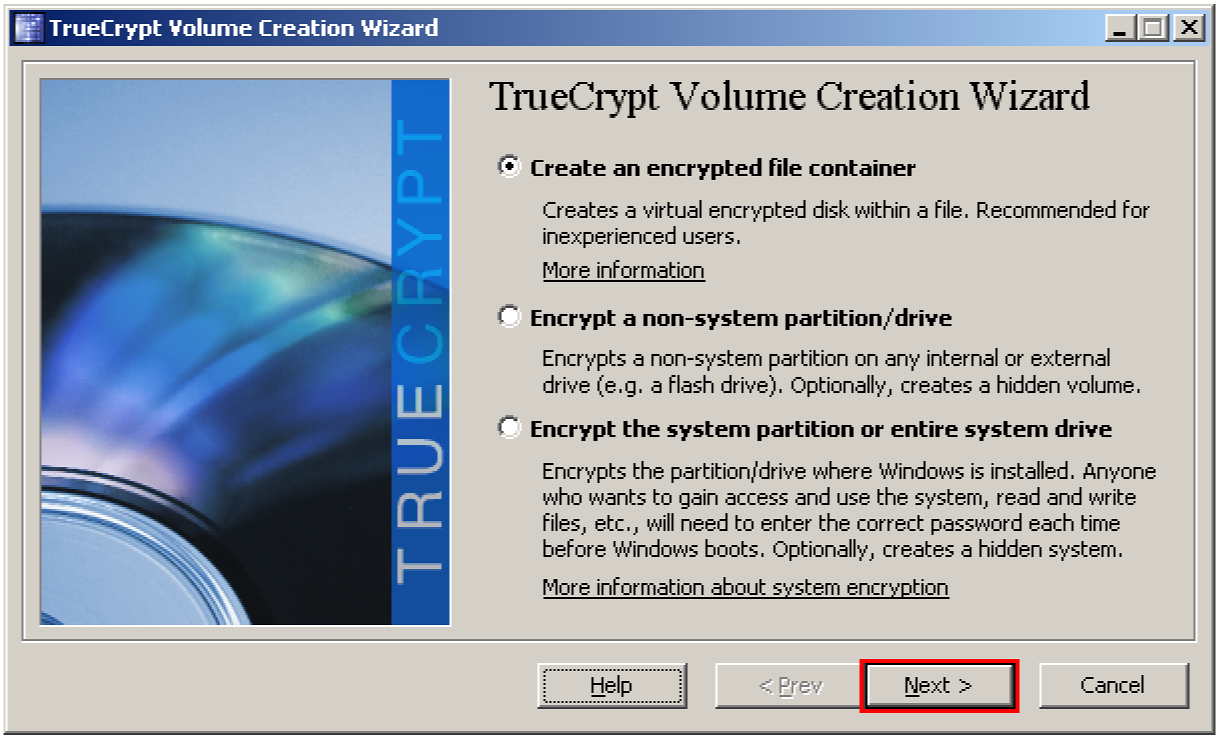


Drive	Volume	Size	Encryption Algorithm	Type
E:				
G:				
H:				
I:				
J:				
K:				
L:				
M:				
N:				
O:				
P:				
Q:				
S:				
T:				

☑ Never save history

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

Step 3:



TrueCrypt Volume Creation Wizard

TrueCrypt Volume Creation Wizard

● Create an encrypted file container

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

More information

○ Encrypt a non-system partition/drive

Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

○ Encrypt the system partition or entire system drive

Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.

More information about system encryption

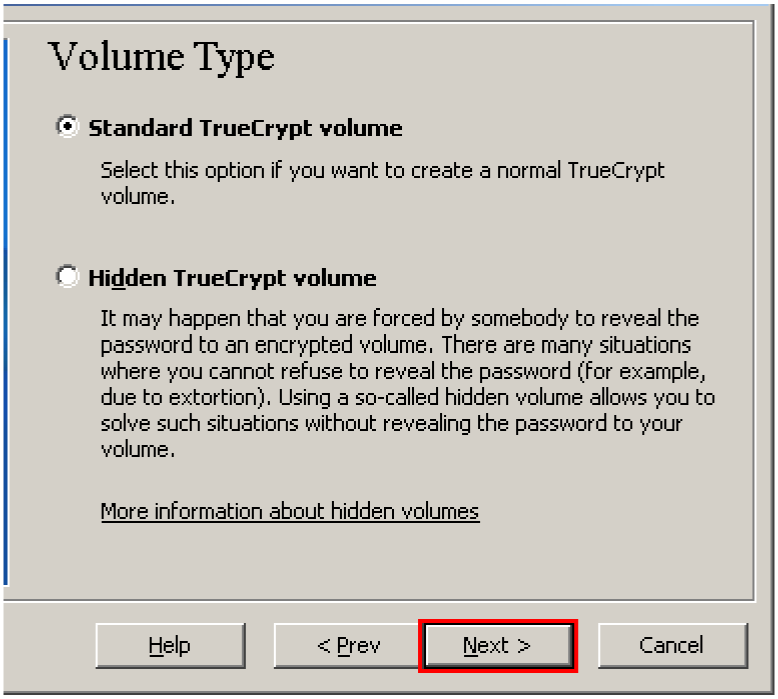
The TrueCrypt Volume Creation Wizard window should appear.

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.

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

Note: In the following steps, the screenshots will show only the right-hand part of the Wizard window.

Step 4:



Volume Type

● **Standard TrueCrypt volume**

Select this option if you want to create a normal TrueCrypt volume.

○ **Hidden TrueCrypt volume**

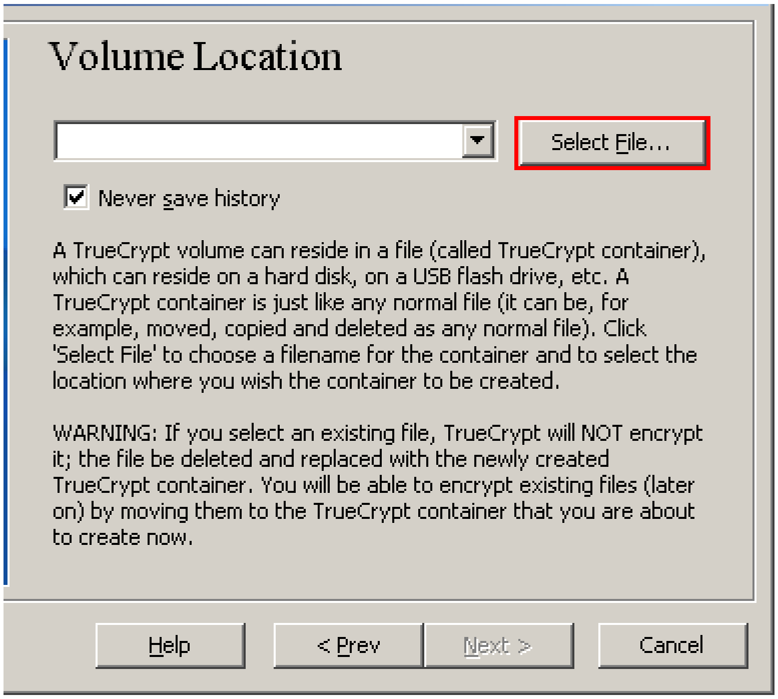
It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.

More information about hidden volumes

In this step you need to choose whether to create a standard or hidden TrueCrypt volume. In this tutorial, we will choose the former option and create a standard TrueCrypt volume.

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

Step 5:



Volume Location

☑ Never save history

A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved, copied and deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

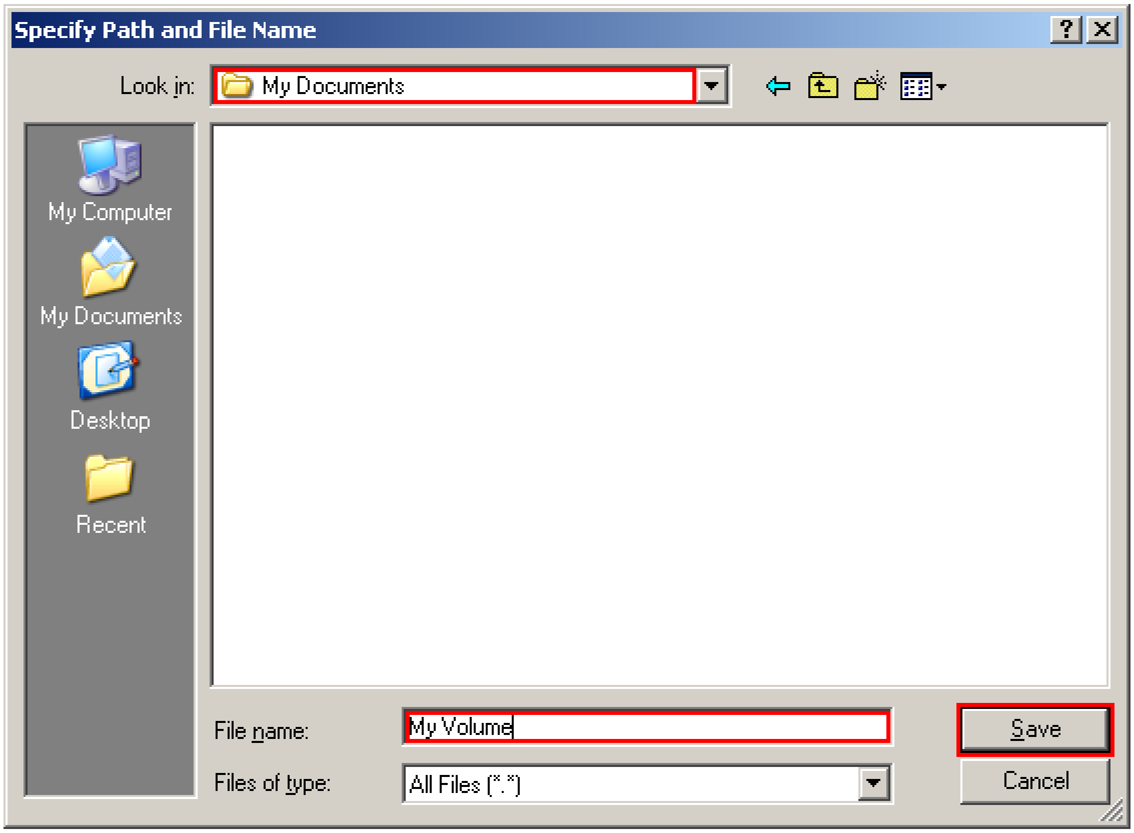
WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.

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:



In this tutorial, we will create our TrueCrypt volume in the folder *D:\My Documents* and the filename of the volume (container) will be *My Volume* (as can be seen in the screenshot above). You may, of course, choose any other filename and location you like (for example, on a USB memory stick). Note that the file *My Volume* does not exist yet – TrueCrypt will create it.

IMPORTANT: **Note that TrueCrypt will *not* encrypt any existing files. If you select an existing file, 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.***

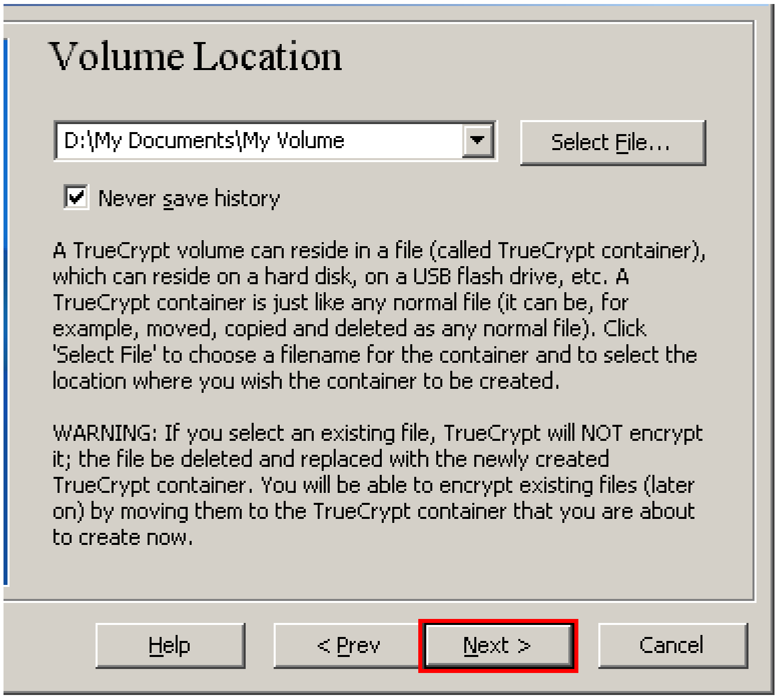
Select the desired path (where you wish the container to be created) in the file selector.

Type the desired container filename in the **File name** box.

Click **Save**.

The file selector window should disappear.

Step 7:



Volume Location

D:\My Documents\My Volume

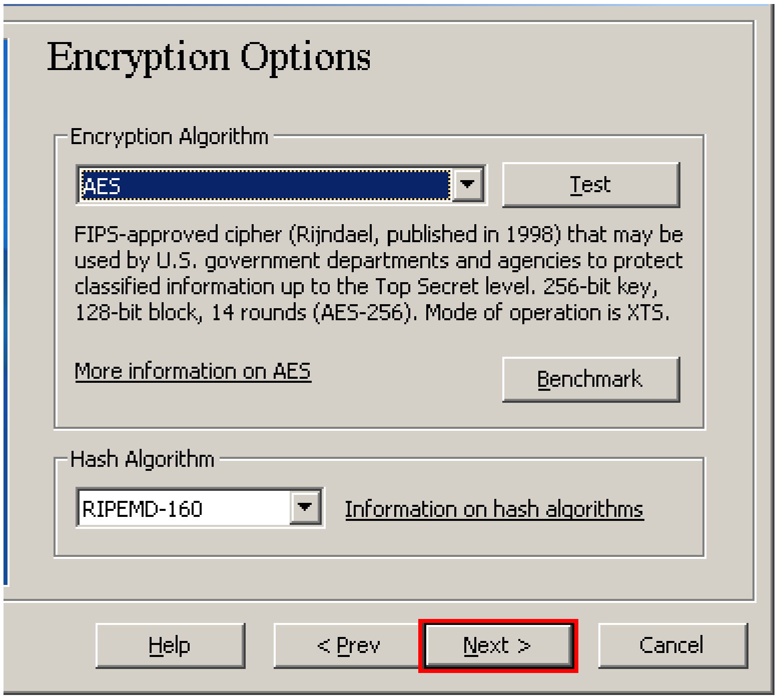
☑ Never save history

A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved, copied and deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.

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

Step 8:



Encryption Options

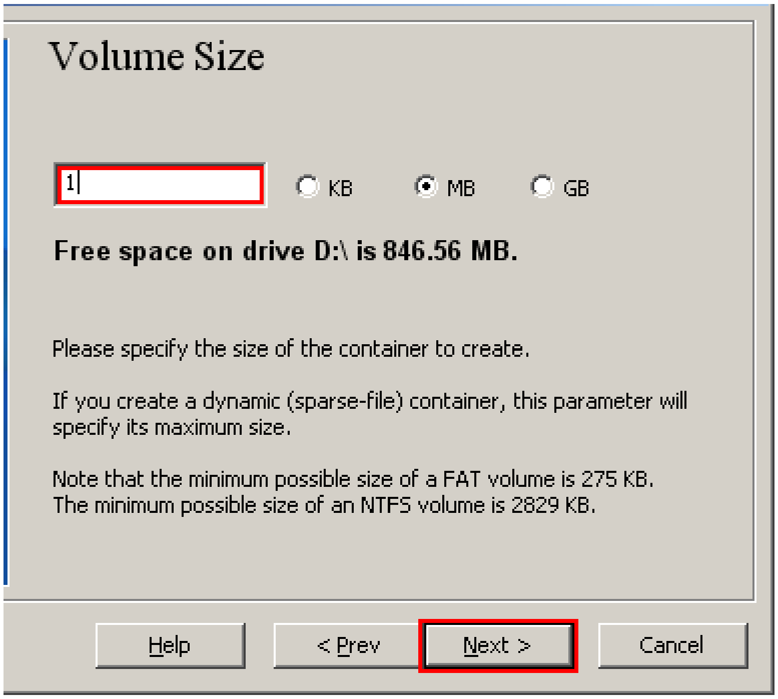
Encryption Algorithm: AES

FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.

Hash Algorithm: RIPEMD-160

Here you can choose an encryption algorithm and a hash algorithm for the volume. If you are not sure what to select here, you can use the default settings and click **Next** (for more information, see Chapters Encryption Algorithms and Hash Algorithms).

Step 9:



Volume Size

1 ○ KB ● MB ○ GB

Free space on drive D:\ is 846.56 MB.

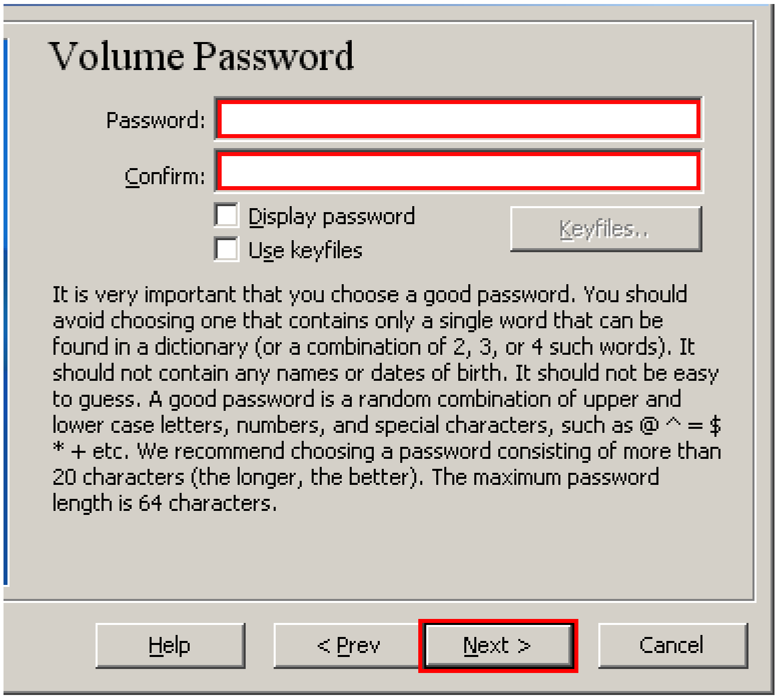
Please specify the size of the container to create.

If you create a dynamic (sparse-file) container, this parameter will specify its maximum size.

Note that the minimum possible size of a FAT volume is 275 KB. The minimum possible size of an NTFS volume is 2829 KB.

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:



Volume Password

Password:

Confirm:

□ Display password

□ Use keyfiles

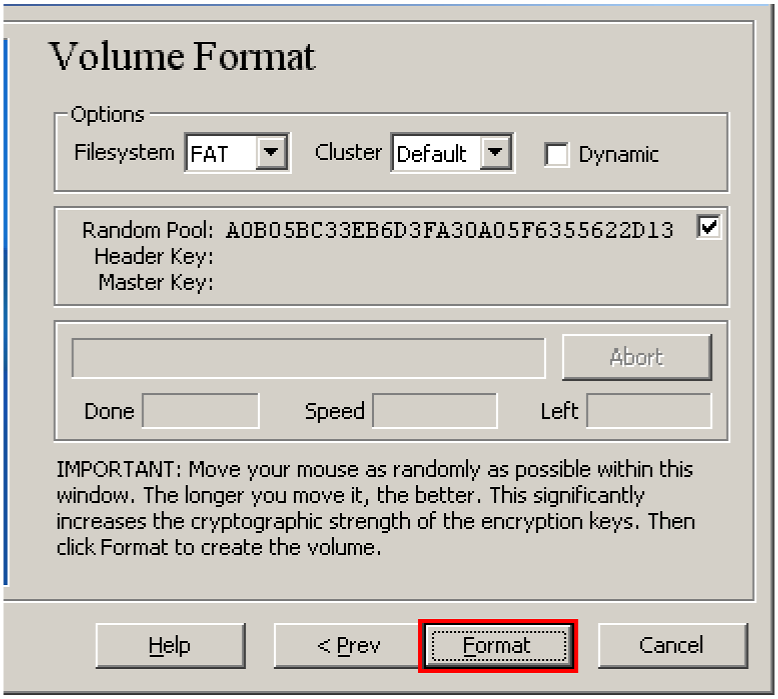
It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum password length is 64 characters.

This is one of the most important steps. Here you have to choose a good volume password.

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**.

Step 11:



Volume Format

Options

Filesystem FAT

Cluster Default

□ Dynamic

Random Pool: A0B05BC33EB6D3FA30A05F6355622D13 ☑

Header Key:

Master Key:

Done

Speed

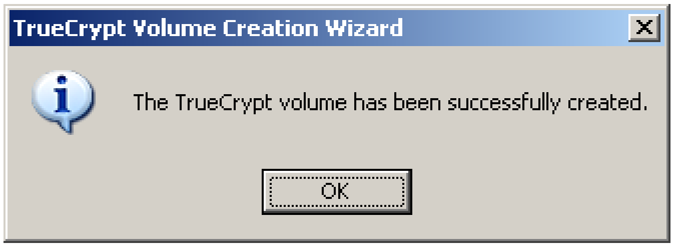
Left

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

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. TrueCrypt will now create a file called *My Volume* in the folder *D:\My Documents* (as we specified in Step 6). This file will be a TrueCrypt container (it will contain the encrypted TrueCrypt volume). Depending on the size of the volume, the volume creation may take a long time. After it finishes, the following dialog box will appear:

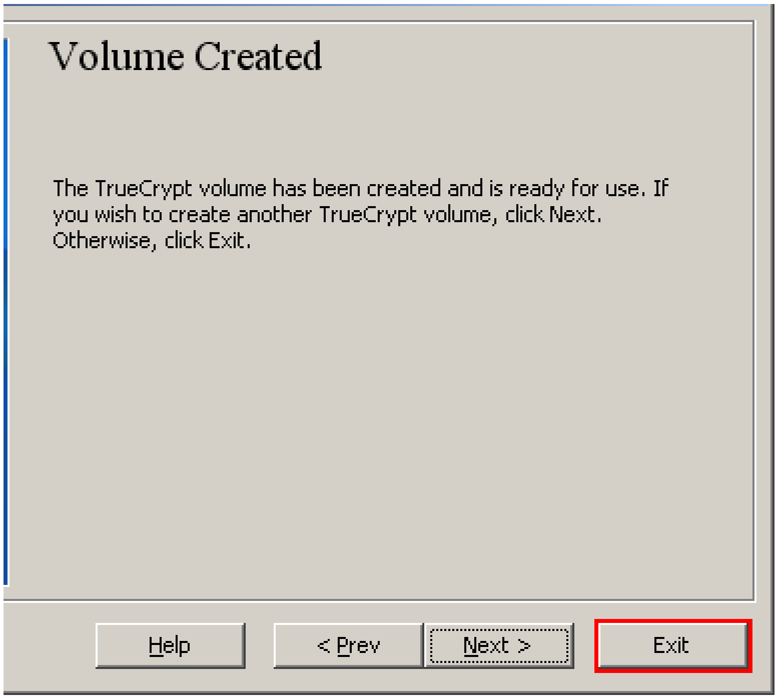


TrueCrypt Volume Creation Wizard

The TrueCrypt volume has been successfully created.

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

Step 12:



Volume Created

The TrueCrypt volume has been created and is ready for use. If you wish to create another TrueCrypt volume, click Next. Otherwise, click Exit.

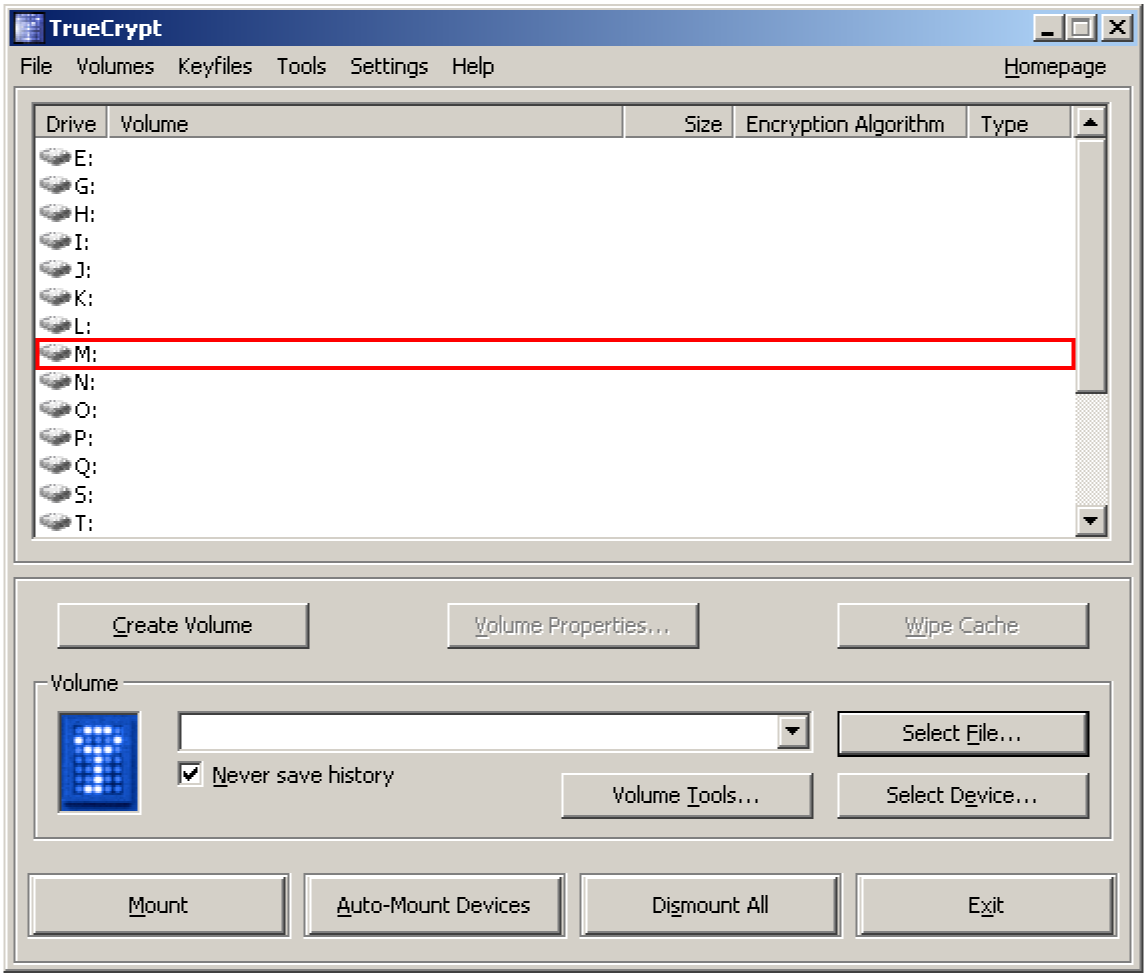
We have just successfully created a TrueCrypt volume (file container).

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

The Wizard window should disappear.

In the remaining steps, we will mount the volume we just created. We will return to the main TrueCrypt window (which should still be open, but if it is not, repeat Step 1 to launch TrueCrypt and then continue from Step 13.)

Step 13:



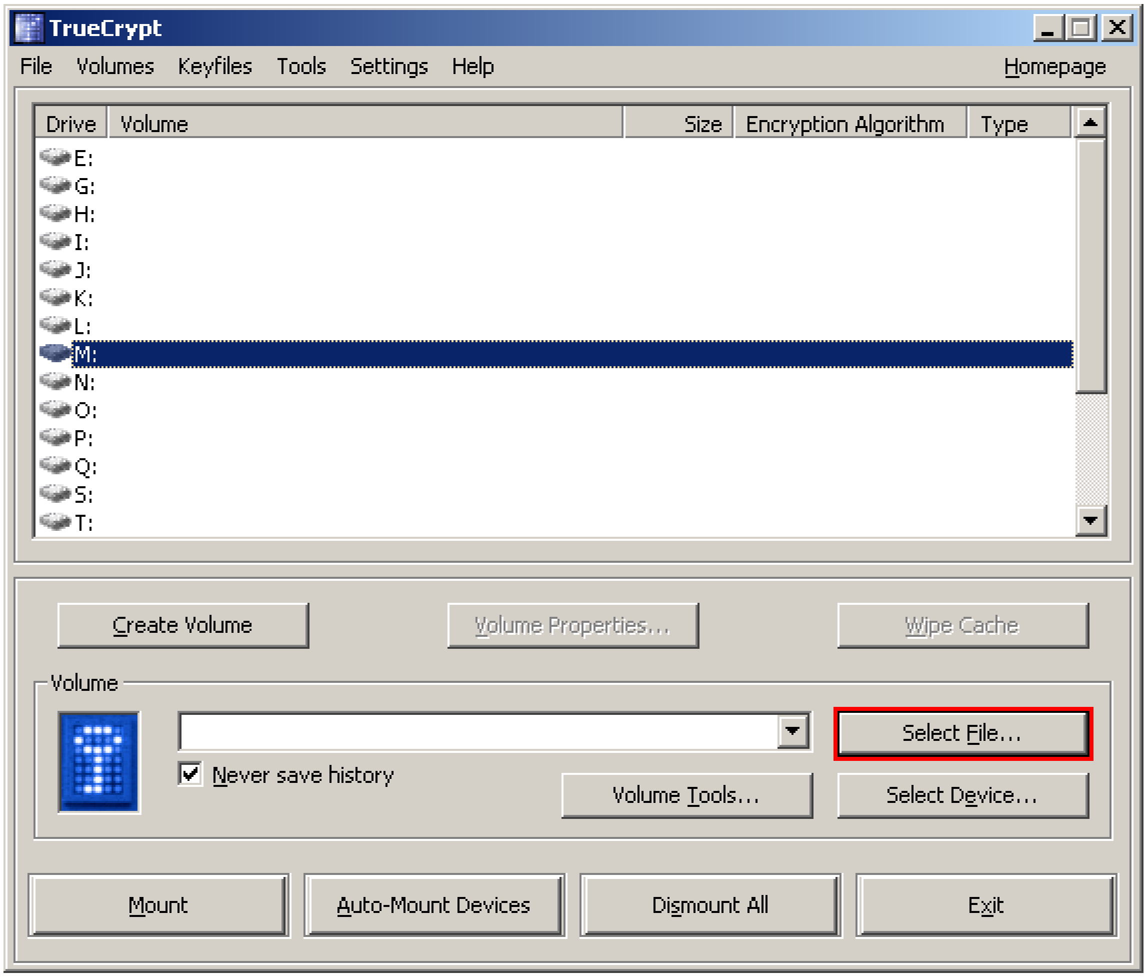
Drive	Volume	Size	Encryption Algorithm	Type
E:				
G:				
H:				
I:				
J:				
K:				
L:				
M:				
N:				
O:				
P:				
Q:				
S:				
T:				

☑ Never save history

Select a drive letter from the list (marked with a red rectangle). This will be the drive letter to which the TrueCrypt container will be mounted.

Note: In this tutorial, we chose the drive letter M, but you may of course choose any other available drive letter.

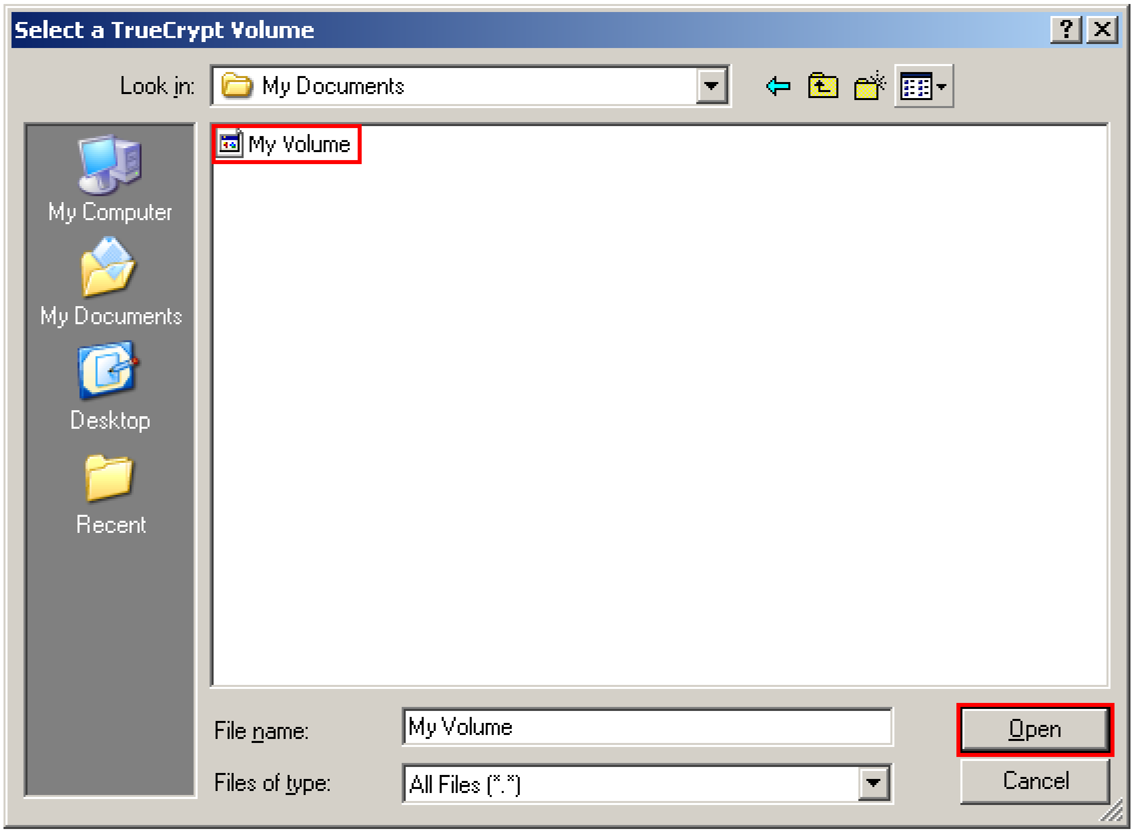
Step 14:



Click **Select File**.

The standard file selector window should appear.

Step 15:



Select a TrueCrypt Volume

Look in: My Documents

File name: My Volume

Files of type: All Files (*.*)

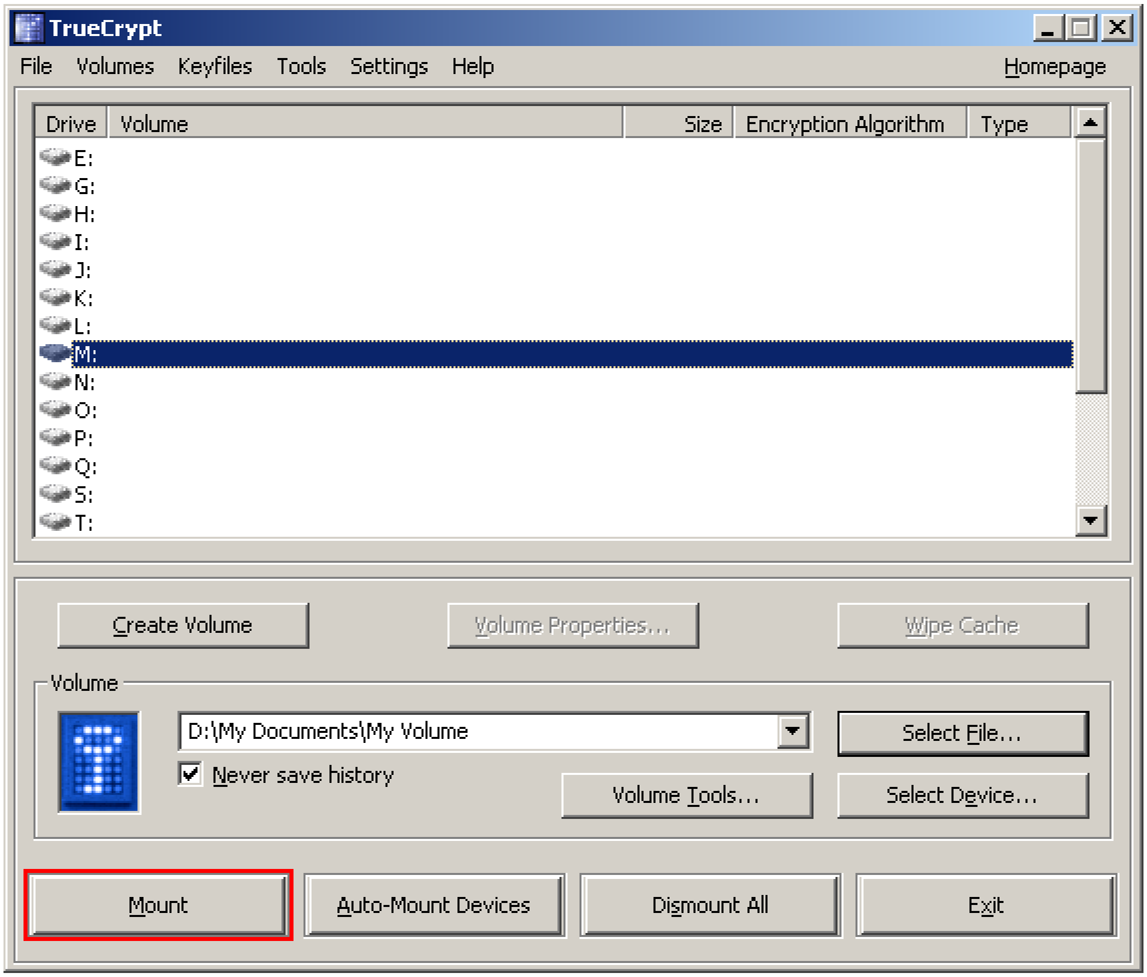
In the file selector, browse to the container file (which we created in Steps 6-11) and select it.

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

The file selector window should disappear.

In the following steps, we will return to the main TrueCrypt window.

Step 16:



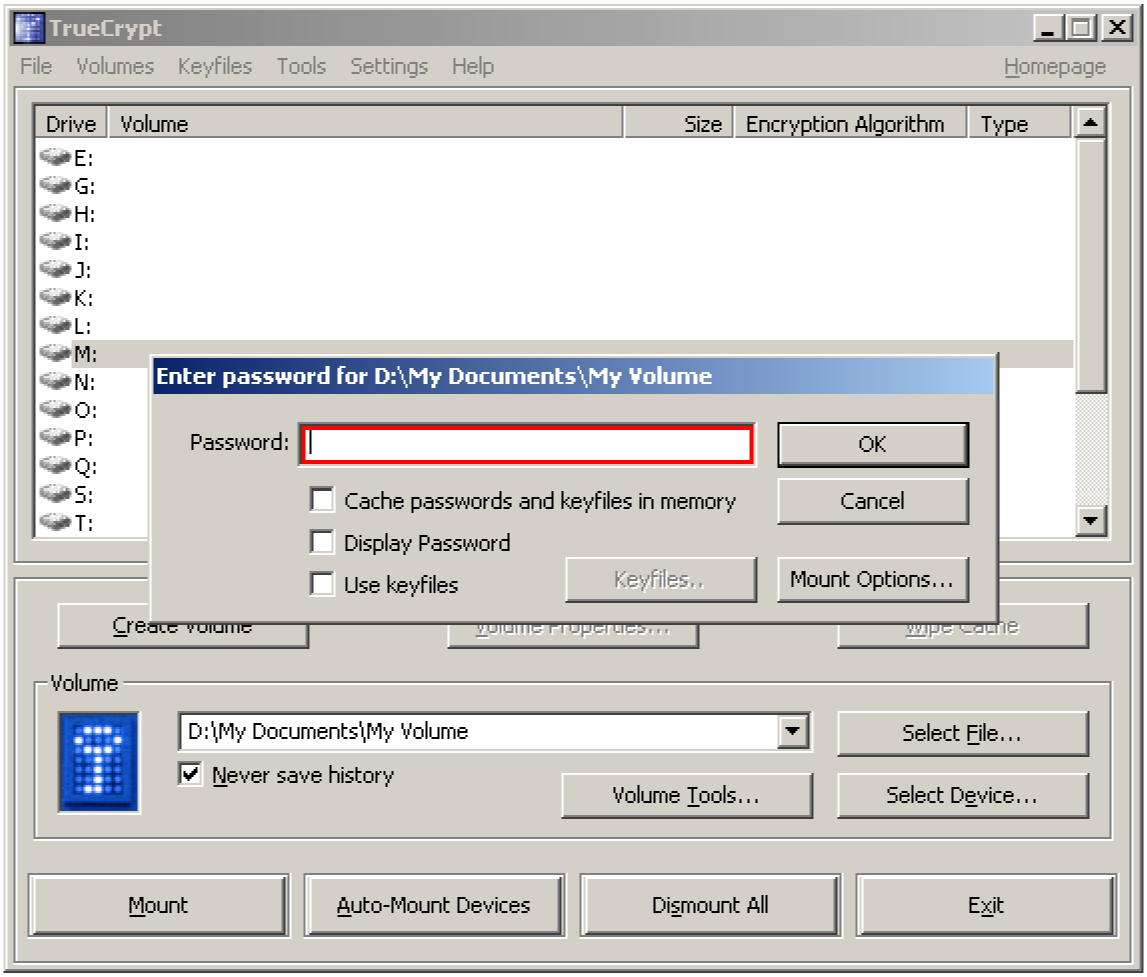
Volume: D:\My Documents\My Volume

☑ Never save history

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

Password prompt dialog window should appear.

Step 17:



Enter password for D:\My Documents\My Volume

Password: |

□ Cache passwords and keyfiles in memory

□ Display Password

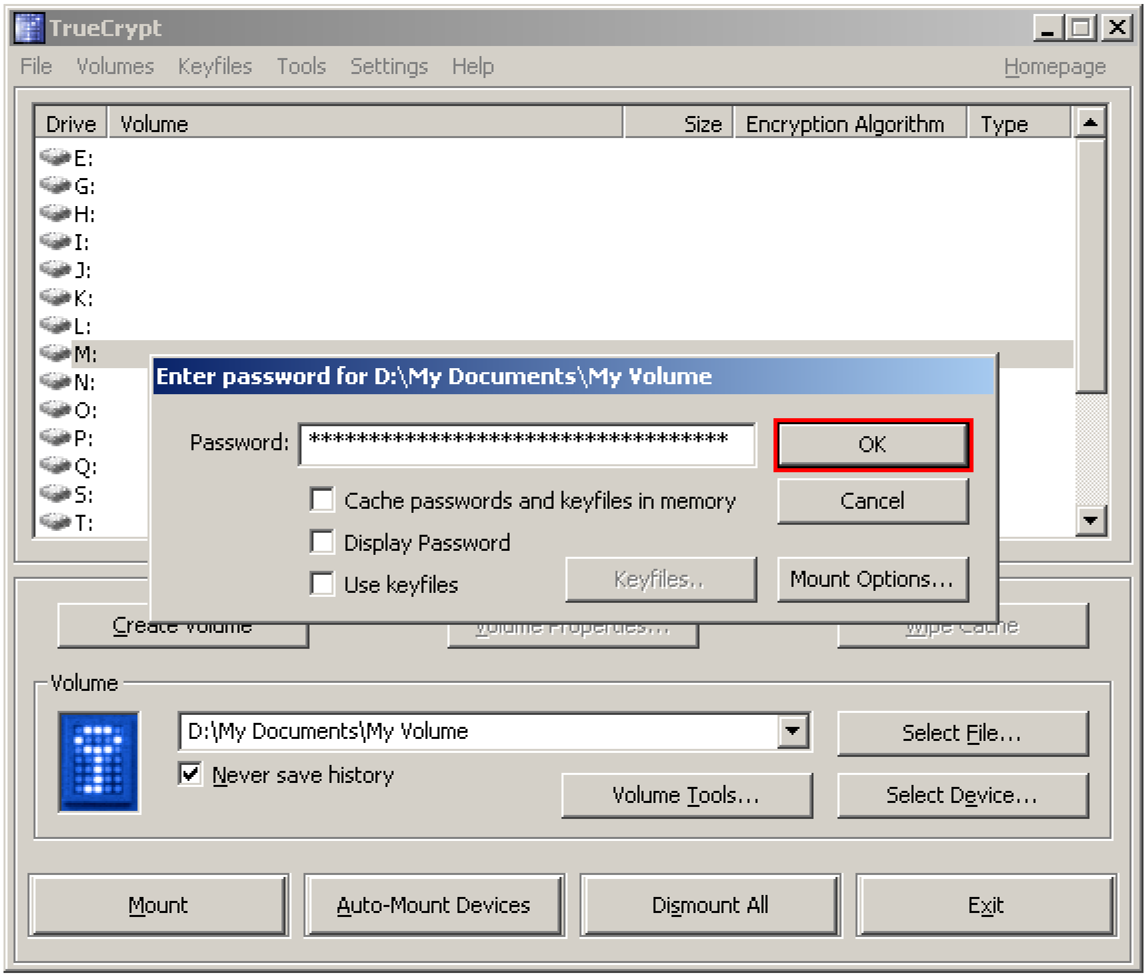
□ Use keyfiles

D:\My Documents\My Volume

☑ Never save history

Type the password (which you specified in Step 10) in the password input field (marked with a red rectangle).

Step 18:



Enter password for D:\My Documents\My Volume

Password: ************************************

☐ Cache passwords and keyfiles in memory

☐ Display Password

☐ Use keyfiles

Volume

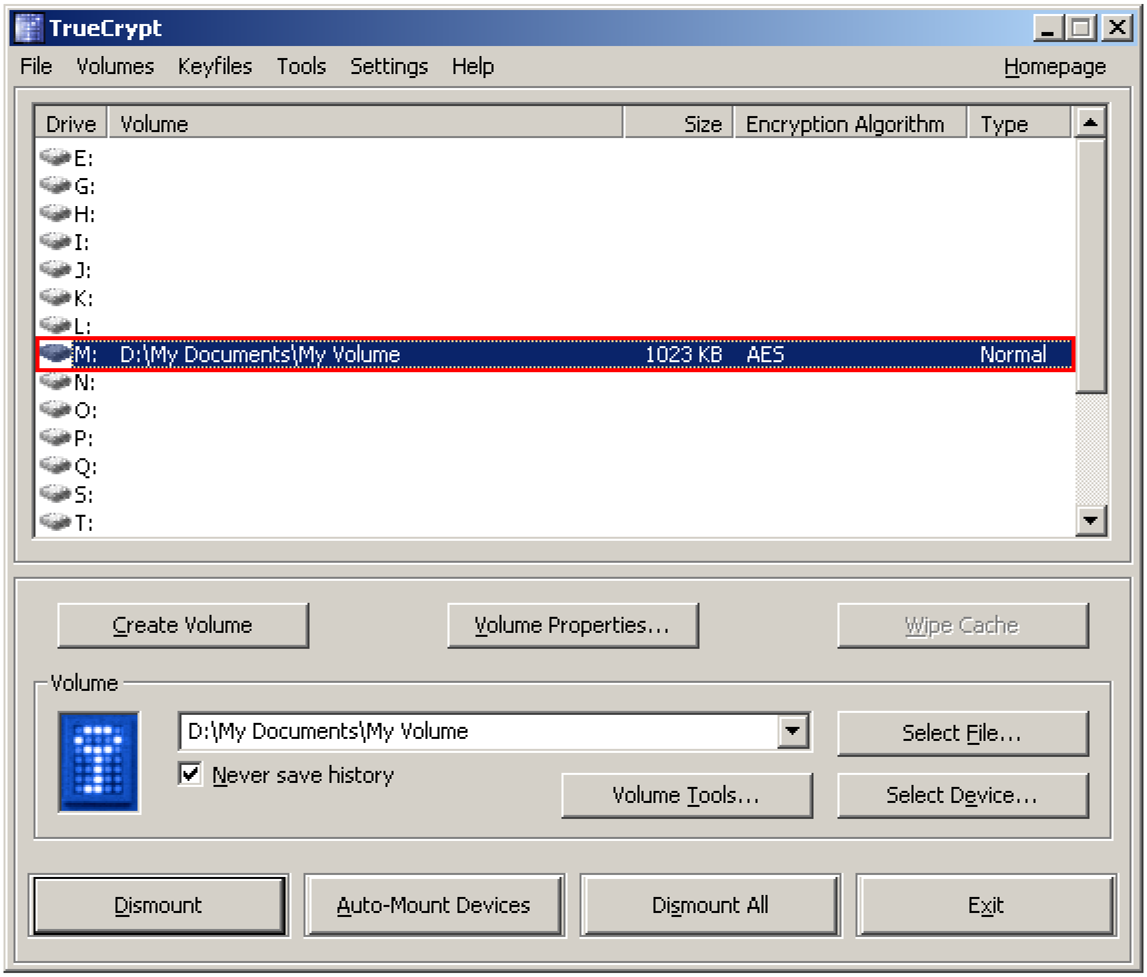
D:\My Documents\My Volume

☑ Never save history

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.

Final Step:



Drive	Volume	Size	Encryption Algorithm	Type
E:				
G:				
H:				
I:				
J:				
K:				
L:				
M:	D:\My Documents\My Volume	1023 KB	AES	Normal
N:				
O:				
P:				
Q:				
S:				
T:				

Volume

D:\My Documents\My Volume

☑ Never save history

We have just successfully mounted the container as a virtual disk M:

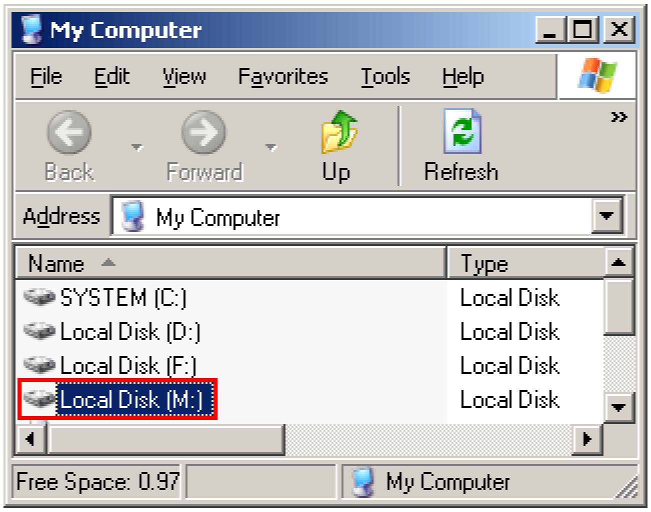
The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves like a real disk. You can save (or copy, move, etc.) files to this virtual disk and they will be encrypted on the fly as they are being written.

If you open a file stored on a TrueCrypt volume, for example, in media player, the file will be automatically decrypted to RAM (memory) on-the-fly while it is being read.

Important: Note that when you open a file stored on a TrueCrypt volume (or when you write/copy a file to/from the TrueCrypt volume) you will not be asked to enter the password again. You need to enter the correct password only when mounting the volume.

You can open the mounted volume, for example, by double-clicking the item marked with a red rectangle in the screenshot above.

You can also browse to the mounted volume the way you normally browse to any other types of volumes. For example, by opening the '*Computer*' (or '*My Computer*') list and double clicking the corresponding drive letter (in this case, it is the letter M).



Address: My Computer

Name	Type
SYSTEM (C:)	Local Disk
Local Disk (D:)	Local Disk
Local Disk (F:)	Local Disk
Local Disk (M:)	Local Disk

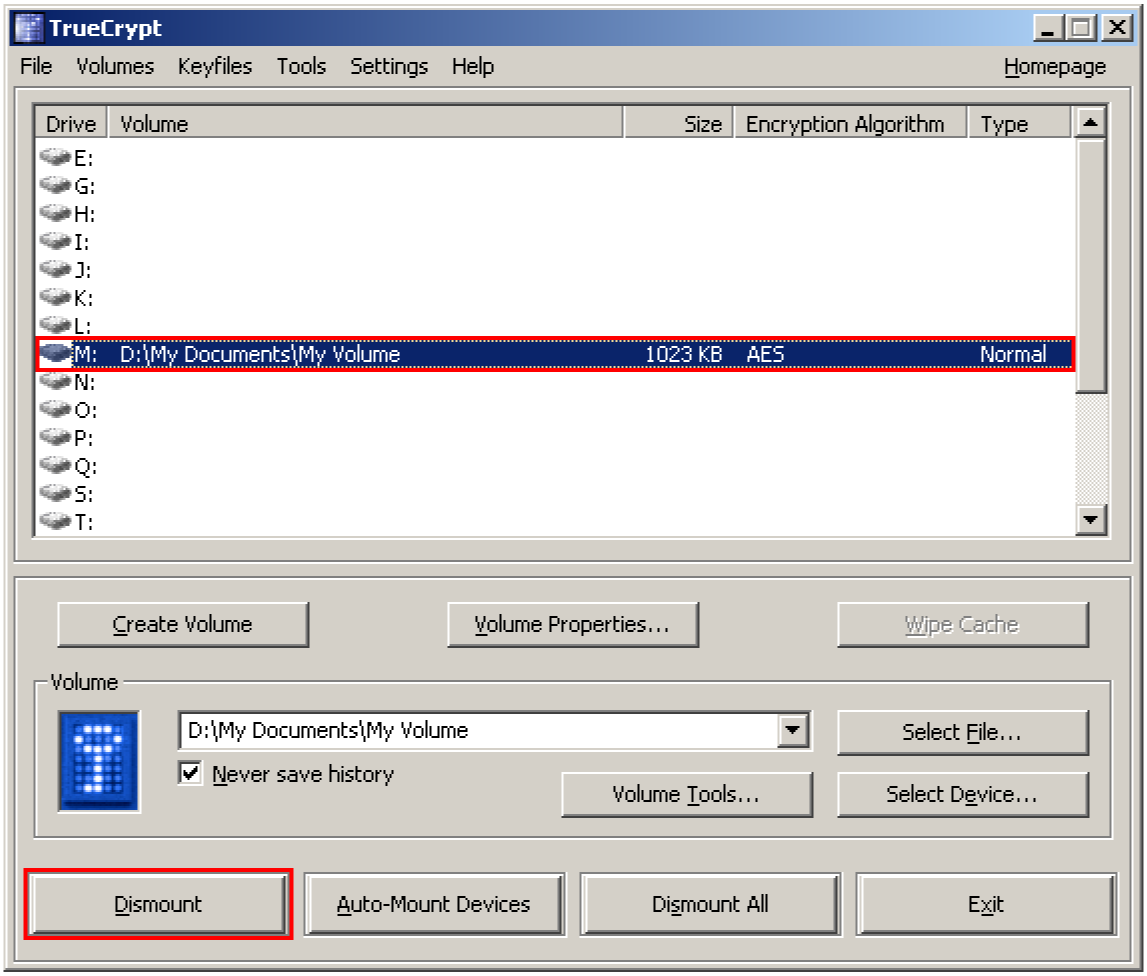
Free Space: 0.97

My Computer

You can copy files 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 memory/RAM). Similarly, files that are being written or copied to the encrypted TrueCrypt volume are automatically encrypted on the fly (right before they are written to the disk) in RAM.

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.

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:



Drive	Volume	Size	Encryption Algorithm	Type
E:				
G:				
H:				
I:				
J:				
K:				
L:				
M:	D:\My Documents\My Volume	1023 KB	AES	Normal
N:				
O:				
P:				
Q:				
S:				
T:				

Volume: D:\My Documents\My Volume

☑ Never save history

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.

How to Create and Use a TrueCrypt Partition/Device

Instead of creating file containers, you can also encrypt physical partitions or drives (i.e., create TrueCrypt device-hosted volumes). To do so, repeat the steps 1-3, but in the step 3 select the second or third option. Then follow the remaining instructions in the wizard. When you create a device-hosted TrueCrypt volume within a *non-system* partition/drive, you can mount it by clicking *Auto-Mount Devices* in the main TrueCrypt window. For information pertaining to encrypted *system* partition/drives, see the chapter System Encryption.

***Important:** We strongly recommend that you also read the other chapters of this manual, as they contain important information that has been omitted in this tutorial for simplicity.*

* Note that after you copy existing unencrypted files to a TrueCrypt volume, you should securely erase (wipe) the original unencrypted files. There are software tools that can be used for the purpose of secure erasure (many of them are free).