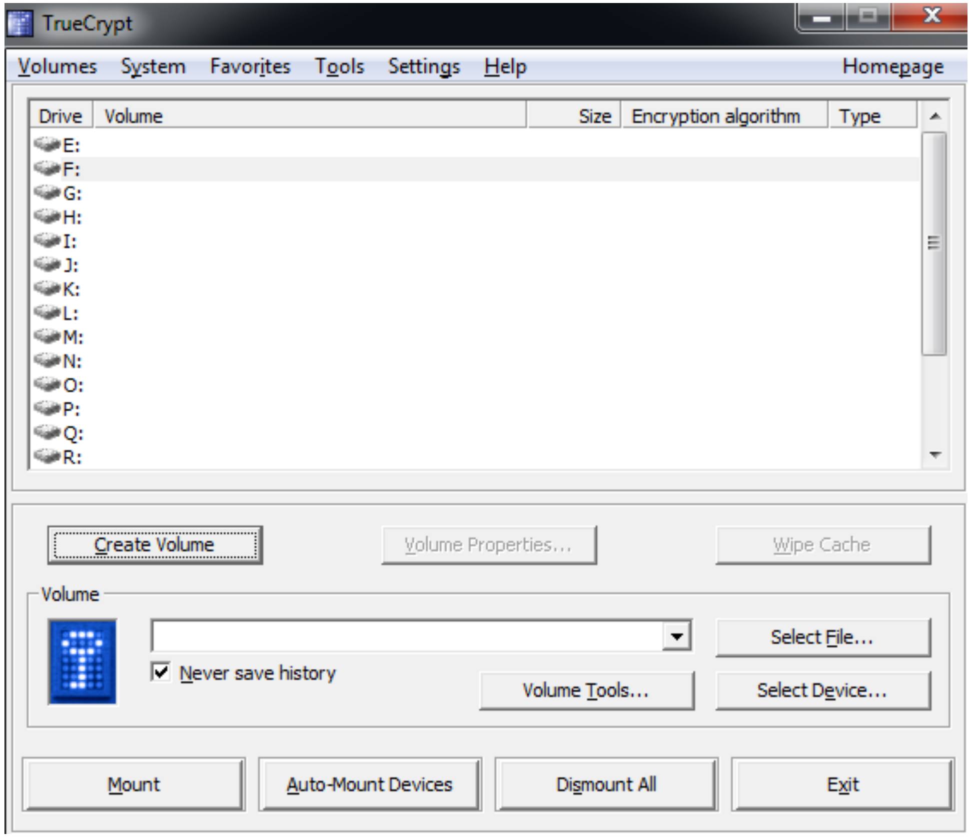
University of Hertfordshire



TrueCrypt User Guide

Cross platform desktop encryption made easy

Mr Mohamed Hansraj, OCIO
Dr Bill Worthington, OCIO

V7, August 2014

Introduction to TrueCrypt

- TrueCrypt is an opensource tool which was developed over a number of years. Development ceased in May 2014 amid much mystery and speculation and a very un-professional termination of the project by its opensource developers. ***There is nothing to suggest that version 7.1a, the last distributed full version, is any less reliable or secure than was held to be the case before the development ceased.*** It is currently the only good cross platform desktop encryption solution, and our recommendation is to carry on using it.

- TrueCrypt is an all-in-one package which can be used to encrypt all of your important data and allow you to work with encrypted files as you would with normal files.

- TrueCrypt creates an encrypted container which appears on the desktop as a mounted volume (a drive on Windows), and functions much in the way as any normal attached storage device. Files are encrypted on the fly as you drag and drop or cut and paste them in and out of the mounted volume.

- Volumes are stored in container files. Unmounted containers are just single large binary files that can be transferred between file systems, via the Internet, and by personal storage devices.

TrueCrypt User Guide

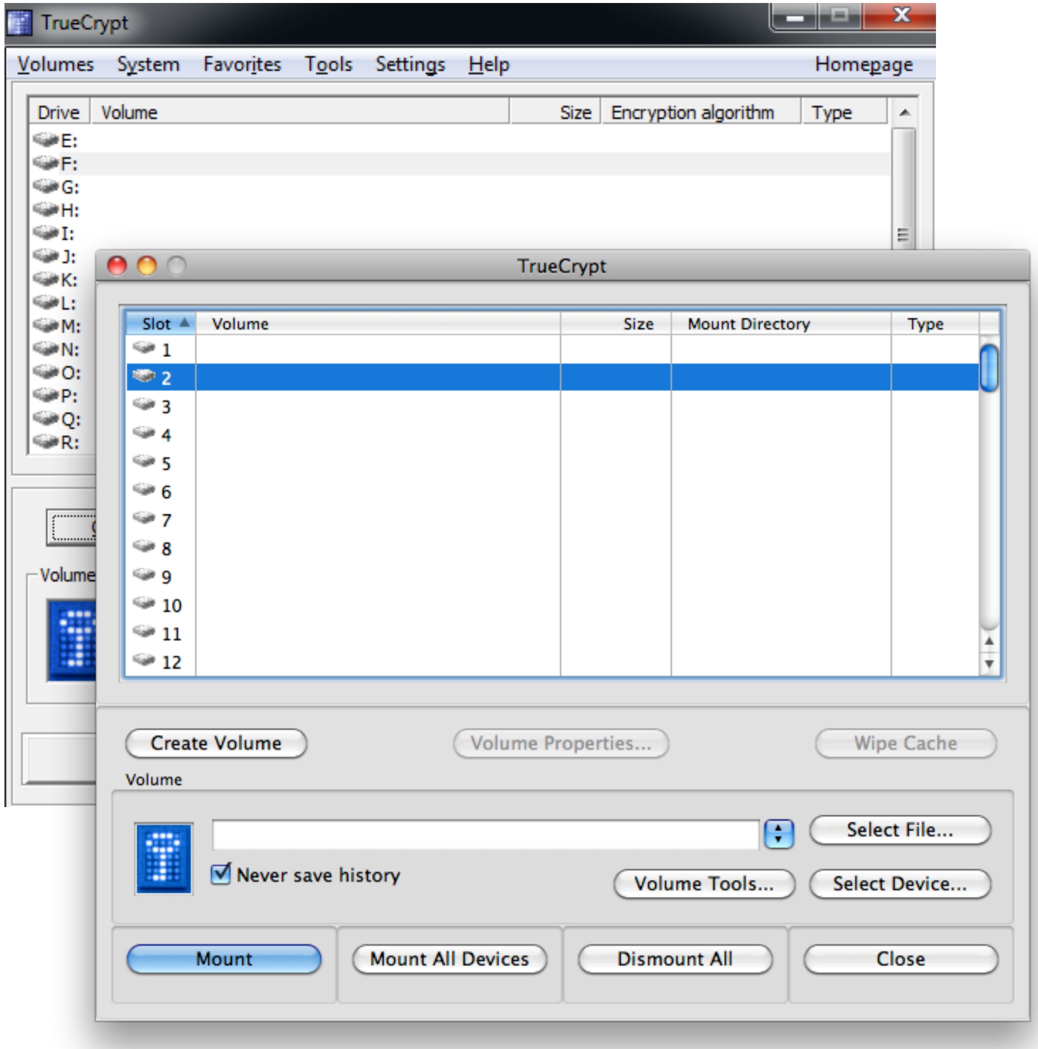
Downloading and installing TrueCrypt

- TrueCrypt can be downloaded from: https://truecrypt.ch/downloads/

- You can download a copy of TrueCrypt for Windows, Apple OSX and Linux.

- To install the package, run the installation application; accept the terms of the user agreement and the select INSTALL. Click finish once the installation is complete. You have now successfully installed TrueCrypt.

- Launch TrueCrypt by double-clicking on TrueCrypt.exe or clicking on the TrueCrypt shortcut in your Windows Start menu. On OSX and Linux open the TrueCrypt application.



TrueCrypt User Guide

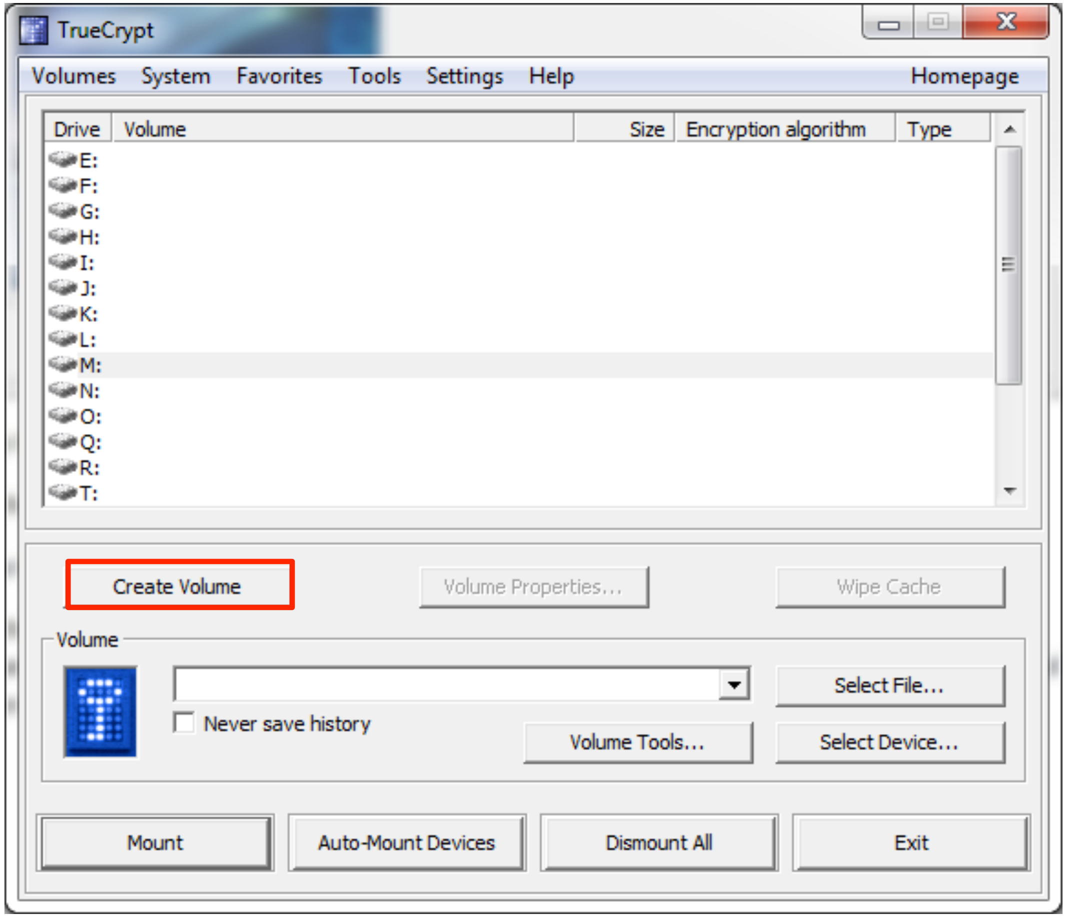
Creating a TrueCrypt volume

TrueCrypt User Guide

Start TrueCrypt and begin creating a TrueCrypt volume

- Launch TrueCrypt. The TrueCrypt application window will appear on your screen.

- Click **Create Volume** (highlighted with a red rectangle in this screenshot).

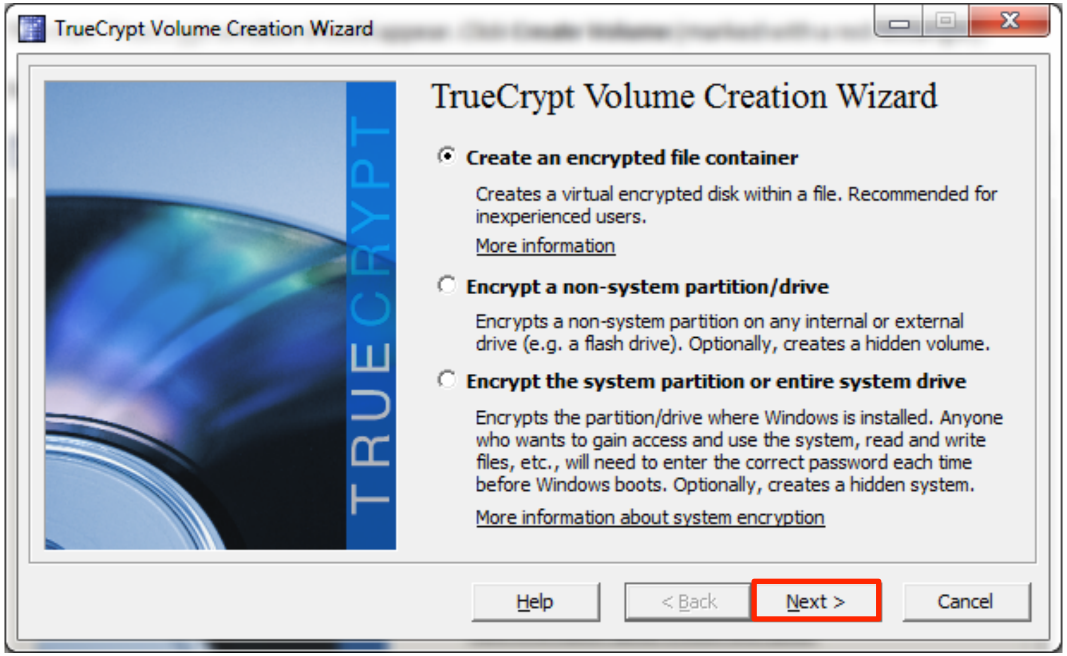


University of Hertfordshire

TrueCrypt User Guide
Volume Creation Wizard: Step 1, container type

In almost all situations you will need to '**Create an encrypted file container**'.

This is the default option, so you can click '**Next**'.



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

Other options:

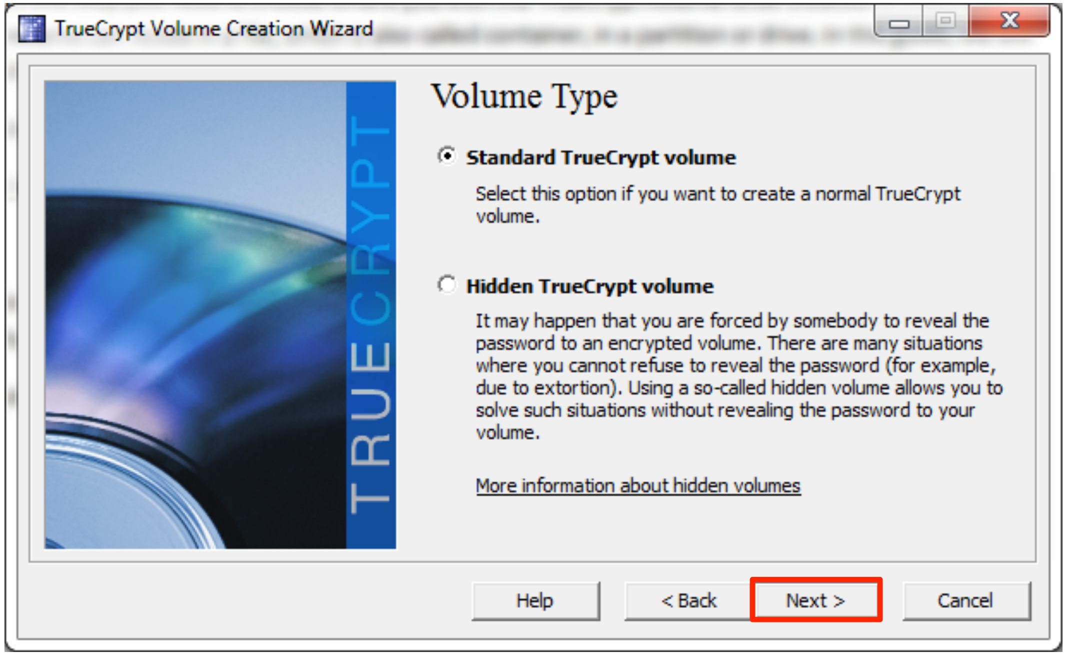
'**Encrypt a non-system partition/drive'** is generally to encrypt an entire device, like a portable hard drive or USB stick. There is no need to do this in most circumstances and the most flexible solution is to create a standalone container using the first option above.

The third option, **'Encrypt the system partition or entire system drive'** will encrypt your entire system. Only an expert user or system administrator should attempt this.

TrueCrypt User Guide
Volume Creation Wizard: step 2, volume type

In almost all situations you will need to create a '**Standard TrueCrypt volume**'.

This is the default option, so you can click '**Next**'.



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

Other options: **'Hidden TrueCrypt volume'**
Unless you have very special circumstances, you won't need to create a hidden volume.

TrueCrypt User Guide
Volume Creation Wizard: step 3, name the container file

Click ‘**Select File’** and use your standard system file selector to select the location for your file and type in its name.

In this example, we will create a container file called ‘*secure-volume.tc*’ on the Desktop.

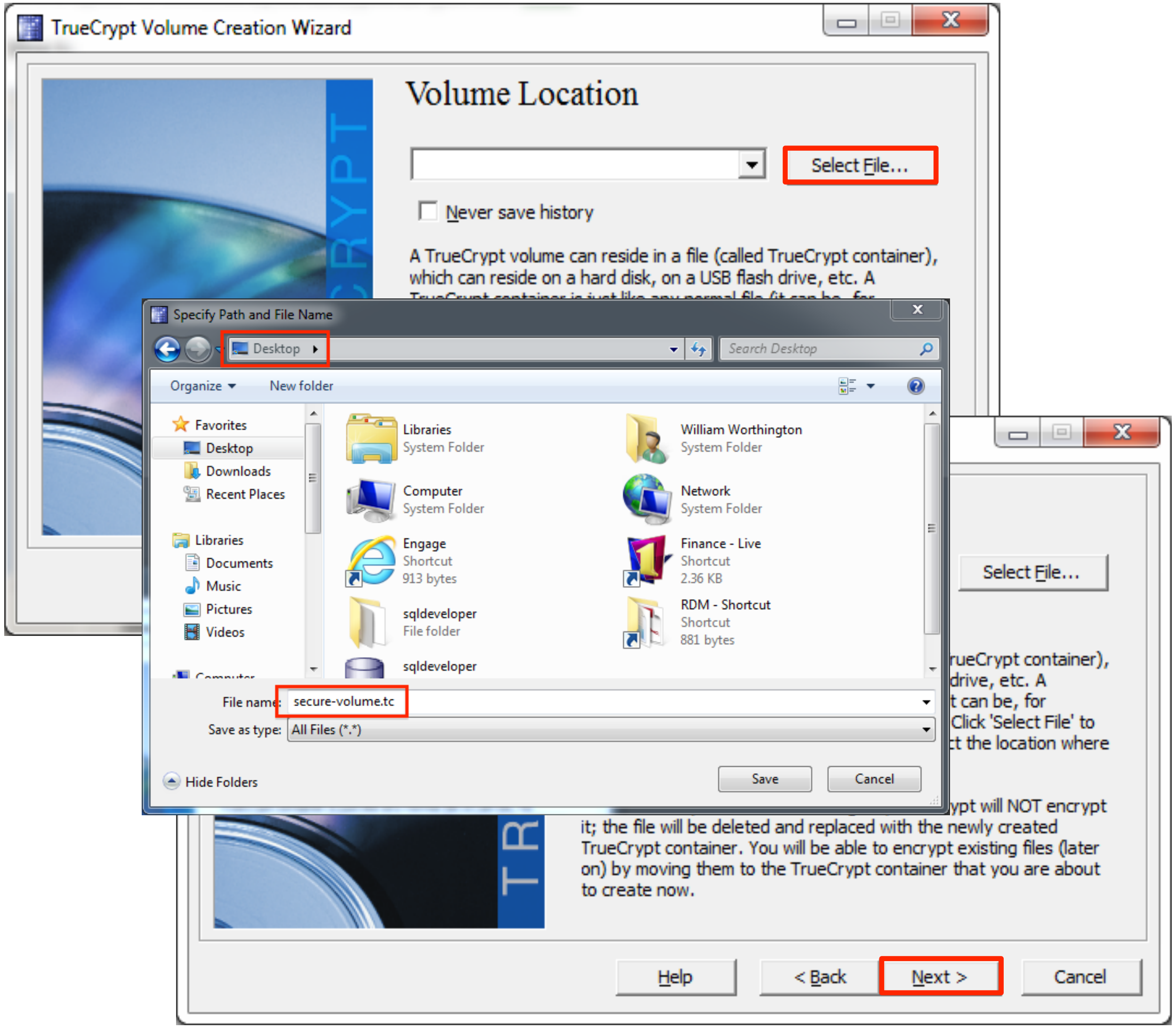
After selecting the path and naming the file click ‘**Next**’

Important:

unfortunately TrueCrypt does not fill in the default file extension for you, so you need to explicitly type **.tc** on the end of your filename.

Take care:

if you select an existing file TrueCrypt will overwrite it without asking you and its contents will be lost.



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

rueCrypt container), drive, etc. A t can be, for Click 'Select File' to t the location where

ypt will NOT encrypt it; the file will 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.

File name: secure-volume.tc

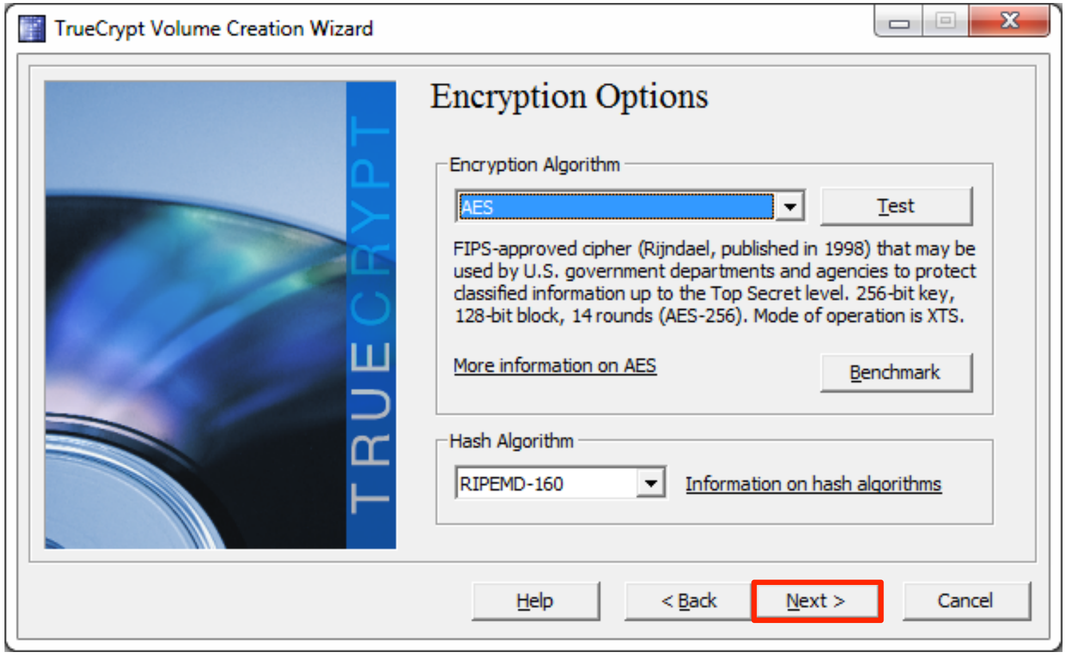
Save as type: All Files (*.*)

University of Hertfordshire UH

TrueCrypt User Guide
Volume Creation Wizard: step 4, encryption method

In almost all situations you can use the AES encryption algorithm.

This is the default option, so you can click ‘**Next**’.



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

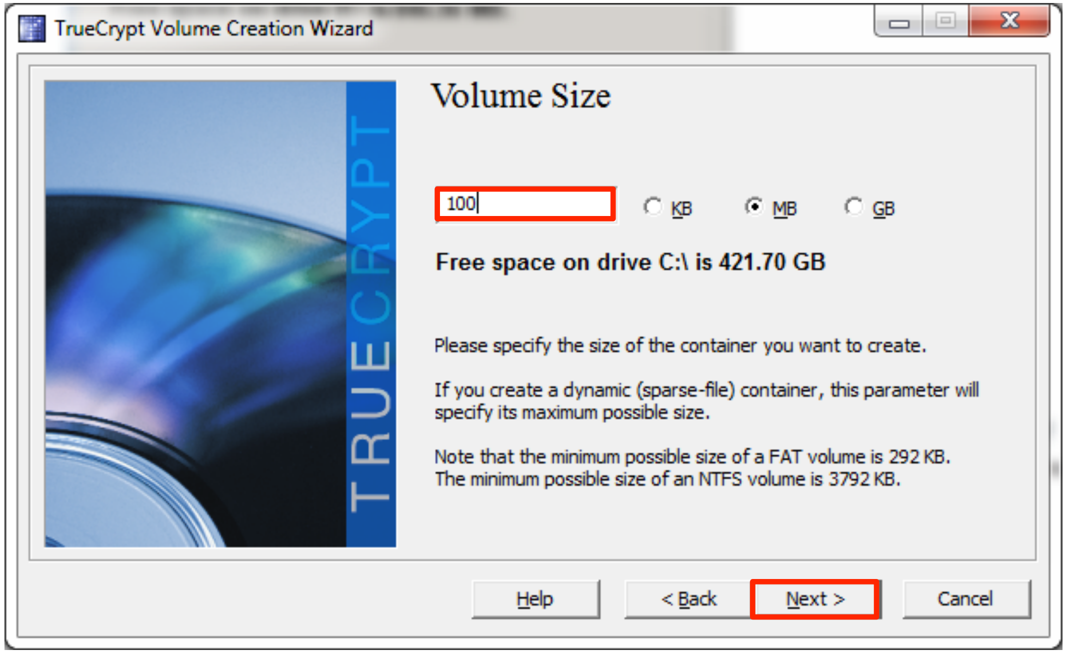
Other options:
The other algorithms available are arguably more secure as they are more complicated but can take significantly longer to create a large container and also impact on the time to encrypt and decrypt files in an open volume, (which with AES is usually so fast as to be not noticeable).

To test the various methods, click ‘**Benchmark**’ – this will open a new window and will display the performance for other algorithms your system.

TrueCrypt User Guide
Volume Creation Wizard: step 5, volume size

Next we specify the size of our TrueCrypt volume. This allocates the space available inside the container for files.

Enter a number of kilobytes (KB), megabytes (MB), or gigabytes (GB), then click ‘**Next**’.



TrueCrypt Volume Creation Wizard

Volume Size

100 ○ KB ● MB ○ GB

Free space on drive C:\ is 421.70 GB

Please specify the size of the container you want to create.

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

Note that the minimum possible size of a FAT volume is 292 KB. The minimum possible size of an NTFS volume is 3792 KB.

Size options:

Choose a size commensurate with space you think you are likely to need and no larger.

The larger the volume - the longer it will take to create and to transfer which may be important if you need to share a container.

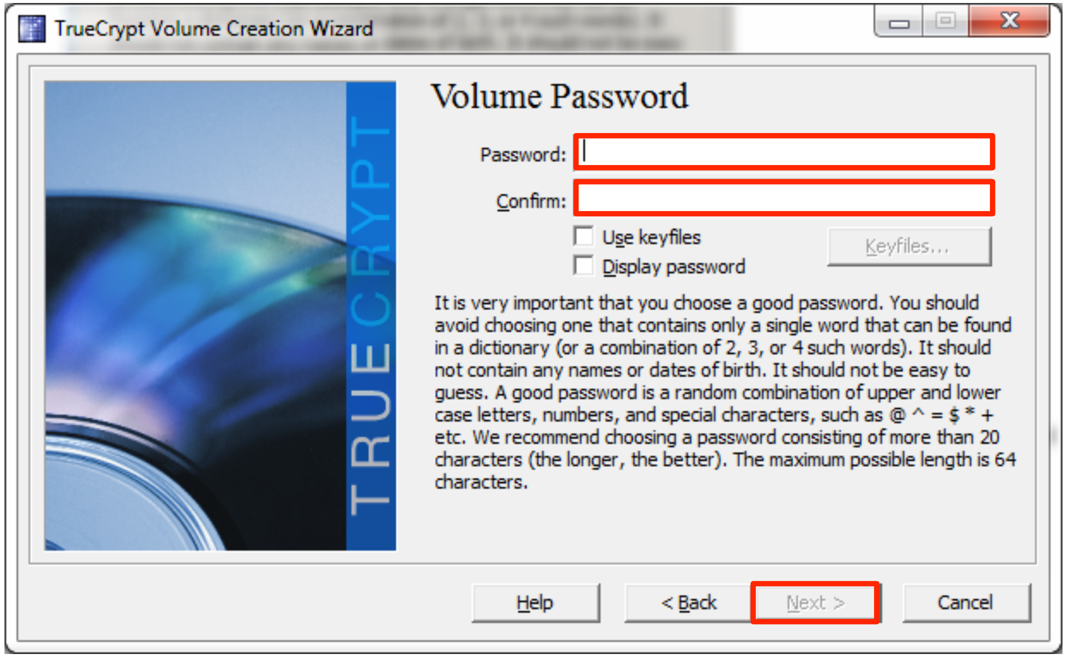
University of Hertfordshire

TrueCrypt User Guide

Volume Creation Wizard: step 6, set the password

Choose a good password - whatever encryption you use, security can be compromised by a weak password.

IMPORTANT: Do not forget or lose your password as it will be impossible to open the container and gain access to your files.



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 possible length is 64 characters.

Good password options :

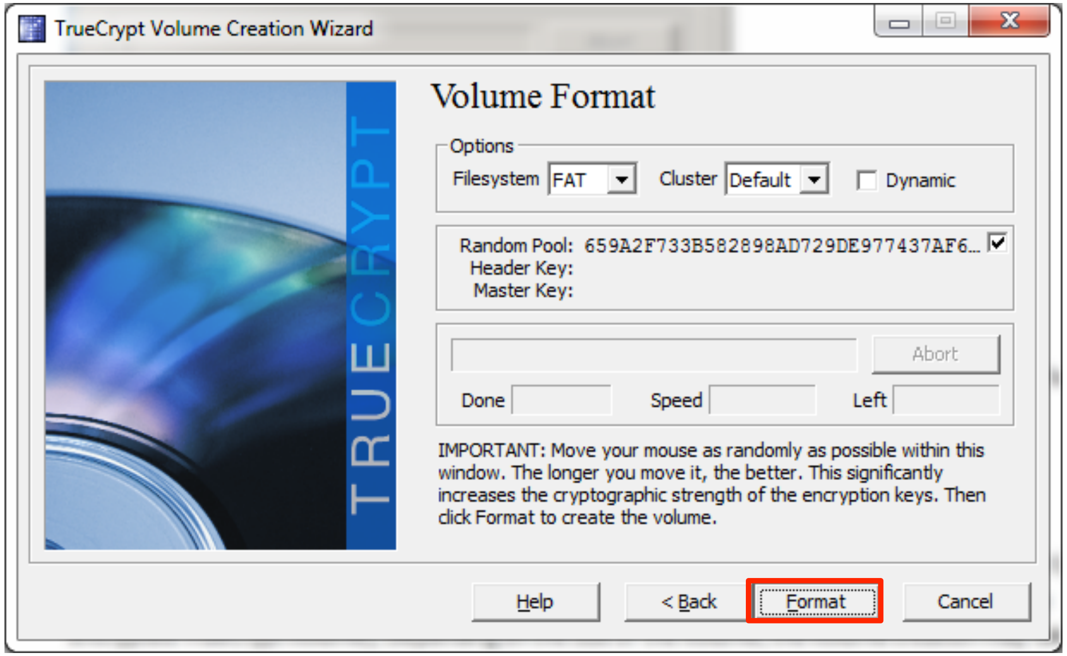
- Avoiding choosing words that can be found in a dictionary
- Avoid dates or names
- Avoid guessable personal details
- Use a mix of upper and lower case letters and special characters (such as £ $ % ^ & # etc.)
- A good length is more than 20 characters (the longer the better)
- The limit is 64 characters

The wizard may complain about your password if it does not think your choice is good enough – but you can override this objection

TrueCrypt User Guide
Volume Creation Wizard: step 7, format the volume

In almost all situations you should use ‘**FAT**’ for the file system, this works on all platforms.

This is the default option, so you can click ‘**Format**’ - but first, move your mouse around randomly within the Volume Creation Wizard window. This randomises the encryption key.



Filesystem FAT   Cluster Default   ☐ Dynamic

Random Pool: 659A2F733B582898AD729DE977437AF6... ☑
Header Key:
Master Key:

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.

Other options :

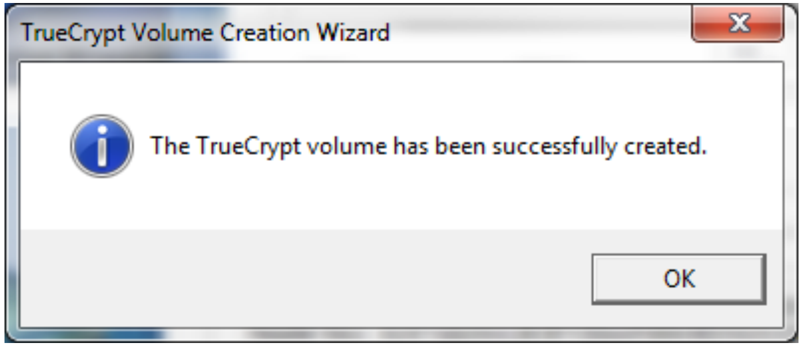
NTFS is a special file system for Windows only and requires admin rights to mount.

Randomising the encryption key is important. The longer you move the mouse the better as this increases the cryptographic strength of the encryption keys (which increase security). If you and everyone else just selected the first key by clicking ‘format’ right away, then the effectiveness of the encryption of your volume would be compromised.

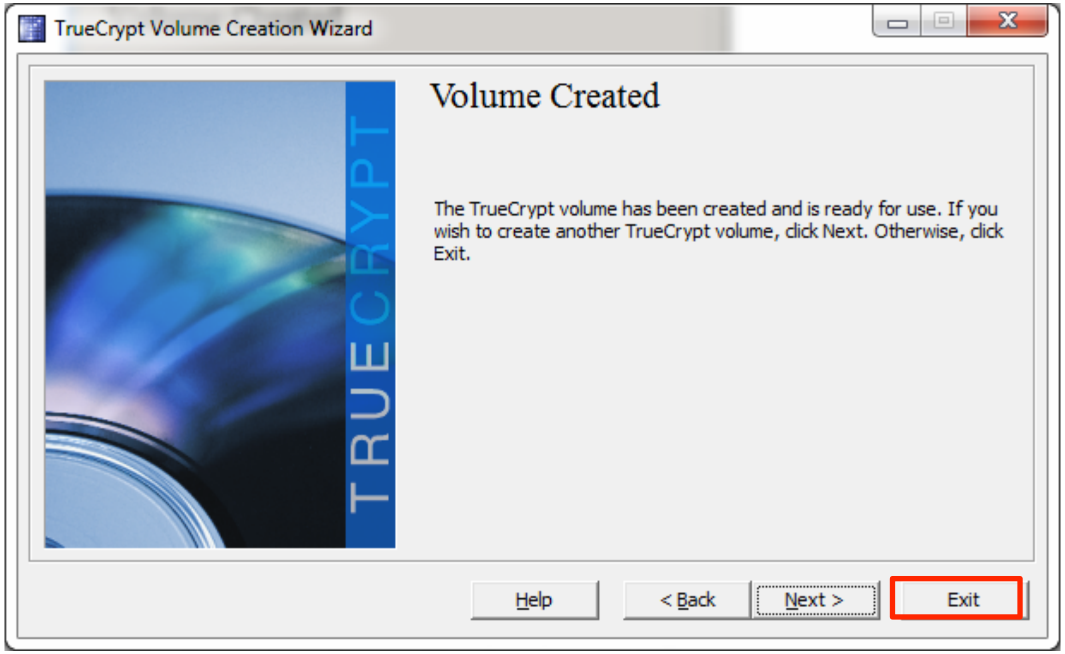
TrueCrypt User Guide
Volume Creation Wizard: step 8, volume created

When you click '**Format**' TrueCrypt will begin encrypting the volume container file. The time this takes depends on the size of the volume you specified. A 'successful' dialog box will appear when it finishes. Click OK to close the dialog box.

Click '**Exit**' to close the Volume Creation Wizard or '**Next**' to create another volume container


TrueCrypt Volume Creation Wizard

The TrueCrypt volume has been successfully created.


TrueCrypt Volume Creation Wizard

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.

University of Hertfordshire

TrueCrypt User Guide

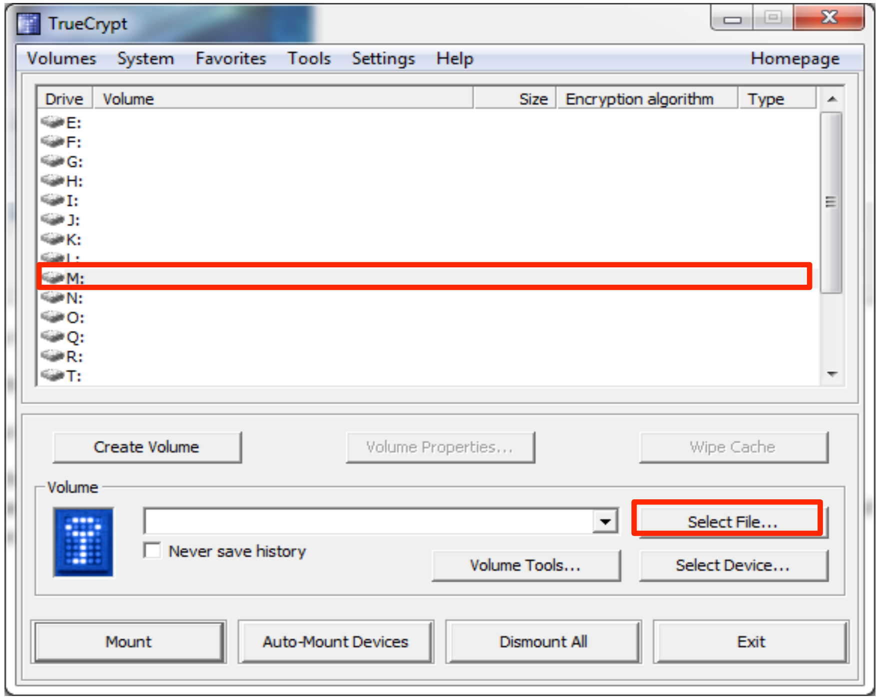
Using your encrypted, password protected container

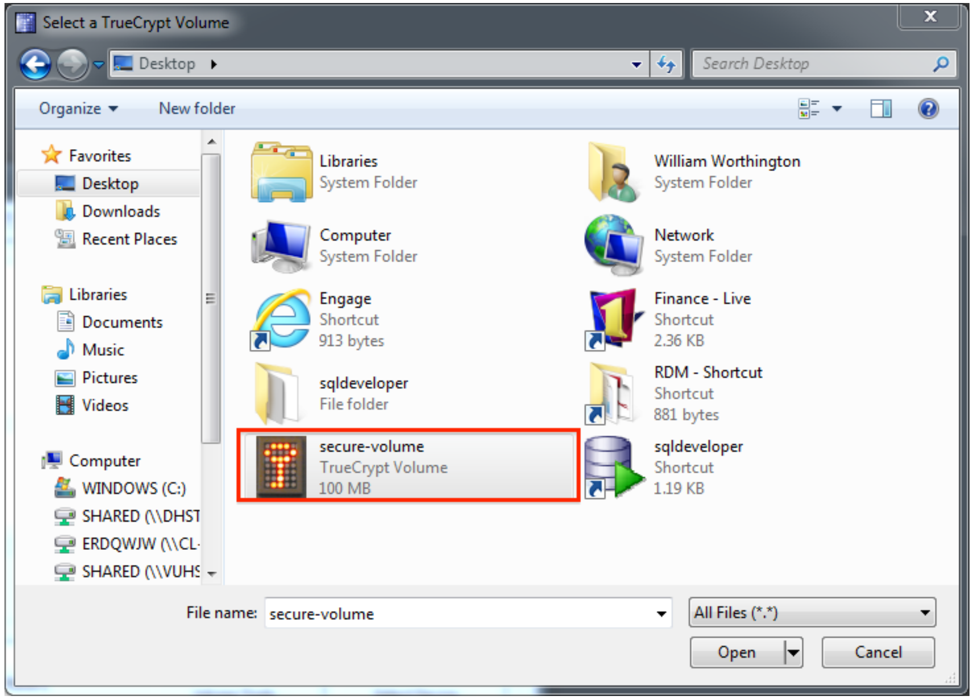
TrueCrypt User Guide

Using your container: step 1, select a mount point and file

Start the TrueCrypt application and make sure the application window is in view.

Click on a **drive letter** to select a volume mount point (OSX and Linux users will select a number). Then click ‘**Select**’ to use your standard system file selector to pick a TrueCrypt container file.





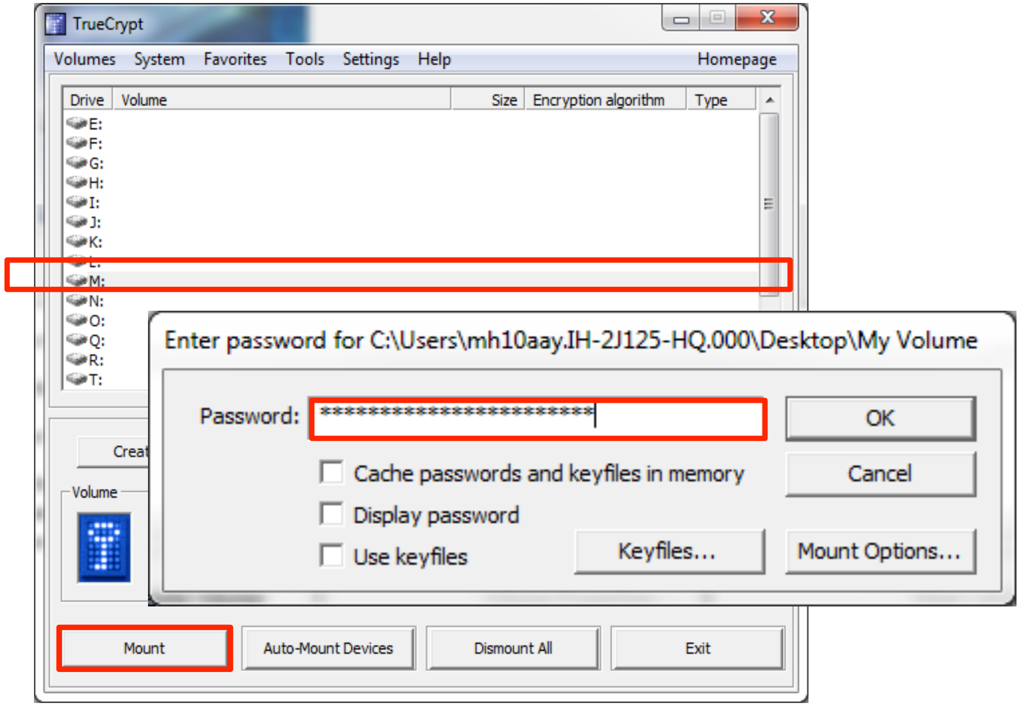
File name: secure-volume

TrueCrypt User Guide

Using your container: step 2, mount and enter password

With a container file and mount point selected, click ‘**Mount**’ and enter your password.
Ignore all the settings on the password dialog.

Note in this example we have selected drive **M:**



Enter password for C:\Users\mh10aay.IH-2J125-HQ.000\Desktop\My Volume

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

□ Cache passwords and keyfiles in memory

□ Display password

□ Use keyfiles

Short cut:

On most systems you should be able simply **double click a TrueCrypt container file (.tc),** whereupon the application will start, select the file, and pick the next available mount point - you just need to click ‘**mount**’.

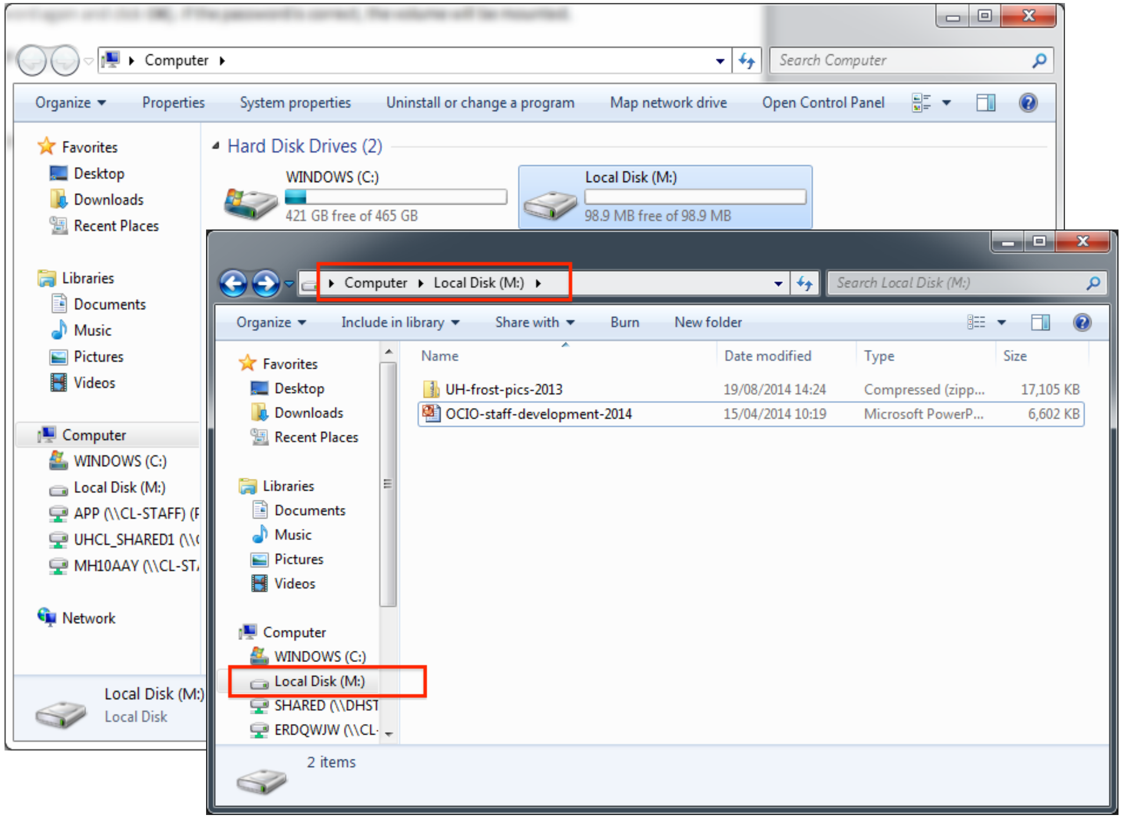
(on OSX and Linux you may need to associate the extension .tc with the TrueCrypt application after installation).

TrueCrypt User Guide

Using your container: step 3, work with the mounted drive

Your secure volume is available to use just like any other storage attached to your computer (in this example as **M:**) Data is encrypted and decrypted without you noticing as you move files in and out.

You can use your preferred way of working to drag and drop, or cut and paste, right click, and save in the volume.



Name	Date modified	Type	Size
UH-frost-pics-2013	19/08/2014 14:24	Compressed (zipp...	17,105 KB
OCIO-staff-development-2014	15/04/2014 10:19	Microsoft PowerP...	6,602 KB

Options:

You can minimise or even close the TrueCrypt application window while you work.

Short cut:

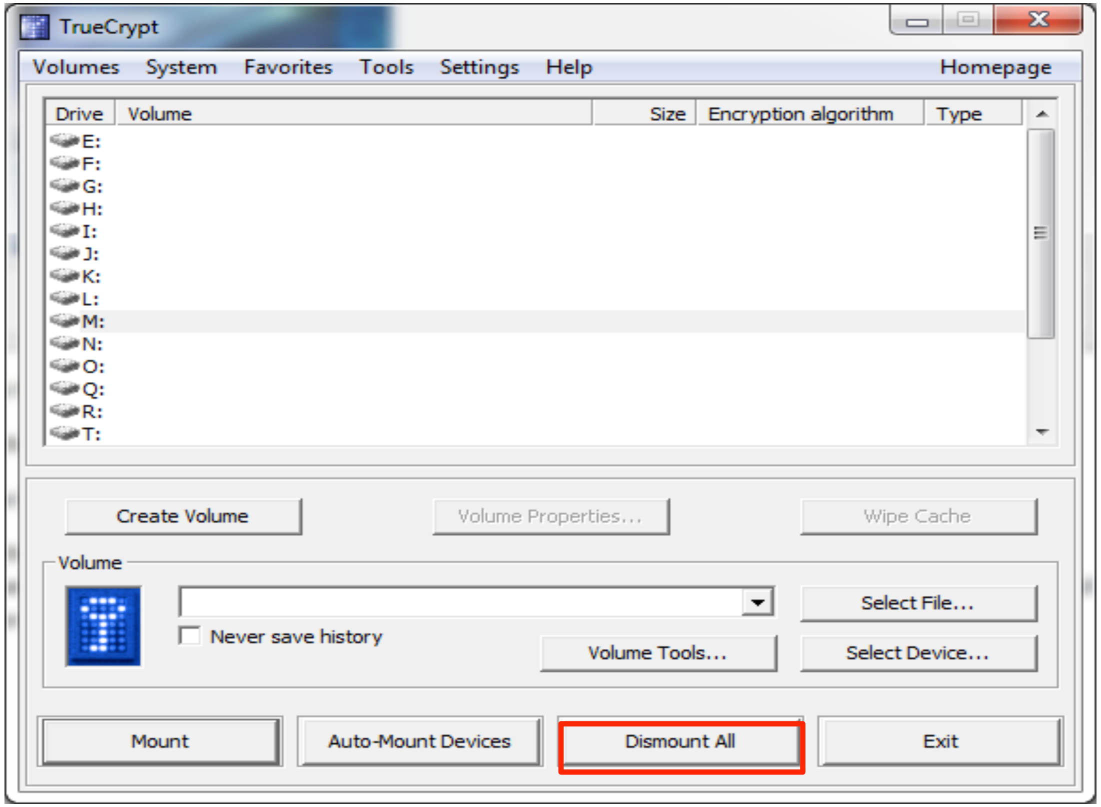
On Windows – press the Windows/Microsoft Key + E to open ‘My computer’ to see your drives.

On OSX – press Apple/Cmd - shift- F to open a new Finder window to see your volumes.

TrueCrypt User Guide

Using your container: step 4, dismount your drive/volume

When you have finished working, return to the TrueCrypt application window and click '**Dismount All**'. All TrueCrypt drives/volumes will be closed and saved.



Options:

If you only want to dismount one drive, select its drive letter and click 'Dismount'

If you shut down or restart or log off TrueCrypt will deal with this gracefully and dismount all drives/ volumes (unless you have left any files open, in which case it will pause the operation in the usual way).

TrueCrypt User Guide

Using your container: backup and tips

You should keep a backup of your TrueCrypt container files just as you would with any other data, because –

- container files are only as good the hardware they are stored on – one damaged byte and everything inside will be lost
- (this is another good reason for making them as only as large as necessary)

Never keep the only copy of something in a TrueCrypt container, because –

- you may lose or forget the password – there is no way around the encryption, everything inside will be lost

If you send your TrueCrypt container files to someone make sure you send the password by a *separate* secure route – encryption is only as good as your password security

Avoid blocking up mail systems by sending container files using https://www.exchangefile.herts.ac.uk

TrueCrypt User Guide

Appendix: Traveler Disks (Windows Only)

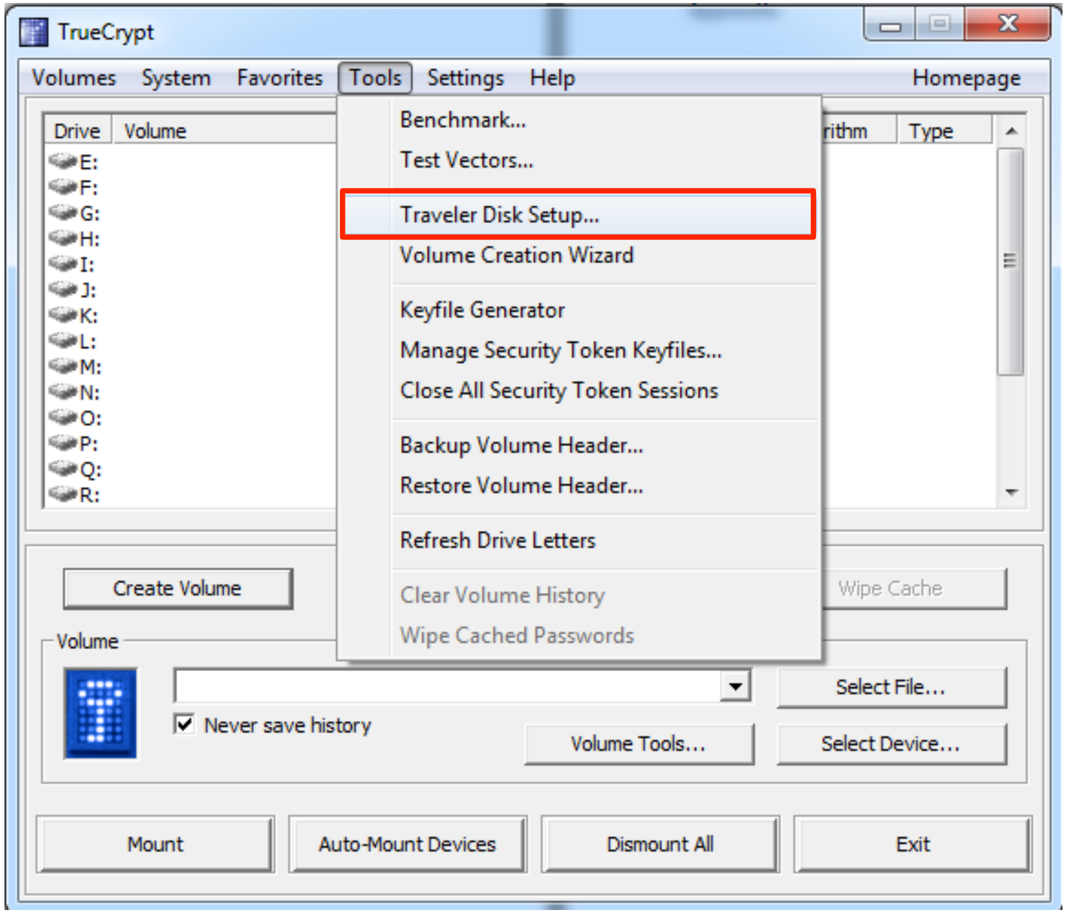
we are sorry – we know it is spelt incorrectly, but we will stick with what is on the application interface ☹

TrueCrypt User Guide

Traveler Disks: step 1, start the setup

Although getting and installing TrueCrypt is easy, there may be times when you (or a collaborator) need to open a container on a machine where TrueCrypt is not installed. On Windows systems you can create a Traveler Disk to achieve this.

With the TrueCrypt application window in view, select ‘**Tools > Traveler Disk Setup**’



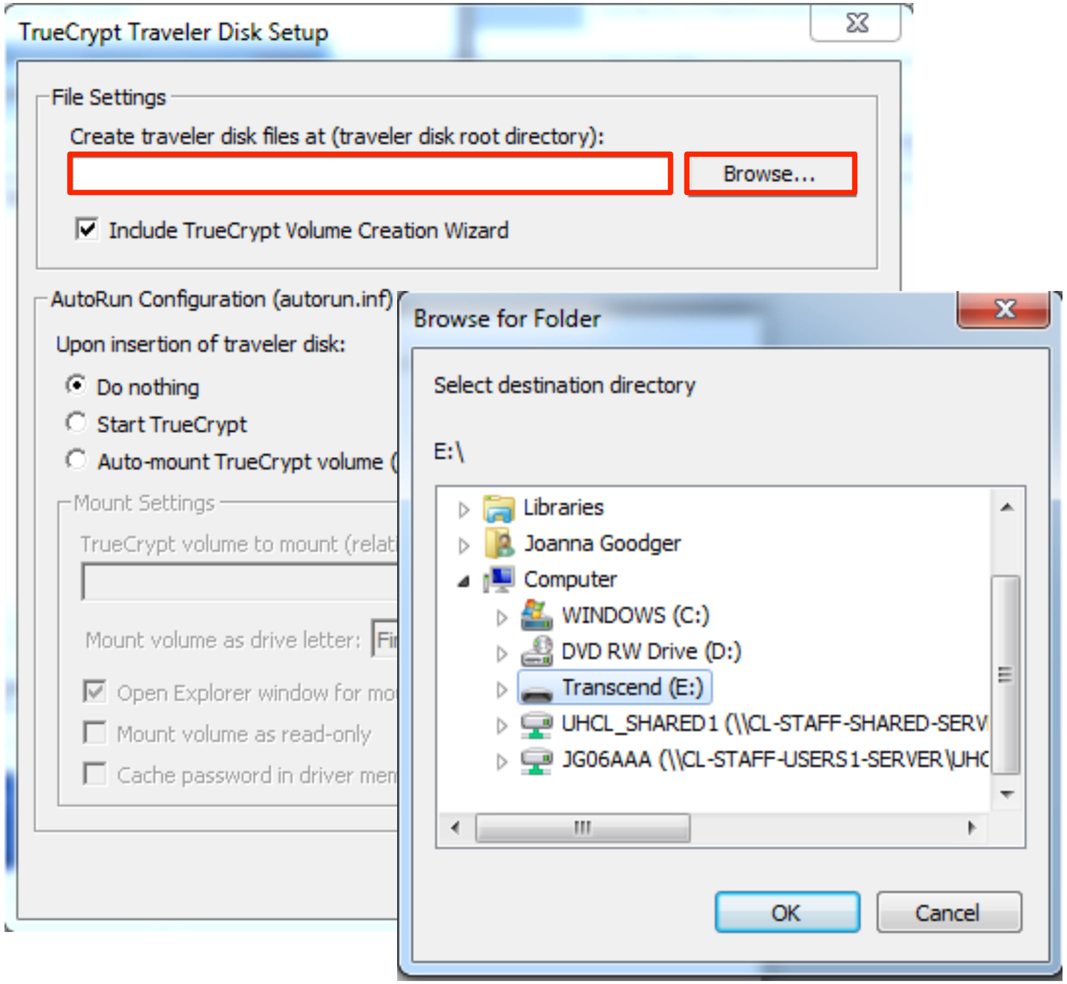
Options:

Traveler disks do not work on OSX or Linux so you will need to get and install the application to use TrueCrypt

TrueCrypt User Guide

Traveler Disks: step 2, select target portable media

Browse and select the destination directory for your Traveler disk. This might be a USB data stick or a portable hard drive.



TrueCrypt Traveler Disk Setup

File Settings

Create traveler disk files at (traveler disk root directory):

Browse...

☑ Include TrueCrypt Volume Creation Wizard

AutoRun Configuration (autorun.inf)

Upon insertion of traveler disk:

● Do nothing

○ Start TrueCrypt

○ Auto-mount TrueCrypt volume (

Mount Settings

TrueCrypt volume to mount (relat

Mount volume as drive letter: Fi

☑ Open Explorer window for mo

□ Mount volume as read-only

□ Cache password in driver men

Browse for Folder

Select destination directory

E:\

Options:

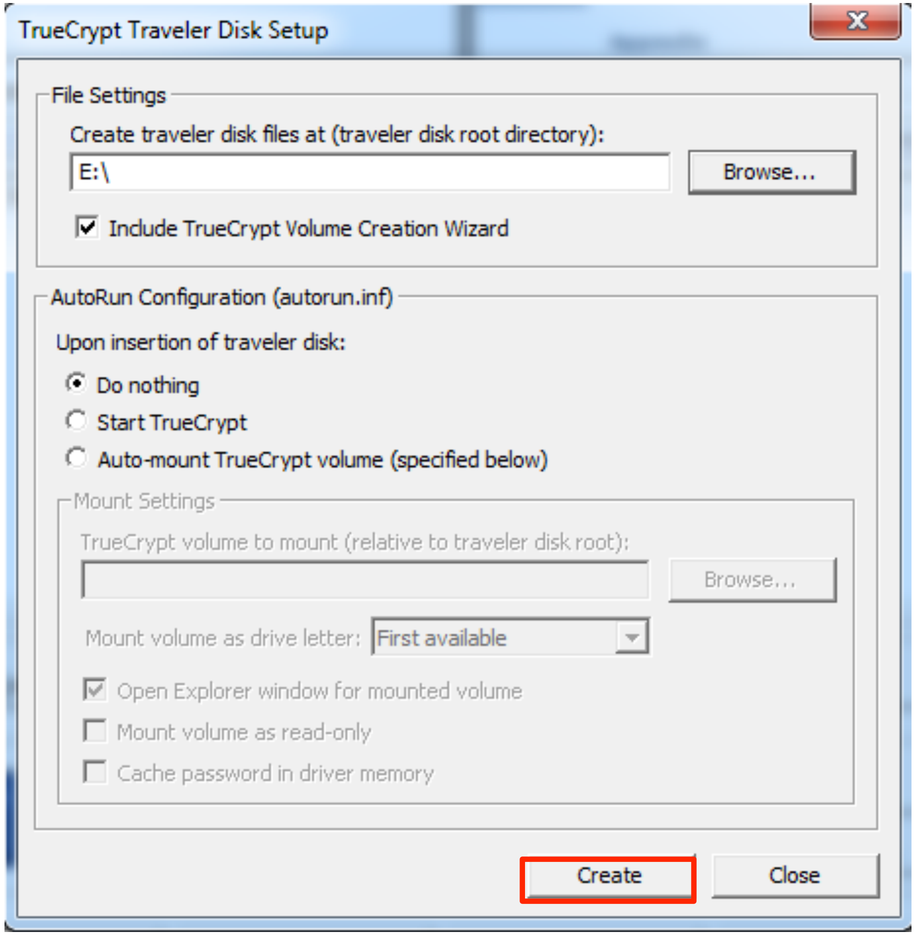
The destination directory may even be a folder which you can add a container file to and then zip up and transfer electronically

TrueCrypt User Guide

Traveler Disks: step 3, create the Traveler disk

Often you will use general purpose portable media which contains other things in addition to TrueCrypt, so you will not want it to start automatically.

Autorun ‘**Do Nothing**’ is the default option, so you can click ‘**Create**’.



TrueCrypt Traveler Disk Setup

File Settings

Create traveler disk files at (traveler disk root directory): E:\

☑ Include TrueCrypt Volume Creation Wizard

AutoRun Configuration (autorun.inf)

Upon insertion of traveler disk:

● Do nothing

○ Start TrueCrypt

○ Auto-mount TrueCrypt volume (specified below)

Mount Settings

TrueCrypt volume to mount (relative to traveler disk root):

Mount volume as drive letter: First available

☑ Open Explorer window for mounted volume

☐ Mount volume as read-only

☐ Cache password in driver memory

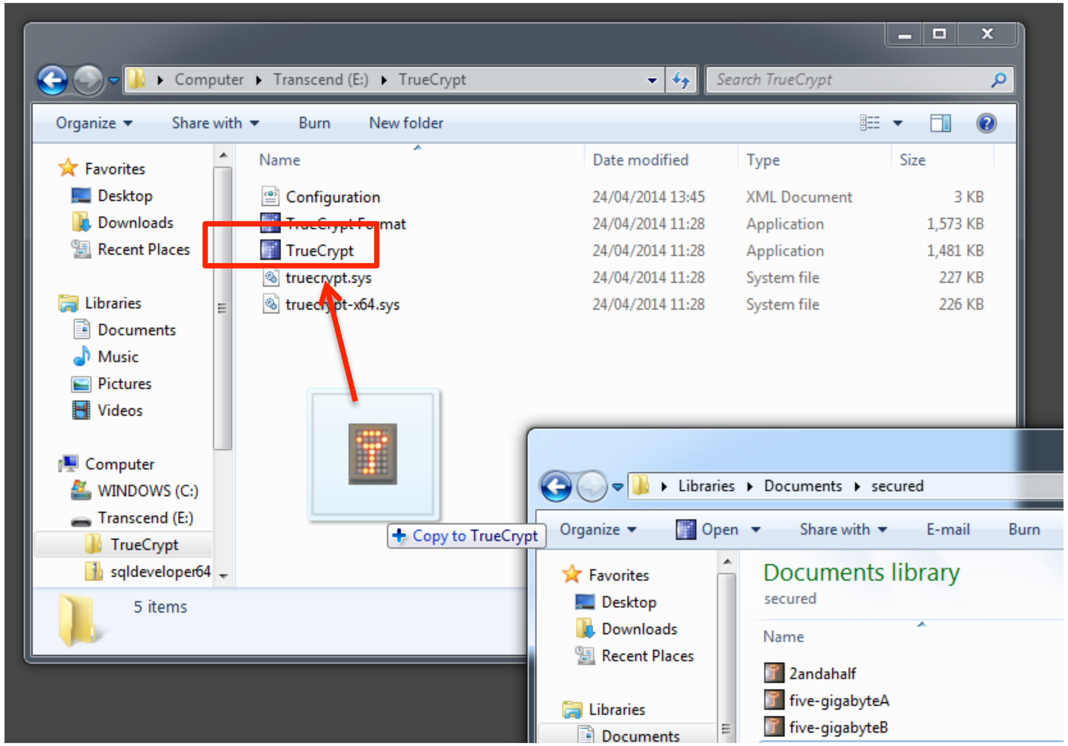
Options:

In some circumstances, you might want TrueCrypt to start and mount a container Automatically. You can do this using the Autorun settings. If you do this *never* tick ‘cache password in driver memory’ – this is a security risk.

TrueCrypt User Guide
Traveler Disks: using you Traveler Disk

The Traveler Disk shows up on portable media as a folder called ‘TrueCrypt’. This contains four or five files including two executables.

To open a TrueCrypt container drag and drop it onto the TrueCrypt(.exe) application.



Name	Date modified	Type	Size
Configuration	24/04/2014 13:45	XML Document	3 KB
TrueCrypt Format	24/04/2014 11:28	Application	1,573 KB
TrueCrypt	24/04/2014 11:28	Application	1,481 KB
truecrypt.sys	24/04/2014 11:28	System file	227 KB
truecrypt-x64.sys	24/04/2014 11:28	System file	226 KB

Options:

Most of the time you probably want to transport a container file with the Traveler Disk, so don’t forget to copy it to the portable media. It is okay to put it in the TrueCrypt folder.

Options:

The TrueCrypt Format application is also included by default, so unless you unticked this option earlier, you can also use your Traveller Disk to create containers.

Support

TrueCrypt is easy to use, but if in doubt contact helpdesk@herts.ac.uk x4678