Preparing an Encrypted USB Flash drive for use with TrueCrypt

If in any doubt about any part of this process, seek advice from your local IT support, or the IT Services Helpdesk. For installation instructions see "Installing TrueCrypt" guide.

Step 1

Insert the USB flash drive that is to be encrypted. Make a note of the drive letter assigned to it.

Step 2

Launch the TrueCrypt application. Click the Create Volume button.

📑 True	Crypt									-	. 🗆 🗙
<u>V</u> olumes	System	<u>K</u> eyfiles	T <u>o</u> ols	Settings	Help					Home	epage
Drive J; K; L; M; N; O; P; Q; R; S; T; U; W; X;	Volume						Size	Encryption	algorithm	Туре	
Volume	<u>C</u> reate Vo	lume <u>N</u> ever sav	/ ve histor	у	<u>V</u> olume F	Properties	ne <u>T</u> ool:	5	<u>Wip</u> r Select	e Cache tt <u>F</u> ile D <u>e</u> vice	
	Mount		Auto	-Mount De	evices		ismoun	it All		E <u>x</u> it	

Select the Encrypt a non-system partition/drive option and click Next.

Create More i	Expt Volume Creation Wizard an encrypted file container as a virtual encrypted disk within a file. Recommended for rrienced users. <u>information</u>
C Create Create inexpe	e an encrypted file container es a virtual encrypted disk within a file. Recommended for rienced users. <u>nformation</u>
Create inexpe	es a virtual encrypted disk within a file. Recommended for rienced users. <u>nformation</u>
More i	nformation
Encryp	it a non-system partition/drive
Encry; drive (ots a non-system partition on any internal or external e.g. a flash drive). Optionally, creates a hidden volume.
C Encryp	t the system partition or entire system drive
Encry who w files, e before	ots the partition/drive where Windows is installed. Anyone wants to gain access and use the system, read and write stc., will need to enter the correct password each time windows boots. Optionally, creates a hidden system.
More i	nformation about system encryption
E	lelp < Back Next > Cancel

Step 4

Keep the Standard TrueCrypt volume and select Next.

TrueCrypt Volume Creation Wizard	<u>- 🗆 ×</u>
	/olume Type
	• Standard TrueCrypt volume
	Select this option if you want to create a normal TrueCrypt volume.
	Hi <u>d</u> den TrueCrypt volume
RUE	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
1	Help < Back Next > Cancel

Step 5 Click on the Select Device button.

TRUEGR	Volume Location Image: Select Device Image: Select Device Image: Never gave history Encrypted device-hosted TrueCrypt volumes can be created within partitions on hard disks, solid-state drives, USB memory sticks, and on any other supported storage devices. Partitions can also be encrypted in place. In addition, encrypted device-hosted TrueCrypt volumes can be created within devices that do not contain any partitions (including hard disks and solid-state drives). Note: A device that contains partitions can be entirely encrypted in place (using a single key) only if it is the drive where Windows is installed and from which it boots.
	Help < Back Next > Cancel

Step 6

Select the drive letter (second column) associated with your flash drive that is to be encrypted, by either double clicking it or selecting it and click OK.

Se	elect a Partition or Device					×
	Device	Drive	Size	Name		_
	Harddisk 0: \Device\Harddisk0\Partition1	C:	74.5 GB 74.5 GB	Local Disk		
	Removable Disk 1:		984 MB			
	\Device\Harddisk1\Partition1	F:	983 MB	GLACERT		
	\Device\Floppy0	A:				
				ок	Cancel	

You will see this warning. We recommend that you select Yes as we wish to encrypt the entire drive, not create a encrypted file on the drive.



Step 8

Click Next.



Move any data from the USB flash drive onto the hard drive of your system and select Create encrypted volume and format it, then click Next.

TrueCrypt Volume Creation Wiza	ard X
	Volume Creation Mode
	• Create encrypted volume and format it
	This is the fastest way to create a partition-hosted or device-hosted TrueCrypt volume (in-place encryption, which is the other option, is slower because content of each sector has to be first read, encrypted, and then written). Any data currently stored on the selected partition/device will be lost (the data will NOT be encrypted; it will be overwritten with random data). If you want to encrypt existing data on a partition, choose the other option.
	C Encrypt partition in place
T B	The entire selected partition and all data stored on it will be encrypted in place. If the partition is empty, you should choose the other option (the volume will be created much faster).
	Help < Back Next > Cancel

Step 10

Keep the default options and click Next.

Encryption Options
Encryption Algorithm
AES I I I I I I I I I I I I I I I I I I I
classified information up to the Top Secret level. 256-bit Key,
128-bit block, 14 rounds (AES-256). Mode of operation is XTS. More information on AES Benchmark
128-bit block, 14 rounds (AES-256). Mode of operation is XTS. More information on AES Benchmark Hash Algorithm RIPEMD-160

Click Next.

TrueCrypt Volume Creation Wizar	d X
	Volume Size
6	Size of \Device\Harddisk1\Partition1 is 983.97 MB
Щ	Please verify that the size of the selected device/partition shown above is correct and click Next.
В	
	Help < Back Next > Cancel

Step 12

Set a password; ensure that it has a reasonable level of complexity then click Next.

IMPORTANT NOTE: If this password is lost the information on the disk will NOT BE RECOVERABLE, and lost forever. You have been warned!

	/olume Pa	issword		
the second secon	Password: *	Use keyfiles Display password t that you choose a t that contains only a combination of 2, 3 mes or dates of birtl sword is a random c ers, and special chai d choosing a passwo iger, the better). Th	consisting of emaximum possi	yfiles You should t can be found s). It should be easy to per and lower $@ ^ = $* +$ more than 20 ble length is 64
	Help	< <u>B</u> ack	<u>N</u> ext >	Cancel

Follow the on screen instructions for the Collecting Random Data dialogue, then press "Next".

TrueCrypt Volume Creation Wizard	d
L	Options Filesystem Fat Cluster Default T
C C C C C C C C C C C C C C C C C C C	Random Pool: 4F8C2F4FDB638954F6DB22039D4E3F3C 🔽 Header Key: CA48E39EA9D63071A3840A8326476275 Master Key: DEAF4066719FE609591D8BAB1FE12F77
	Done 10.096% Speed 3.3 MB/s Left 4 minutes
L R	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.
	Help < Back Eormat Cancel

Step 14

You may be presented with this warning, if you agree, click Yes.

TrueCry	t Volume Creation Wizard 🛛 🕹
⚠	CAUTION: ALL FILES CURRENTLY STORED ON THE SELECTED PARTITION '\Device\Harddisk1\Partition1' (F: 'GLACERT') WILL BE ERASED AND LOST (THEY WILL NOT BE ENCRYPTED)! Are you sure you want to proceed with format?
	<u>Y</u> es

Step 15

Read this notice which explains how to access the encrypted flash drive for use.

TrueCry	pt Volume Creation Wizard
1	IMPORTANT: Please keep in mind that this volume can NOT be mounted/accessed using the drive letter F:, which is currently assigned to it! To mount this volume, click 'Auto-Mount Devices' in the main TrueCrypt window (alternatively, in the main TrueCrypt window, click 'Select Device', then select this partition/device, and click 'Mount'). The volume will be mounted to a different drive letter, which you select from the list in the main TrueCrypt window. The original drive letter F: should be used only in case you need to remove encryption from the partition/device (e.g., if you no longer need encryption). In such a case, right-click the drive letter F: in the 'Computer' (or 'My Computer') list and select 'Format'. Otherwise, the drive letter F: should never be used (unless you remove it and assign it to another partition/device).
Step 1	16
Click O	К.
TrueC	Crypt Volume Creation Wizard



Click Exit.

