Computer Services

Quick Guide on How to Use **Vera**Crypt Disk Encryption

Introduction

This guide shows you how to use VeraCrypt to securely store confidential and sensitive data on an encrypted storage device (eg USB pen drives, External hard drive etc.)

VeraCrypt Disk Encryption encrypts a full disk (e.g. usb drives, external hard drives etc.) Once files are moved to the drive they are automatically encrypted.

This guide shows you how to:

- Download and install VeraCrypt
- Create an encrypted storage disk
- Mount the VeraCrypt disk (to use as a normal drive)
- Add / Remove files to the encrypted disk.

You should read this document in its entirety before attempting this procedure.

By following the guidance in this document you are helping to improve compliance with the Institutes Information Security and Data Protection Policies.

What is encryption?

Encryption helps secure confidential and sensitive data by converting it into a form that cannot be understood by criminals.

Why use VearCrypt?

Use VeraCrypt to securely store confidential and sensitive data on an encrypted storage device (e.g. USB pen drives, External hard drive etc.) When you place your files into the VeraCrypt *Container* it automatically encrypts the data using encryption and your pre-determined password. This version of VeraCrypt will encrypt an entire external storage device.

When do I need to create an encrypted storage drive?

Encrypted storage drives need to be used for all confidential and sensitive data when:

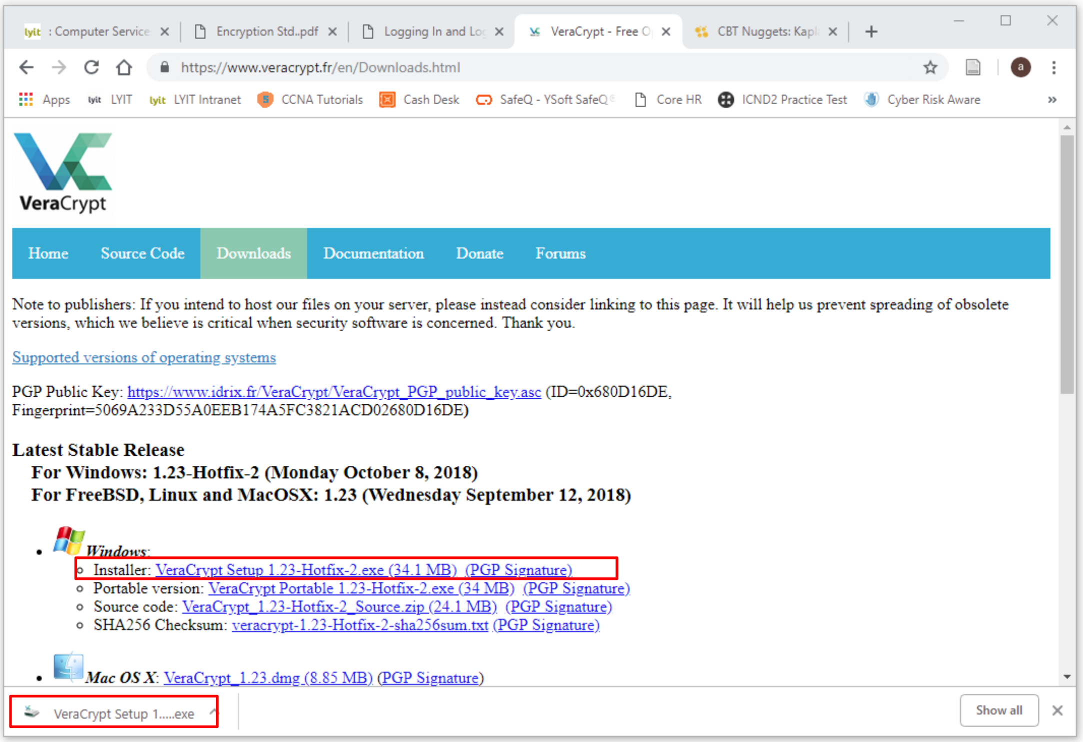
- It is not possible to store the data on secure Institute servers.
- It is kept on a portable storage device (e.g. USB thumb drive, External Hard Drive etc...)

1. Download and Install VeraCrypt

Go to https://www.veracrypt.fr/en/Downloads.html and download the version of VeraCrypt that is best suited to your operating system (typically Microsoft Windows).

VeraCrypt will automatically download after you have clicked on the appropriate link.

Click on the download in your browser to initiate the instillation.
(Alternatively if installing at a later date, double click on the ‘VeraCrypt Setup 1.23-Hotfix-2.exe’ file in downloads VeraCrypt Setup 1.23-Hotfix-2.exe)



Note to publishers: If you intend to host our files on your server, please instead consider linking to this page. It will help us prevent spreading of obsolete versions, which we believe is critical when security software is concerned. Thank you.

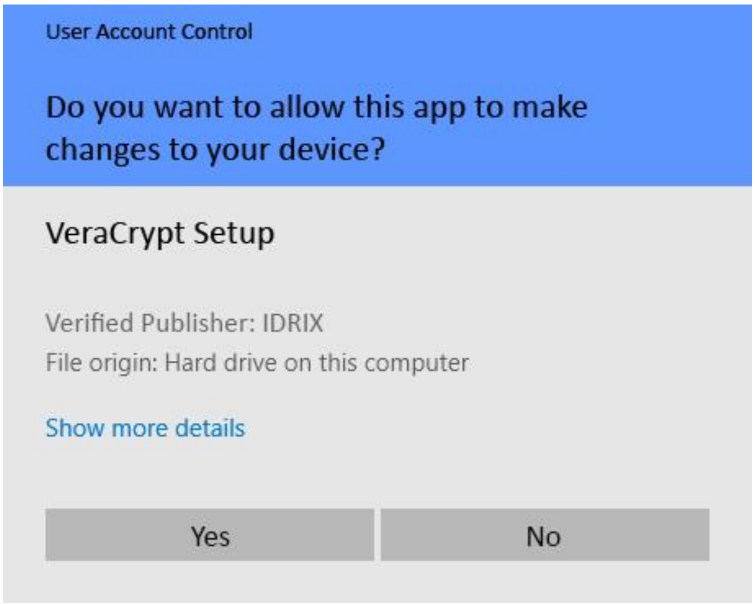
Supported versions of operating systems

PGP Public Key: https://www.idrix.fr/VeraCrypt/VeraCrypt_PGP_public_key.asc (ID=0x680D16DE, Fingerprint=5069A233D55A0EEB174A5FC3821ACD02680D16DE)

Latest Stable Release
For Windows: 1.23-Hotfix-2 (Monday October 8, 2018)
For FreeBSD, Linux and MacOSX: 1.23 (Wednesday September 12, 2018)

- *Windows*:
  - Installer: VeraCrypt Setup 1.23-Hotfix-2.exe (34.1 MB) (PGP Signature)
  - Portable version: VeraCrypt Portable 1.23-Hotfix-2.exe (34 MB) (PGP Signature)
  - Source code: VeraCrypt_1.23-Hotfix-2_Source.zip (24.1 MB) (PGP Signature)
  - SHA256 Checksum: veracrypt-1.23-Hotfix-2-sha256sum.txt (PGP Signature)
- *Mac OS X*: VeraCrypt_1.23.dmg (8.85 MB) (PGP Signature)

Click **Yes** to allow the instillation.



User Account Control

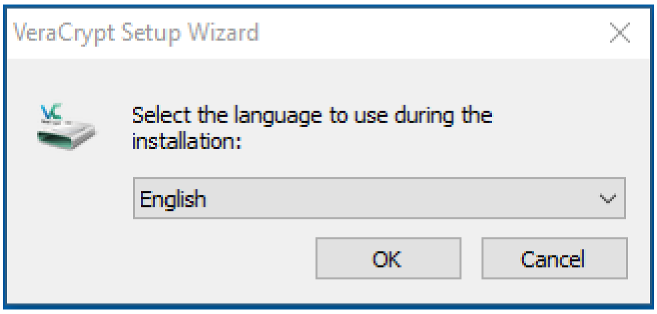
Do you want to allow this app to make changes to your device?

VeraCrypt Setup

Verified Publisher: IDRIX
File origin: Hard drive on this computer

Show more details

Select your language and click **OK**.

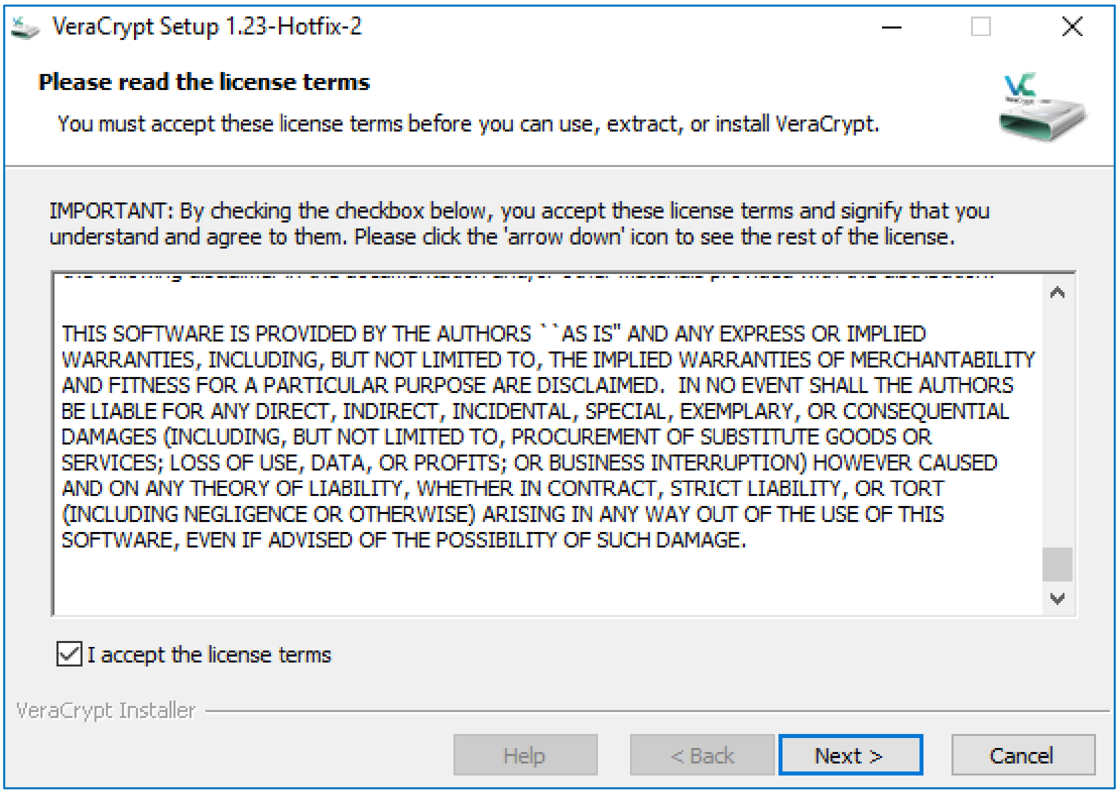


VeraCrypt Setup Wizard

Select the language to use during the installation:

English

Read and Accept the License Terms and click **Next**.



VeraCrypt Setup 1.23-Hotfix-2

Please read the license terms

You must accept these license terms before you can use, extract, or install VeraCrypt.

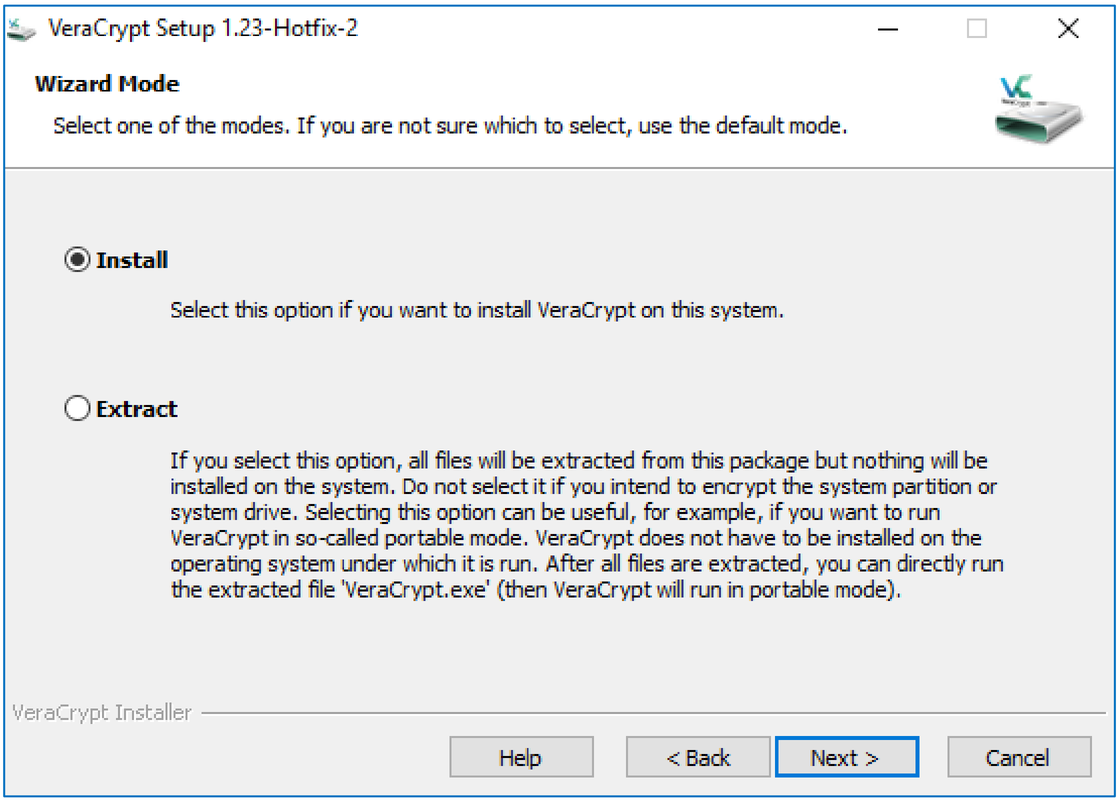
IMPORTANT: By checking the checkbox below, you accept these license terms and signify that you understand and agree to them. Please click the 'arrow down' icon to see the rest of the license.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

☑ I accept the license terms

VeraCrypt Installer

Choose to Install and click **Next**



VeraCrypt Setup 1.23-Hotfix-2

Wizard Mode

Select one of the modes. If you are not sure which to select, use the default mode.

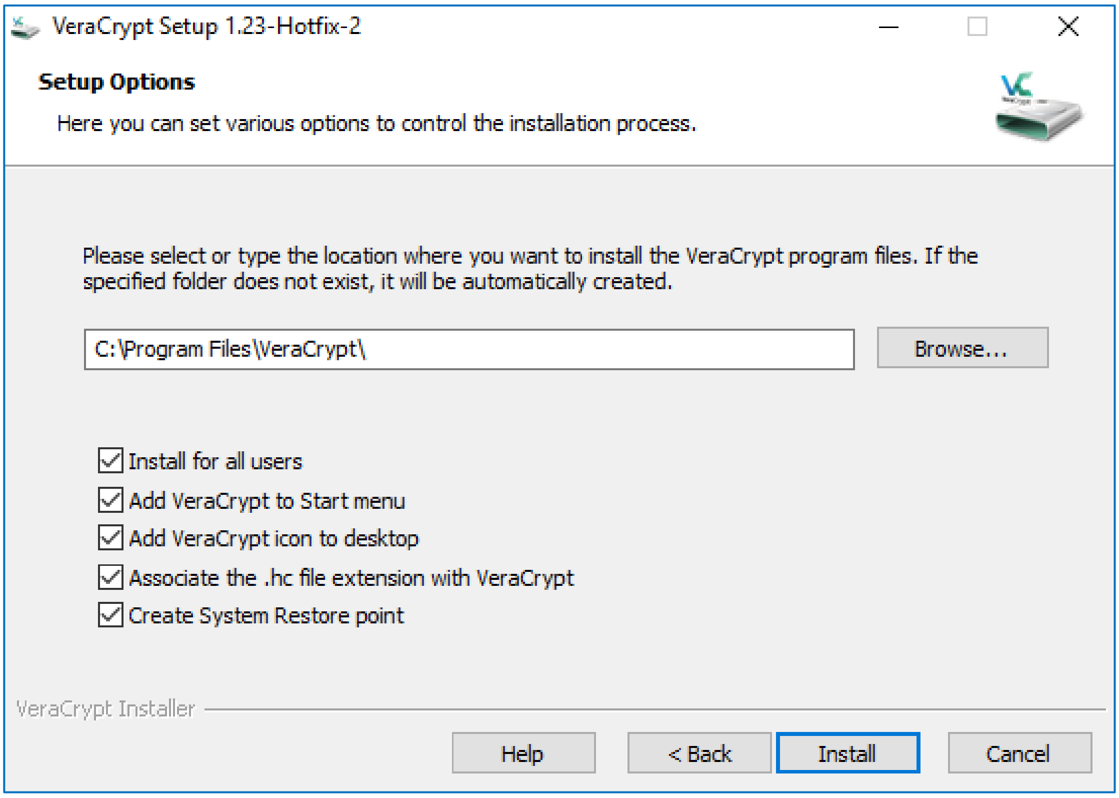
● **Install**

Select this option if you want to install VeraCrypt on this system.

○ **Extract**

If you select this option, all files will be extracted from this package but nothing will be installed on the system. Do not select it if you intend to encrypt the system partition or system drive. Selecting this option can be useful, for example, if you want to run VeraCrypt in so-called portable mode. VeraCrypt does not have to be installed on the operating system under which it is run. After all files are extracted, you can directly run the extracted file 'VeraCrypt.exe' (then VeraCrypt will run in portable mode).

Select the location to install VeraCrypt and click **Install**.



VeraCrypt Setup 1.23-Hotfix-2

Setup Options

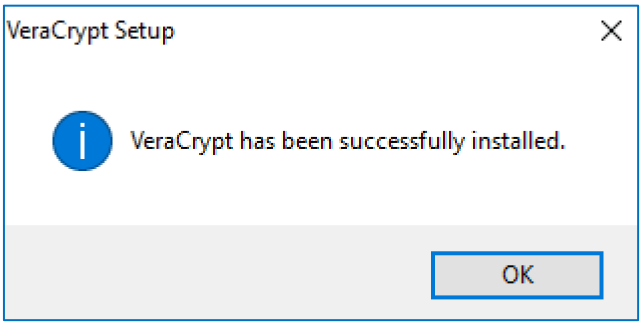
Here you can set various options to control the installation process.

Please select or type the location where you want to install the VeraCrypt program files. If the specified folder does not exist, it will be automatically created.

C:\Program Files\VeraCrypt\

☑ Install for all users
☑ Add VeraCrypt to Start menu
☑ Add VeraCrypt icon to desktop
☑ Associate the .hc file extension with VeraCrypt
☑ Create System Restore point

Click **OK** once the instillation has completed.



VeraCrypt Setup

VeraCrypt has been successfully installed.

Once complete a Donation Page will pop up – Click ‘Finish’.

You will then be asked to read the VeraCrypt User Guide. You should read the Beginner’s Tutorial if this is your first time using VeraCrypt.

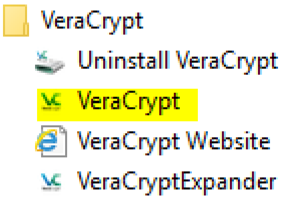
The Beginners Tutorial can be found at:
C:\Program Files\VeraCrypt\docs\html\en\Beginner's Tutorial.html (once instillation has completed and if installed to the default location) or online at https://www.veracrypt.fr/en/Beginner%27s%20Tutorial.html

Now you will need to create a VeraCrypt encrypted drive to store your files.

2. How to Create a VeraCrypt encrypted drive

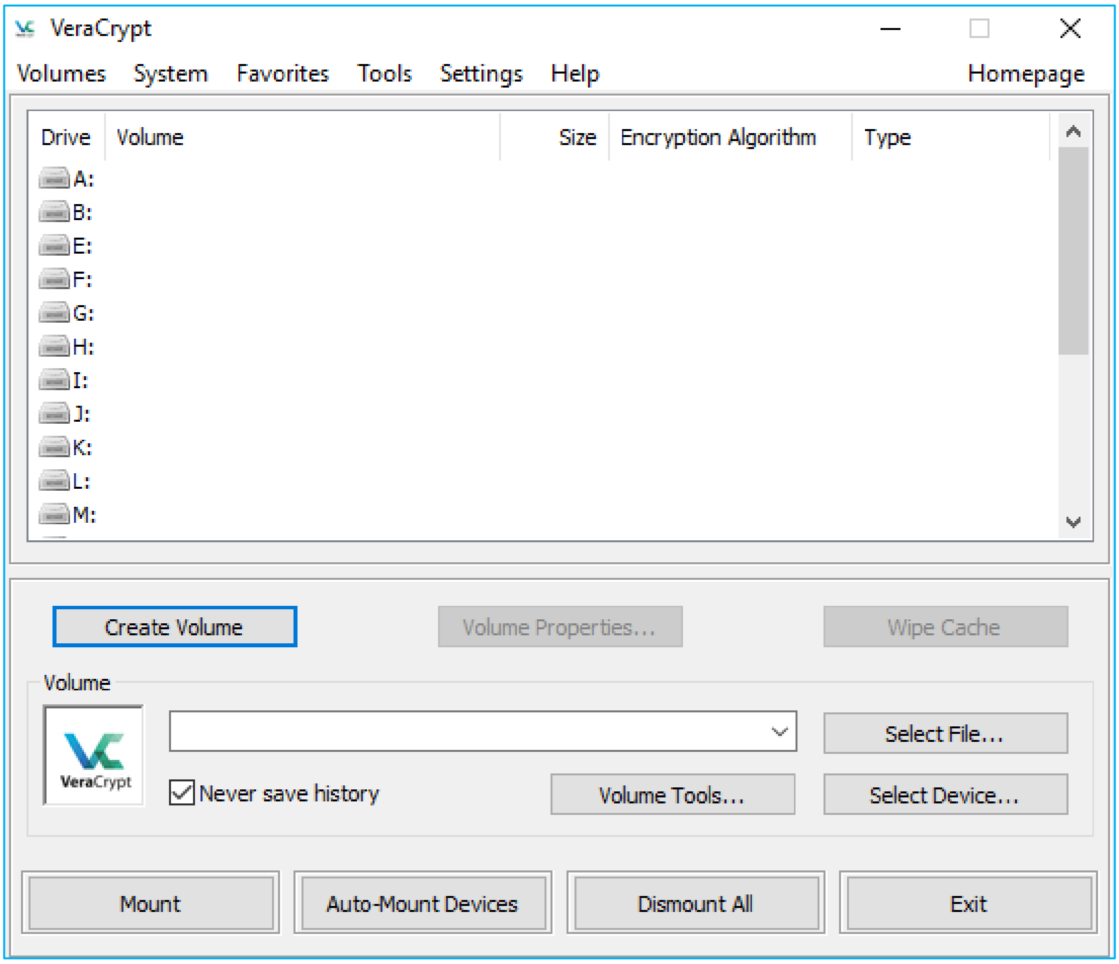
Step 1:

Open VeraCrypt by clicking on the VeraCrypt icon located on your desktop or in your Windows Start Menu.



Step 2:

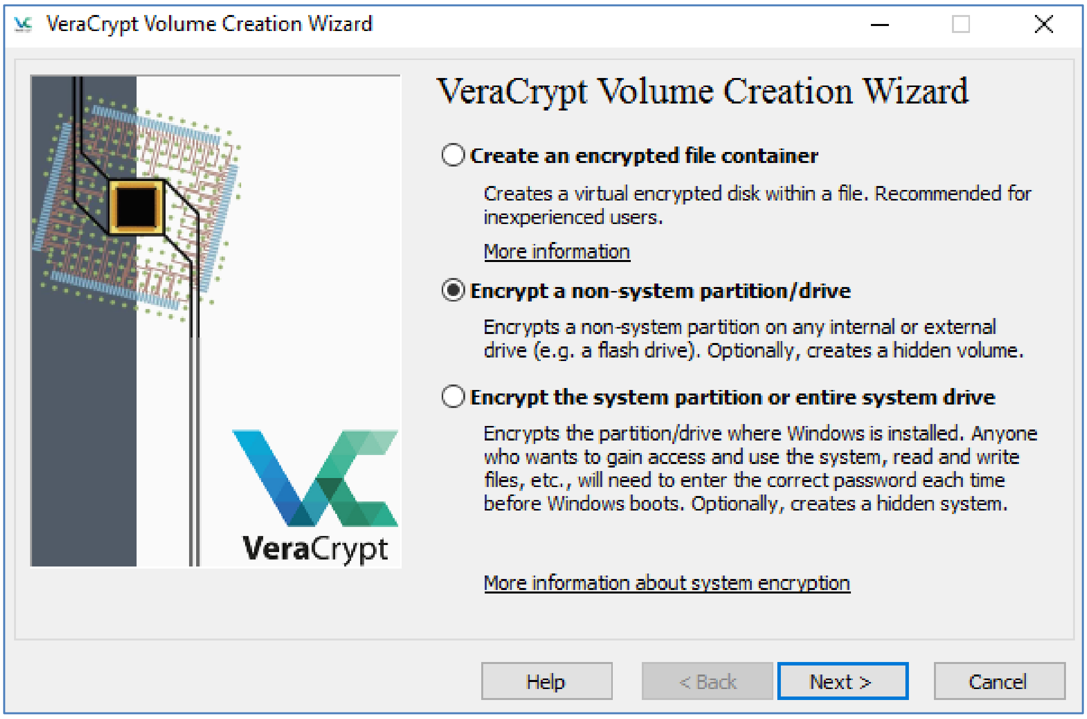
The main VeraCrypt window should appear. Click **Create Volume**



Step 3:

The VeraCrypt Volume Creation Wizard window should appear.

Choose *Encrypt a non-system partition/drive* and click **Next**.



VeraCrypt Volume Creation Wizard

VeraCrypt 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.

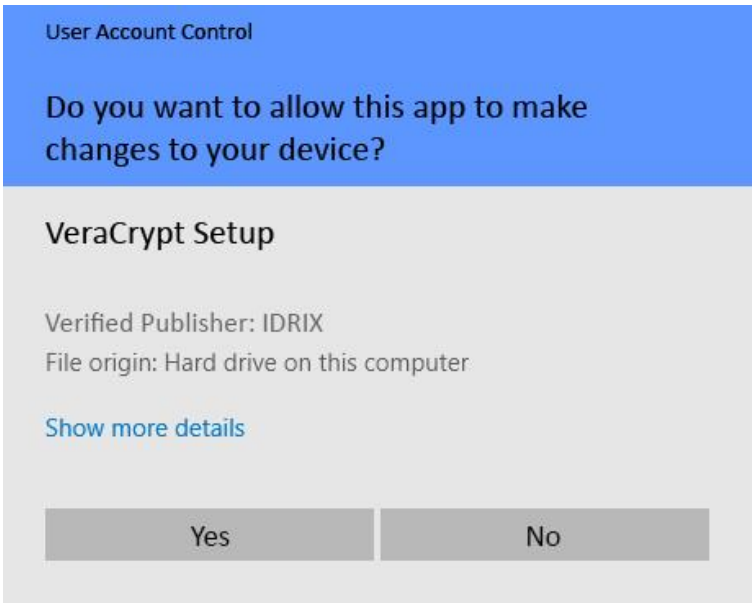
○ **Encrypt the system partition or entire system drive**

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

Step 4:

Click **Yes** to allow the instillation.



User Account Control

Do you want to allow this app to make changes to your device?

VeraCrypt Setup

Verified Publisher: IDRIX

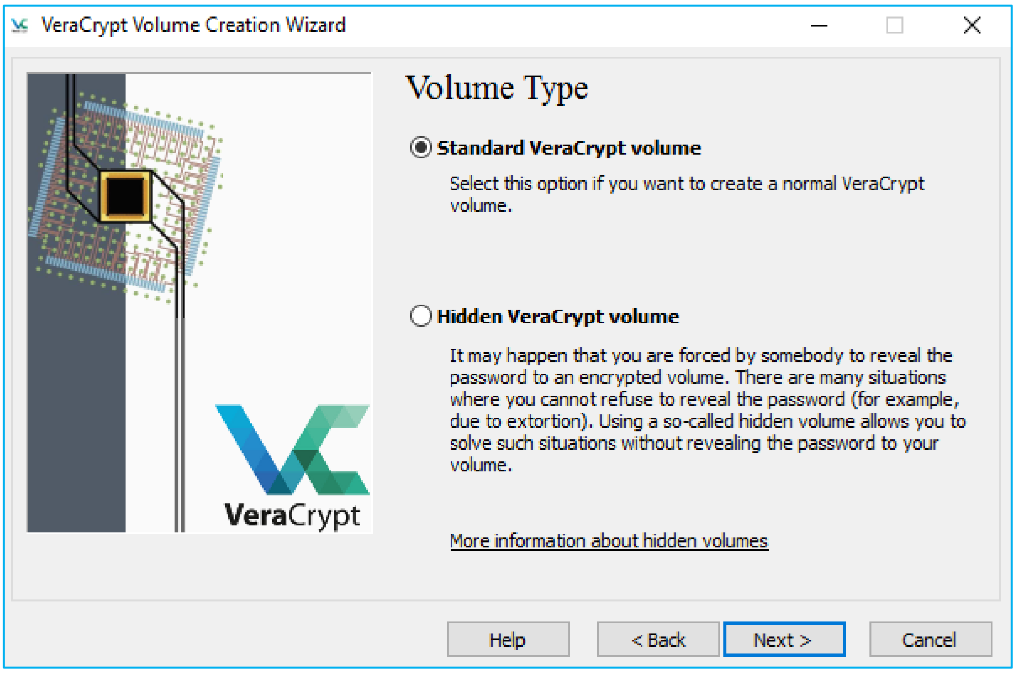
File origin: Hard drive on this computer

Show more details

STEP 5:

In this step we will create a *Standard VeraCrypt volume*.

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



Volume Type

● Standard VeraCrypt volume

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

○ Hidden VeraCrypt volume

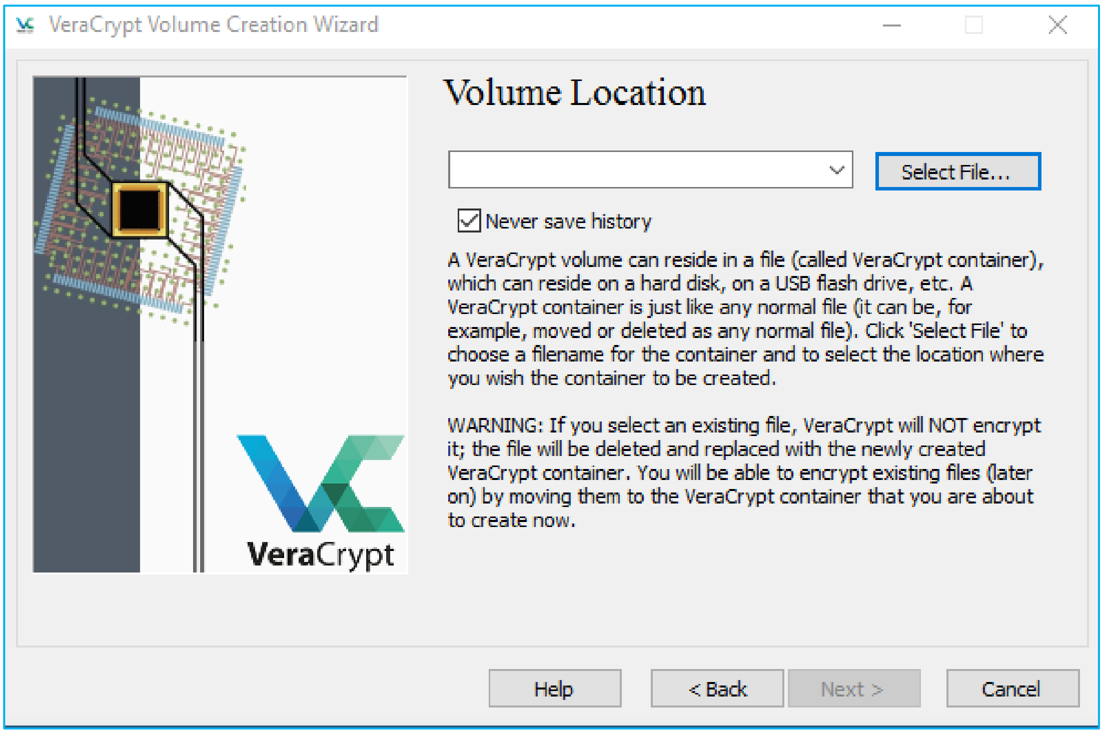
It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to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

More information about hidden volumes

(Fig 11 – Create a standard VeraCrypt Volume)

Step 6:

In this step you have to specify the disk drive to be encrypted. Click **Select File**.



Volume Location

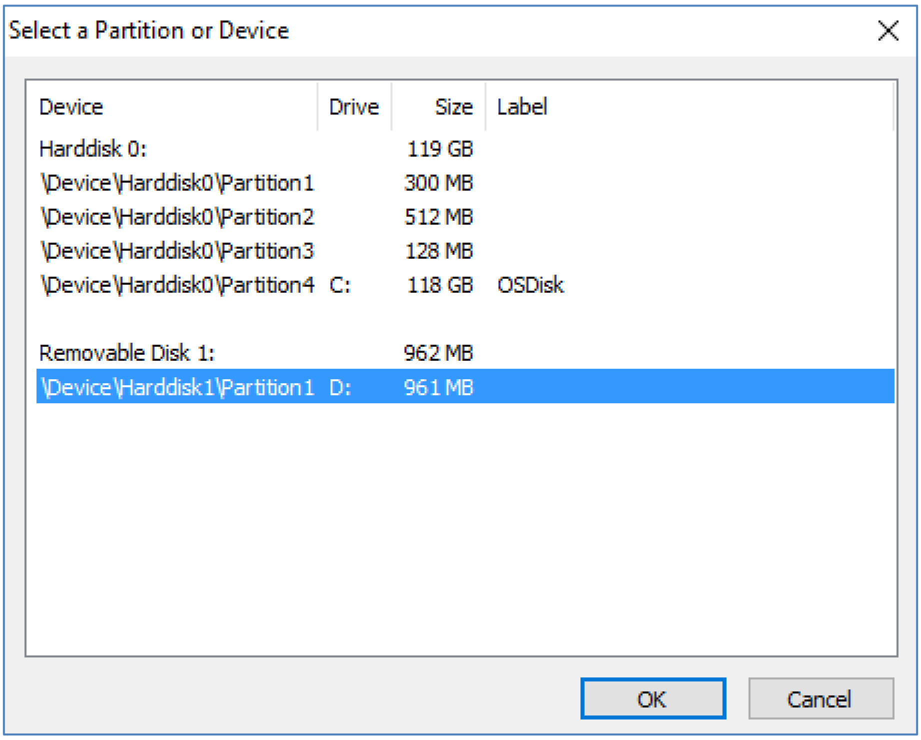
☑ Never save history

A VeraCrypt volume can reside in a file (called VeraCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A VeraCrypt container is just like any normal file (it can be, for example, moved or 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, VeraCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created VeraCrypt container. You will be able to encrypt existing files (later on) by moving them to the VeraCrypt container that you are about to create now.

STEP 7:

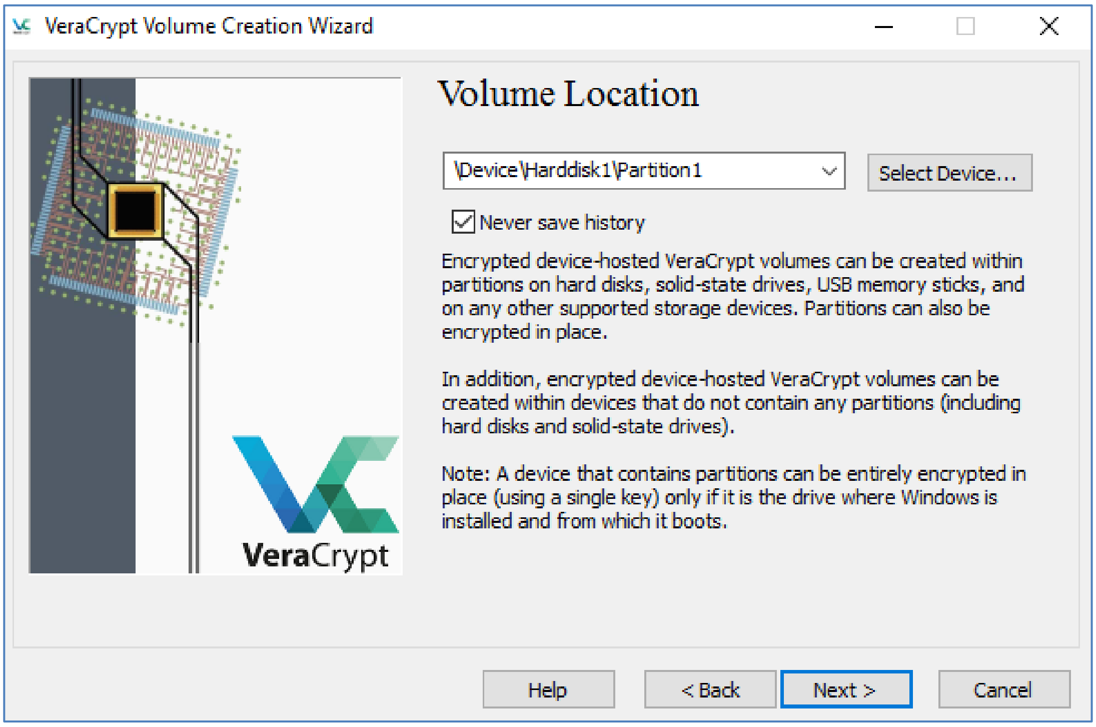
Select the drive to be encrypted (e.g. USB drive, external hard drive.. etc.) Click **OK**



Device	Drive	Size	Label
Harddisk 0:		119 GB	
\Device\Harddisk0\Partition1		300 MB	
\Device\Harddisk0\Partition2		512 MB	
\Device\Harddisk0\Partition3		128 MB	
\Device\Harddisk0\Partition4	C:	118 GB	OSDisk
Removable Disk 1:		962 MB	
\Device\Harddisk1\Partition1	D:	961 MB	

STEP 8:

Once the drive is selected click **Next**



Volume Location

\Device\Harddisk1\Partition1

☑ Never save history

Encrypted device-hosted VeraCrypt 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.

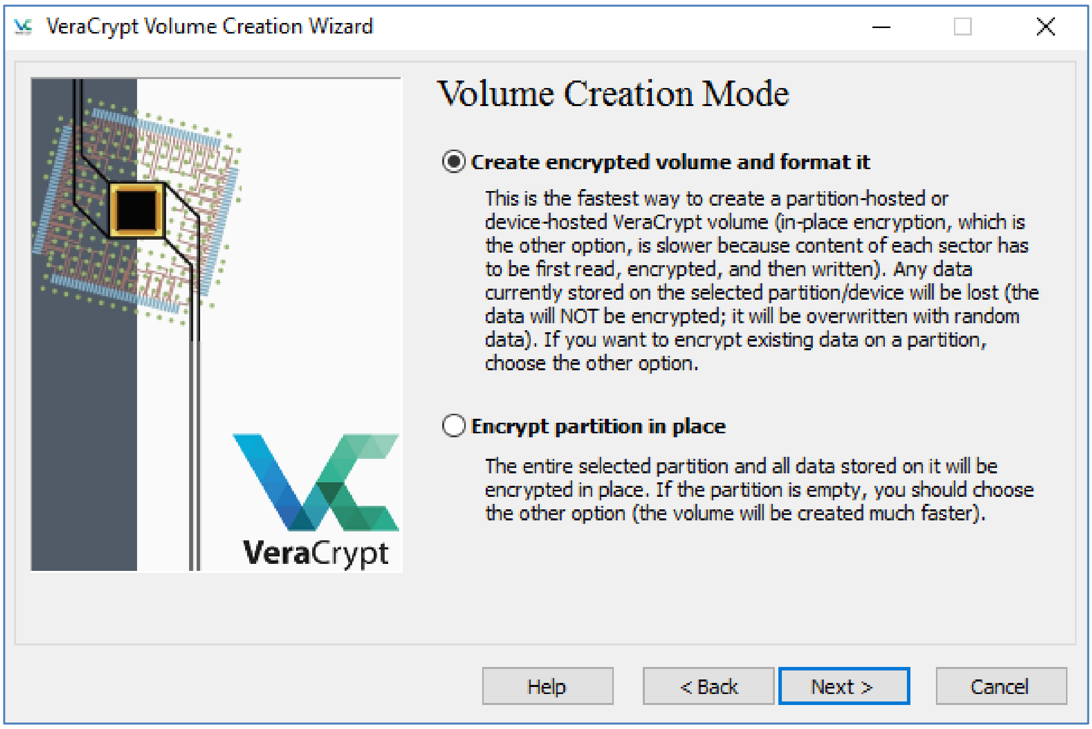
In addition, encrypted device-hosted VeraCrypt volumes can be created within devices that do not contain any partitions (including hard disks and solid-state drives).

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.

Step 9:

If the storage device is empty choose '*Create encrypted volume and format it*'. **Important: Any data currently on the device will be lost with this option.**

If there are files on the device choose '*Encrypt partition in place*'. This will encrypt the data currently on the device but will take a lot longer to complete.



VeraCrypt Volume Creation Wizard

Volume Creation Mode

● **Create encrypted volume and format it**

This is the fastest way to create a partition-hosted or device-hosted VeraCrypt 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.

○ **Encrypt partition in place**

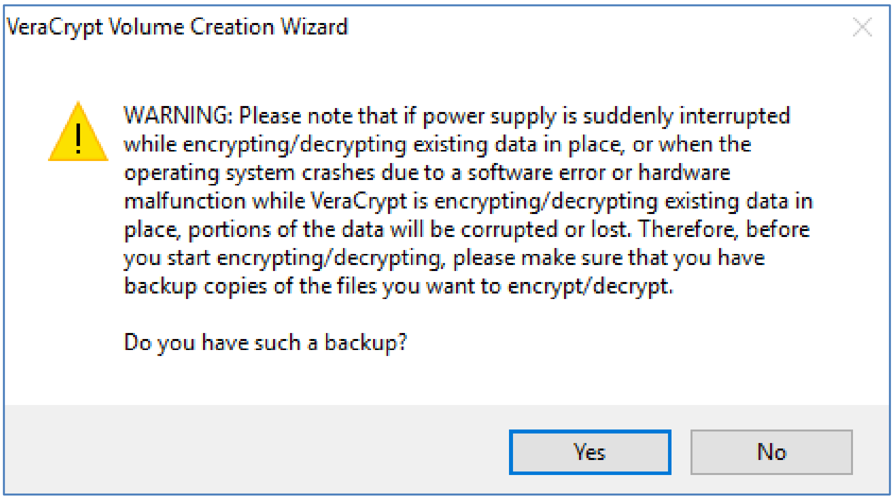
The entire selected partition and all data stored on it will be encrypted in place. If the partition is empty, you should choose the other option (the volume will be created much faster).

If **'*Create encrypted volume and format it*'** was chosen skip to **Step 17**:

If **'*Encrypt partition in place*'** was chosen complete the following steps:

Step 10:

Create backup copies of any files currently on the disk before continuing (if not already done). This will ensure against loss of files in the event of power supply outage, software error or hardware malfunction issues when encrypting the device.



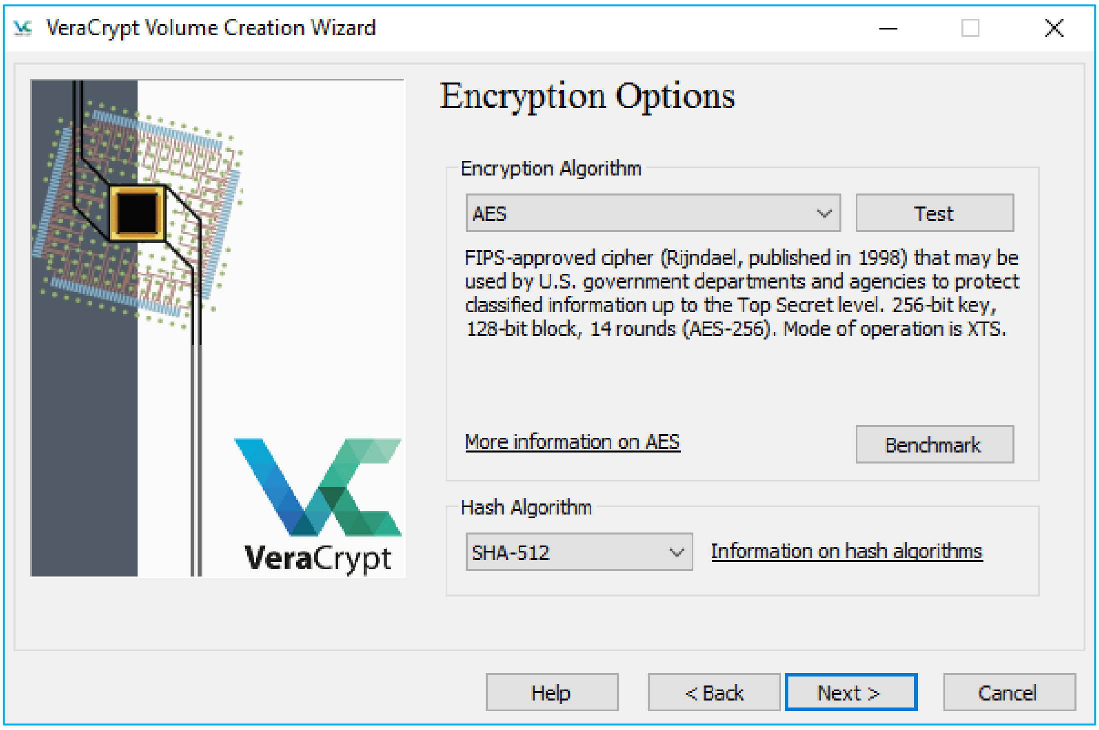
VeraCrypt Volume Creation Wizard

WARNING: Please note that if power supply is suddenly interrupted while encrypting/decrypting existing data in place, or when the operating system crashes due to a software error or hardware malfunction while VeraCrypt is encrypting/decrypting existing data in place, portions of the data will be corrupted or lost. Therefore, before you start encrypting/decrypting, please make sure that you have backup copies of the files you want to encrypt/decrypt.

Do you have such a backup?

STEP 11:

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**.



VeraCrypt Volume Creation Wizard

Encryption Options

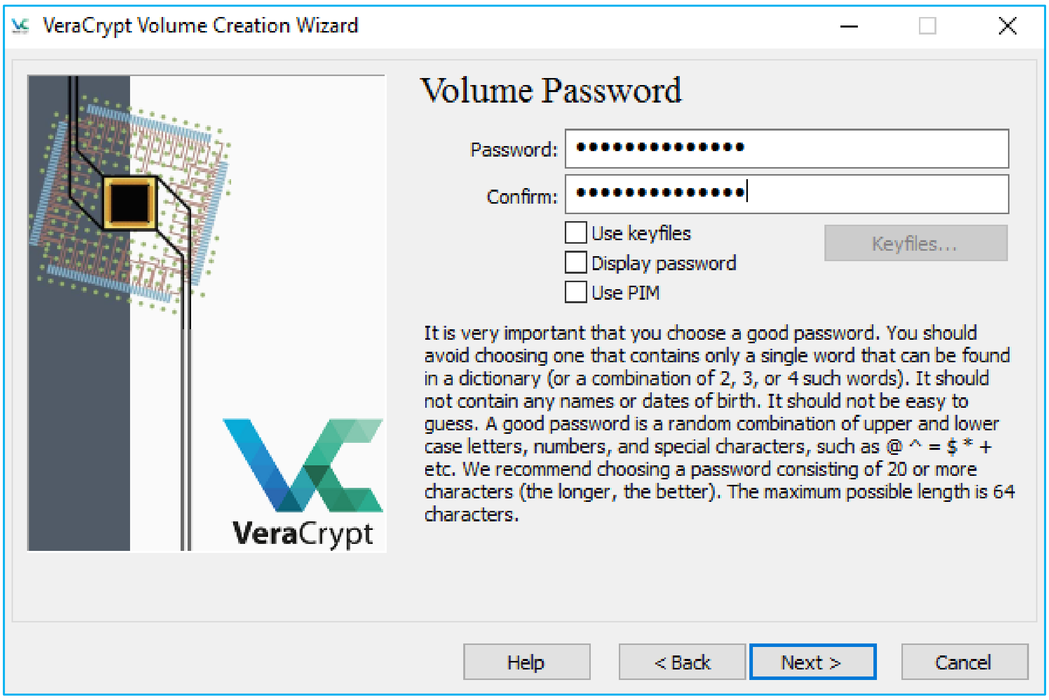
Encryption Algorithm: AES

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: SHA-512

STEP 12:
Choose a volume password. Read carefully the information displayed in the Wizard window about what is considered a good password.

Type your password in the Password field, then re-type it in the Confirm field. The **Next** button will be disabled until passwords in both input fields are the same.



VeraCrypt Volume Creation Wizard

Volume Password

Password: ••••••••••••••

Confirm: ••••••••••••••

□ Use keyfiles

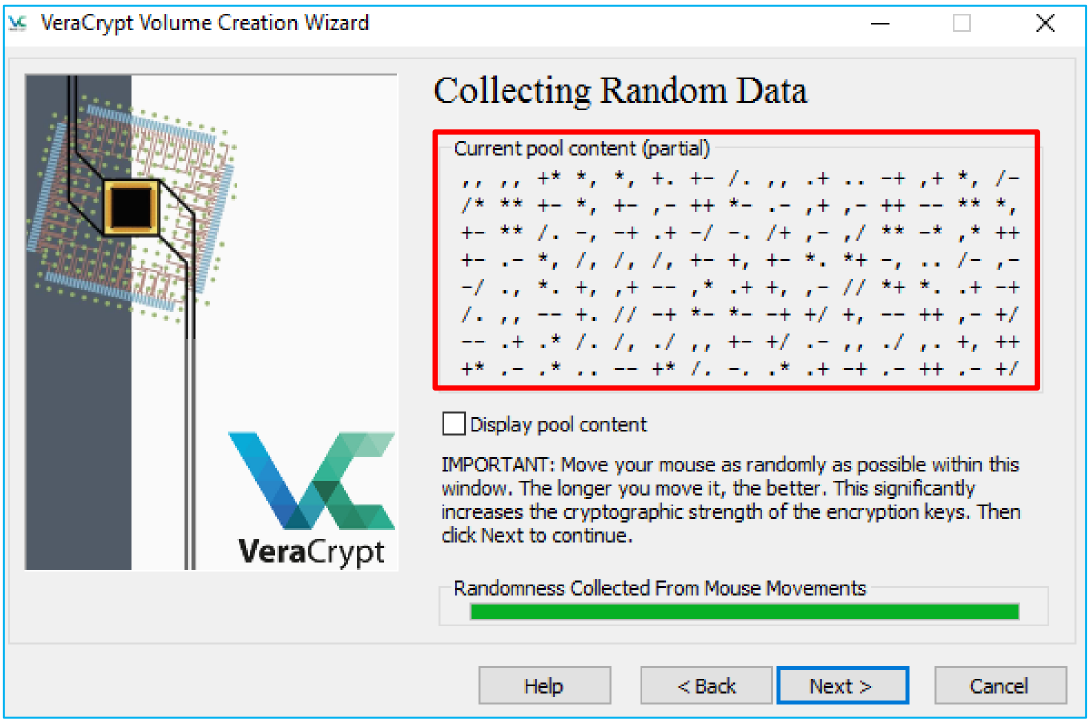
□ Display password

□ Use PIM

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 20 or more characters (the longer, the better). The maximum possible length is 64 characters.

STEP 13:

Move your mouse as randomly as possible within the window (inside the red square) at least until the randomness indicator becomes green. The longer you move the mouse, the better. This significantly increases the cryptographic strength of the encryption keys (which increases security).
Click **Next**.



VeraCrypt Volume Creation Wizard

Collecting Random Data

Current pool content (partial)

```
,, ,, +* *, *, +. +- /. ,, .+ .. -+ ,+ *, /-
/* ** +- *, +- ,- ++ *- .- ,+ ,- ++ -- ** *,
+- ** /. -, -+ .+ -/ -. /+ ,- ,/ ** -* ,* ++
+- .- *, /, /, /, +- +, +- *. *+ -, .. /- ,-
-/ ., *. +, ,+ -- ,* .+ +, ,- // *+ *. .+ -+
/. ,, -- +. // -+ *- *- -+ +/ +, -- ++ ,- +/
-- .+ .* /. /, ./ ,, +- +/ .- ,, ./ ,. +, ++
+* .- .* .. -- +* /. -. .* .+ -+ .- ++ .- +/
```

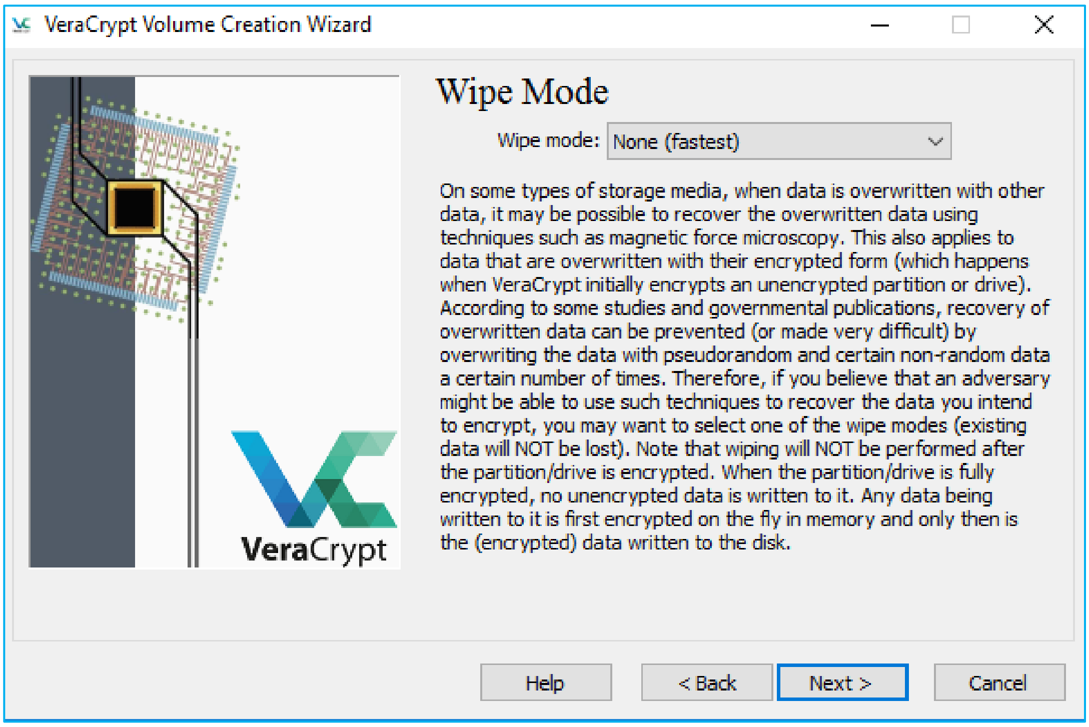
□ Display pool content

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 Next to continue.

Randomness Collected From Mouse Movements

STEP 14:

For the wipe mode choose '*None (fastest)*' and click **Next.**



VeraCrypt Volume Creation Wizard

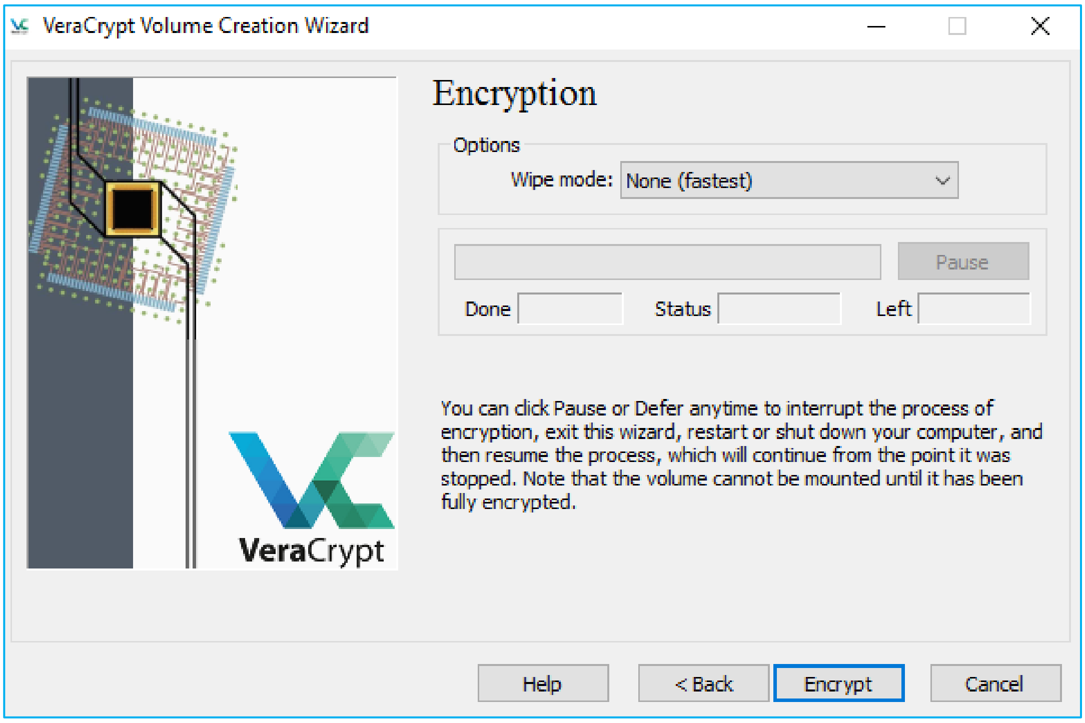
Wipe Mode

Wipe mode: None (fastest)

On some types of storage media, when data is overwritten with other data, it may be possible to recover the overwritten data using techniques such as magnetic force microscopy. This also applies to data that are overwritten with their encrypted form (which happens when VeraCrypt initially encrypts an unencrypted partition or drive). According to some studies and governmental publications, recovery of overwritten data can be prevented (or made very difficult) by overwriting the data with pseudorandom and certain non-random data a certain number of times. Therefore, if you believe that an adversary might be able to use such techniques to recover the data you intend to encrypt, you may want to select one of the wipe modes (existing data will NOT be lost). Note that wiping will NOT be performed after the partition/drive is encrypted. When the partition/drive is fully encrypted, no unencrypted data is written to it. Any data being written to it is first encrypted on the fly in memory and only then is the (encrypted) data written to the disk.

STEP 15:

Click **Encrypt** to encrypt the disk. Once started you can pause or defer the encryption to a later date / time and then resume encryption later which will pick up from the point it was stopped.



Encryption

Options

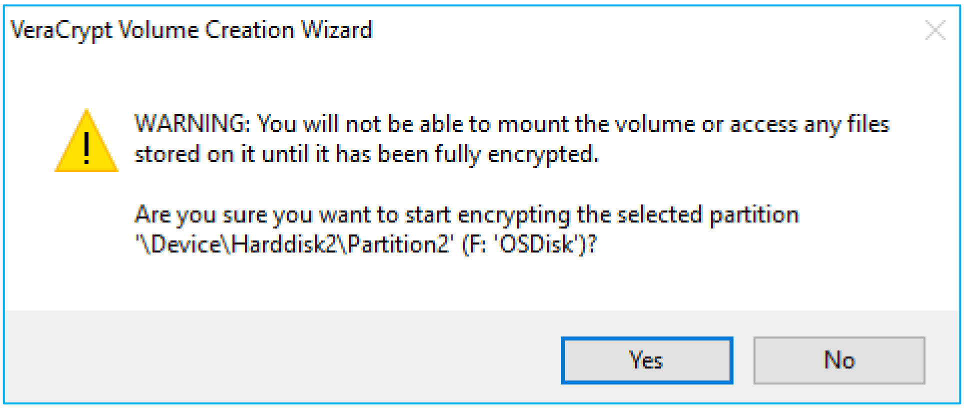
Wipe mode: None (fastest)

You can click Pause or Defer anytime to interrupt the process of encryption, exit this wizard, restart or shut down your computer, and then resume the process, which will continue from the point it was stopped. Note that the volume cannot be mounted until it has been fully encrypted.

STEP 16:

Click **Yes** to start the encryption.

Note: You will not be able to mount the encrypted volume or access any files on the drive until the encryption has been completed.



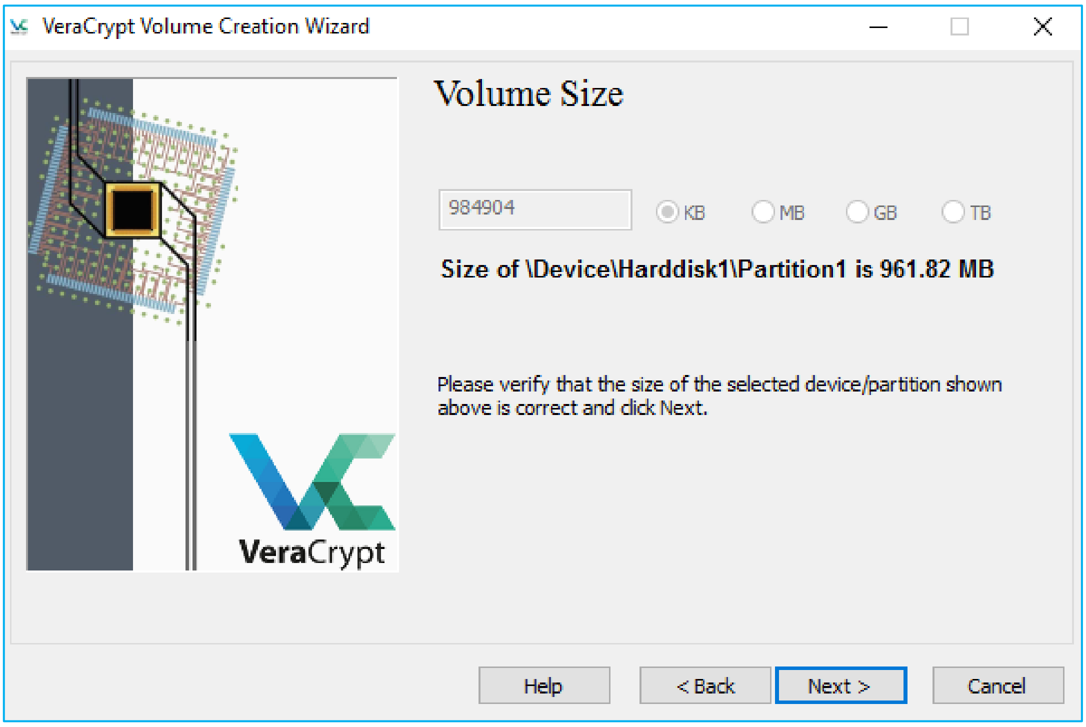
WARNING: You will not be able to mount the volume or access any files stored on it until it has been fully encrypted.

Are you sure you want to start encrypting the selected partition '\Device\Harddisk2\Partition2' (F: 'OSDisk')?

This will now encrypt the drive. You can now Skip to Step 22:

STEP 17:

Verify the size of the storage device. Click **NEXT**.



Volume Size

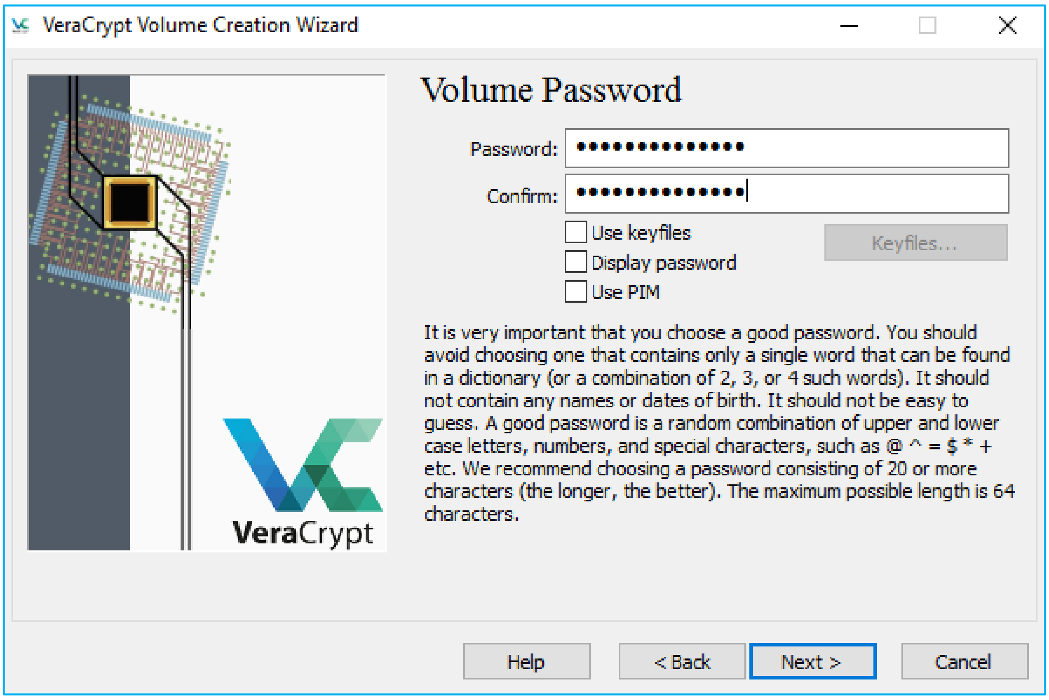
984904 ● KB ○ MB ○ GB ○ TB

Size of \Device\Harddisk1\Partition1 is 961.82 MB

Please verify that the size of the selected device/partition shown above is correct and click Next.

STEP 18:
Choose a volume password. Read carefully the information displayed in the Wizard window about what is considered a good password.

Type your password in the Password field, then re-type it in the Confirm field. The **Next** button will be disabled until passwords in both input fields are the same.



Volume Password

Password: ••••••••••••••

Confirm: ••••••••••••••

□ Use keyfiles

□ Display password

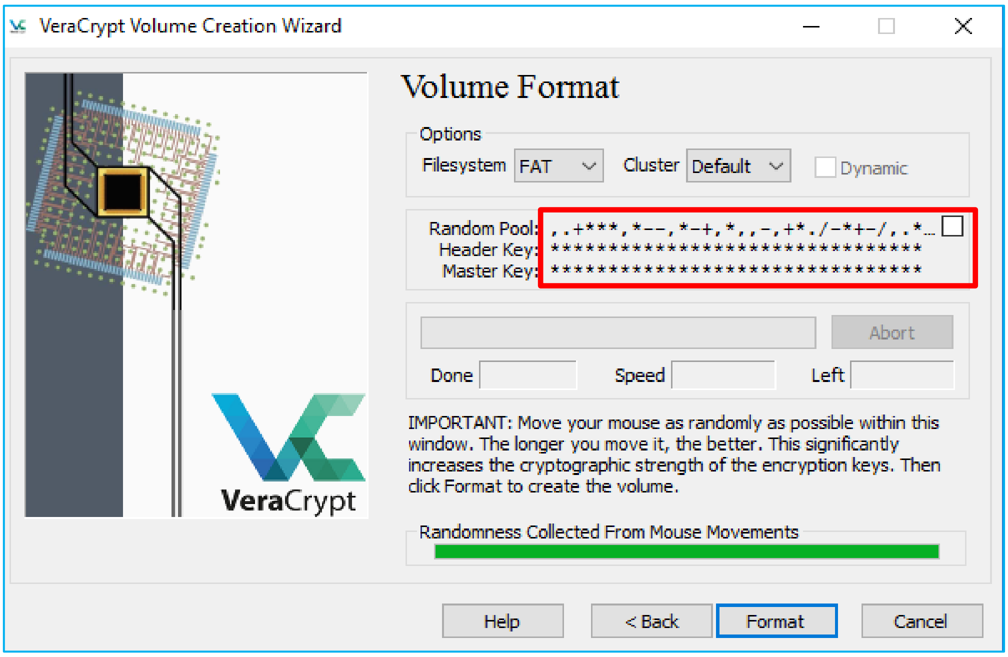
□ Use PIM

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 20 or more characters (the longer, the better). The maximum possible length is 64 characters.

STEP 19:

Move your mouse as randomly as possible within the Volume Creation Wizard window (inside the red square) at least until the randomness indicator becomes green. The longer you move the mouse, the better (moving the mouse for at least 30 seconds is recommended). This significantly increases the cryptographic strength of the encryption keys (which increases security).

Click **Format**.


VeraCrypt Volume Creation Wizard

Volume Format

Options

Filesystem FAT Cluster Default □ Dynamic

Random Pool: ,.+***,*--,*-+,*,,-,+*./-*+-/,.*... □
Header Key: ********************************
Master Key: ********************************

Done Speed Left

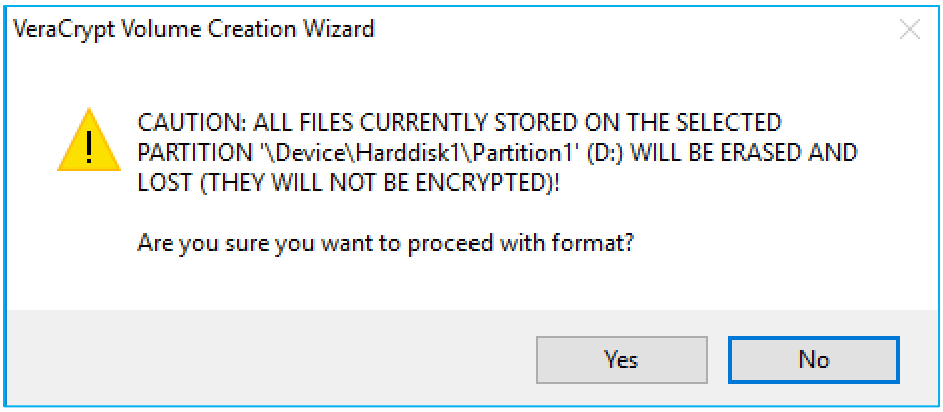
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

Randomness Collected From Mouse Movements

STEP 20:

Confirm you want to proceed with the device formatting. (Any data on the device will be lost.

Click **Yes**.

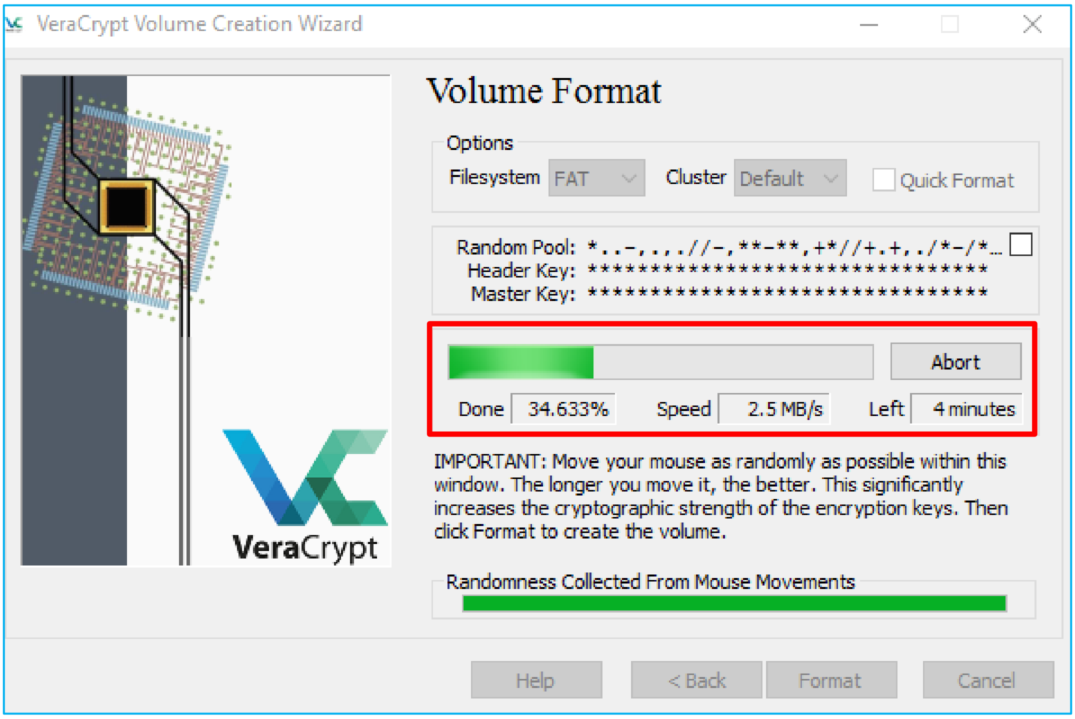

VeraCrypt Volume Creation Wizard

CAUTION: ALL FILES CURRENTLY STORED ON THE SELECTED PARTITION '\Device\Harddisk1\Partition1' (D:) WILL BE ERASED AND LOST (THEY WILL NOT BE ENCRYPTED)!

Are you sure you want to proceed with format?

STEP 21:

The drive will now be formatted with the remaining time displayed.



Volume Format

Options

Filesystem FAT Cluster Default □ Quick Format

Random Pool: *..-,.,.//-,**-**,+*//+.+,./*-/*... □
Header Key: ********************************
Master Key: ********************************

Done 34.633% Speed 2.5 MB/s Left 4 minutes

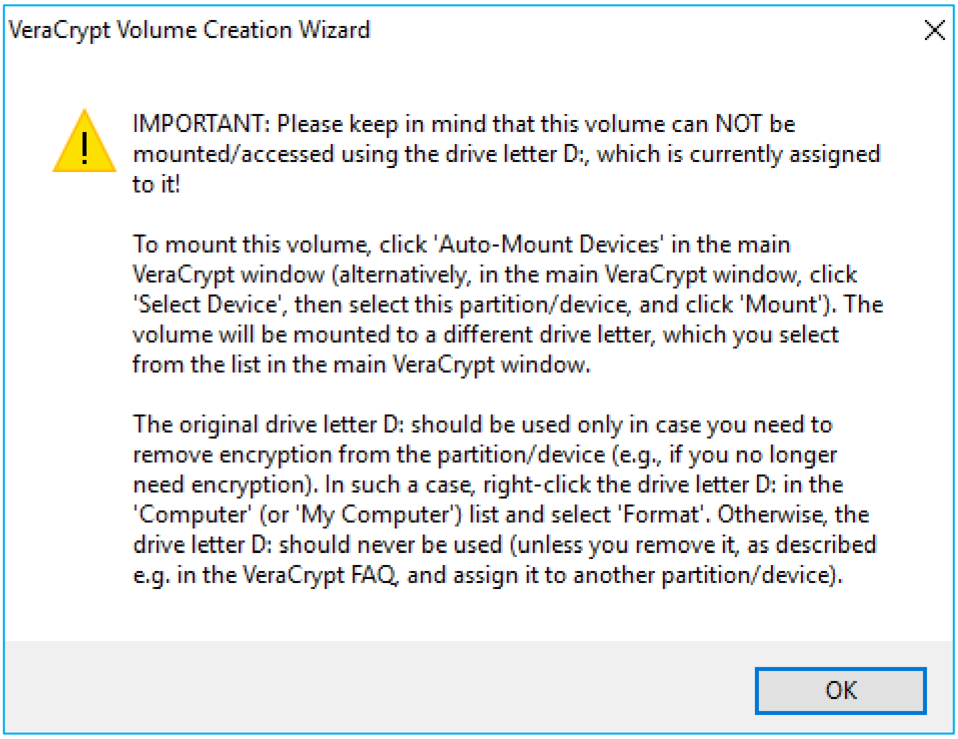
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

Randomness Collected From Mouse Movements

STEP 22:

Once created the new encrypted drive will have to be mounted to add or remove files to it.

Click **OK**.



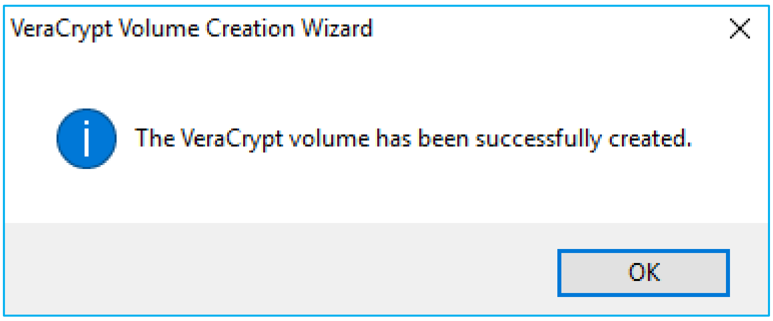
IMPORTANT: Please keep in mind that this volume can NOT be mounted/accessed using the drive letter D:, which is currently assigned to it!

To mount this volume, click 'Auto-Mount Devices' in the main VeraCrypt window (alternatively, in the main VeraCrypt 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 VeraCrypt window.

The original drive letter D: 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 D: in the 'Computer' (or 'My Computer') list and select 'Format'. Otherwise, the drive letter D: should never be used (unless you remove it, as described e.g. in the VeraCrypt FAQ, and assign it to another partition/device).

STEP 23:

Click **OK**.

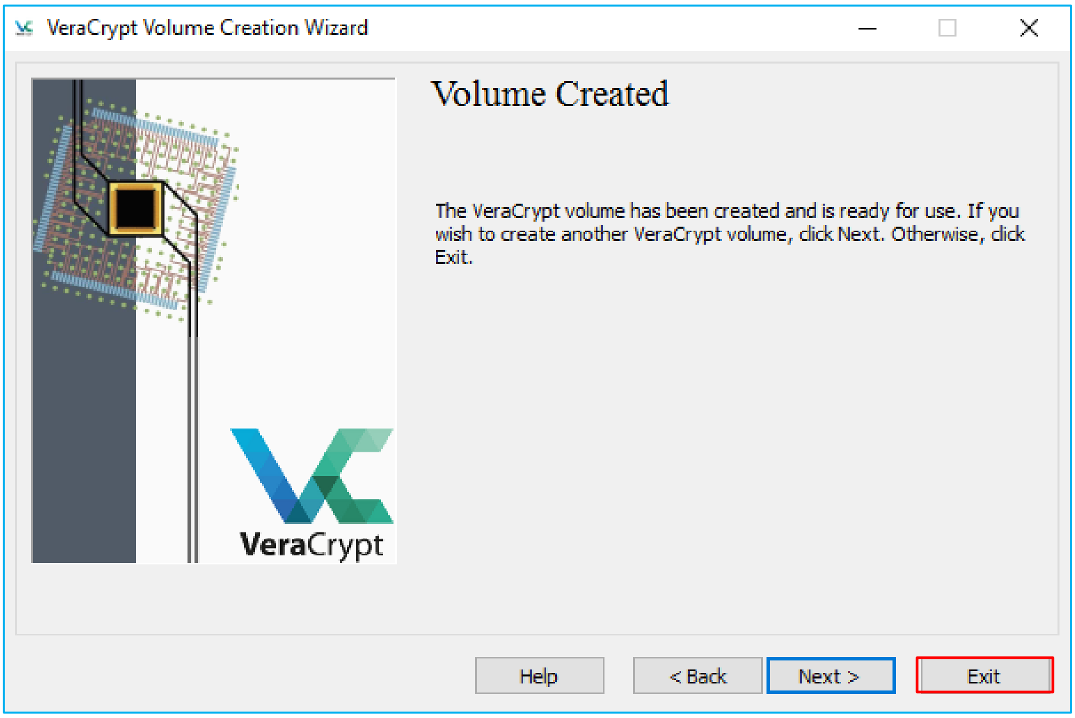


VeraCrypt Volume Creation Wizard

The VeraCrypt volume has been successfully created.

STEP 24:

Exit the VeraCrypt Volume Creation Wizard.



VeraCrypt Volume Creation Wizard

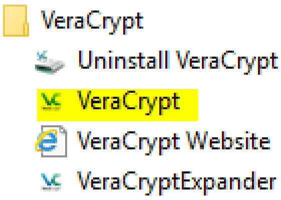
Volume Created

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

3. How to mount the VeraCrypt container

Step 25:

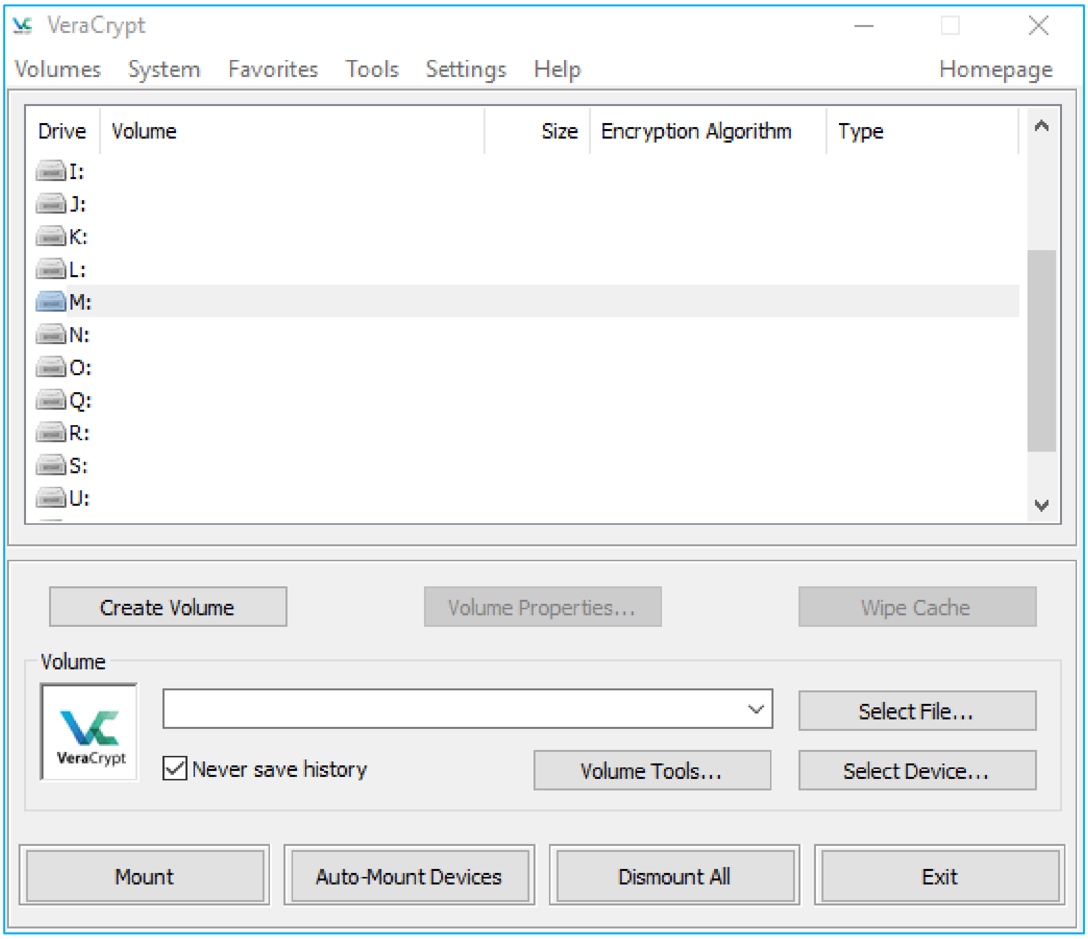
Open VeraCrypt by clicking on the VeraCrypt icon located on your desktop or in your Windows Start Menu.



VeraCrypt
Uninstall VeraCrypt
VeraCrypt
VeraCrypt Website
VeraCryptExpander

STEP 26:

Click **Auto-Mount Devices**

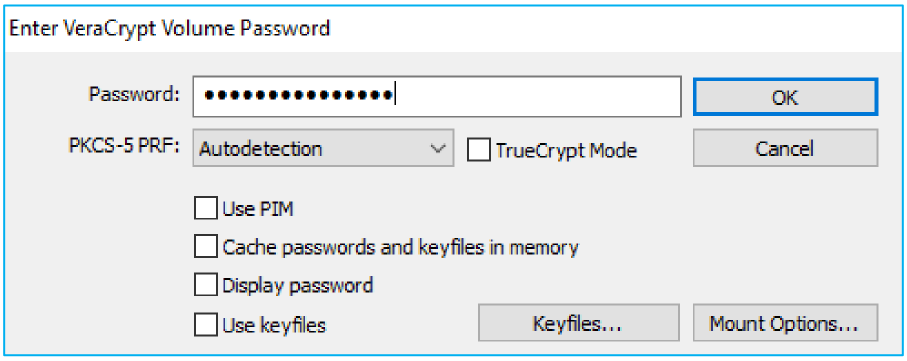


Drive	Volume	Size	Encryption Algorithm	Type
I:				
J:				
K:				
L:				
M:				
N:				
O:				
Q:				
R:				
S:				
U:				

☑ Never save history

STEP 27:

Enter your password (from Step 12). Click **OK**



Enter VeraCrypt Volume Password

Password: •••••••••••••••

PKCS-5 PRF: Autodetection

□ TrueCrypt Mode

□ Use PIM

□ Cache passwords and keyfiles in memory

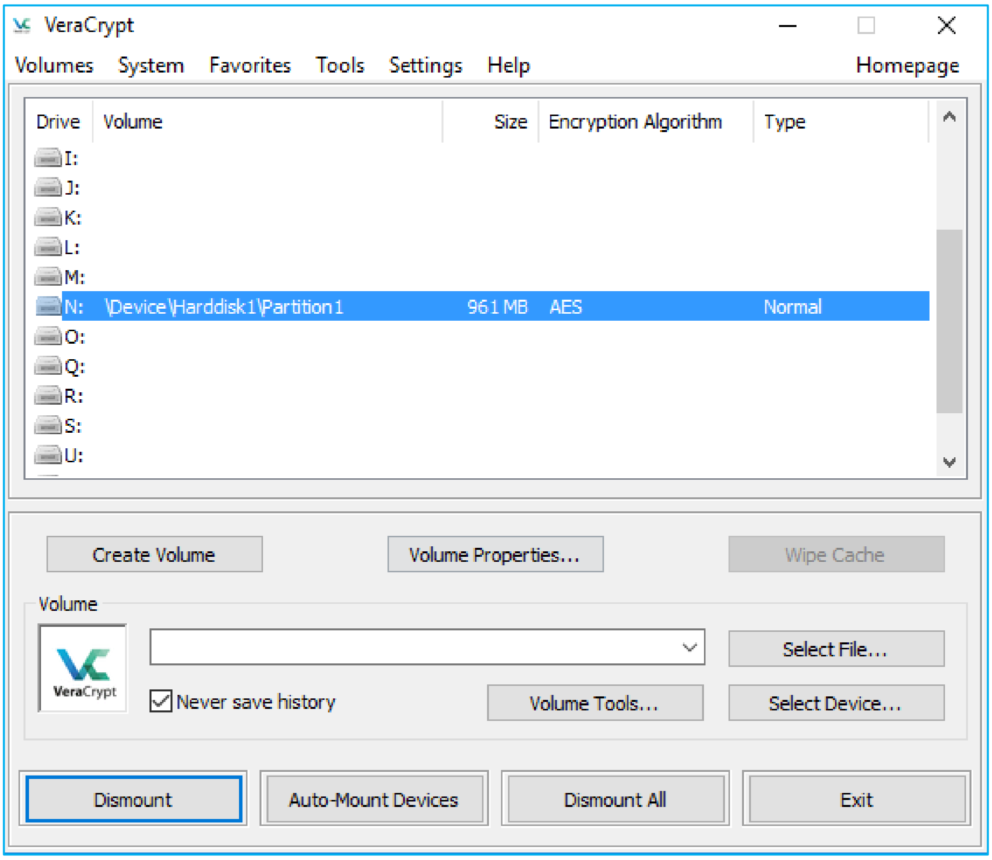
□ Display password

□ Use keyfiles

STEP 28:

VeraCrypt will now attempt to mount the encrypted drive.

Once mounted, the device will appear as a virtual disk (N in the below example).

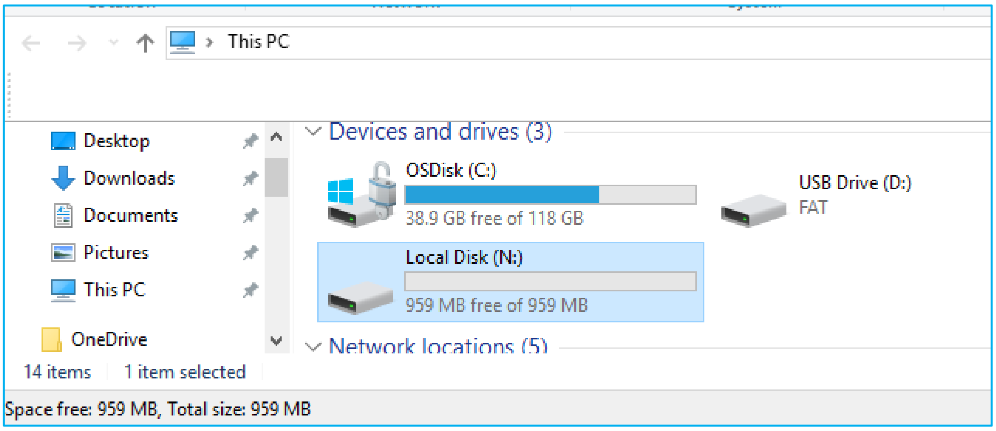


VeraCrypt

Drive	Volume	Size	Encryption Algorithm	Type
I:				
J:				
K:				
L:				
M:				
N:	\Device\Harddisk1\Partition1	961 MB	AES	Normal
O:				
Q:				
R:				
S:				
U:				

Volume

☑ Never save history



This PC

Devices and drives (3)

OSDisk (C:)
38.9 GB free of 118 GB

USB Drive (D:)
FAT

Local Disk (N:)
959 MB free of 959 MB

Network locations (5)

14 items 1 item selected

Space free: 959 MB, Total size: 959 MB

4. Add / Remove files to the encrypted drive

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

You can copy files (or folders) to and from the VeraCrypt volume just as you would copy them to any normal disk (for example, by simple drag-and-drop operations).

If you open a file stored on a VeraCrypt volume, for example, in media player, the file will be automatically decrypted while it is being read.

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

If you want to close the volume and make files stored on it inaccessible, either restart your operating system or **dismount** the volume. The volume will have to be remounted (entering your password) to access the data on the volume again.

5. Protecting your encryption password / passphrase

Your password / passphrase is the only thing that stops a criminal from accessing the contents of your encrypted drive if it falls into the wrong hands.

Do not forget your password / passphrase. It is not possible for us to recover your data if you forget your password / passphrase.

6. Information security incidents

If you discover an incident that places sensitive or confidential information at risk, then you must notify the Computer Services Team through the Helpdesk by email (helpdesk@lyit.ie) or by telephone (0749186050).

7. Information Security checklist

Ref	**Requirement**	
1	Have you familiarised yourself with the prerequisites for using VeraCrypt?	
2	Have you downloaded and installed VeraCrypt?	
3	Do you know how to create a VeraCrypt container?	
4	Do you know how to mount the VeraCrypt container?	
5	Do you know how to add / remove files to the encrypted drive?	
6	Do you know how to protect your passphrase?	
7	Do you know how to report an information security incident?	