Encrypt data using VeraCrypt

Keep Research Data Securely
Data Encryption
Beginner

Introduction

This document describes how VeraCrypt may be used to protect your personal and sensitive files using encryption.

What is Encryption?

Encryption is a process through which data is scrambled in order to make it impossible, or at least extremely difficult, to access by others.

The need to encrypt specific types of sensitive or confidential data is established in the UK Data Protection Act. This states "*appropriate technical and organisational measures*" must be applied to prevent "*unauthorised or unlawful processing of personal data*".

Further information on data encryption can be found on the Research Data management website at http://www.lshtm.ac.uk/research/researchdataman/.

What is VeraCrypt?

VeraCrypt is a free, open source encryption tool for Microsoft Windows, Apple MacOS and Linux platforms. It applies a technique called On-the-fly encryption, which transparently encrypts/decrypts files being accessed, without the need for user intervention. VeraCrypt is an enhancement of the now-discontinued TrueCrypt project, which makes several security improvements.

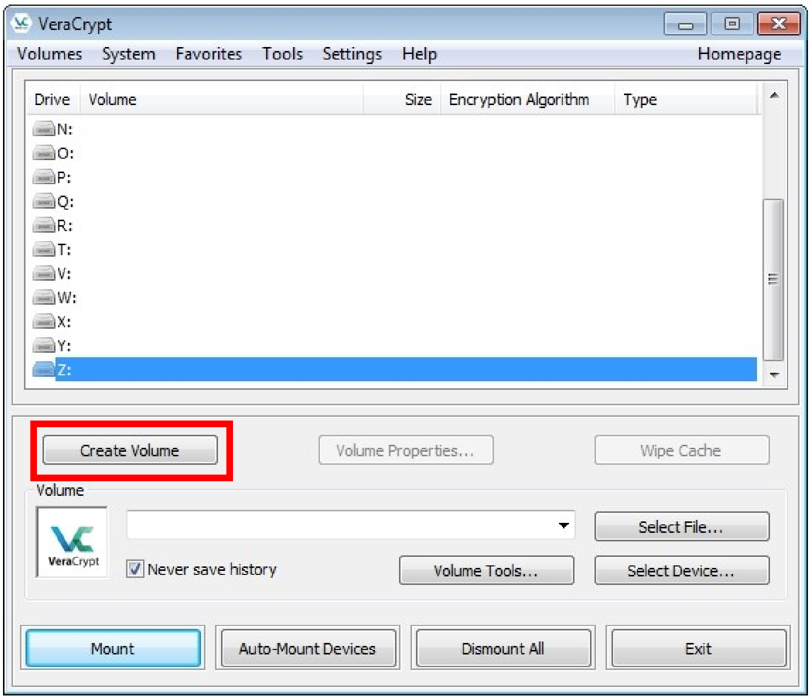
Visit https://veracrypt.codeplex.com/releases/ to download the current version for your operating system.

How do I get more help?

The LSHTM Research Data Management Support Service provides advice and guidance on topics related to the creation, management, and sharing of research data. Support material can be found at http://www.lshtm.ac.uk/research/researchdataman/.

Create a VeraCrypt Volume

1. Click ‘Create Volume’ to launch the VeraCrypt Volume Creation Wizard.



☑ Never save history

2. The first screen asks you to specify the type of encrypted volume to be created. Three options are available:

No	Title	Description	Suitable for:
1	**Create an Encrypted file container**	Creates a virtual encrypted disk within a file. This will appear as a normal file in a directory and a virtual drive in which you can create, update and delete files.	This may be used if you wish to: • Store data in an encrypted area without reformatting the disk • Create an encrypted file that can be moved between computers
2	**Encrypt a non-system partition / drive**	This provides the option to: • Format a partition as an encrypted drive, removing all data in the process • Convert a partition and all of its data using the ‘*encrypt partition in place*’ option This option may be used for non-bootable disks only, i.e. those that do not contain installed operating system,	This may be used if you wish to: • Protect all data held on a memory stick or hard disk partition. • Create a hidden partition as an additional level of protection
3	**Encrypt the system partition or entire system drive**	Encrypts the disk in its entirety, covering all partitions. A user wishing to gain access to the machine will need to provide a password before the operating system can be loaded.	This may be used if you wish to: • Protect all data held on a drive.

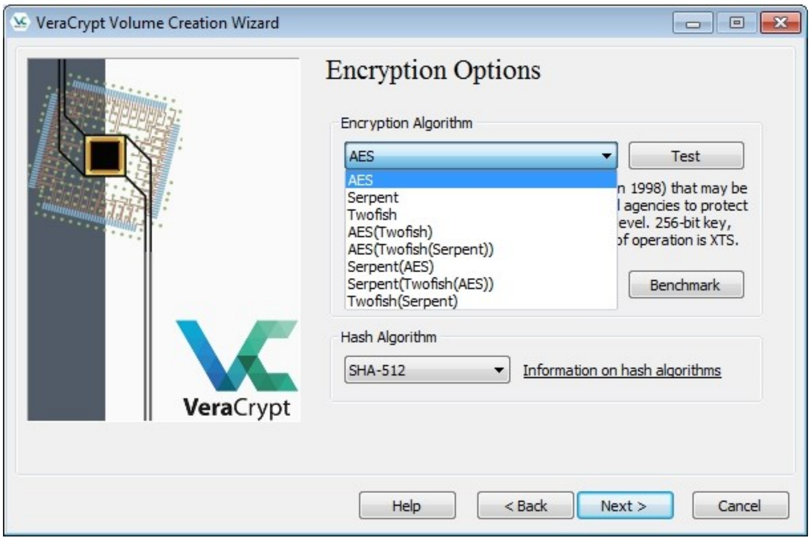
We shall create an encrypted file container (option 1) for this exercise. Ensure this option is selected and press '*Next'*.

3. Select the '*Standard VeraCrypt Volume*' option and press '*Next*'.

4. Press the '*Select File'* button to:
   a. Select the drive/folder where the encrypted file will be kept (e.g. your H: drive)
   b. Specify a descriptive filename for the file container

5. Choose an appropriate encryption algorithm (below). AES is sufficient for most purposes, balancing security with access speed.

   Many security experts state that 'cascaded ciphers', which involve the use of 2-3 levels of encryption, offer greater security, e.g. 'AES-Twofish-Serpent' or 'Serpent-Twofish-AES'. This works by encrypting data using algorithm A (e.g. AES), the output of which is encrypted using algorithm B (e.g. TwoFish), followed by algorithm C (e.g. Serpent). A 3rd party would need to decode algorithm C, followed by algorithm B and A, in order to access the data. However, you may find that file access & saving is slower.



VeraCrypt Volume Creation Wizard

Encryption Options

Encryption Algorithm: AES

n 1998) that may be
l agencies to protect
evel. 256-bit key,
of operation is XTS.

Hash Algorithm: SHA-512

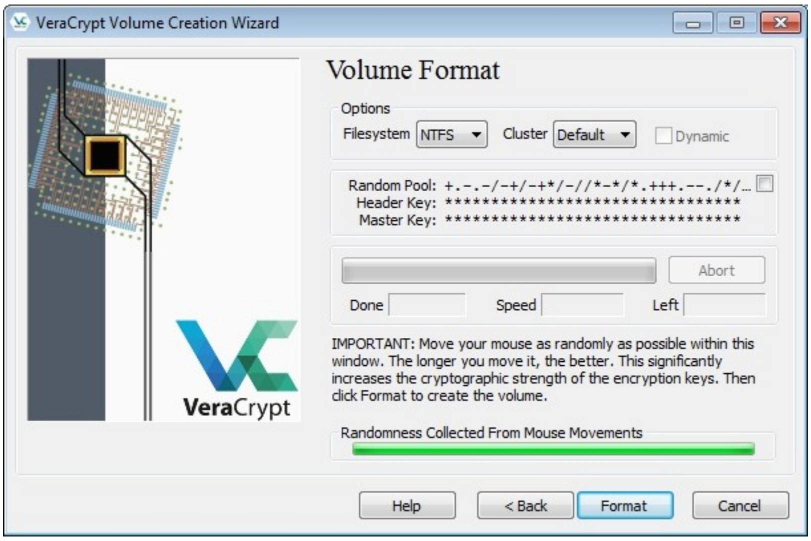
6. Select an appropriate hash algorithm using the drop-down menu - SHA-512 or Whirlpool is recommended. Press '*Next*'

7. Specify the maximum size of the file container:
   - To create a 500-megabyte container: enter '500' in the text box and ensure the 'MB' option is selected
   - To create a 4 gigabyte container (e.g. for writing to DVD), enter '2' in the text box and select the 'GB' option.

Press *NEXT* to move to the subsequent screen.

8. Choose a suitably strong password. General rules to follow include:
    - Use a password of 20 or more characters.
    - Use numbers to improve the password security, e.g. abc123, abc2014.
    - Do not use a single well-known word found in a dictionary. Instead, combine multiple words (e.g. “act-consortium-2014-project-data”) or create your own (actprojfiles2014).
    - Use a combination of upper and lowercase letters, e.g. Act-Consortium

9. The Volume Format menu will ask for information on the chosen format of your virtual drive.



VeraCrypt Volume Creation Wizard

Volume Format

Options

Filesystem NTFS 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

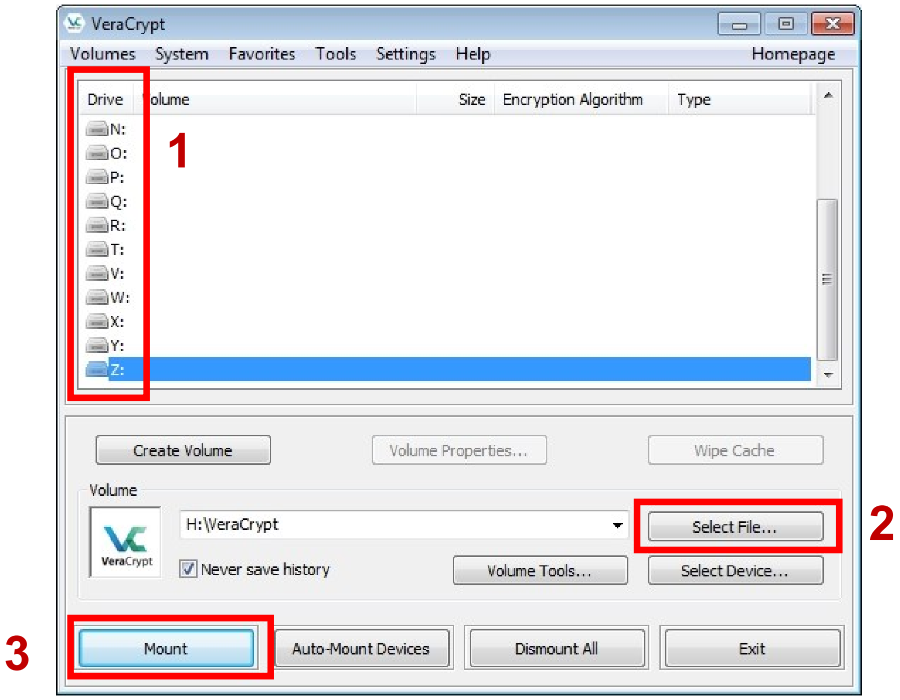
The Volume Format menu will ask for information on the chosen format of your virtual drive.

- Select the NTFS option if you are likely to create files over 2GB
- To save disk space, select the dynamic checkbox. This will create a dynamic container file that will start small, but grow when files are added/updated. This has the benefit of saving disk space (avoiding the possibility that a 2GB container will contain only 50MB of files). However, file access to dynamic containers is noticeably slower in comparison to non-dynamic files.
- The ‘Cluster’ drop-down menu may be left in its default position.

Click *FORMAT*.

10. A ‘Volume Created’ message will appear once the virtual disk has been created. You now have the option to:
    - Create a second encrypted volume by pressing ‘NEXT’
    - Close the Wizard interface by pressing ‘EXIT’.

Access an existing encrypted file container



Volume: H:\VeraCrypt

☑ Never save history

Perform the following to access your encrypted file container:

1. Select a drive letter from the list (a in the above diagram). This will be the drive to which the VeraCrypt container will be assigned.

2. Click SELECT FILE (2) and locate your VeraCrypt file. Once chosen, the path and filename should appear in the Volume menu.

3. Click the 'Mount button (3).

4. You should now be prompted to enter an access password.

    - Click the 'Display password' box to see your password as you enter it
    - VeraCrypt is configured to auto-detect the PRF algorithm by default. If your encrypted file is not recognised, you may need to select your chosen option from the drop-down list.

    The 'Mount Options' menu contains various configuration settings. For example, mount the volume as read-only if you do not wish to change files.

5. Finally, confirm that the file container has been mounted in Windows Explorer.

To protect your encrypted data:

- **Only mount the file container as a virtual drive when you're working on it. Once you've finished, remove the mapped drive by selecting it and pressing the DISMOUNT button.**
- **Do not store the password in the same location as the encrypted file.**