Protecting data

Many forms of data are sensitive and unauthorised access must be prohibited. Access to local machines (your office computer) is usually protected both physically and electronically. A concern can be expressed with removable media. USB sticks can be physically lost or stolen and so the information in there needs to be protected.

Access protection can be software-based (encryption) or hardware-based (finger print scanner). In this how-to, we will show you how to software encrypt a whole partition in a USB flash drive so as to protect access to the data on the partition. We will be using a software called VeraCrypt v1.24 that can encrypt files, folders and whole partitions of storage devices.

Obtaining the software

VeraCrypt is open source software freely available. Visit https://www.veracrypt.fr/en/Home.html and you can download either installation of the software or even download a portable version. In this how-to, we have used a portable version.

Encrypting a partition.

A USB flash drive includes a partition using the drive letter Z. We want to encrypt this partition. Here are the steps to follow

1. Start VeraCrypt
2. You can start the wizard for encrypting a partition by using the 'Volumes' menu and selecting command 'Create new volume'.
3. The wizard starts, select 'Encrypt a non-system partition / drive' and click next
4. Select 'Standard VeraCrypt volume and click next
5. Click 'Select device', select the Z drive from the USB flash, and click next

Depending on the status of the partition

- *If the partition has no data (is empty) then select 'Create encrypted volume and format it'.*
- *If the partition has data then select 'Encrypt partition in place*

For this how-to we will use an empty drive so…

6. Select 'Create encrypted volume and format it' and click next
7. The wizard allows for configuration of the encryption algorithm, click next
8. The wizard confirms the size of the partition, click next

9. The wizard prompts for the password to use. Enter the password twice to confirm and click next

The software uses a variety of factors to strengthen the encryption. In addition to the password, random factors like the time, the location, other system parameters as well as the random movement of the mouse pointer are used.

10. The next screen allows the user to randomly move the mouse pointer and in this manner strengthen the cryptographic encryption. Move your cursor as random as possible and once the bar at the bottom fills-up click the 'Format' button
11. Once the format is complete (it might take a few minutes), a dialog comes up to remind you that since the original letter of the partition is Z, when you mount the encrypted drive you must not use the letter Z. Click ok.
12. The partition is now encrypted.

Once a partition is encrypted, the drive is inaccessible unless it is mounted by VeraCrypt.

Mounting an encrypted partition

1. Start VeraCrypt
2. Use the 'Select device' button and select the encrypted (Z:) drive
3. Use the listing above and select a drive letter to mount to (anything except Z:). Say that you select letter V:
4. Click 'Mount'
5. The program prompts you for the encryption password and click 'OK'
6. VeraCrypt will perform the mounting.

You can now use drive V: as normal and store any information you want on it.

<u>NOTE</u>: Remember to use VeraCrypt and unmount the drive before you remove the flash drive from the machine. This you can do by clicking the 'Dismount all' button at the bottom of the interface.

Decrypting an encrypted partition

1. Start VeraCrypt

2. Use the 'Select device' button and select the encrypted drive
3. Use the 'Volumes' menu and select command 'Permanently Decrypt'
4. Enter the encryption password and click next
5. VeraCrypt will perform some operations
6. The wizard switches to a dialog to start decrypting, click 'Decrypt'
7. Decryption starts and in a few minutes a dialog confirm the completion of the operation. Click OK
8. Click 'Finish' on the wizard
9. Click 'Exit' to exit VeraCrypt.

The Z drive is no longer encrypted.

VeraCrypt is available for Windows, MacOS, Linux, and FreeBSD