Ways to set USB passwords for data protection

USB is small, compact, portable storage devices and users can read on any device that supports USB port. Because of these features, USB becomes one of the perfect data transfer and storage devices among computers.

USB is small, compact, portable storage devices and users can read on any device that supports USB port. Because of these features, USB becomes one of the perfect data transfer and storage devices among computers.

However, the drawback is that data stored on USB is easily lost, especially important data. Therefore protecting USB data is quite important. In the following article, the network administrator will guide you how to set a password to protect important data in your USB.

Ways to set a USB password to protect data

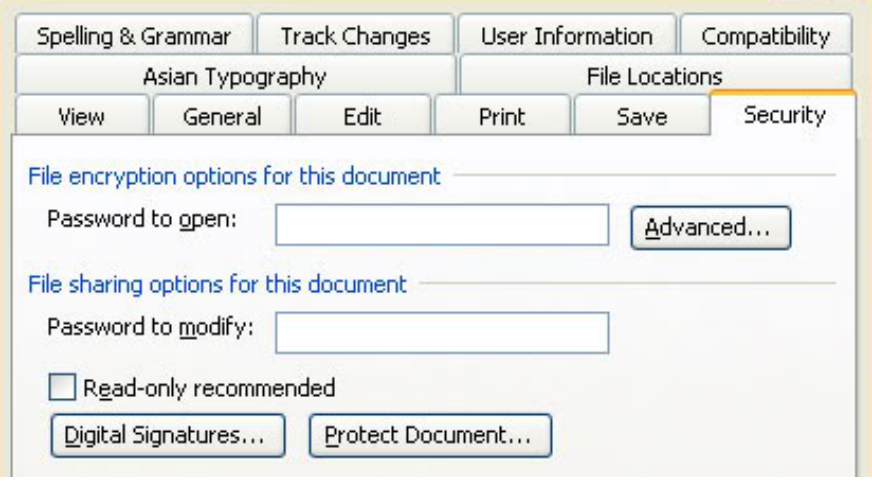
1. 1. Traditional method: save files with password
2. 2. Create a secure encrypted partition with Rohos Mini Drive
3. 3. Lock USB Flash drive with USB Safeguard
4. 4. Set password protection USB with BitLock
5. 5. Set USB protection password with Wondershare
6. 6. Set the password to protect the USB with DiskCrytor
7. 7. Set password to protect USB by Kakasoft USB Security
8. 8. Other USB password protection software
    1. 1. Rohos Disk Encryption
    2. 2. USB Flash Security
    3. 3. StorageCrypt
    4. 4. VeraCrypt
    5. 5. Gili USB Stick Encryption

1. Traditional method: save files with password

In order to protect the data in USB safe, users will have to use the encryption function for each file and folder one. However, if the USB has a lot of data, the encryption will take a lot of time. So if you are 'afraid' of having to encrypt the entire directory, you can use the password encryption function built into applications or programs to encrypt important files. there.

Quite a number of programs, including Word and Excel, allow users to save password attachments. For example, in Word, while the document is open, go to **Tools** => **Options** and switch to the **Security tab** . Next enter a password in the **Password to open box** , then click **OK** , re-enter the password again when requested. Finally save your document and don't forget the password you set.

Details: Set password to protect and encrypt documents in Office 2013



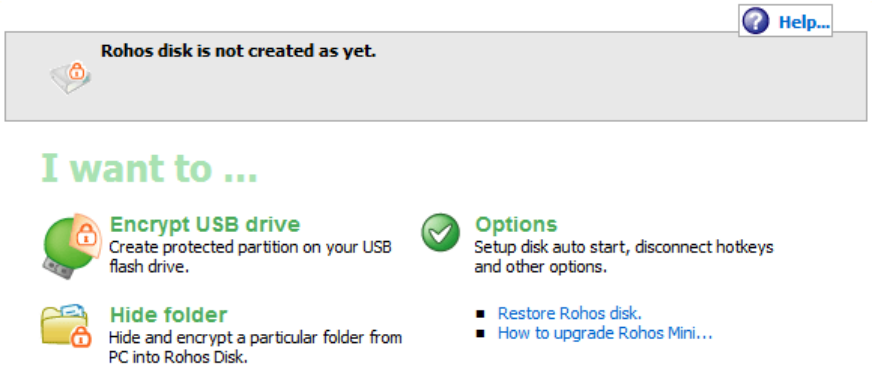
2. Create a secure encrypted partition with Rohos Mini Drive

There are many tools you can use to encrypt and set up your data protection password. However, most tools require Admin permissions to run on the computer.

This means that security tools will not be a viable solution in case if you need to securely transfer data to a computer that you do not have Admin rights to.

Rohos Mini Drive is one of the tools that can help you encrypt data protection without having or without Admin rights. The free version can create a hidden partition, encrypted and password protected partition that can protect 2 GB of data on your USB.

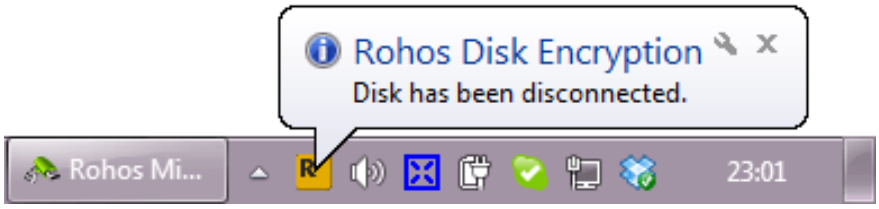
This tool uses automatic on-the-fly encryption (on-the-fly encryption) with 256-bit AES encryption technology. Rohos Mini Drive will be installed directly on your USB, no encryption driver must be available on different systems. So all your data can be transferred to this encrypted partition and you can access it anywhere you want.



After creating the password protection and encryption partition on the USB, you can open it by clicking on the **Rohos Mini.exe** icon from the root directory.

After entering the password, the Rohos drive will be mounted and accessed via Computer, from which you can access the data on the secure partition and transfer data between the computer and this secure partition.

To close the Rohos partition, right-click the Rohos icon under the system tray and select **Disconnect** .



1. Download Rohos Mini Drive to your device and install it here.

3. Lock USB Flash with USB Safeguard

Like Rohos Mini Drive, USB Safeguard is a portable application that runs directly from USB and therefore users do not need to have Admin rights on the computer. Utility uses AES 256 bit encryption technology, free USB limited version with a maximum size of 2 GB.

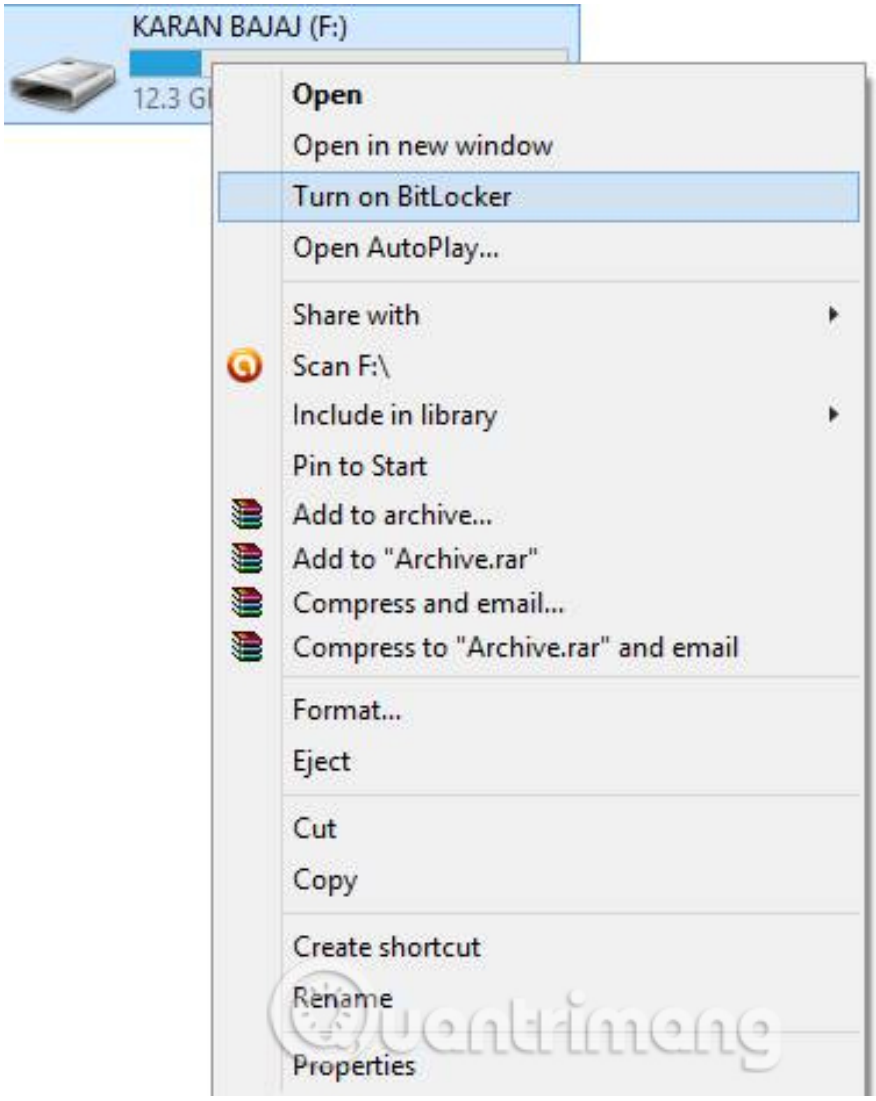
To use USB Safeguard, after downloading the tool, proceed to copy the file **usbsafeguard.exe** to your USB. Then run the file **usbsafeguard.exe** from USB, then enter a password to lock the USB. To unlock it, rerun the **usbsafeguard.exe** file again, then enter the unlock password.

This means you can change your password every time you use USB Safeguard.

1. Download USB Safeguard to your device and install it here.

4. Set password protection USB with BitLock

Step 1. First, plug USB Pendrive into your computer, then click on USB and select **Turn on BitLocker** .



Step 2 . Now click **Use password to protect the drive** , enter the password you want to place in both password fields.

Step 3. Now click on **Next** until printing or save the key for later reference.

Step 4. Now the encryption process will start and your USB will be secured with the password set in the previous step.

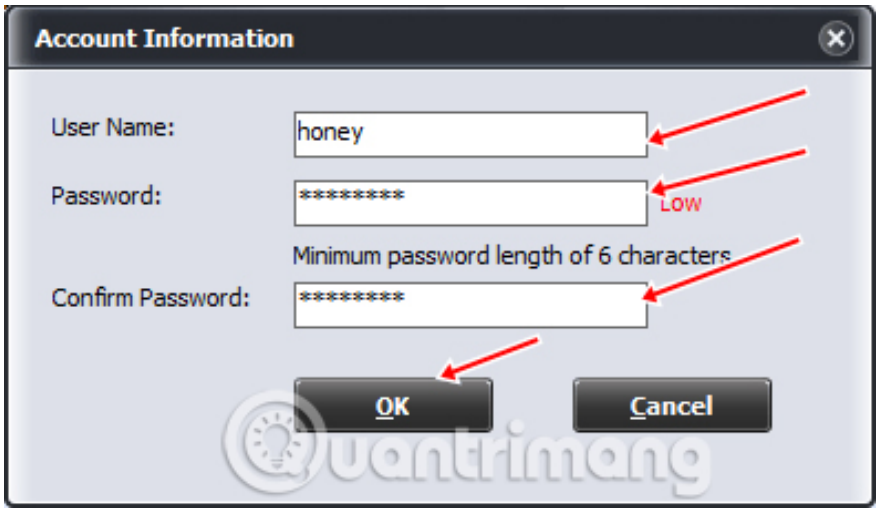
1. How to use Bitlocker to encrypt data on Windows 10 (Part 1)

5. Set USB protection password with Wondershare

Step 1. First of all download and install Wondershare USB Drive Encryption.

Step 2. After installing, open the software and plug the USB into the computer. Select the drive in the program and the security level, then click the **Install** button.

Step 3. Enter the username and password for USB Pendrive.



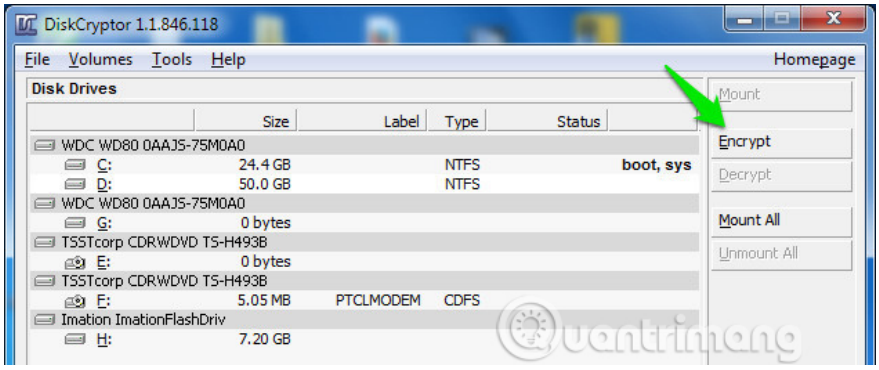
Then, click **OK** so you have completed the steps to protect USB Pendrive with your password and username.

6. Set the password to protect the USB with DiskCrytor

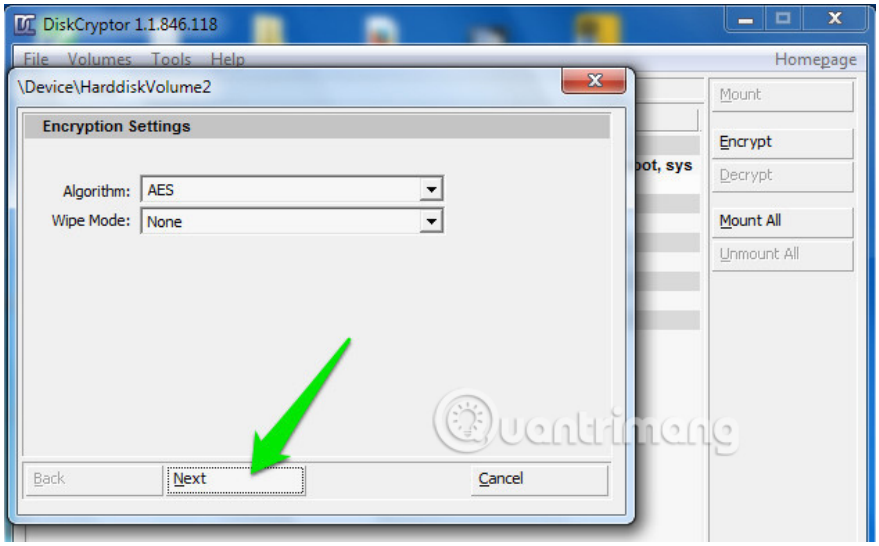
DiskCryptor is an open encryption solution, providing encryption for all disk partitions, including system partitions.

1. Create data security partition on USB

Step 1 . Download and install DiskCryptor, then click on USB and from this interface click **Encrypt** .

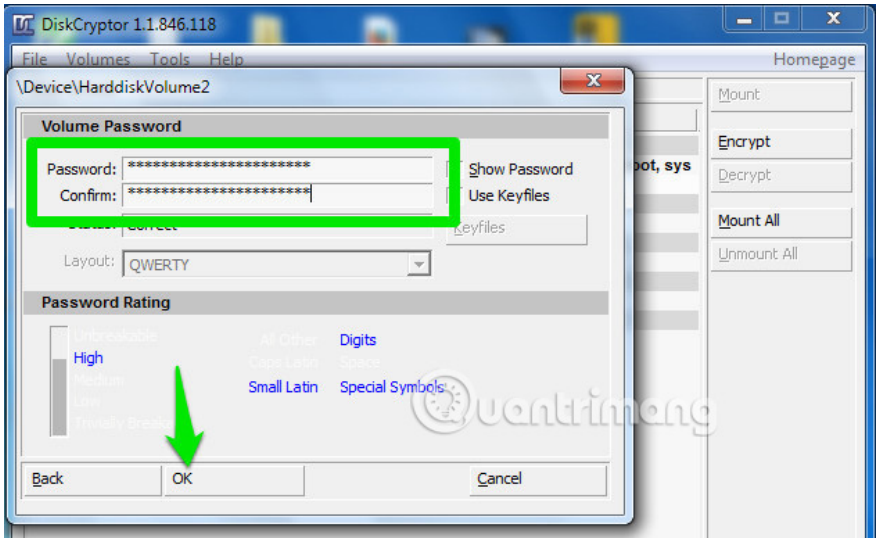


Step 2. A window will appear and ask you to select the encryption process. Leave the default settings and do not change anything unless you know for sure what you do, then just click **Next** .

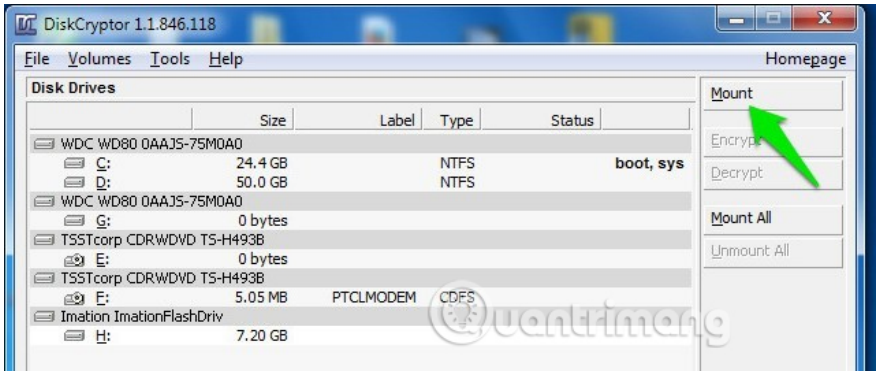


Step 3. On the next window, enter and confirm the password. You should set a strong password then click **OK** to start the encryption process.

1. How to check password strength



Step 4. After the encryption process is complete, click on USB and then ' **Mount** '.

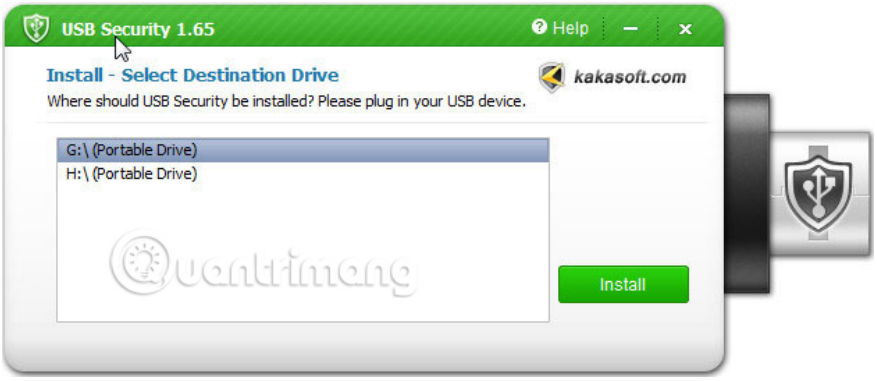


So now if someone wants to open your USB, they will have to enter the password to know the contents.

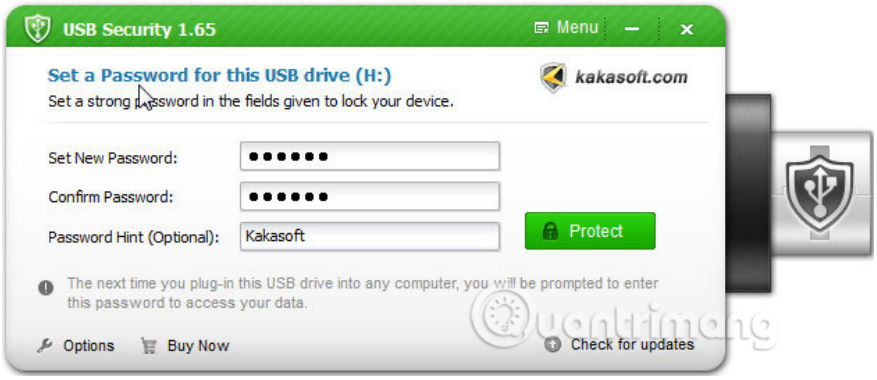
7. Set password to protect USB by Kakasoft USB Security

Kakasoft USB Security is one of the best tools used to protect USB Pendrive on Windows computers. This small tool will help prevent any unauthorized access to files on your USB.

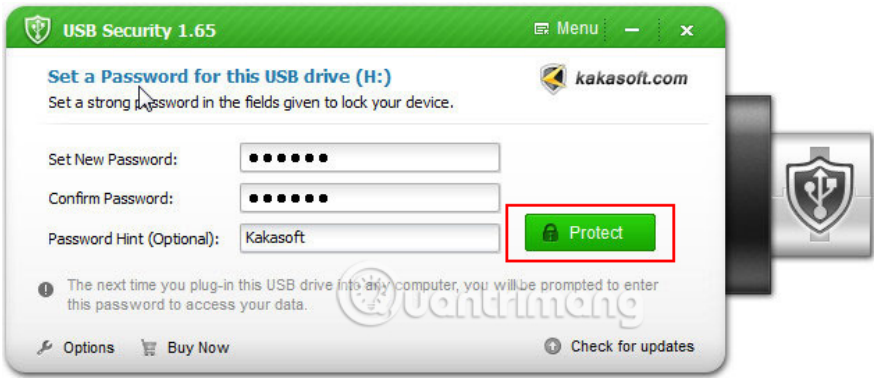
Step 1. First of all, you need to plug USB Pendrive into the computer and then double-click Kakasoft USB Security and install it normally.



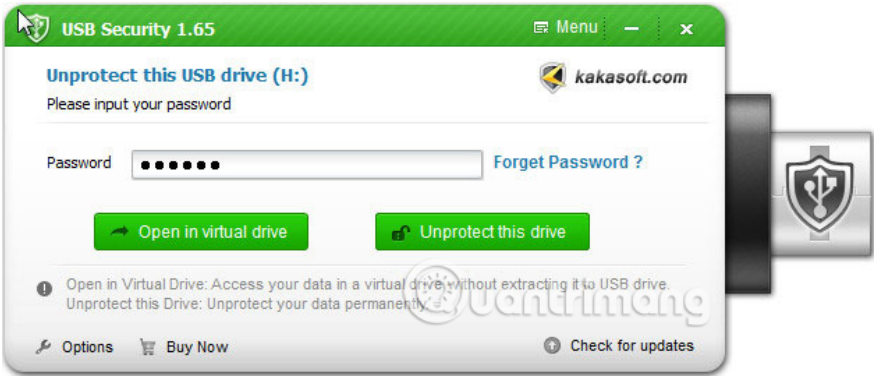
Step 2. Now to create a password to protect USB Pendrive, you need to open the USB and run the **USBSecurity.exe** file and enter the password.



Step 3. Confirm the password and then click ' **Protect** '.



Now whenever you open Pendrive, you will see an interface like the one below. Here you need to enter the password to continue.



8. Other USB password protection software

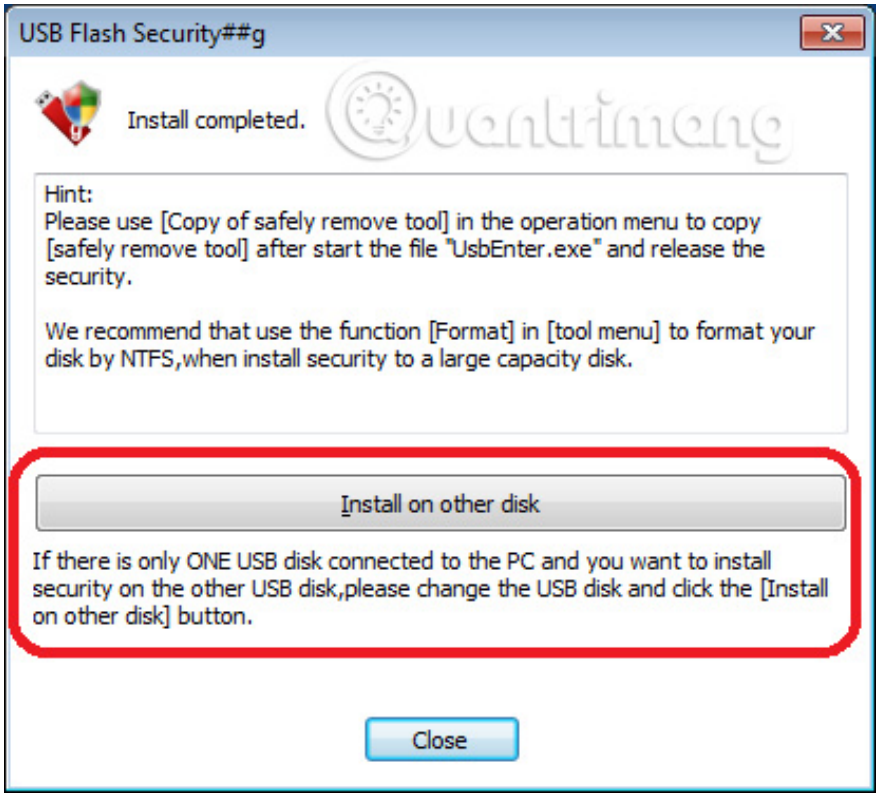
Here are some other software with similar functions, create a password to protect USB. If you don't like the software, you can choose one of these.

1. Rohos Disk Encryption

Rohos Disk Encryption is capable of creating protected and hidden partitions on your computer or USB flash drive; Create passwords that protect or block access to your Internet applications. Rohos Disk uses AES encryption which is approved by NIST and its encryption length is 265 bits, automatic and online encryption.

Download : Rohos Disk Encryption

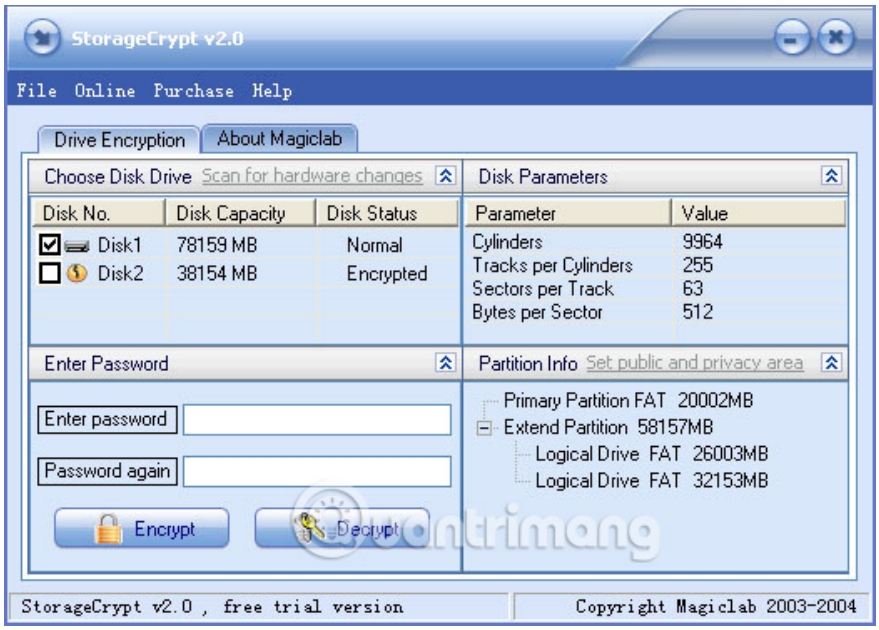
2. USB Flash Security



USB Flash Security is a security software that protects data in USB Flash with passwords and encryption functions (AES256). This is a lightweight but effective application.

Download : USB Flash Security

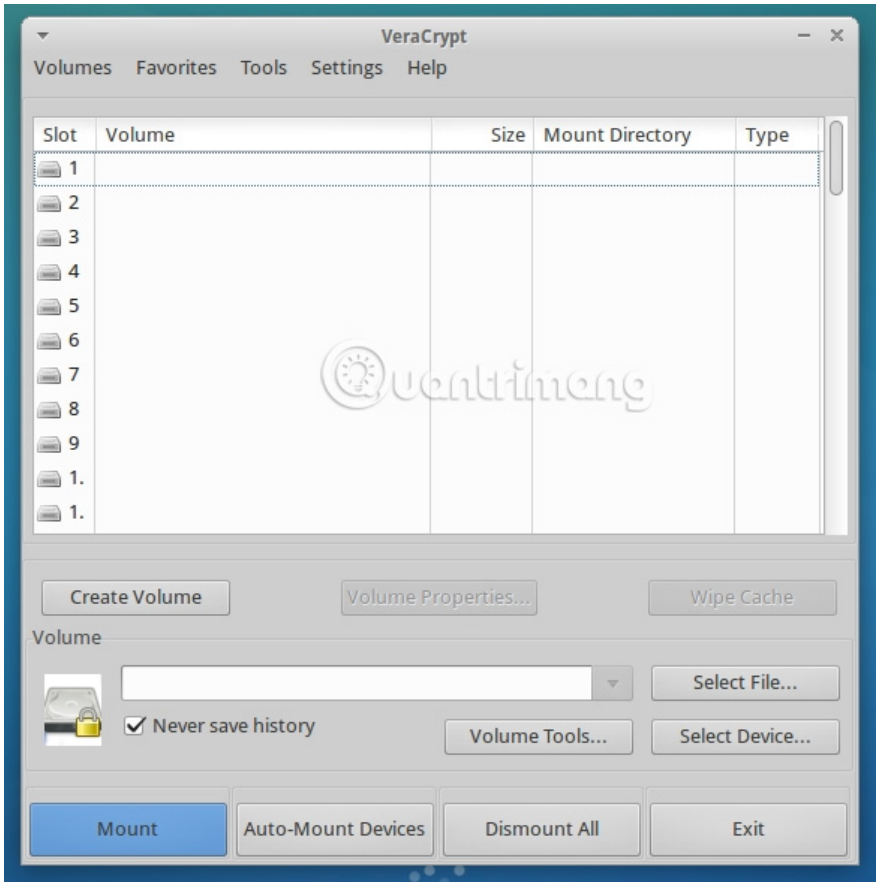
3. StorageCrypt



StorageCrypt allows you to encrypt and create password-protected removable drives like USB, eSATA drives, firewire drives, flash cards, PCMCIA drives and many other drives. The software uses 128 bit AES encryption for maximum security and user password length of up to 50 characters.

Download : StorageCrypt

4. VeraCrypt



VeraCrypt is a free encryption software that effectively protects your data. This tool can encrypt hard drives, USB and many other drives. It comes with many advanced features such as creating disk volume lock password.

1. Instructions for USB encryption with VeraCrypt

Download : VeraCrypt

5. Gili USB Stick Encryption

This is another free encryption tool available for extremely efficient Windows operating system. This tool helps users encrypt the USB quickly.

Download : Gili USB Stick Encryption

Refer to some of the following articles:

1. How to speed up the process of copying and moving data on USB drives
1. Using USB to lock or unlock Windows computer, have you tried it or not?
1. 4 ways to fix USB errors without formatting: 'Windows was unable to complete the format'

Good luck!

You finished reading the article "**Ways to set USB passwords for data protection**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
