How to enable Full-Disk Encryption on Windows 10?

On Windows 10, some use encryption by default, but some do not. In the following article, Network Administrator will show you how to check if the memory on Windows 10 computer is encrypted.

On Windows 10 operating systems, some use encryption by default, but some do not. In the following article, Network Administrator will show you how to check if the memory on Windows 10 computer is encrypted.

Sometimes encryption plays a rather important role, enabling you to protect your "sensitive" data from being used by other users and unauthorized access.

Unlike other modern operating systems - macOS, Chrome OS, iOS and Android, on Windows 10 Microsoft has not yet integrated encryption tools for users. If you want to use it, you will have to pay a decent fee to buy Windows 10 Pro version or use 3rd party encryption tools.

1. If your computer supports: Windows Device Encryption

On many new Windows 10 computers are automatically enabled features called Device Encryption. This feature was first introduced and integrated on Windows 8.1, and has some specific hardware requirements. Not all computers will have this feature integrated, but some will.

There are also a few other limitations you should keep in mind: this feature only really encrypts your drive when you sign in to Windows with your Microsoft account. After that, your Recovery Key will be uploaded to Microsoft's server.

This helps you recover your files even if you are not logged in to the computer. This is why the FBI is not too worried about this feature. But this feature is recommended to encrypt data on computers and laptops to protect

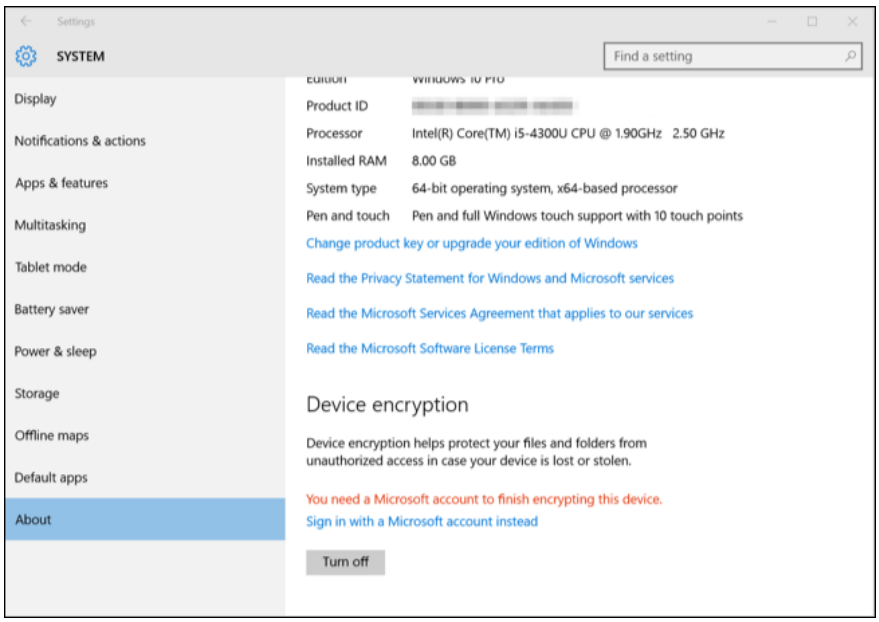
your data from "thieves" only.

If you're worried about NSA, you can use other encryption solutions.

Device Encryption is also enabled if you log in to the domain (domain) of the organization (.org or organization). For example, you can log into a domain (domain) of your business or school. Your Recovery Key will be uploaded to the server of the organization domain.

However, this method does not apply to "intermediate" computers but only domain computers (domain).

To check if Device Encryption is enabled, open the **Settings** application, then navigate to **System** => **About** , and find the setting called **Device Encryption** in the bottom corner of the About window. If you do not see any information about Device Encryption here, it means that your computer does not support Device Encryption and the feature is not enabled.



If Device Encryption is enabled or if you activate with your Microsoft account, you will see a message there.

2. For Windows Pro users: BitLocker

If Device Encryption is not enabled or if you want to use a more "strong" encryption solution to encrypt USB removable hard drives, you can use BitLocker.

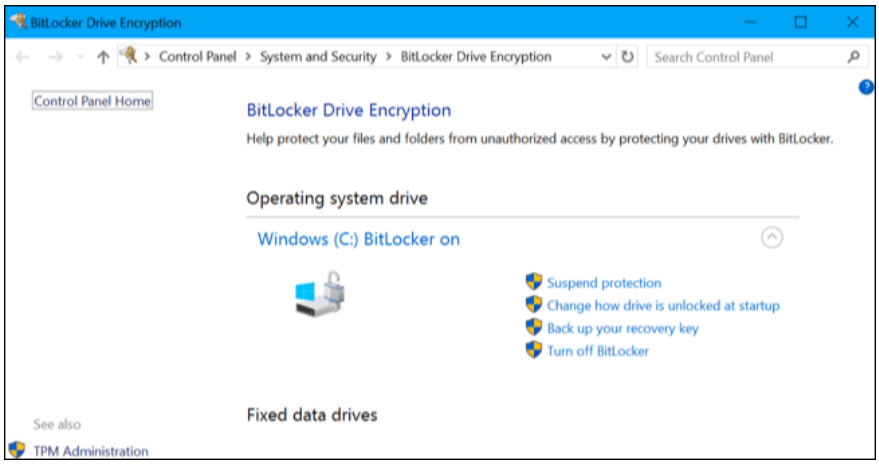
Also, readers can refer to what BitLocker is and how BitLocker and EFS differ here.

Microsoft BitLocker encryption tool is part of Windows and is integrated on many current versions. However, Microsoft still restricts BitLocker on Professional, Enterprise, and Education versions of Windows 10.

BitLocker is the safest solution for your computer, the tool that contains Trusted Platform Module (TPM) - integrated on modern computers. You can quickly check whether your computer has a Trusted Platform Module (TPM) right on Windows, or you can check your computer manufacturer if you are unsure.

Windows often says that BitLocker requires TPM, but you can activate BitLocker without TMP by using the hidden option. To do this you will have to use a USB Flash drive as a "Startup Key" to boot every time you activate this option.

If you're using Windows 10 Pro, BitLocker is built into the system, you can search BitLocker by entering the **BitLocker** keyword into the **Search** box on the Start Menu and then press **Enter** and use the BitLocker Control Panel to activate the tool. tools.



If you don't use Windows 10 Pro, you'll have to pay a fee, which is about $ 99 to upgrade Windows 10 Home version to Windows 10 Pro version. Just open the **Settings** app, then navigate to **Update & security** => **Activation** and click the **Go to Store** button.

You will have to assign permissions for BitLocker and other features available in Windows 10 Pro version.

3. Other options: VeraCrypt

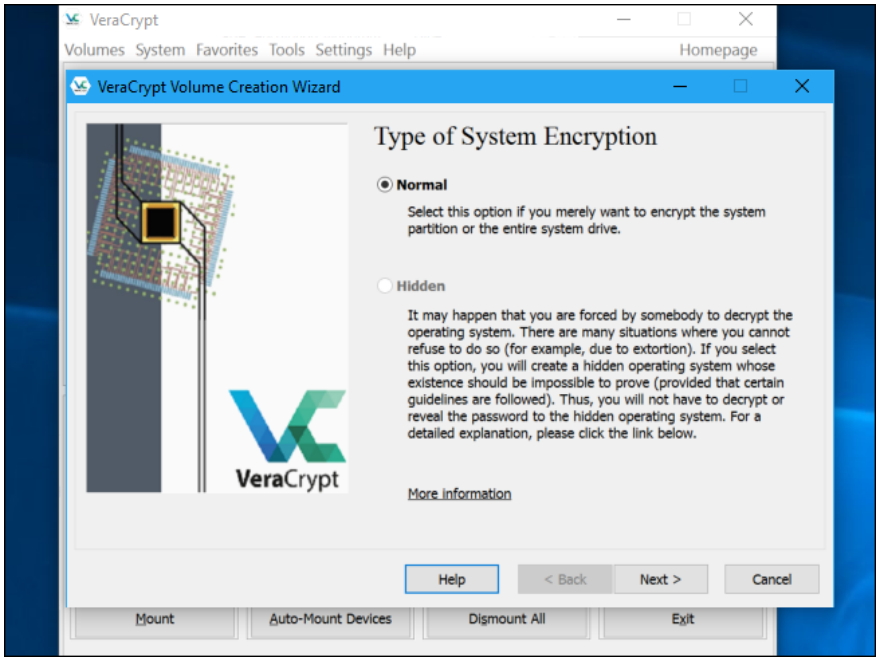
BitLocker is not the only option, so if you don't want to spend a lot of money to use BitLocker, you can use other encryption tools instead.

TrueCrypt is an open source encryption tool that you can use to replace BitLocker. Although it was developed not long ago, TrueCrypt has a few drawbacks: it cannot encrypt the GPT system partition and uses UEFI to boot.

Download TrueCrypt to your computer and install it here.

VeraCrypt is another open source encryption tool developed based on TrueCrypt code. This tool supports encoding EFI system partitions on versions 1.18a and 1.19. In other words, VeraCrypt allows you to encrypt the Windows 10 computer system partition for free.

Download VeraCrypt to your device and install it here.



In terms of security, VeraCrypt is better than TrueCrypt. Therefore, if you intend to encrypt some files or the entire system partition, Network Administrator recommends using VeraCrypt.

Refer to some of the following articles:

1. Instructions for using EFS to encrypt files and folders on Windows 8.1 Pro

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

1. How to use Bitlocker to encrypt data on Windows 10 (The last part)

Good luck!

You finished reading the article "**How to enable Full-Disk Encryption on Windows 10?**" 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.
