How are BitLocker and EFS different?

On Windows 10, 8.1, 8, and 7 integrated BitLocker drive encryption. However, this is not the only encryption solution. Windows also provides another encryption solution called file system encryption (encrypting file system - EFS).

On Windows 10, 8.1, 8, and 7 integrated BitLocker drive encryption. However, this is not the only encryption solution. Windows also provides another encryption solution called file system encryption (encrypting file system - EFS).

So how is BitLocker and EFS different? EFS is only available on Windows Professional and Enterprise versions.

Windows Home versions can only use the "device encryption" feature and only if this feature is enabled on your computer.

1. BitLocker is Full Disk Encryption (full disk encryption)

BitLocker is the solution to encrypt your entire drive.

When setting up BitLocker, you'll encrypt an entire partition - like a Windows system partition, a partition on an internal drive, or even a partition on a USB flash drive .

You can encrypt some files with BitLocker by creating a file that contains encryption.

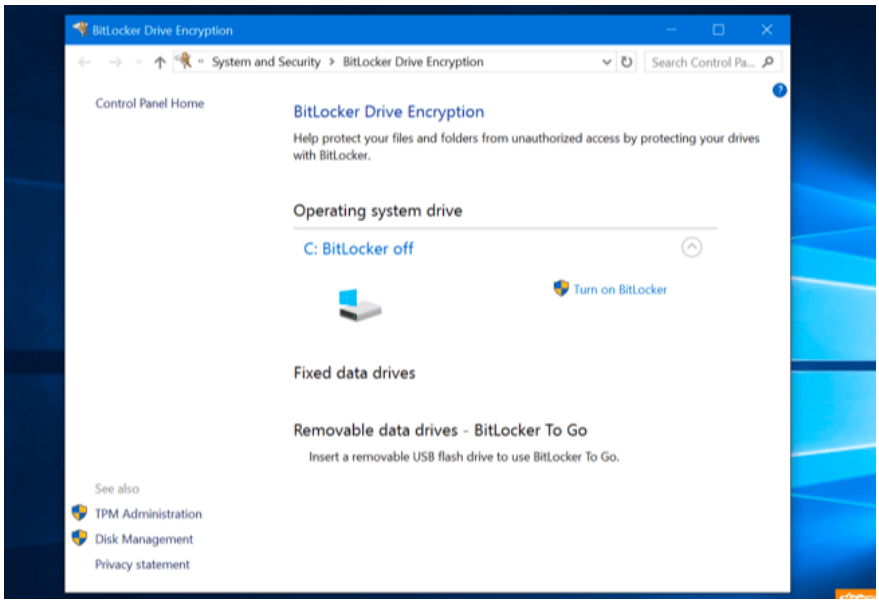
Basically the file containing this encryption is a virtual hard disk (virtual disk or disk image). BitLocker will work by working with the virtual hard drive and encrypting all that is in the virtual hard drive.

If you want to encrypt your hard drive to protect sensitive data from falling into the wrong hands, especially if your laptop is stolen, BitLocker is the first choice.

BitLocker encrypts the entire drive so you don't need to worry about which files are encrypted and which files are not encrypted. Your entire system will be encrypted.

Encryption is not dependent on user accounts. When an Admin activates BitLocker, files on other user accounts on the computer will be encrypted.

On Windows 10 and 8.1, drive encryption is somewhat more restrictive, because it only encrypts the entire drive without encrypting individual files on it.



2. EFS encrypts individual files

Instead of encrypting your entire drive, you can use EFS to encrypt files and folders separately.

While the cker feature is "set and forget it", EFS requires you to select the files you want to encrypt and change the settings.

To select the files you want to encrypt, on the File Explorer door, select a folder or personal file, then open the Properties window. In the Attributes option, select Advanced, then activate the "Encrypt contents to secure data" option.

This encryption is based on each user. You can only access encrypted files with a specific user account that has encrypted those files.

When you log in to the encrypted user account files, you can access the files without having to confirm any additional information.

If you log in with another account, you cannot access the files.

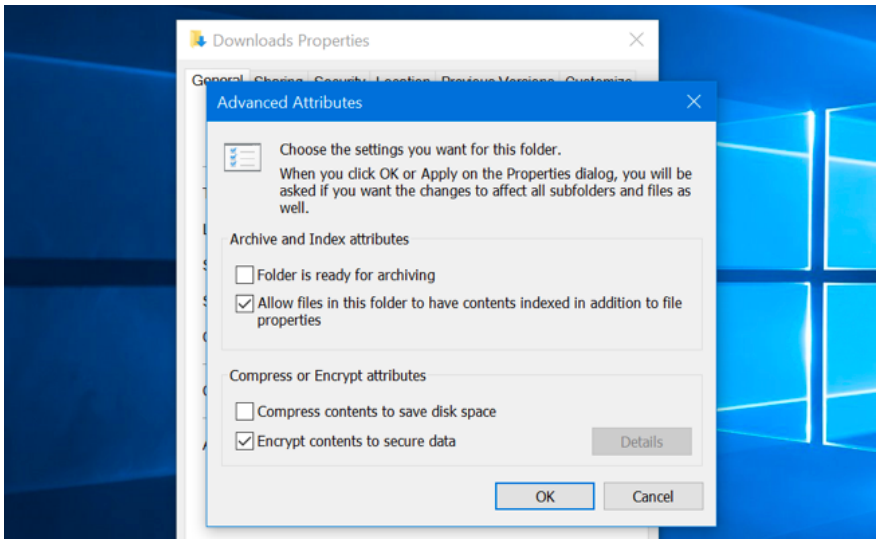
Encryption keys are stored in its operating system and almost never use TPM hardware on your computer. However, these keys can be hacked by hackers.

EFS does not encrypt the entire drive but only encrypts individual files, so the files on a particular system will not be protected.

Also encrypted files can be "leaked" to unencrypted areas.

For example, if a program creates a temporary cache file after you open an encrypted document using EFS, sensitive information, cache files and sensitive data of that document will be saved. Store in another unencrypted folder.

Essentially BitLocker is a Windows feature that encrypts the entire drive, and EFS loses points in protecting NTFS file systems.



3. Why use BitLocker without using EFS?

In fact, you can still use both BitLocker and EFS at the same time, because they are two different encryption classes.

You can encrypt your entire drive, and even after you've finished encrypting the entire drive, you can activate the "Encrypt" attribute for files and folders.

However, it is recommended that you use BitLocker to encrypt the entire drive. It is not simply that you "set it and forget it", but you can activate it once and forget it. BitLocker is also a much safer solution than EFS.

This is also the reason EFS is not mentioned in Windows encryption solutions.

Why does EFS exist? The reason is simple, because EFS is an old feature of Windows.

BitLocker was introduced since Windows Vista, while EFS was introduced since Windows 2000.

Refer to some of the following articles:

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

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

3. Instructions for encrypting USB or memory cards with Bitlocker on Windows 10

Having fun!

You finished reading the article "**How are BitLocker and EFS different?**" 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.
