What is Mac OS X FileVault and how to use it?

In fact, a password only prevents someone from trying to log in and access the operating system, but your hard drive is not encrypted like that. With an Ubuntu boot disk, or by removing the hard drive, everyone will still be able to access all the files on your computer. Only by manually encrypting files on your hard drive can you really keep your files safe. That's why Mac OS X FileVault appears.

You can feel safe when you have set a password on your Mac OS X account, but the truth is that it is only formal and only works to prevent people from having temporary access to it. your computer. It is only useful in case you leave your computer at home, or go get drinks in the library, but someone with certain knowledge and a little time can still access your data.

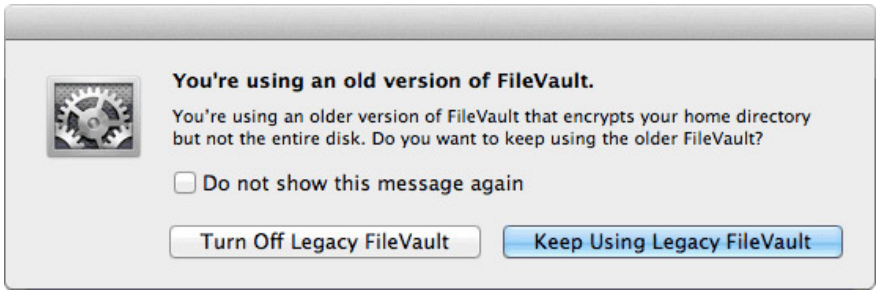
In fact, a password only prevents someone from trying to log in and access the operating system, but your hard drive is not encrypted like that. With an Ubuntu boot disk, or by removing the hard drive, everyone will still be able to access all the files on your computer.

Only by manually encrypting files on your hard drive can you really keep your files safe. That's why Mac OS X FileVault appears.

Mac OS X FileVault 1 and 2

FileVault is the technology that Apple provides to encrypt files on the hard drive. After encrypting those files with strong enough algorithms, these files cannot be accessed by any means. Mac OS X launched FileVault for the first time on Mac OS X Panther (10.3). Then FileVault only encrypts the personal folders of individual users in a large file using the encrypted string mode (CBC). Since Mac OS X Lion (10.7), FileVault 1 - now called Apple Legacy FileVault by Apple - has been replaced by FileVault 2.

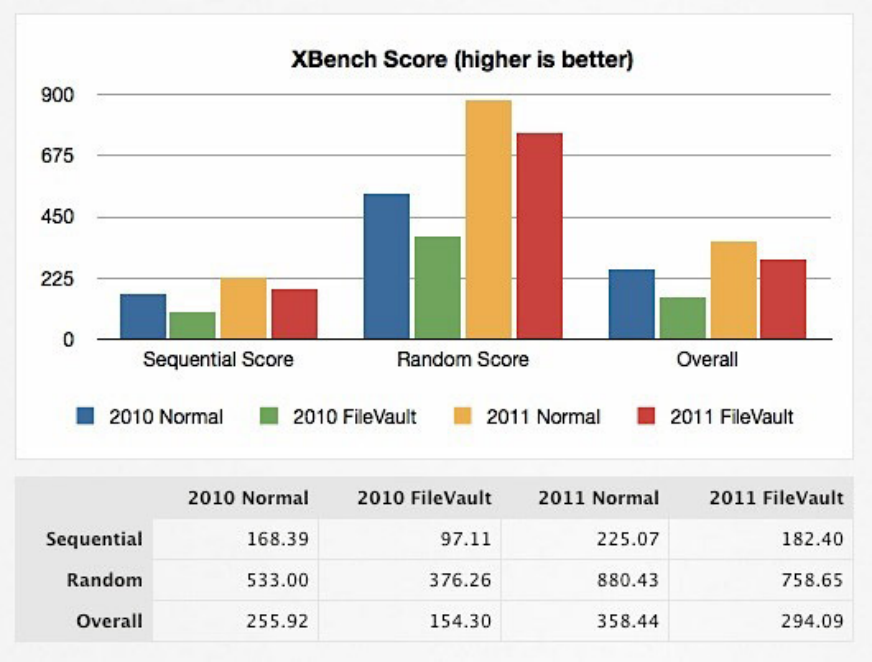
In contrast, FileVault 2 encrypts the entire boot disk in numerous smaller files. It also replaces today's unsafe CBC encryption with XTS-AES 128 mode and uses a more notable encryption algorithm. In short, it has a wider and safer scope. The full encryption of this drive has some additional security effects, which you can read below.



Legacy FileVault users will be notified of the difference if they access the FileVault options window in Mac OS X Lion version or later. You can switch to FileVault 2 by disabling the old FileVault file. Users of Mac OS X Lion or newer versions and those who start using FileVault by default, use FileVault 2.

Reduce performance

Because FileVault continuously decodes hard drive data, its use results in a loss of performance. Jason Discount from The Practice of Code put FileVault 2 into trial when Max OS X Lion debuted.



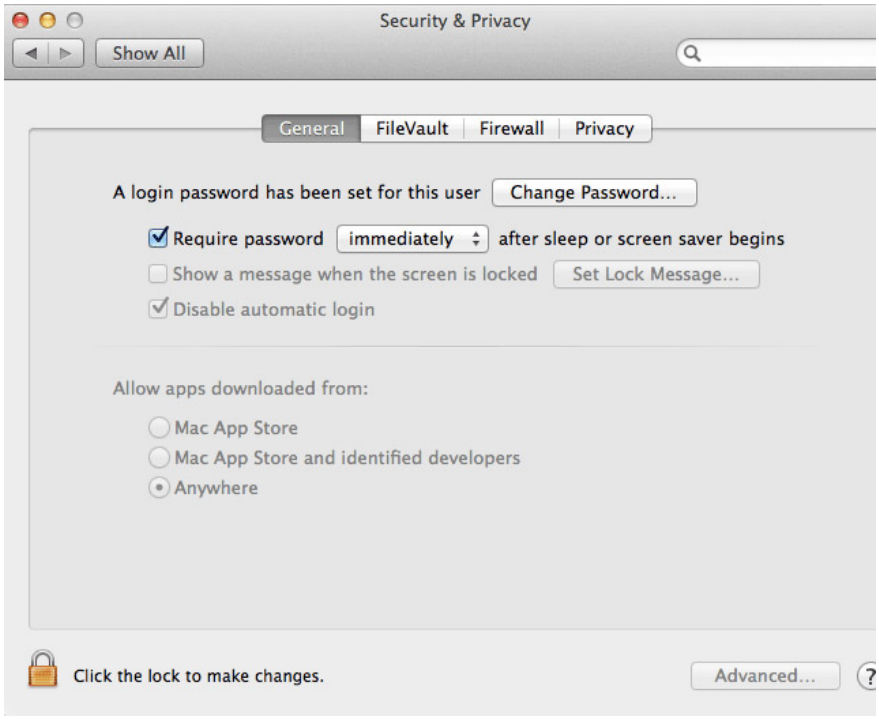
	2010 Normal	2010 FileVault	2011 Normal	2011 FileVault
Sequential	168.39	97.11	225.07	182.40
Random	533.00	376.26	880.43	758.65
Overall	255.92	154.30	358.44	294.09

These tests are done on the 2011 MacBook Air (from the time Lion launched). The hard drive I / O performance (SSD) averages about 18%. This is negligible, but SSD data transfer is still much faster than older hard drives. If you are using a normal hard drive. This performance reduction will be more noticeable. You should consider whether security benefits are really worth sacrificing performance.

Encrypt the entire drive and unlock the menu

As mentioned above, FileVault now encrypts the entire boot disk instead of the personal user's home directory. After booting, the entire drive is unlocked by logging in with an authorized user account. This has both positive and negative consequences.

On the positive side, there is no risk for incompatible applications. The entire drive is unlocked after logging in, so for applications running on the computer it seems that the drive is not encrypted. However, the drive is still unlocked until it is turned off. In other words, if a third party has access to your computer after the drive has been unlocked, they can theoretically still be able to access your data, even if you have logged out.



In addition to using FileVault, you should password protect your computer when it is not working. You can ask Mac OS X to request a password immediately after it is in Sleep mode or after the screen saver starts working, in **System Preferences> Security & Privacy> General** . Combined with Hot Corners, found in **System Preferences> Desktop & Screen Saver> Screen Saver> Hot Corners** , you can enable screen saver mode with a password if you need to leave the computer for a short time .

Note that although this additional security measure prevents a lot of intruders, it does not lock the hard drive, only completely shuts down the computer.

Boot Camp and special drive configuration

FileVault 2 relies on and expects to configure a standard Mac OS X drive: the volume starts Mac OS X with a Recovery partition. Recent Mac OS X installations come with this Recovery partition, but you can test it by trying the recovery boot. Reboot your Mac and hold **cmd + R** to boot Recovery immediately, or hold down the **Alt** key to list the available boot options. If for any reason, Recovery partition is no longer available on a Mac, you should not try to use FileVault. Doing so will fail and potentially lead to data loss.

Other non-standard drive settings, like advanced RAID configurations, face the same problem. Even if you use Boot Camp, compatibility is not guaranteed. Some people have successfully reported if they configured Boot Camp and installed all drivers before turning on FileVault, but note that compatibility is not guaranteed.

How to activate FileVault

Before starting, back up files on your Mac. Encrypting the entire drive is an extensive process and you never know when a problem might occur. In any case, backing up data is very important.

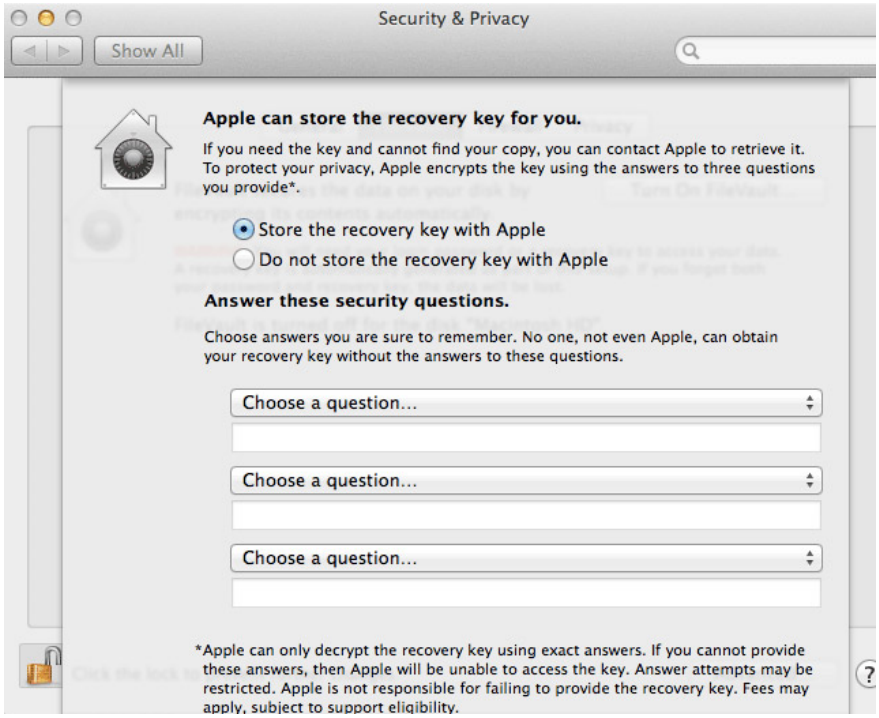
Open **System Preferences** , go to the **Security & Privacy section** and select the **FileVault** tab. Before you can change these settings, you need to unlock the control panel with your username and password. Click **Turn On FileVault .** to start the process. Note that enabling FileVault may take a while, because it needs to encrypt the entire drive. Depending on the size and type of drive, this can range from half an hour to a few hours.

If there are multiple user accounts on the same computer, you can choose which users can unlock the drive after booting. Authorized users will first have to unlock the drive after booting, before any unauthorized user can log in.

Next, you will be provided with a recovery key with a long number of digits. Write (or put it in a secure password manager like LastPass) and keep it carefully. If you forget your normal password, this will be a backup key. Without this recovery key, losing the password is equivalent to losing all data.

You can choose to save your recovery key with Apple. If you lose your key, you can contact Apple support and retrieve the key with security questions. You still need to be able to accurately reproduce the answer to your security question or Apple support staff will not be able to access your key. Retrieving this key is an additional feature, so it may be charged.

This is controversial. Finally, it is better to keep your key carefully. You may need this safety net in the future. In any case, you should carefully choose security questions, since they are often the weakest link in a secure network.



After that, the Mac will prompt you to restart the computer. After restarting, Mac OS X will start encrypting all data on the drive. You can continue to use your Mac in the meantime, but note that disk performance may be hampered.

After restarting, you can return to FileVault option to check the encryption process, along with the estimated completion time.

Have you used FileVault or any other security solution? Let us know in the comment section below!

See more:

1. 10 encryption tools for Mac
2. Create encrypted disk image to store sensitive data in Mac
3. Secure folders in Mac OS X Lion with a password

You finished reading the article "**What is Mac OS X FileVault and how to use it?**" 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.