Frequently Asks Questions (FAQs)

FileVault 2

What is **FileVault 2**?

FileVault 2 is a whole-disk encryption program that encrypts data on a Mac to prevent unauthorized access from anyone that does not have the decryption key or user's account credentials.

Why does **FileVault 2** matter?

Encryption of data at rest or stored on a disk is often the last resort to ensuring that data is protected against unauthorized access. The recent high-profile security breaches make it even more important to know about encryption programs such as FileVault 2.

Is **FileVault 2** available to all macOS users?

All MAC OS users can enable FileVault 2 to protect their data. Some users running more recent versions of OS X can also enable disk encryption, while others using older versions of OS X will only be able to utilize legacy FileVault, which encrypts just their home folder.

Apple's FileVault encryption program was initially introduced with OS X 10.3 (Panther), and it allowed for the encryption of a user's home folder only. Beginning with OS X 10.7 (Lion), Apple redesigned the encryption scheme and released it as FileVault 2—the program offers whole-disk encryption alongside newer, stronger encryption standards. FileVault 2 has been available to each version of OS X/macOS since 10.7; the legacy FileVault is still available in earlier versions of OS X.

What are the pros and cons to using **FileVault 2?**

Some of the **pros**:

- FileVault 2 supports legacy hardware, even for devices that are no longer officially supported by Apple.
- Deployment of FileVault 2 may be locally or centrally managed by users or the IT department.
- Whole-disk encryption works to safeguard all data stored on disk now and in the future.
- Backup of encrypted data works seamlessly with Time Machine to create automated backup sets.
- Disks encrypted with FileVault 2 must first be unlocked by user accounts that are "unlocked enabled"; these are typically accounts with administrative privilege, preventing non-admin accounts from accessing the disk's contents, regardless of the ACL permissions configured.
- FileVault 2 uses a strong form of block-cipher chain mode, XTS, based off the AES algorithm using 128-bit blocks and a 256-bit key.

Some of the **cons**:

- Legacy FileVault (or FileVault 1) does not encrypt the whole-disk—only the contents of a user's home folder. This affects legacy hardware that do not support the features in FileVault 2.
- Backing up encrypted data with Time Machine can only be done when a user is logged off of the session. For on-the-fly backups, the destination path must be a Time Machine Server, which requires macOS Server to perform online backups.
- The encryption passphrase used to encrypt the disk is the same as the end-user's password that enabled FileVault 2. If the password becomes compromised, the disk may be encrypted and data may be compromised.
- Enabling FileVault 2 can have a negative impact on I/O performance of approximately 20-30% of modern CPUs, and it noticeably worsens performance on older processor hardware.
- If the passphrase or recovery key must be changed, the entire volume will need to be decrypted and have the encryption process run again with the new key.
- Any device with FileVault 2 enabled must be unlocked by an admin credentialed account prior to being accessed or used by a non-admin account. If the device is not unlocked, non-admin accounts will not be able to use the computer until it is first successfully unlocked.
- Individual files, folders, or any other kind of data cannot be encrypted on the fly. Only data that resides on the local disk or FileVault 2-encrypted volumes may be encrypted in their entirety.

How can I get **FileVault 2**?

FileVault 2 is baked in to all versions of macOS and supported versions of OS X. The encryption program is turned off by default, though it's easy to enable.

Do I need to encrypt my computer using **FileVault 2**?

Currently, laptops and other portable storage devices (i.e. portable hard drives, USB memory sticks) that contain personal information requiring notification should be encrypted. If you want to use FileVault, please submit a Footprint ticket so that a technician can assist with the installation. Local IT policy may require additional safeguards to ensure that - should you leave San Antonio College, be unavailable, or forget your password - someone from Office of Technology Services and assist with accessing the important business files on the encrypted computer.

How does **FileVault** protect my data?

FileVault 2 is an encryption program created by Apple that provides full-disk encryption of the startup disk on a Mac computer. By utilizing the latest encryption algorithms and leveraging the power and efficiency of modern CPUs, the entire contents of the startup disk are encrypted, preventing all unauthorized access to the data stored on the disk; the only people that can access the data have the account credentials that enabled FileVault on the disk, or possess the master recovery key.

By enabling FileVault 2's whole-disk encryption, data is secured from prying eyes and all attempts to access this data (physically or over the network) will be met with prompts to authenticate or error messages stating the data cannot be accessed—even when attempting to access data backups, which FileVault 2 encrypts as well.

Does **FileVault** protect against malware?

FileVault offers no protection for malware (computer virus) infections. Users must maintain their operating system and practice good computing habits such as applying patches, security updates, creating strong passwords, and staying away from unknown links and untrusted web sites.

Does **FileVault** encrypt email or attachments?

FileVault does not encrypt email or attachments. Users must look to other tools for protecting data in transit.

Where is my recovery key stored?

It is highly recommended to store the recovery key to a secure location. Computers and/or laptops that are setup on the SAC domain will be stored centrally in our Active Directory (AD). The key can be recovered by calling the San Antonio College OTS (Office of Technology Services) helpdesk.

Is my computer protected when it is in sleep mode or when the screen saver is active?

Yes. FileVault on operating system drives in its basic configuration provides additional security for the hibernate mode.

Can I share my password with Desktop Support?

San Antonio College Office of Technology Services will have access to your workstation so you should not need to, and doing so may violate state laws that require you to protect personal information that is on your computer.

My computer is prompting me for the F**ileVault** Recovery Key. Where do find my **FileVault** Recovery Key?

If your computer is:

- Managed, on the SAC domain - The key is stored in San Antonio College Active Directory. Please call the Office of Technology Services Help desk to assist in obtaining your recovery key.

Can you encrypt a flash drive?

Yes,
Insert your USB flash drive into your Mac. When the icon appears on your desktop, right click on it and select Encrypt. You will then need to enter and confirm a password (as well as a password hint). Encryption should only take a few minutes; once complete, you USB flash drive will be fully protected.

Can **FileVault 2** encrypt more than just the operating system drive?

Yes.

Is there a noticeable performance impact when **FileVault** is enabled on a computer?

Generally it imposes a single-digit percentage performance overhead.