FileVault

FileVault

On this page:

Overview

FileVault is the native data encryption tool for macOS. FileVault uses a whole disk encryption schema similar to BitLocker (the native Windows encryption client). It is the recommended solution for enabling encryption on a Mac computer.

> ⚠️ **Before enabling FileVault**
>
> - Make sure your user account password is strong (tips on strong passwords). With FileVault, your user account password unlocks the encrypted disk.
> - Back up your data before you encrypt your computer, using a backup tool such as CrashPlan/Code42 or Apple's built-in Time Machine.
> - **Recommended for machines not in Jamf**: Save your recovery password using LastPass

How to Enable

Once you are ready to activate FileVault, follow these instructions in The Knowledge Base:

Managed machines

- Macs managed by Jamf

Stand alone machines

- Enable FileVault

Recovering a lost key

Depending on how your machine was encrypted, it may be possible to recover a lost decryption key. If the machine was encrypted manually then IS&T will not be able to recover it for you, but it is possible the key is stored in your personal iCloud account. If your machine is enrolled in Jamf Pro, then it is likely the key is escrowed there. Contact your IT Technician or the Service Desk at 617.253.1101, servicedesk@mit.edu, or by submitting a request online (http://ist.mit.edu/help).

See Also

The following Knowledge Base and Apple articles provide additional guidance for FileVault use and support:

- Enable FileVault and recovery keys
- Enable encryption on external media

- Disable FileVault
- Encryption Landing Page

Help

- Apple FileVault Support
- Users in need of further assistance can contact the Service Desk at 617.253.1101, servicedesk@mit.edu, or by submitting a request online (http://ist.mit.edu/help).