FileVault

Overview

FileVault is the native data encryption tool for OS X Mavericks (10.9) and later. 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

- PGP and Mac OS X users: IS&T recommends that users who handle sensitive data on Macs and use PGP for encryption switch to FileVault, the native encryption system on Macs. To make the switch from PGP to FileVault, first uninstall PGP.
- Make sure your user account password is strong (tips on strong passwords). With FileVault, your user account password unlocks the encrypted disk.
- Backup your data before you encrypt your computer with BitLocker, using a backup tool such as CrashPlan.
- Recommended for machines not in Casper: 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 Casper

Stand alone machines

- Enable FileVault

How to Use

- Recover Key: It depends how your machine was encrypted. If the machine was encrypted manually then IS&T will not be able to recover it for you. It is possible the key is stored in iCloud. If you are unsure how your machine was encrypted it is likely the key is escrowed in Casper. Contact your IT Technician or the Help Desk at 617.253.1101, helpdesk@mit.edu, or by submitting a request online (http://ist.mit.edu/help).
- Decrypt El Capitan drive:
- Decrypt Yosemite drive:
- Encrypt a Portable drive:

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

- Enable FileVault and recovery keys
- Enable FileVault on external disks
- Disable FileVault

Help

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