Learn About FileVault 2 (Encryption for Macs)
Stephanie Obodda - 2017-02-16 - 0 Comments - in Encryption

- What is FileVault 2?
- Who should be using FileVault 2?
- How can I obtain it?
- How do I use FileVault 2 to encrypt my laptop?
- What should I know about decryption?
- What restrictions are there when traveling outside of the country with an encrypted laptop?

Q. What is FileVault 2?
A. FileVault 2 is an integral security feature for Macs that allows you to encrypt the contents of your entire drive. It uses full disk, XTS-AES 128 encryption to help keep your data secure. FileVault 2 requires OS X Lion or later, and OS X Recovery installed on your startup drive.

Q. Who should be using FileVault 2?
A. ISG recommends that faculty and staff use FileVault on their laptops if they contain Brown Restricted Information (especially frequent travelers). Use Identity Finder to determine the presence of BRI. If detected, either remove it, or if necessary, encrypt it.

Q. How can I obtain it?
A. FileVault 2 is built into the OS X operating system. It is available from the Security & Privacy pane of System Preferences. Click the FileVault tab in the Security & Privacy pane to enable or disable FileVault.

Q. How do I use FileVault 2 to encrypt my laptop?
A. Detailed installation instructions can be found in the Apple document OS X: About FileVault 2.

Q. What should I know about decryption?
A. When you turn off FileVault, encryption is turned off and the contents of your disk are decrypted. The decrypting of your disk could take a while, depending on how much
information you have stored. However you can still use your computer to do other tasks while the decryption is occurring.

Q. What restrictions are there when traveling out of the country with an encrypted laptop?

A. U.S. federal regulations control the export of “encryption commodities, software and technology” (see Code of Federal Regulations, Title 15, Section 740.17). There are, however, license exceptions that allow you to take encrypted laptops with them, provided that they return within the year and “retain effective control and ownership.” This coverage is global except for a handful of embargoed and sanctioned countries designated by the U.S. government. Travel to any of these countries requires that you remove any encryption technology from your laptop before entering it.

In addition, as some countries ban or severely regulate the use of encryption, you should check country-specific information before traveling with an encrypted laptop. Following is a partial list of those countries. Check the U.S. State Department website before traveling to verify that the information is still current. In addition, any faculty, post-docs, graduate students and PI’s should check-in with OVPR, Insurance and Risk, and the Director of Information Technology Security before travelling overseas.

- Burma (you must apply for a license)
- Belarus (import and export of cryptography is restricted; you must apply for a license from the Ministry of Foreign Affairs or the State Centre for Information Security or the State Security Agency before entry)
- China (you must apply for a permit from the Beijing Office of State Encryption Administrative Bureau; travelers should also refrain from purchasing a replacement laptop when visiting China. It is known for intellectual espionage and such laptops could contain malware to steal content added to it.)
- Hungary (import controls)
- Iran (strict domestic controls)
- Israel (personal-use exemption – must present the password when requested to prove the encrypted data is personal)
- Morocco (stringent import, export and domestic controls enacted)
- Russia (you must apply for a license)
- Saudi Arabia (encryption is generally banned)
- Tunisia (import of cryptography is restricted)
- Ukraine (stringent import, export and domestic controls)

Resources

- OS X Sierra: Use FileVault to encrypt the startup disk on your Mac
- OS X Mountain Lion: About FileVault disk encryption
- OS X Yosemite: Encrypt the contents of your Mac with FileVault
- OS X El Capitan: Encrypt the contents of your Mac with FileVault
Internal links about traveling:

- Brown's Travel Portal and Export Controls guidelines
- International Travel Information for all Brown University Travelers
- Export Controls at Brown | Brown's Export Control Policy

Note: For questions or further information related to export controls or international research administration, please contact Juliane_Blyth@brown.edu, Associate Director of Research Operations at (401) 863-3295.

External links about traveling:

- Encryption FAQs (Bureau of Industry & Security, BIS)
- EAR Controls for Items That Use Encryption (Bureau of Industry & Security, BIS)
- Cornell University - Travel Internationally with Technology
- FBI - Safety and Security Guidance for Traveling Abroad
- Department of State - Travel Alerts and Warnings
- Department of Homeland Security - "Know Before You Go" Resources
- Department of State - Websites of US Embassies Consulates, and Diplomatic Missions
- Department of State - "Smart Traveler Enrollment Program"