

Learn About FileVault 2 (Encryption for Macs)

Stephanie Obodda - 2023-01-18 - Comments (0) - Apple Macintosh Computers

- [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 out of the country with an encrypted laptop?](#)
- [Resources](#)

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 if they use laptops containing data with a [risk of Level 2 or 3](#) (especially frequent travelers).

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 taking encrypted laptops, provided that the traveler returns within the year and "retains effective control and ownership." This coverage is global except for a handful [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, since laws can change at any time and some countries ban or severely regulate the use of encryption, you should consult [country-specific information](#) before traveling with an encrypted laptop to verify that your information is still current. In addition, any faculty, post-docs, graduate students and PI's should check-in with [OVPR](#), read its [International Travel page](#) as well as that of the [Office of Insurance and Purchasing Services](#) , and contact the Chief Information Security Officer before travelling overseas.

Finally, note that many nations do not recognize a "personal use exemption." Before traveling to these countries with an encrypted laptop, you will need to apply to their specified governmental agency for an import license. Additional information about international encryption controls can be found at the following websites:

[The Wassenaar Arrangement](#)

[Bureau of Industry and Security of the U.S. Department of Commerce - Export Administration Regulations](#)

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 Control Regulations at Brown | Brown's Export Control Policy and Procedures](#)
- Note: For questions or further information related to export controls or international research administration, please contact Juliane_Blyth@brown.edu, Senior Director, Office of Research Integrity 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](#)
- [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"](#)