Encrypt Your Mac Using FileVault

May 2017
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>3</td>
</tr>
<tr>
<td>WHO THIS MANUAL IS FOR</td>
<td>3</td>
</tr>
<tr>
<td>DESCRIPTION OF FileVault</td>
<td>3</td>
</tr>
<tr>
<td>WHY SHOULD YOU USE FileVault</td>
<td>3</td>
</tr>
<tr>
<td>HOW TO ENCRYPT AN APPLE COMPUTER</td>
<td>4</td>
</tr>
<tr>
<td>SETTING A FIRMWARE PASSWORD</td>
<td>9</td>
</tr>
<tr>
<td>HOW TO ENCRYPT A TIME MACHINE BACKUP</td>
<td>10</td>
</tr>
<tr>
<td>HOW TO ENCRYPT AN EXTERNAL STORAGE DEVICE USING DISK UTILITY</td>
<td>11</td>
</tr>
<tr>
<td>HOW TO ENCRYPT AN EXTERNAL STORAGE DEVICE USING FINDER</td>
<td>12</td>
</tr>
<tr>
<td>HOW TO USE AN ENCRYPTED EXTERNAL STORAGE DEVICE</td>
<td>15</td>
</tr>
<tr>
<td>HOW TO DECRYPT AN APPLE COMPUTER</td>
<td>16</td>
</tr>
</tbody>
</table>
Introduction

Who this manual is for
This manual is for users that would like to protect the data on their Mac computer from prying eyes. On laptop computers that may be misplaced or stolen this is important to prevent your data from being compromised. If the computer is owned by OSU and contains PII (Personal Identifiable Information), such as social security numbers, driver’s licenses numbers, foreign identification numbers, passport numbers, credit card numbers or bank account numbers the encryption is required.

Description of FileVault
Apple has included full-disk encryption with the last few versions of its operating system, which they refer to as FileVault. FileVault may be easily enabled and is transparent to the user of the computer. Problems may be encountered if the encryption process is not followed, typically if the IT support department needs to recover your data for any reason.

The encryption process can take a long time to complete, even several days, depending on the amount of data on the computer. While the computer is encrypting you may continue to use as you normally would, there may be a slight performance hit while the computer is encrypting. The computer may be turned off during the encryption process. When turned back on the computer will continue the encryption process.

After the computer is encrypted the initial log in screen will appear faster, but only the users that have been set to unlock the computer will be able to log in when first starting the computer. Other users will have wait until an authorized person logs in to unlock the drive then logs out of the computer before being able log in.

External hard drives may be encrypted also. Time Machine backups should be encrypted for any encrypted computer otherwise, the Time Machine drive can be opened with any one that has access to the drive and another Apple computer.

Why should you use FileVault
FileVault should be used to protect your data from being compromised. This includes your personal data as well of those of others you may have on your computer.

NOTE: All screen shots are from computer using Mac OS X 10.12.4 (macOS Sierra) and your view may vary some with older versions of Mac OS X.
How to Encrypt an Apple Computer

To encrypt an Apple computer, follow these steps to give you the best experience:

1. Log onto the computer with a local admin account
2. Quit all applications as the computer will need to be restarted
3. Open the App Store and run all updates for the Mac operating system
4. Open System Preferences > Security & Privacy > FileVault tab

5. Unlock the FileVault tab by clicking the lock in the lower left corner and authenticating with an administrative account
6. Click the button to Turn on FileVault

7. In the dialog box that appears, select the ‘Create a recovery key and do not use my iCloud account’ then click continue

Allow my iCloud account to unlock my disk option
This may be used for personal computer, never use for an OSU computer as the account to unlock the drive is personal information to the owner of the Apple ID. If the person owning the Apple ID leaves the University or forgets the Apple ID password the drive cannot be unlocked.

8. The next dialog box will display the recovery key that will be needed to unlock the drive if the user passwords stop working or the hard drive has to be removed from the computer for
9. If there is more than one local user on the system, a dialog box appears where you can enable existing users to unlock the encrypted system. Click the Enable User button next to each user you wish to be able to unlock the system.

The enabled users will each have to enter their password to enable this feature.

Any user not initially enabled to unlock FileVault can be configured for this ability later; just click the Enable User button in the FileVault pane of Security & Privacy preferences. Only local users or cached mobile network users can be FileVault enabled. New local users or cached mobile network users created after FileVault is turned on are automatically able to unlock FileVault.
10. The next dialog box will prompt for restarting the computer, click restart.

11. After the computer restarts, log back in with same account used to enable FileVault.
12. After getting logged in, the FileVault system preference window will still be displayed indicating that the computer is encrypting. The FileVault system preference window may be closed. If you want to check on the process of the encryption, just reopen the FileVault system preference window.

Note: It may take some time to encrypt, depending on how much information is stored on your Mac. However, you can use your Mac as usual while the disk is being encrypted.
Setting a Firmware Password

To completely secure the Apple computer from being compromised the final step is to set a firmware password to prevent someone from using the recovery console to change the password of a user that may unlock the drive.

1. Turn the computer off
2. Turn the computer on while holding the `option` key
3. Hold the `option` key until you see the bootable disks, one being the Recovery Console

   **Note:** If the Recovery Console does not display then you will need to boot using a USB formatted and set up for installing the Mac OS X.

4. Chose the Recovery Console and press `return`
5. When you are in the Recovery console, from the menu bar chose Utilities > Firmware Password Utility
6. Click the button to Turn on Firmware Password…
7. Enter a new password and then reenter the password in the verify box, click `Quit Firmware Password Utility` to close
8. The next dialog box will show that Password protection is enabled, click `Quit Firmware Password Utility` to close
9. Restart the computer

The firmware password will only be required when using the `option` key to boot into another startup mode.

**Note:** If the firmware password is forgotten it may be reset you an Apple technician. If this is a personal computer, be prepared to prove that you positively own the computer.

If this is an OSU Client Services maintained computer, make an entry in KeePass with the computer serial number and the firmware password.
How to Encrypt a Time Machine Backup

*Note:* A drive with no data will need to be used to set up a new Time Machine backup. If you have Time Machine backups previous to the time you decide to encrypt the backup you may use the drive, but all data will be erased.

1. When you first connect an external hard drive to an Apple computer and time Machine has not been enabled you will be prompted to create a Time Machine backup.

2. Check the box to Encrypt Backup Disk then the button to use as Backup Disk

3. Enter a password in both the Encryption and Verify password fields. A password hint is required. When all the fields are completed, click the Encrypt Disk button. The hard drive will then be reformatted and then Time Machine will complete the backup process.

4. Whenever the hard drive is connected you will be prompted for the password, which may be stored in the keychain.
How to Encrypt an External Storage Device using Disk Utility

To encrypt an external storage device that is not formatted with the Mac OS Extended format and contains no data you may use Disk Utility to encrypt the drive. The encryption process will delete all the information on the storage device.

1. Finder > Go > Utilities > Disk Utility

2. Select the drive and click the Erase
3. A dialog box for entering a password will appear, use a secure password

How to Encrypt an External Storage Device Using Finder

To encrypt an external storage device that is formatted with the Mac OS Extended format you may use Finder to encrypt the drive. The encryption process is similar to encrypting the computer and will not delete all the information on the storage device

**Warning:** If the storage device is formatted with the FAT or FAT32 format the drive will be encrypted, but the data will be erased.

**Note:** If the storage device is formatted with the NTFS format a dialog box will appear warning that the drive cannot be encrypted. You will have to move the data from the drive and then use Disk Utility to reformat the drive.

1. Open Finder
2. In the side bar Control-click the item you want to encrypt

3. Enter a password in both the Encryption and Verify password fields. A password hint is required. When all the fields are completed, click the Encrypt Disk button.
4. The encryption process can be checked at any time by Control-clicking the drive to see if the drive is still *Encrypting*. Once the encryption process is completed the drop down will show *Decrypt the drive*.

**Note**: It may take some time to encrypt or decrypt, depending on how much information is stored on your Mac. However, you can use your Mac as usual while the disk is running the encryption or decryption process.
How to Use an Encrypted External Storage Device

1. When an external encrypted device is inserted to a Mac you will be prompted for the password used to encrypt the drive.

![Password Prompt](image)

Optionally, you may add the password to the keychain of the Mac if you will be accessing this drive often.

![Password Prompt](image)

2. Once the password is accepted the drive will mount and be available to the computer as any normal external drive.

**Note:** This is the same behavior of a Mac computer is booted to Target Disk mode then connected to another Mac. Any password of an authorized user of the encrypted Mac will unlock the drive.
How to Decrypt an Apple Computer

1. Close all open applications as the computer will need to restart to complete the decryption process
2. Open System Preferences > Security and Privacy > FileVault
3. Unlock the preference pane
4. Click the Turn Off FileVault… button

5. A pop-up warning will appear to verify you want to turn off FileVault. Click Restart & Turn Off Encryption button

6. The computer will restart and the decryption process will begin.
7. The process can be checked at any time by opening the Security & Privacy preferences and checking the FileVault tab.