Linux: Encrypting external USB drive

To prevent your important or personal information from falling into the wrong hands, you can easily encrypt the files on your USB-drive with a password. Windows, macOS and Linux all have their built-in encryption tool. This built-in encryption works on all computers with the same operating system. After encryption, only the person knowing the right password can read and change the files on your USB-drive. This quick reference describes how to use encryption on a Linux system.

NOTE: The ISSC cannot help you with decryption of your files if you forget your encryption password.

Ubuntu Disk Utility

Ubuntu includes built-in support for encryption, and so do many other Linux distributions. Ubuntu and other GNOME-based Linux distributions also allow you to easily encrypt removable drives with the Disk Utility application.

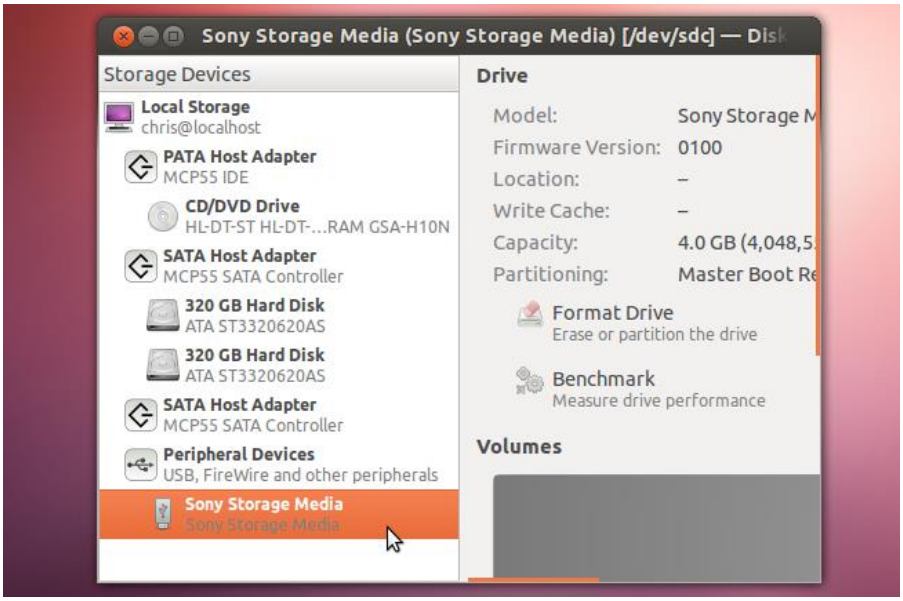
NOTE: Drive encryption requires you to format your drive, so backup data on the USB drive before encryption and then write the data back when the USB disk is encrypted.

Encrypting a Drive

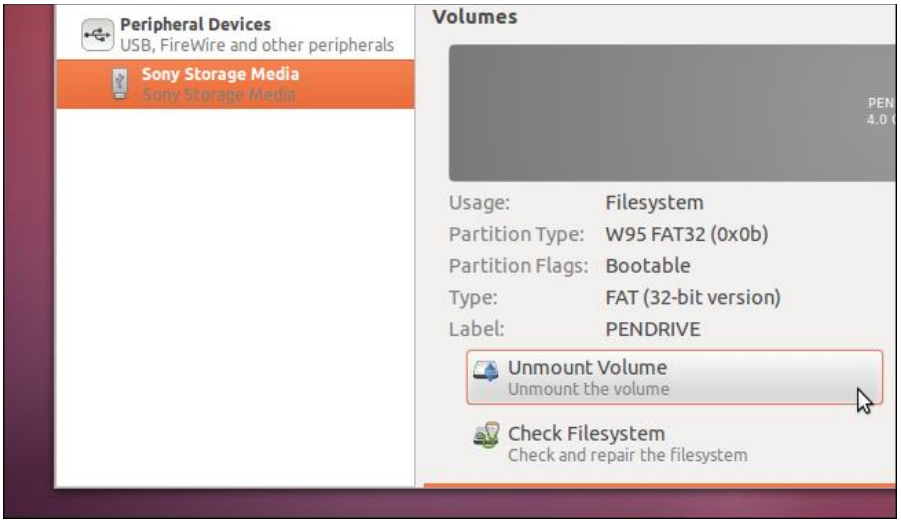
1. To encrypt a drive, launch the Disk Utility from one of the ISSC supported Ubuntu desktops:

   - Unity: Find Disk Utility from the Dash
   - XFCE: Click Applications Menu, Settings, Disk Utility
   - Gnome Classic: Click Applications, Accessories, Disk Utility

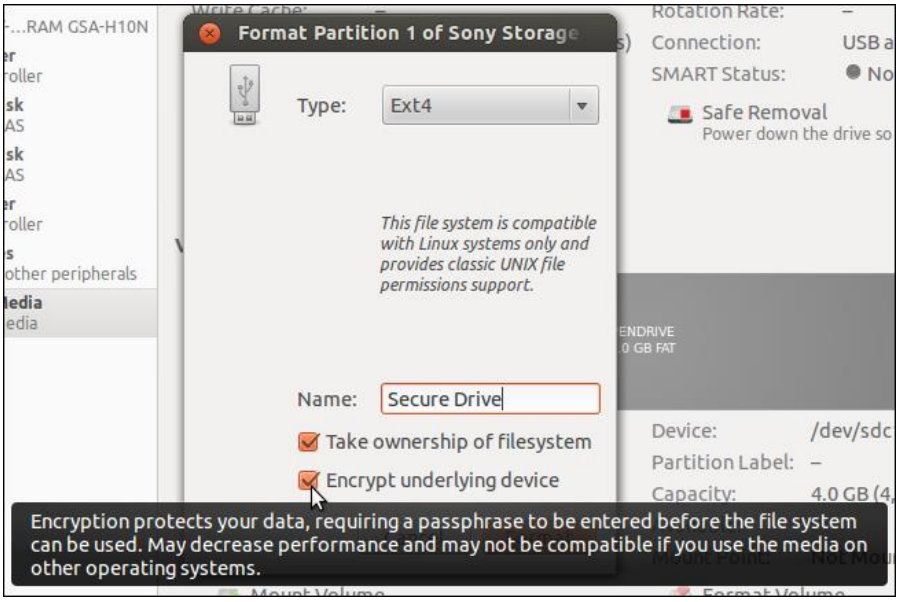
2. Connect the removable storage device – for example, a USB flash drive or external hard drive – and select it from the Peripheral Devices section. Ensure you select the correct device so you don't accidentally wipe important files.



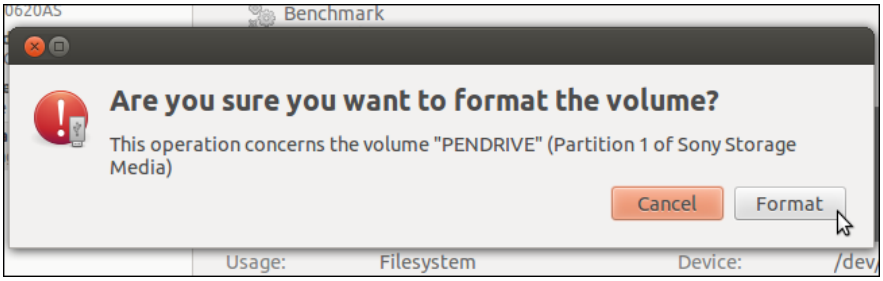
3. After selecting the drive, click the Unmount Volume button in the right pane — you can't format the device's partition while it's mounted. A removable storage device normally has a single partition on it, but you can create additional partitions here – for example, you could have one unencrypted partition and one encrypted partition on a USB stick.



4. Click the Format Volume button and enable the Encrypt underlying device check box.



The confirmation dialog doesn't say so, but the formatting process will erase all files on the drive. Ensure you're formatting the correct drive and you've backed up its files before continuing.



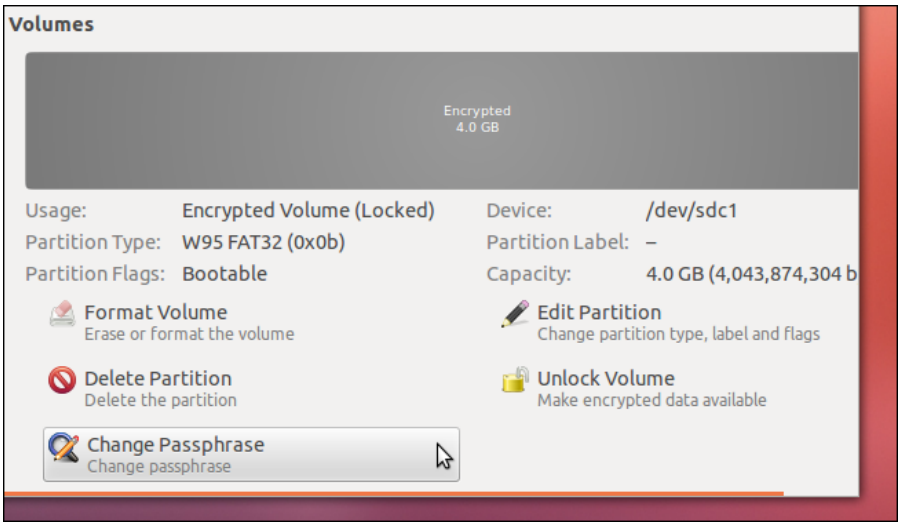
5. You'll be prompted to create a passphrase – ensure you use a strong one. You can have Ubuntu remember the passphrase forever, if you like – this decreases security, but allows the drive to work on your current system without any prompts. If you take the drive to another system, you'll be prompted to enter the appropriate password before using it.

Using an Encrypted Drive

Connect the removable storage device to any Ubuntu system – or any system running the GNOME desktop – and you'll be prompted to enter your password. After you enter the password, the device will be usable.

A padlock icon identifies encrypted drives in the file manager.

If you ever want to change your passphrase in the future, you can use the Change Passphrase option in the Disk Utility. You can also format the volume again to remove the encryption.



Multi platform encrypting applications

If the default operating system encryption methods don't work for you or if you need multi platform encryption, you might consider one of these tools:

- https://www.veracrypt.fr/en/Home.html
  This open source encryption tool replaces the once popular TrueCrypt and is available for Windows, macOS and Linux.
  NOTE: You can have Veracrypt installed on a standard Windows work place via the application form 'Request software'.

- https://www.axcrypt.net/
  This encryption tool is known for its intuitive user interface and availability for Windows, macOS, iOS and Android.

- https://www.boxcryptor.com/en/boxcryptor-portable-download
  A commercial encryption tool with a free version for local, portable installation (Windows, macOS, Linux) on one or two devices.

You may install VeraCrypt, Axcrypt or BoxCryptor yourself on any PC where you have administrator rights. (This means you can not install these programs on a standard Mac or Linux work place).

This Quick reference was adapted from:

- an article on the How-to Geek website http://www.howtogeek.com/115955/how-to-quickly-encrypt-removable-storage-devices-with-ubuntu/ .