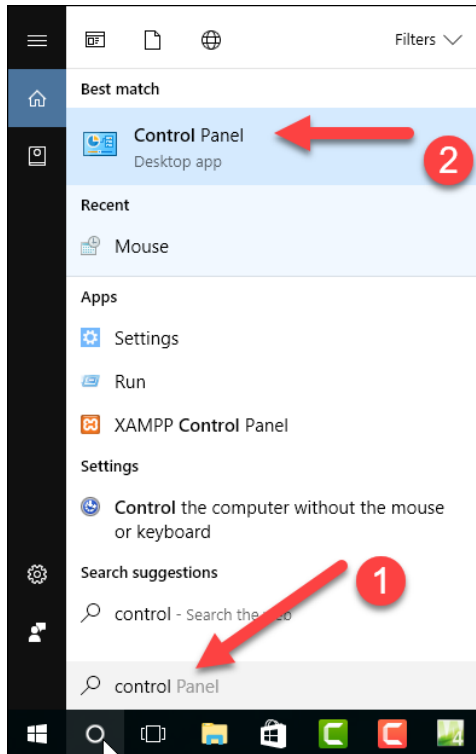


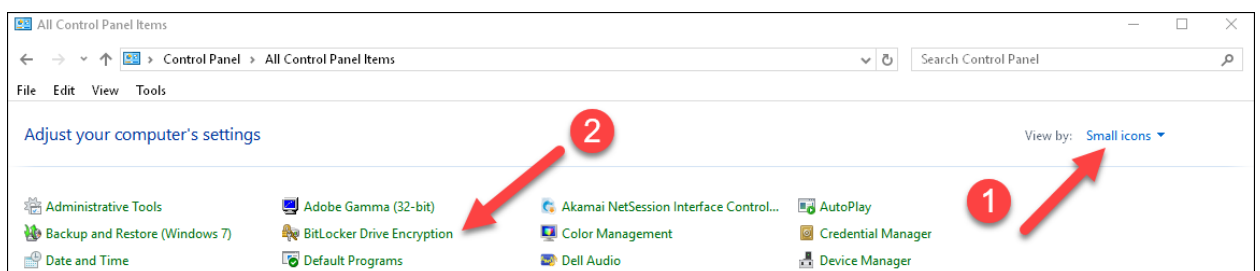
BitLocker

First locate the Control Panel

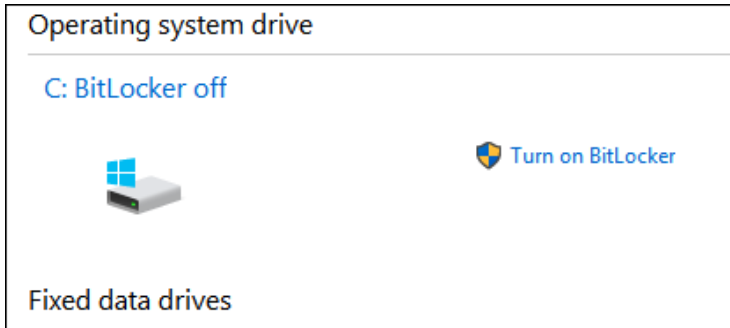
1. In the search box type: **Control Panel**



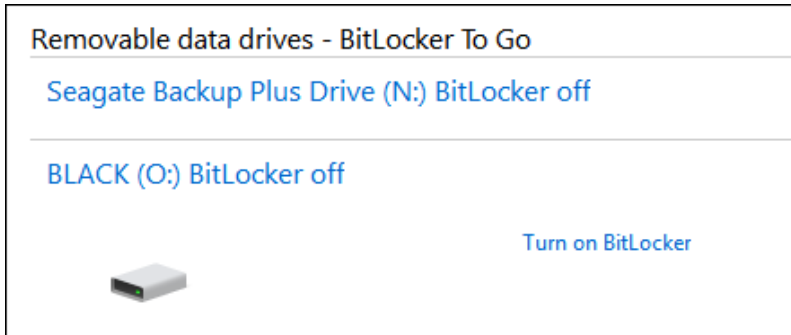
2. Change View by: to **Small icons**.



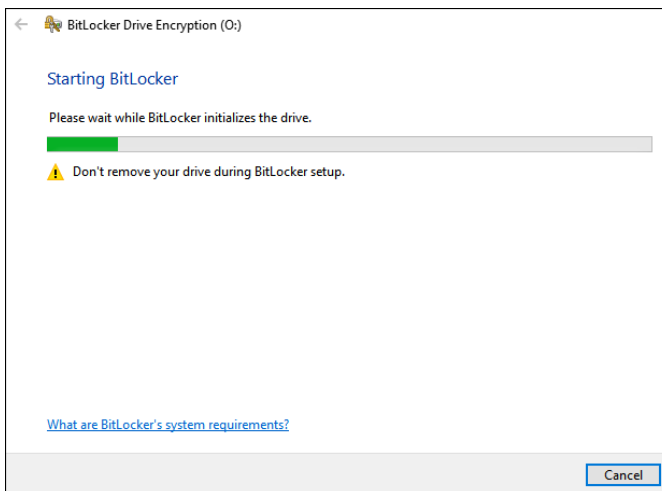
3. Click **BitLocker Drive Encryption** menu.
4. Click **Turn on BitLocker** link



You can do memory sticks also:

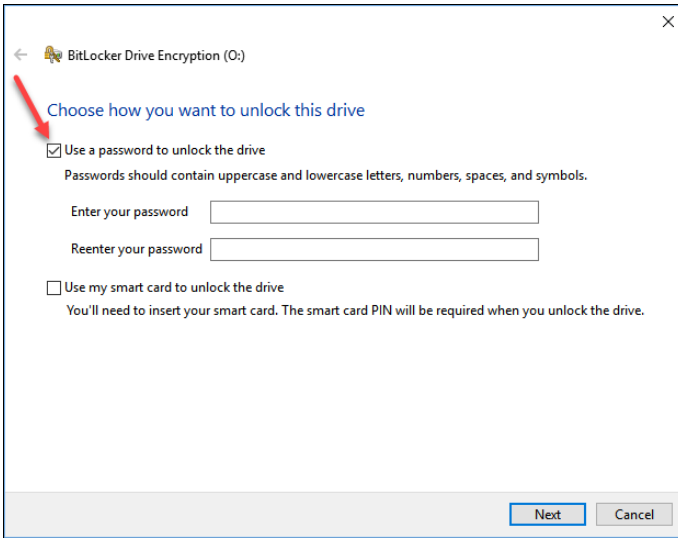


5. The initializes of your drive will start.

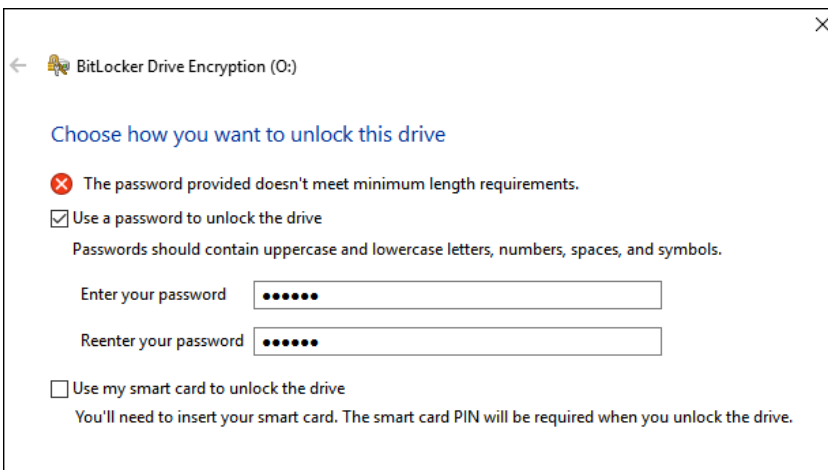


6. Next you will be asked for a password.

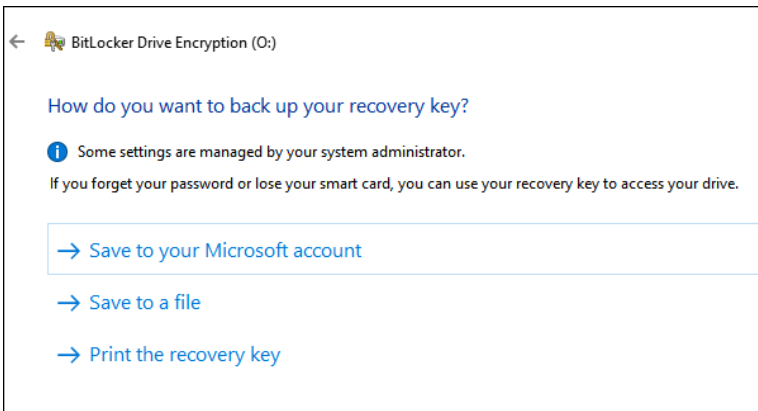
Pick your password carefully.



7. If you do not use a good password you will get an error.



8. You will now be asked to save your recovery key.



9. Click **Save to file**.

This will be a text file with your recovery key inside.

Your file should look something like this.

```
BitLocker Drive Encryption recovery key[REDACTED]

To verify that this is the correct recovery key, compare the storage
Identifier:

    CC77746D-8FDF-[REDACTED]-BA4923F8329B

If the above identifier matches the one displayed by your PC, then
Recovery Key:

    318791-163317-[REDACTED]-225599-590942

If the above identifier doesn't match the one displayed by your PC,
Try another recovery key, or refer to https://go.microsoft.com/fwlink/?linkid=864876
```

10. Select one of the options and click Next.

Choose how much of your drive to encrypt

If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected—even data that you deleted but that might still contain retrievable info.

Encrypt used disk space only (faster and best for new PCs and drives)

Encrypt entire drive (slower but best for PCs and drives already in use)

11. Here you mostly will select Compatible mode for memory sticks.

← BitLocker Drive Encryption (O:)

Choose which encryption mode to use

Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AES). This mode provides additional integrity support, but it is not compatible with older versions of Windows.

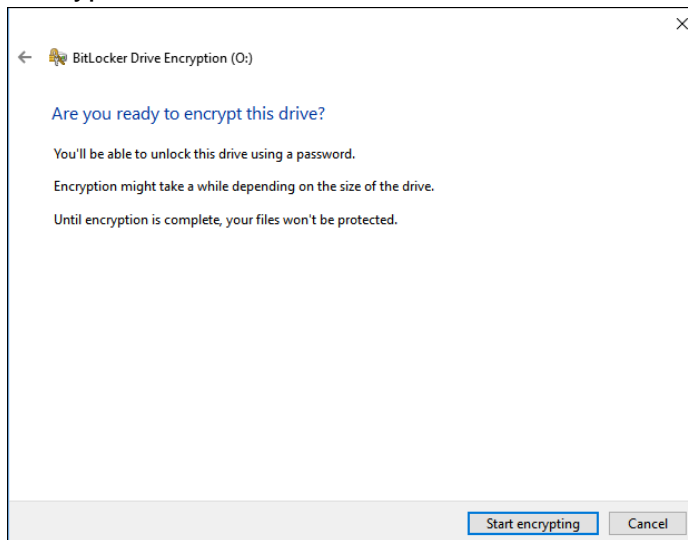
If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode

New encryption mode (best for fixed drives on this device)

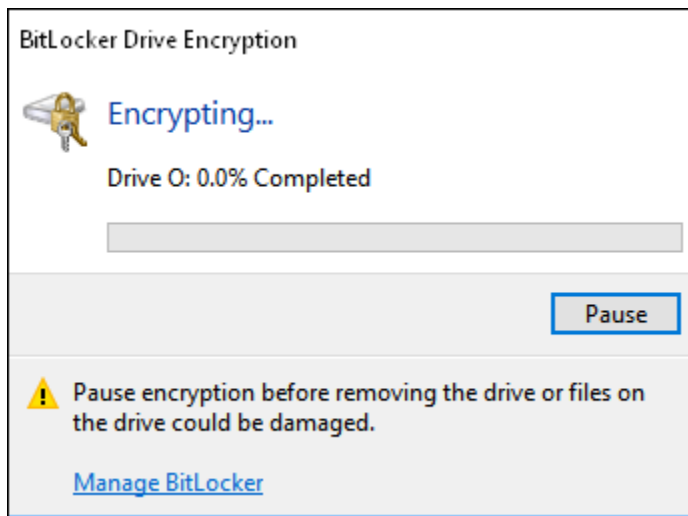
Compatible mode (best for drives that can be moved from this device)

12. Click the **Next** button to start encryption. You are now read to start the Encryption.



13. Click **Start encrypting** button.

Your screen will look like this:



14. After a few moments, you will get a complete message. Click **Close**.

