SECURITY WITH PLYMOUTH UNIVERSITY

Technology & Information Services

SEC-GDL-009-W10 – Encrypting Personal Computers (Windows 10)

Author: Paul Ferrier

Date: 14/10/2016

Document Security Level: **PUBLIC**
Document Version: 1.0
Document Ref: SEC-GDL-009-W10
Document Link:
Review Date: 01/10/2017

SEC-GDL-009-W10 – Encrypting Personal Computers (Windows 10)

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.9	Paul Ferrier	Enterprise Security Architect	Created the document	28/06/2016 09:30			
1.0	PF	ESA	Updated the document following peer review	14/10/2016 08:15			

Contents

SEC-GDL-009-W10 – Encrypting Personal Computers (Windows 10)

1. Introduction

Windows 10 offers users the ability to protect their files and folders with full disk encryption. This means that if the hard drive is kept in the computer, or removed and connected to another computer the password or key will need to be supplied to be able to access the data stored on the hard drive.

Encrypting devices does not make them exempt from the DPA or the FOI act and hence you must be able to comply with the requirements to provide information, or the encryption key if required.

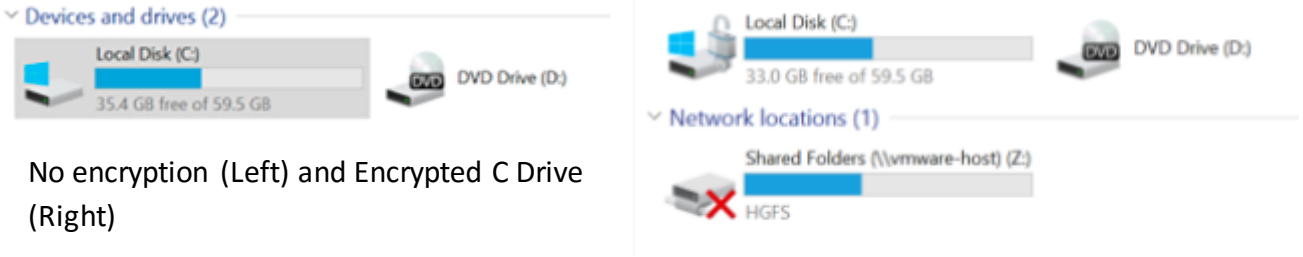
IMPORTANT

One word of caution, if you lose your encryption password or recovery key your data will be inaccessible. There are many ways to securely store your recovery key and these are detailed in section 3.4.

These guidelines provide the steps required to encrypt (and decrypt, if required) a personal computer running Windows 10.

2. Encryption – Quick Check

If you are not sure whether your hard drive is encrypted, there is a simple way to check. Open File Explorer and look at your hard drives.



No encryption (Left) and Encrypted C Drive (Right)

The padlock with the drive icon shows that it is encrypted.

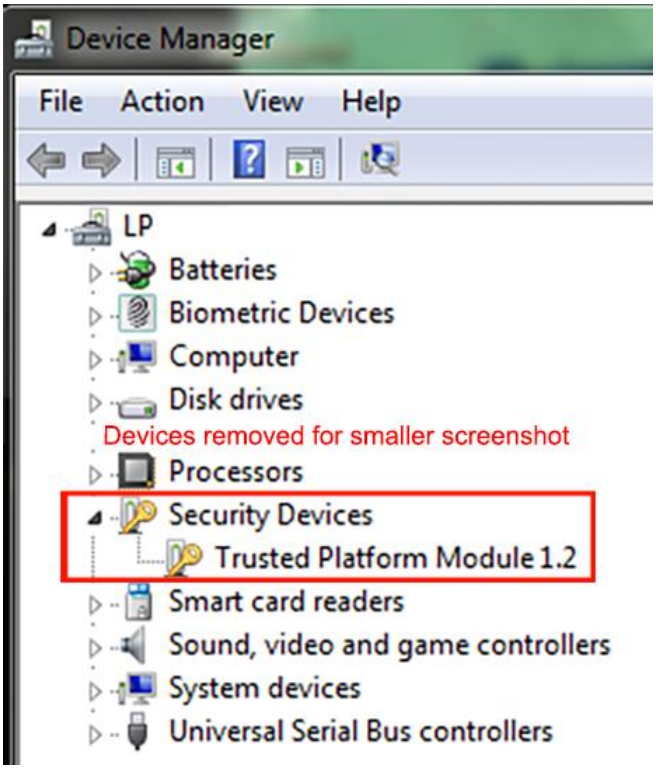
3. TPM chip or not

What is a TPM chip?

A TPM (Trusted Platform Module) chip is specifically designed to hold RSA Encryption Keys (in this document it refers to your Encryption Password (Key)).

How to check if your computer has a TPM chip

In **Device Manager** (available through the Control Panel) look through the list of components that your computer has and try and find a section entitled **Security Devices** open this and in there should be a **Trusted Platform Module** entry, if there isn't then your computer does not have this capability.



With a TPM chip

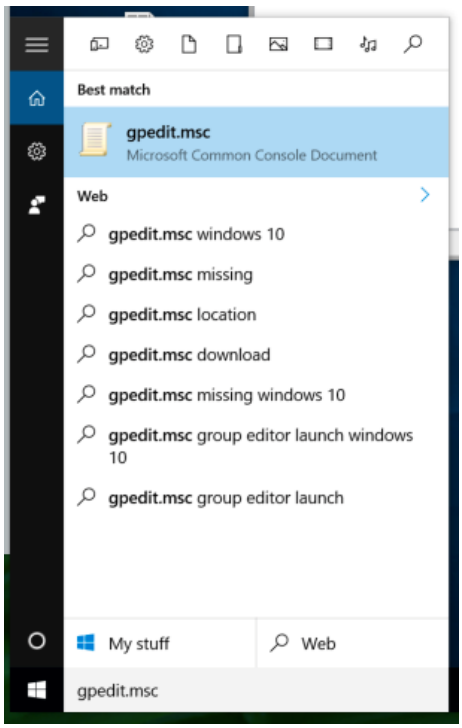
If a TPM chip is available, then it can be applied during the booting process and will not prompt the user for a password before the login prompt is reached.

Please do not use the same password that you use to log in to the computer – if those details are compromised you are providing full access to all of your data, whether encrypted or not.

Without a TPM chip

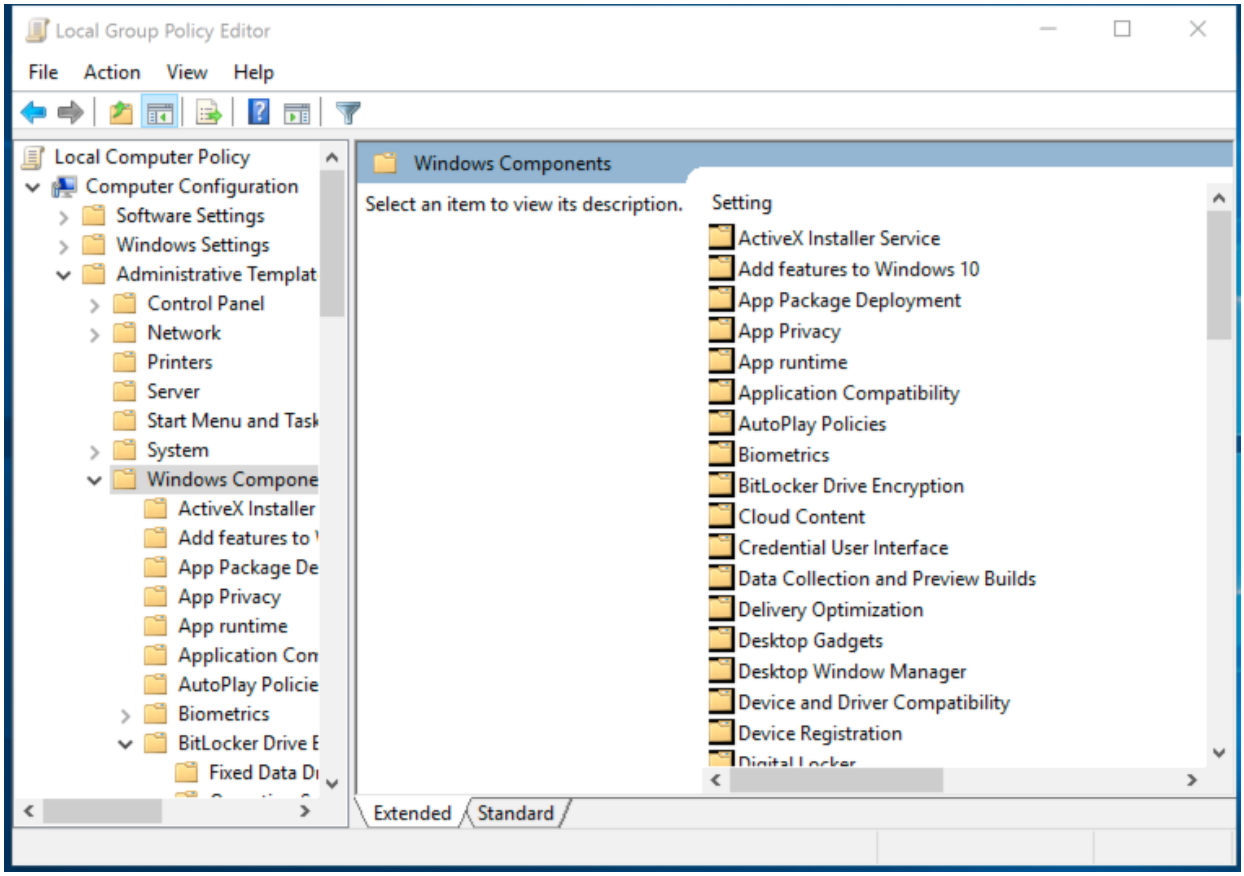
You will be prompted to provide an encryption password (key) at the start of the process and then at each time the operating system starts-up. While this slows down the time to get to a login prompt, or desktop, it means that the data can't be accessed until the correct information is provided.

Required registry changes

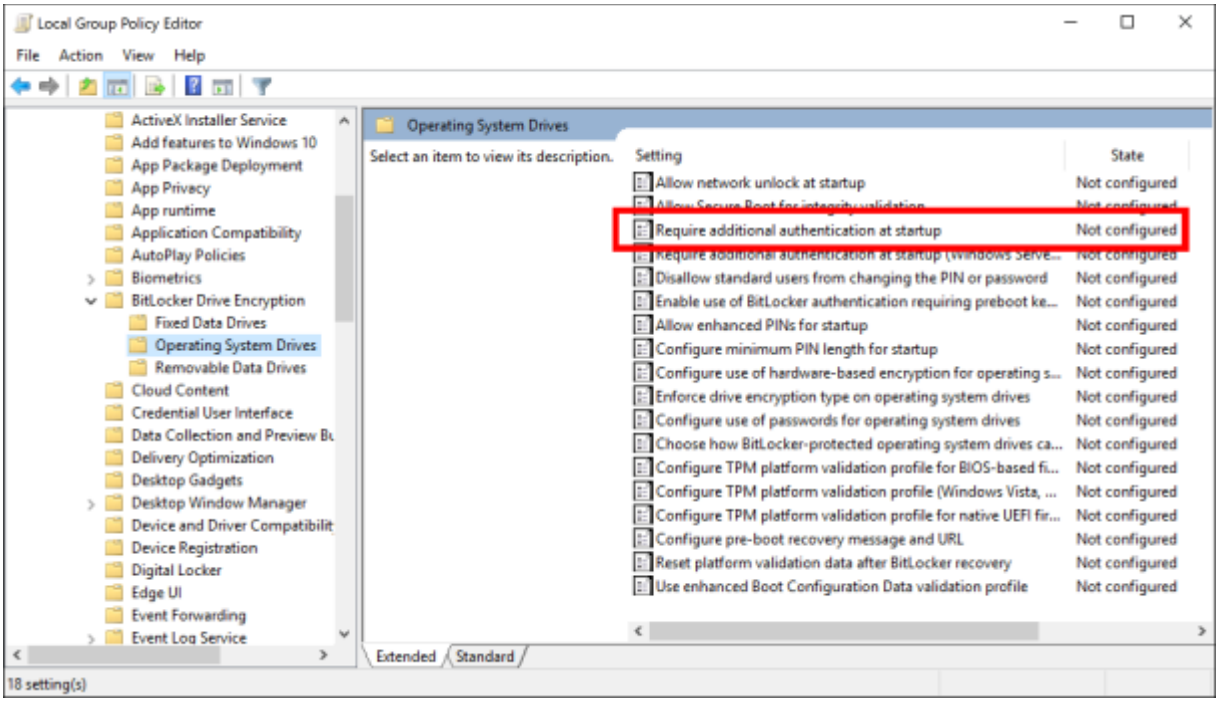
2.1 

Open up the **Local Group Policy Editor**, this can be found by searching (in the Cortona search bar on the bottom ribbon, unless you have removed it) for gpedit.msc.

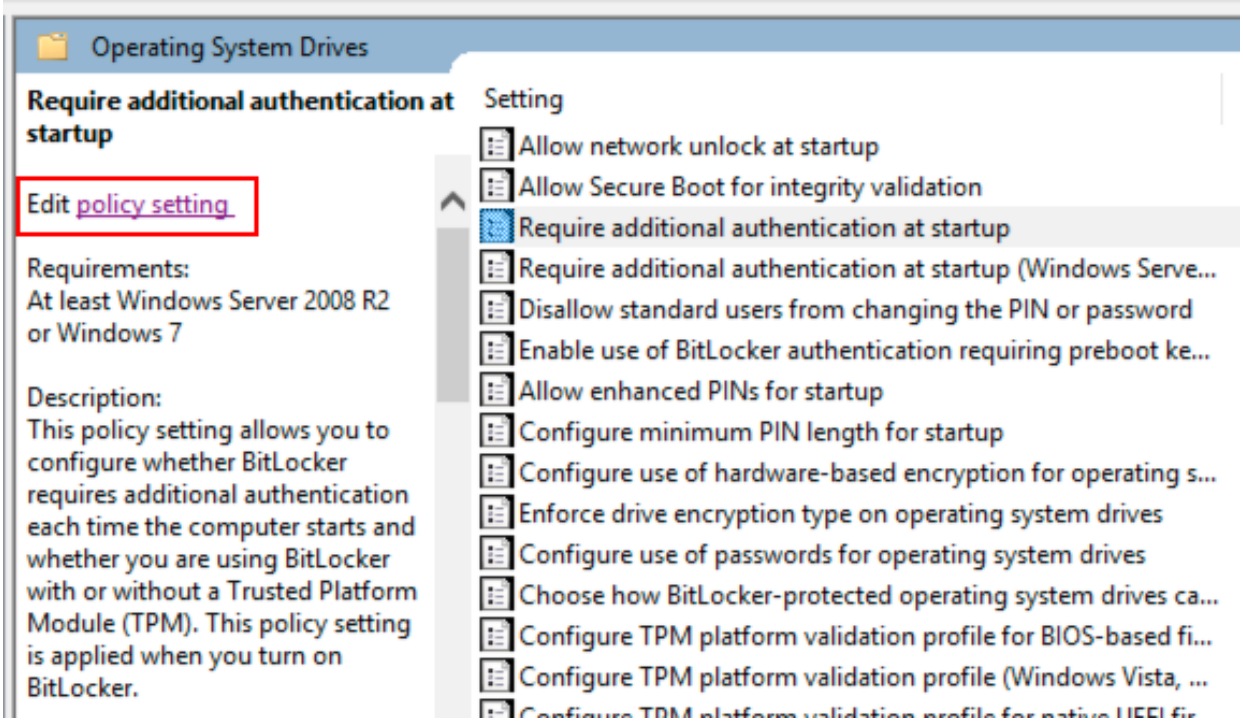
2.2 Select Computer Configuration, Administrative Templates, Windows Components.



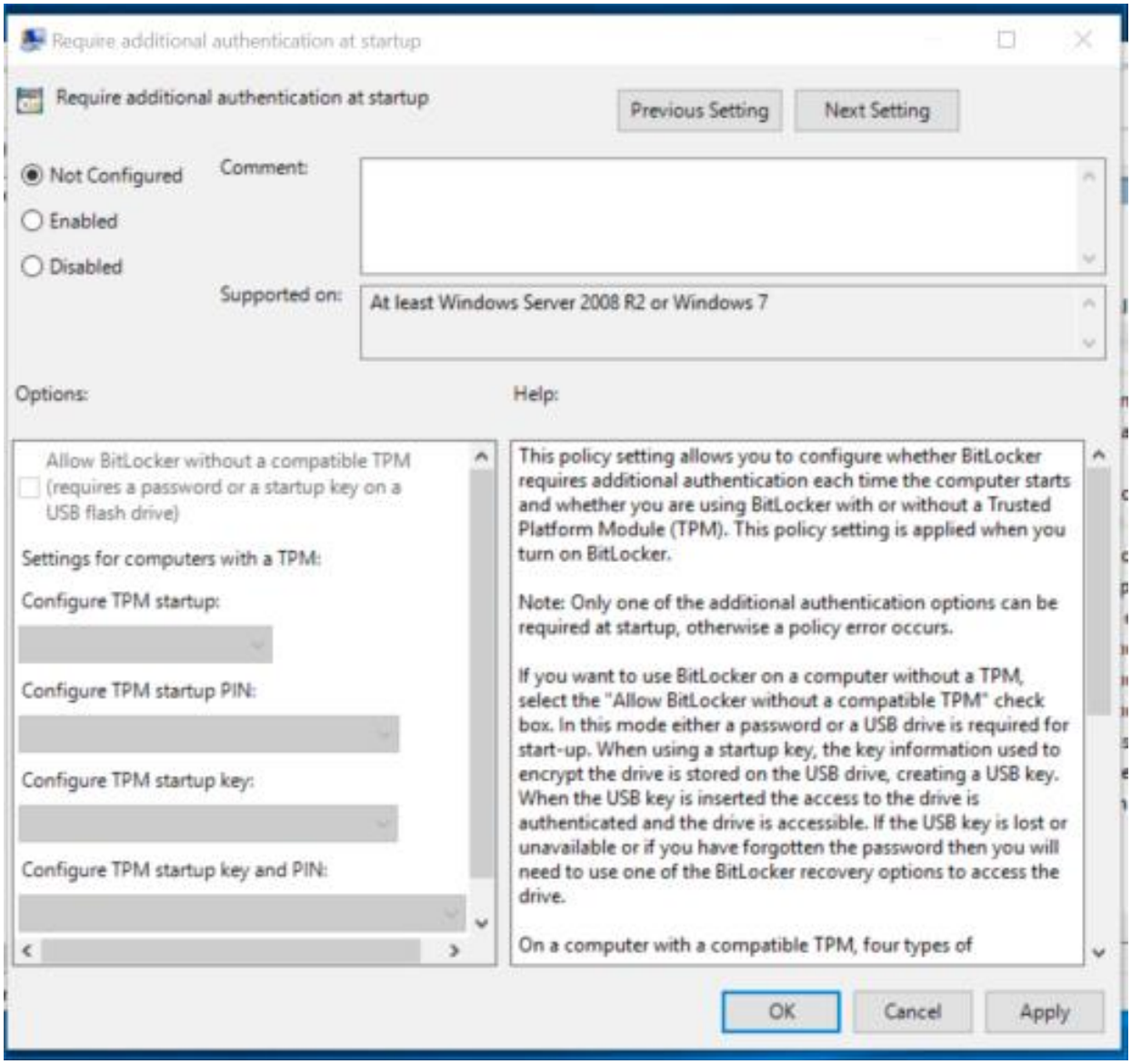
2.3 Then select BitLocker Drive Encryption, Operating System Drive and finally the 'Require additional authentication at startup' setting.



2.4 Now click the 'Edit policy setting'.



2.5 You will see a raft of options, you should **enable** Require additional authentication at startup, this will then allow the options to be selected.

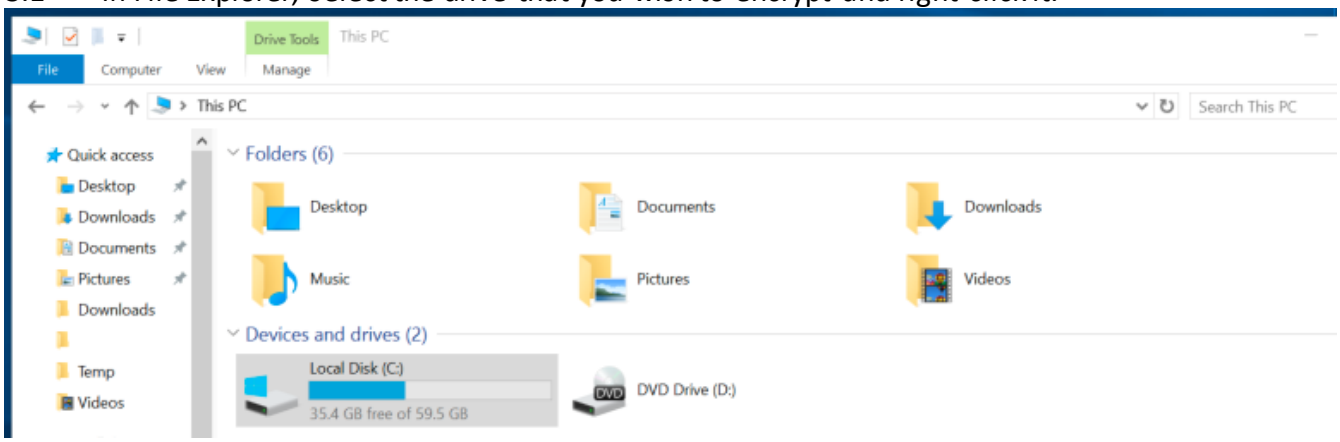


2.6 When BitLocker is enabled, either a password is required (before reaching the login prompt) or booting with a USB device attached to the computer (holding the encryption key).

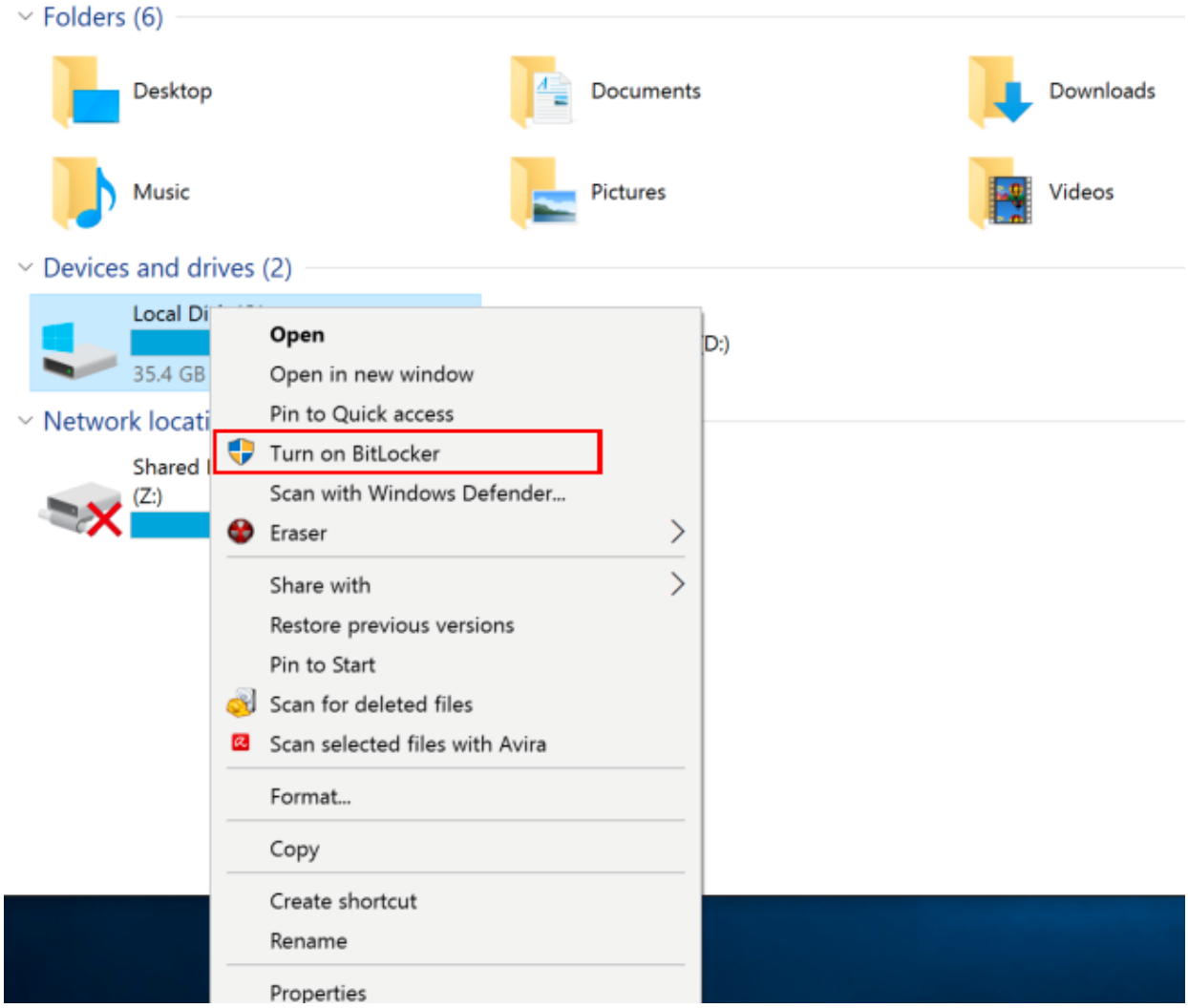
Please note: in this example, a password is being used.

4. Encrypting a drive

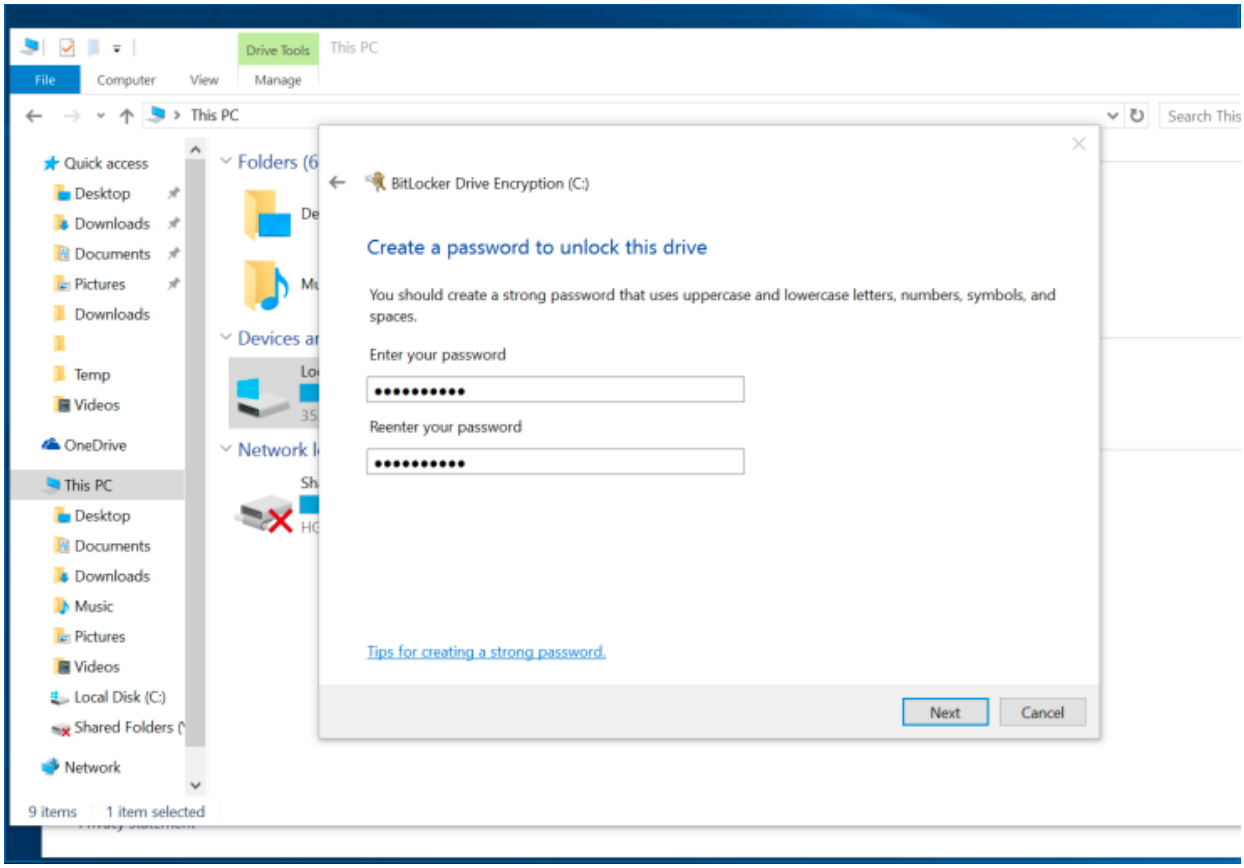
3.1 In File Explorer, select the drive that you wish to encrypt and right-click it.



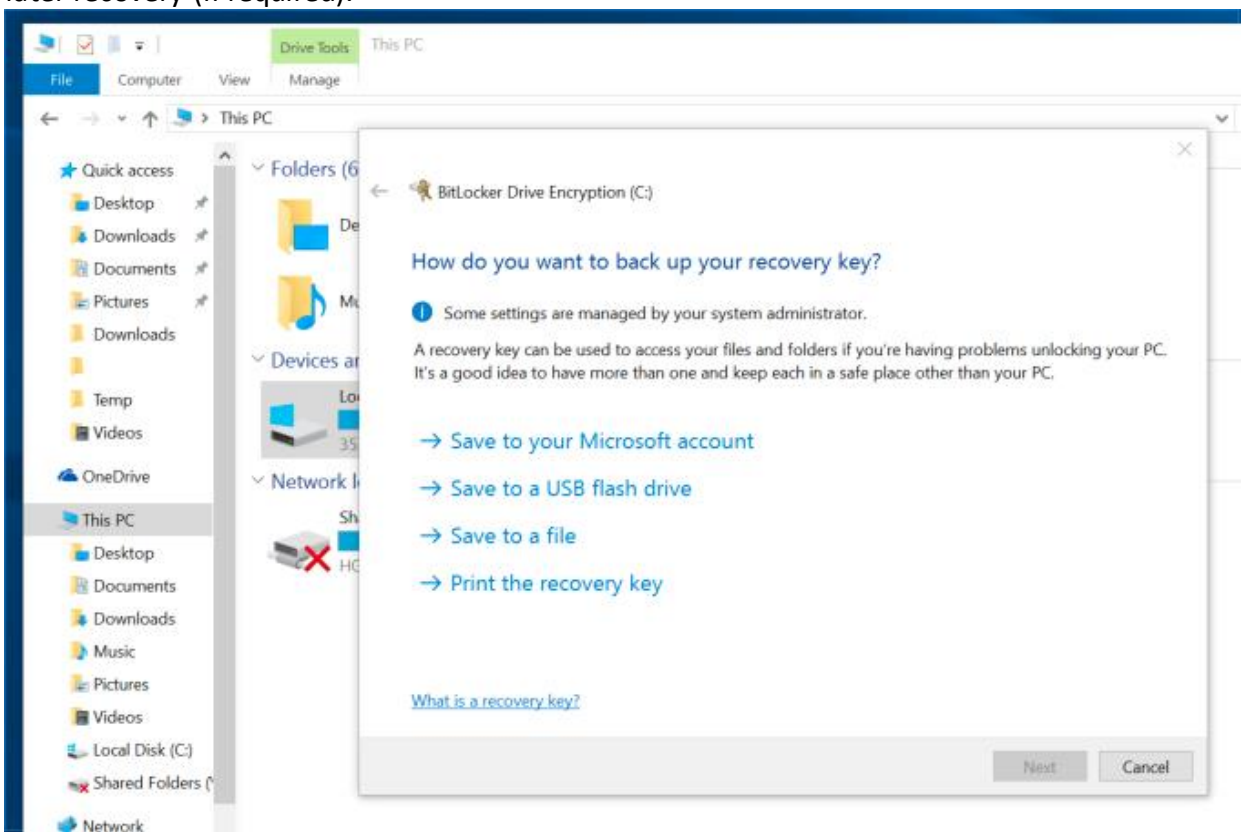
3.2 From the menu select Turn on BitLocker, depending on how your computer is set up, you may need to provide an administrative account username and password to proceed.



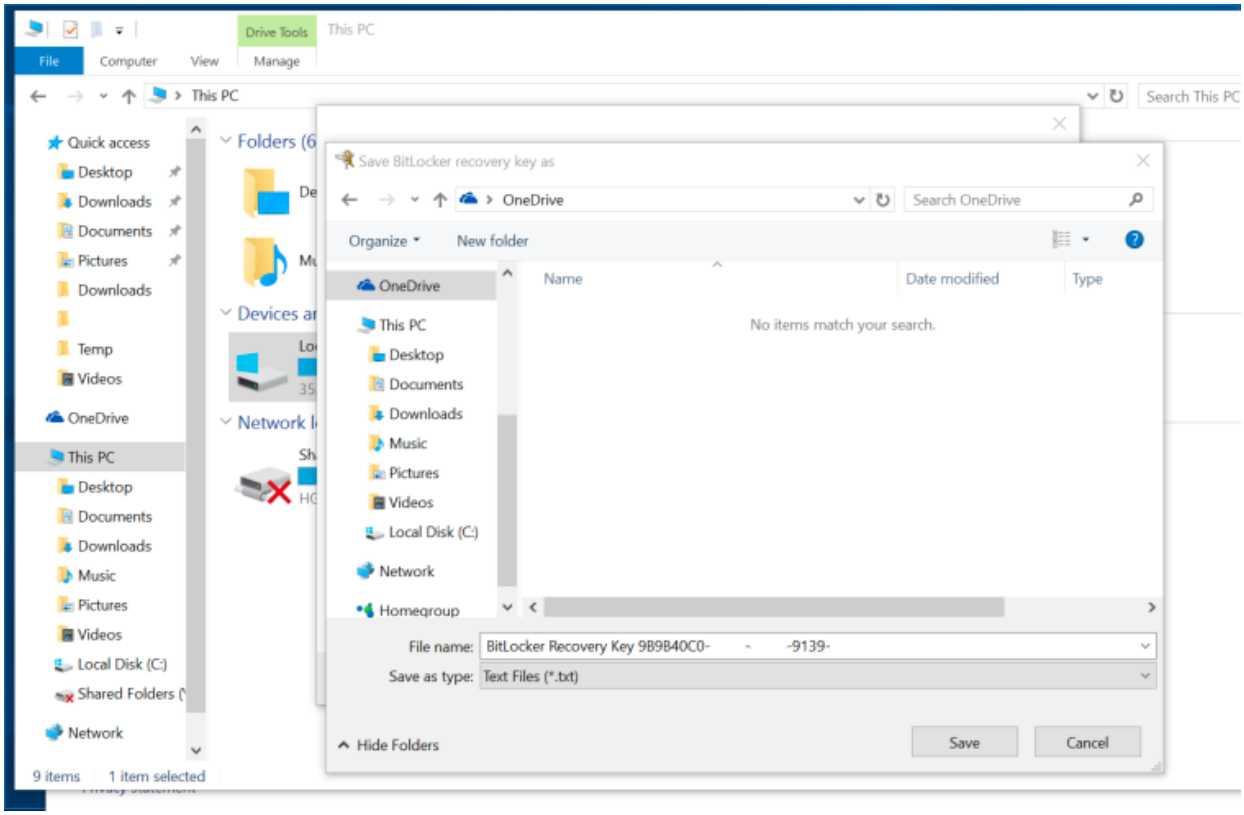
3.3 Provide and confirm a strong password – would you protect your house by having really strong locks, but leave the key in the lock? The same applies here, this password will provide (or deny) access to your information.



3.4 Should you forget the password, you can do a number of things to store your password for later recovery (if required).



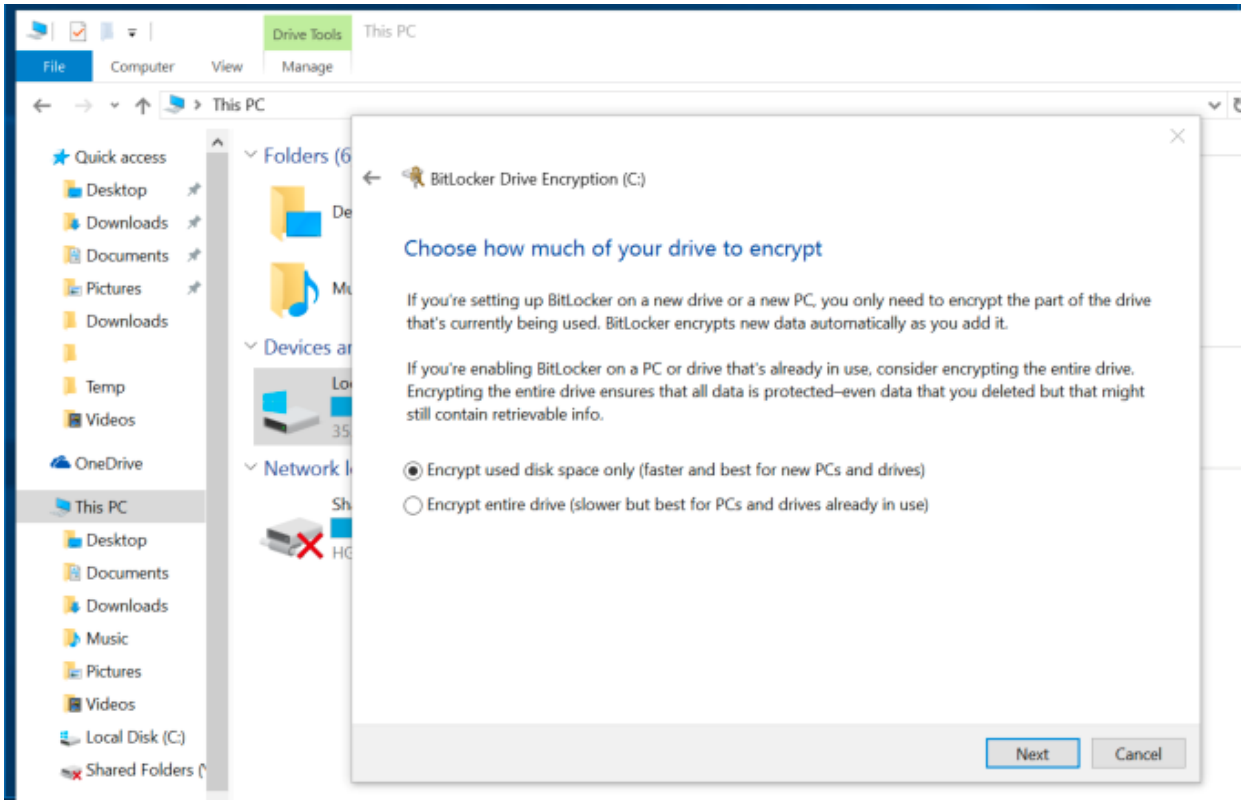
3.5 In this example, the recovery key will be stored in a file, this is turn will be stored on a personal OneDrive. If you are using a USB stick, this then needs to be appropriately protected (do not leave it with your computer).



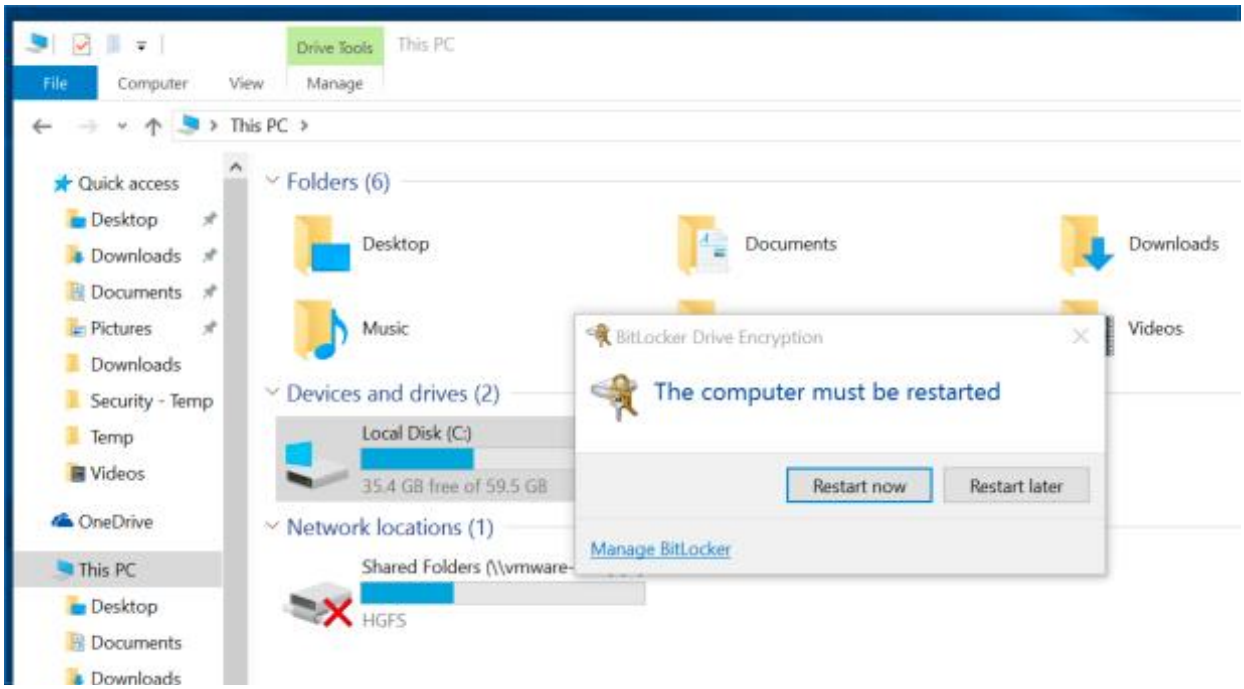
3.6 Once the recovery key has been safely stored, you are presented with the option of how much of the hard drive you would like to encrypt. The best option would be to encrypt the entire hard drive.

NOTE – Use of your computer throughout the encryption process

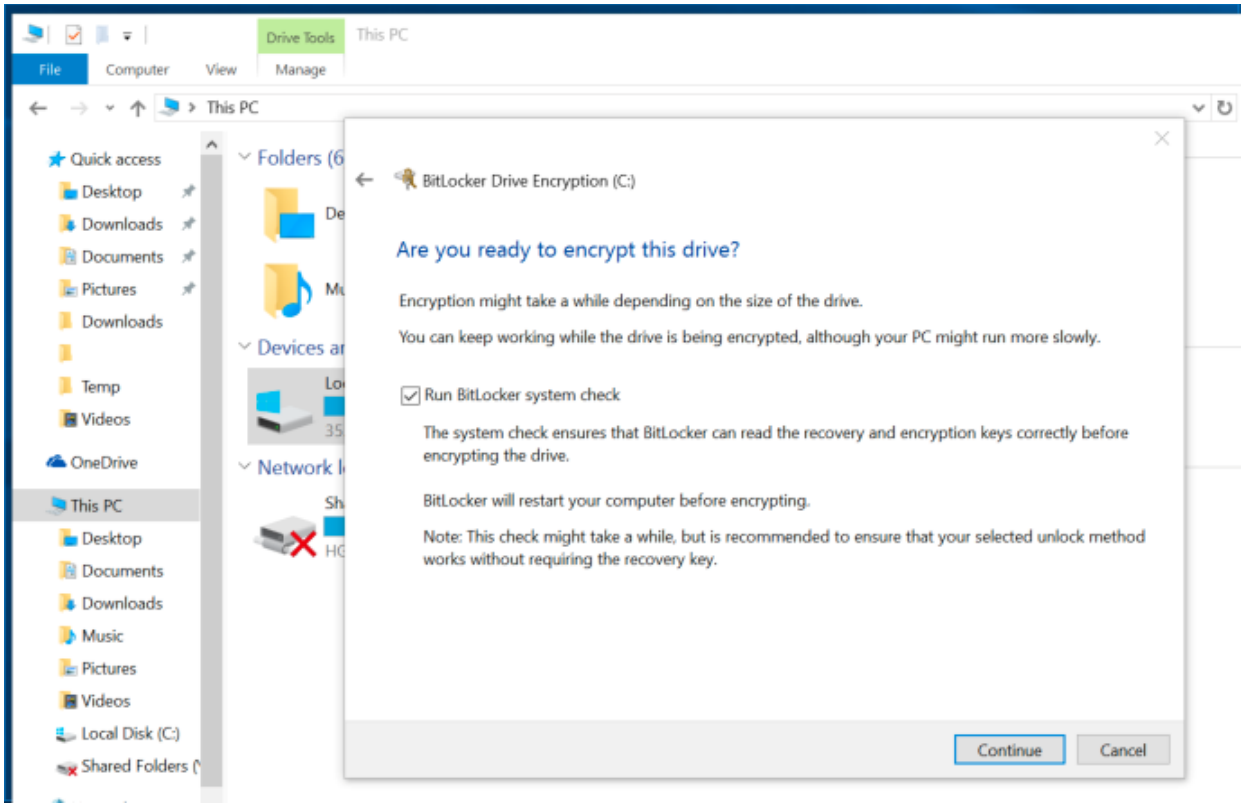
Once you start the encryption process, it doesn't render your computer unusable, in fact you are able to continue using your computer with little or no slow down to responsiveness.



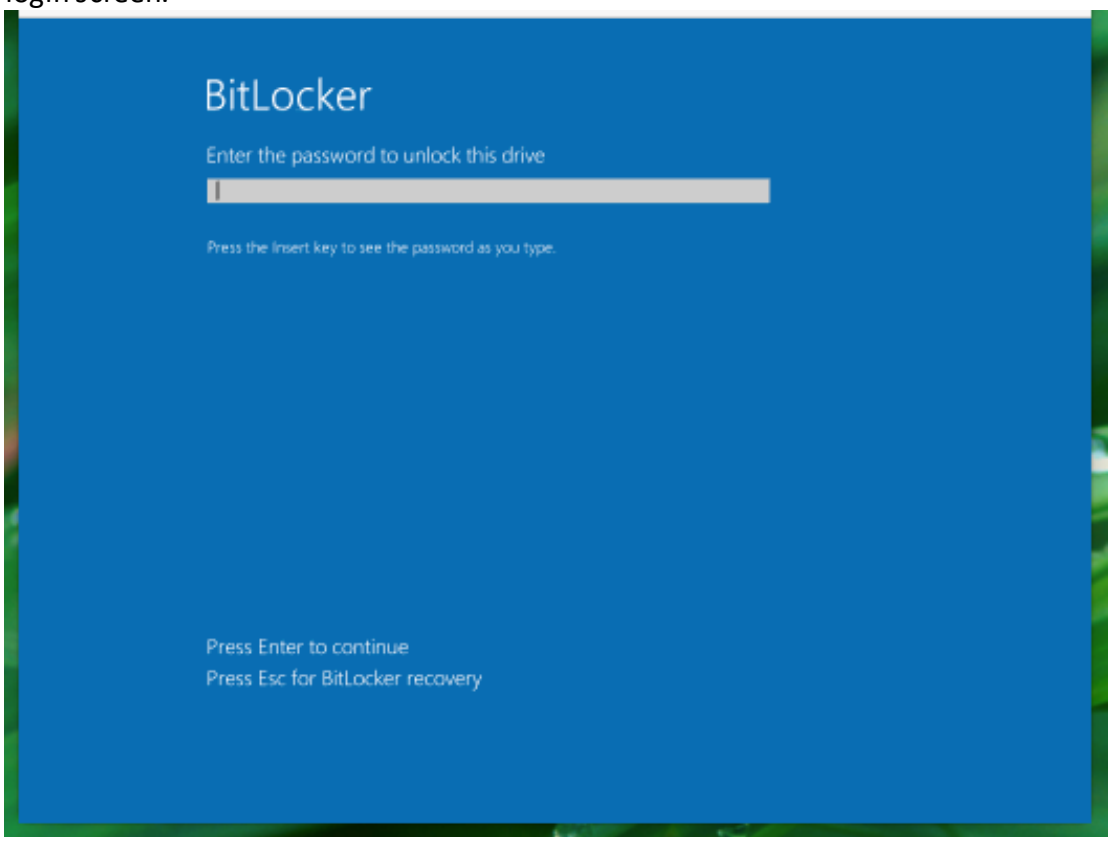
3.7 To allow BitLocker to start the changes that have been made require the computer to be rebooted.



3.8 When the computer gets to the desktop, you then need to once more right click on the drive and select the BitLocker Option. By default, there is a system check that should be run, afterwards there is one more reboot required.

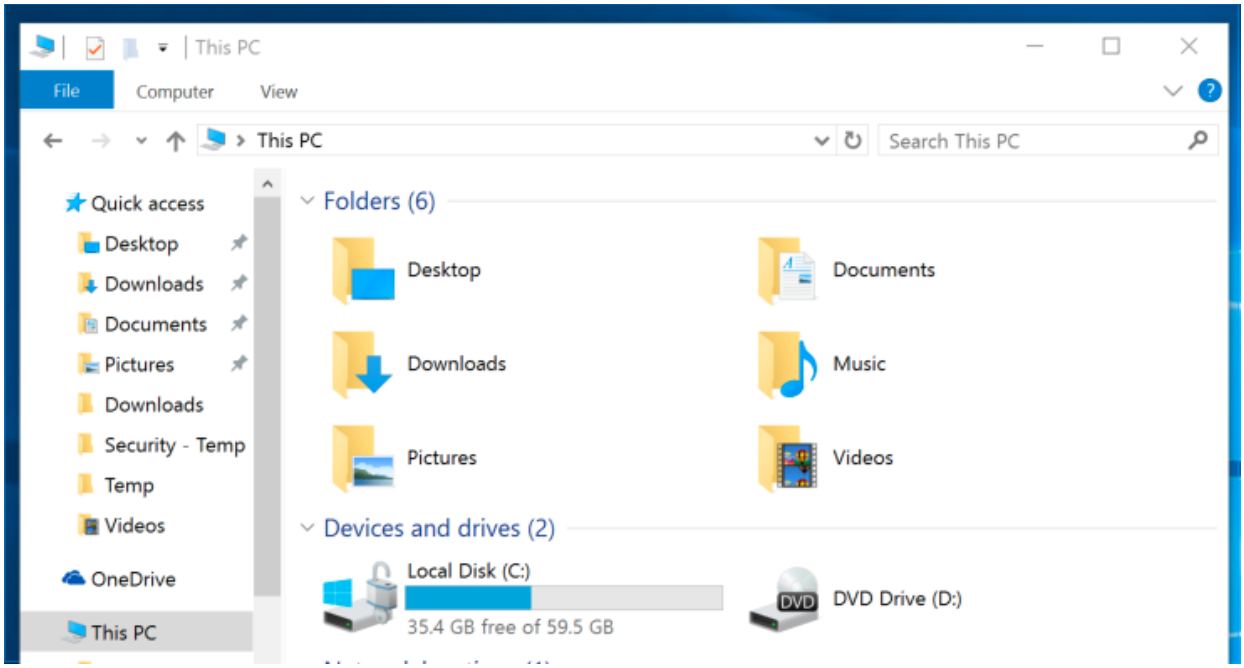


3.9 Upon the reboot, if you have provided a password this will be required before getting to the login screen.



3.10 The encryption of the drive will now continue. You will be able to use your computer while the drive is encrypting, but you will have a lot less disc space until the operation completes.

When it does, you will be able to see the hard drive icon has changed to have a padlock and key next to it.

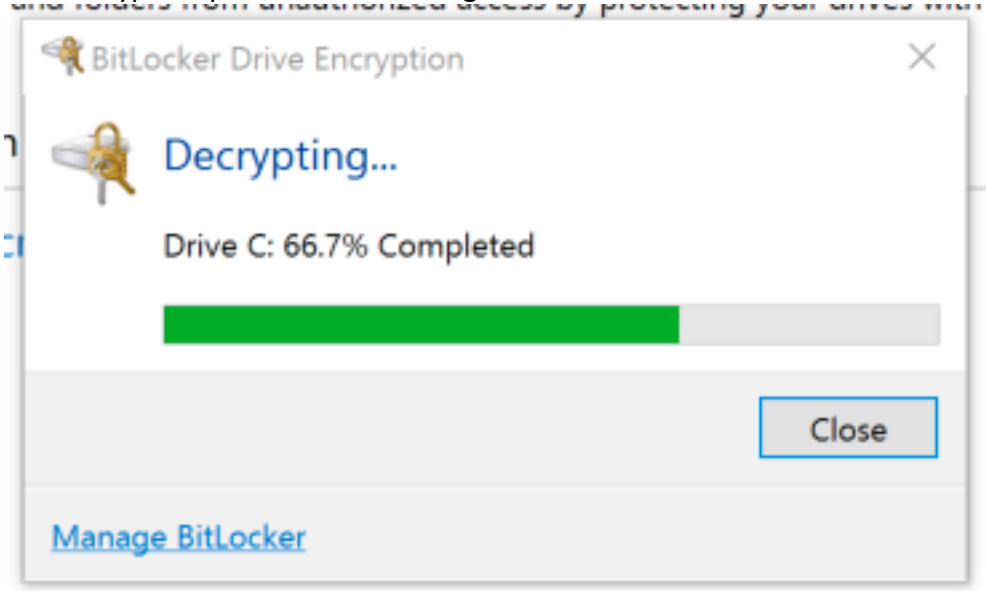


5. Decrypting a drive

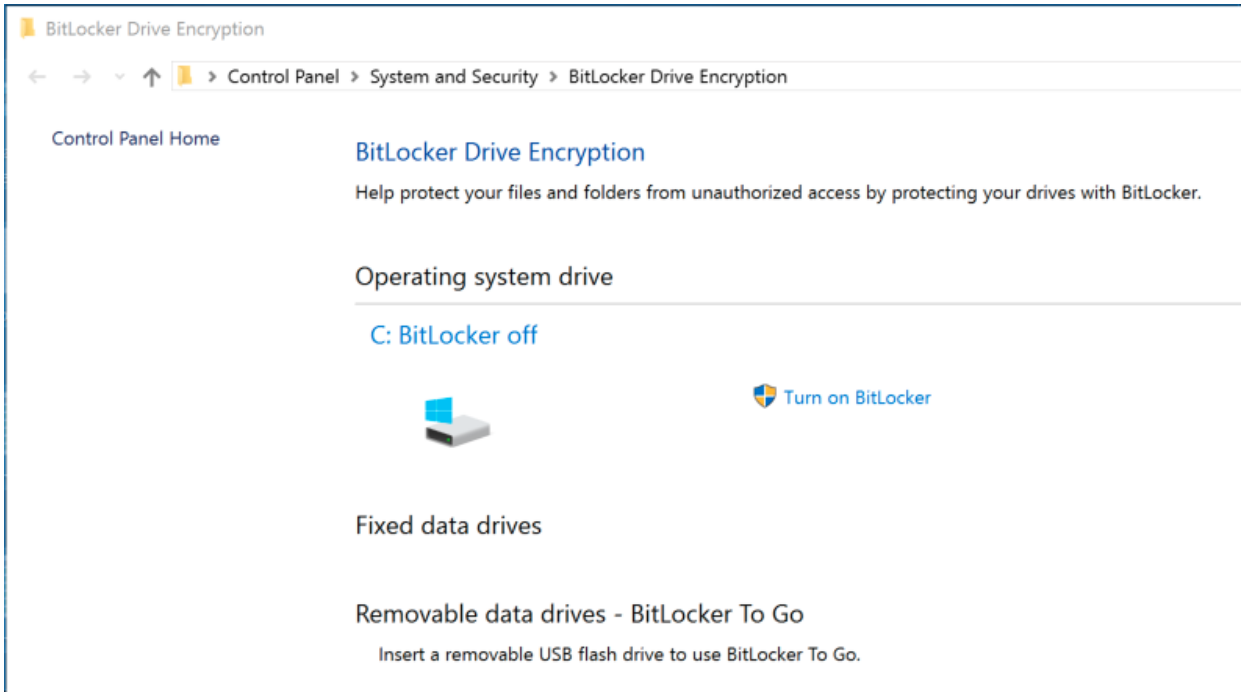
4.1 If you have the need to remove the encryption, the process is just as easy as encrypting. Select the drive you want, right click the icon and select Manage BitLocker.

4.2 You will now need to choose Turn off BitLocker, you may be required to provide an administrative account username and password to allow this action to occur.

4.3 The decryption process will now begin.



4.4 Once the operation is complete, now will notice that in the BitLocker Drive Encryption window, it reports that BitLocker is off, and using Windows Explorer the drive icon has returned to normal.


BitLocker Drive Encryption
Control Panel › System and Security › BitLocker Drive Encryption
Control Panel Home
BitLocker Drive Encryption
Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.
Operating system drive
C: BitLocker off
Turn on BitLocker
Fixed data drives
Removable data drives - BitLocker To Go
Insert a removable USB flash drive to use BitLocker To Go.