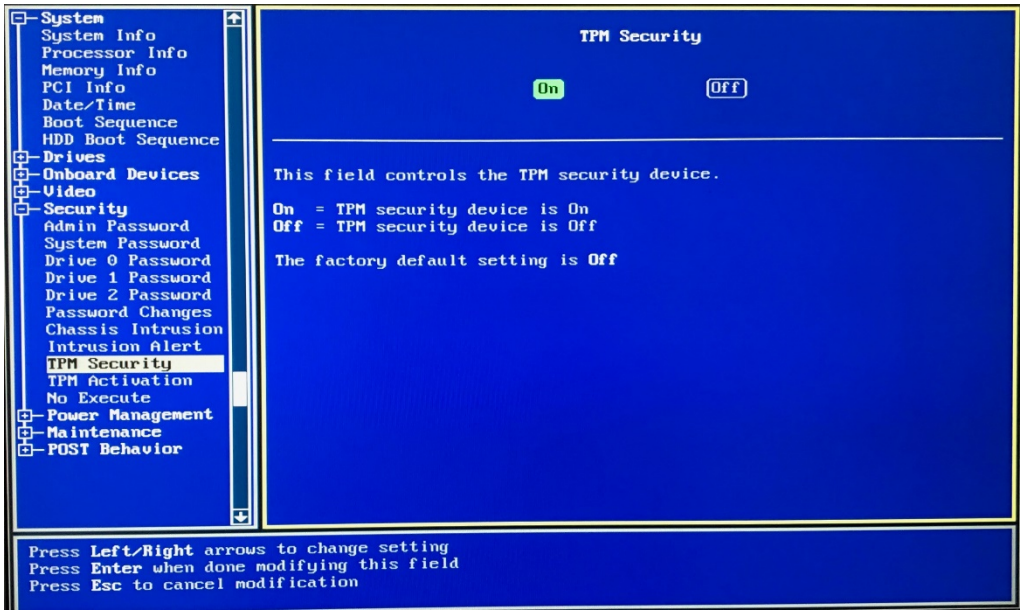
Windows Full Disk Encryption

This guide takes you through the process of configuring Microsoft BitLocker ***full disk encryption*** on a system running Windows 7 or later. BitLocker can be enabled on an existing system – that is, existing data is kept and there should be no need to reinstall things. However, it is highly recommended that all important data be backed up first.

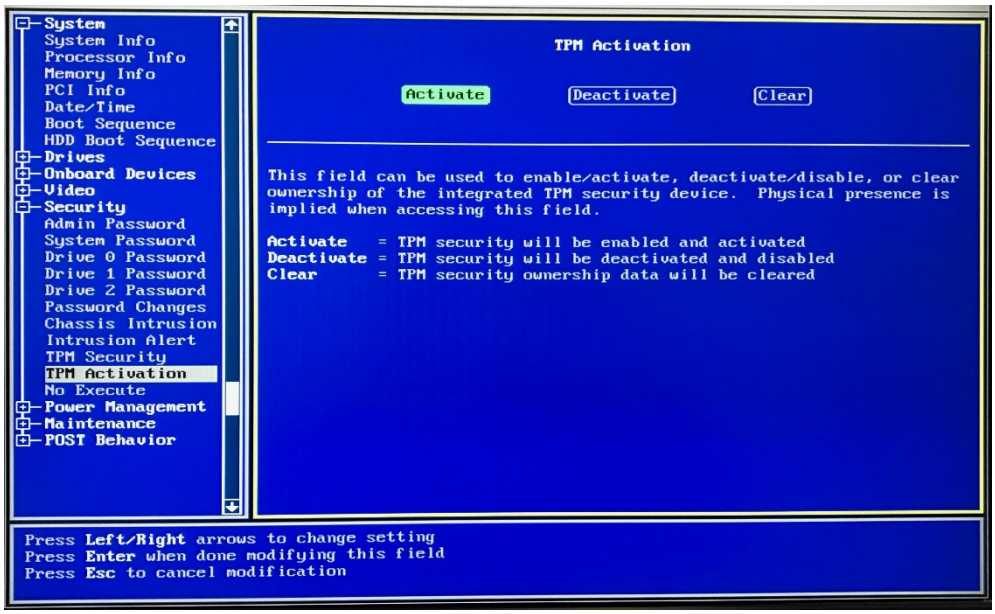
TPM

First, we must ensure the Trusted Platform Module (TPM) chip is enabled and active. You should check this in the system BIOS/UEFI. If you find that you can't enable BitLocker, it's probably due to the TPM not being enabled or activated.

Enable TPM

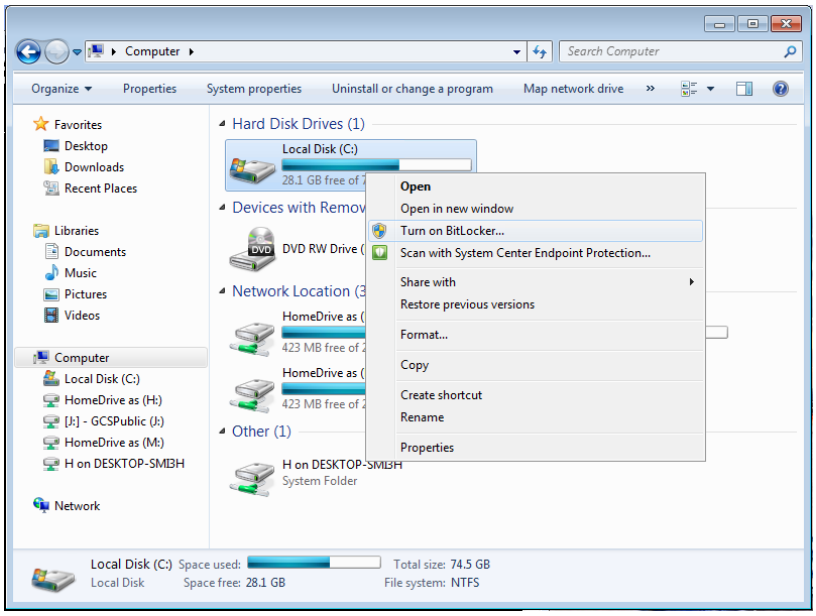


Activate TPM



BitLocker

To enable BitLocker, in Windows Explorer right-click on the system drive (or any other drive you want to encrypt) and select ***Turn BitLocker on***.



This will start the process by first checking the system's configuration. After that, the system will need to be restarted. BitLocker will then begin its setup.

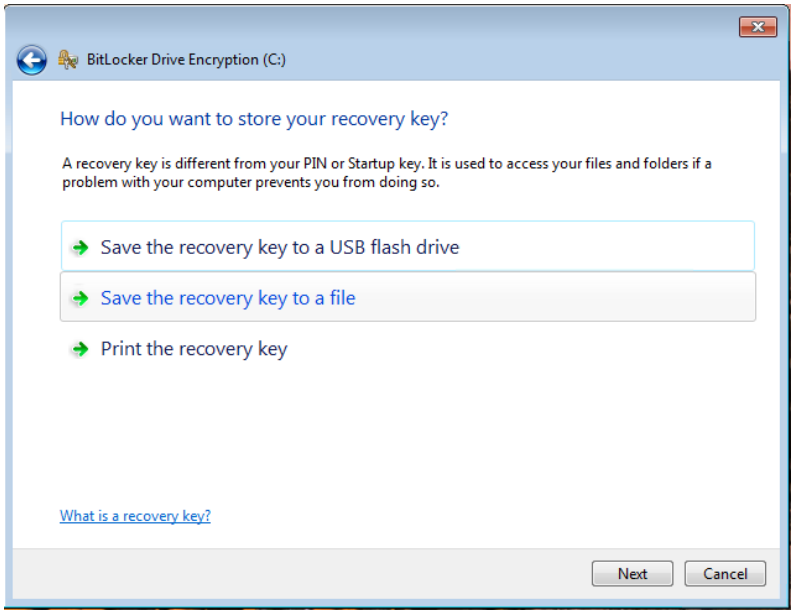
NOTE: You may be asked how much of your drive you wish to encrypt. The options are used space only or entire drive. If this is a brand new computer, you can select the ***used space*** *option. Otherwise, it's safest to choose* ***entire disc.***

NOTE: For Windows 10 you may be asked an additional question during the process about whether you want to use the newer ***XTS-AES*** *encryption. We recommend you select this option for system drive encryption.*

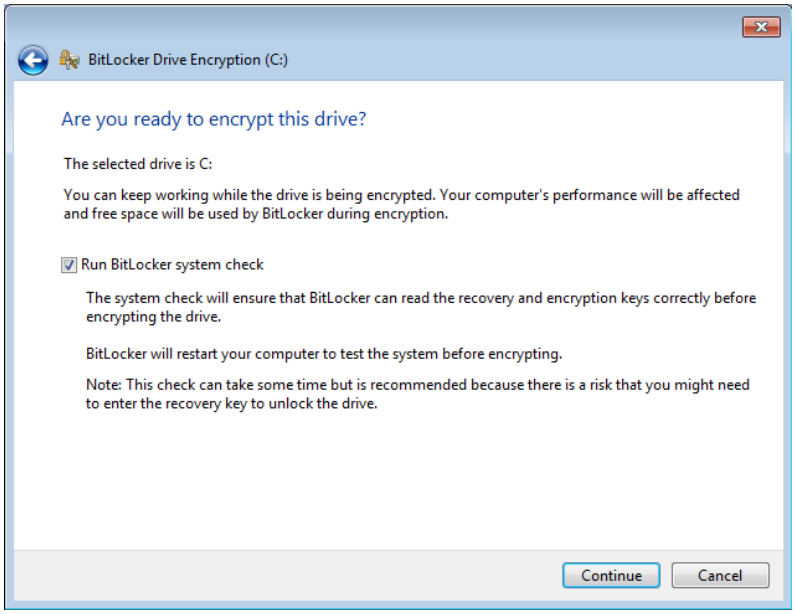
Recovery Key

You will then be asked how you would like to store your recovery key. This is an important step, as the key may be required at a later date. For example, whenever certain changes or upgrades are made to the hardware, BitLocker may require the recovery key to be entered.

We recommend that you store the recovery key in a secure network drive, on a memory stick, or print a copy and keep it in a safe place. (Consider doing more than one of these). For obvious reasons, the system will not allow storing the key in the drive you are encrypting!

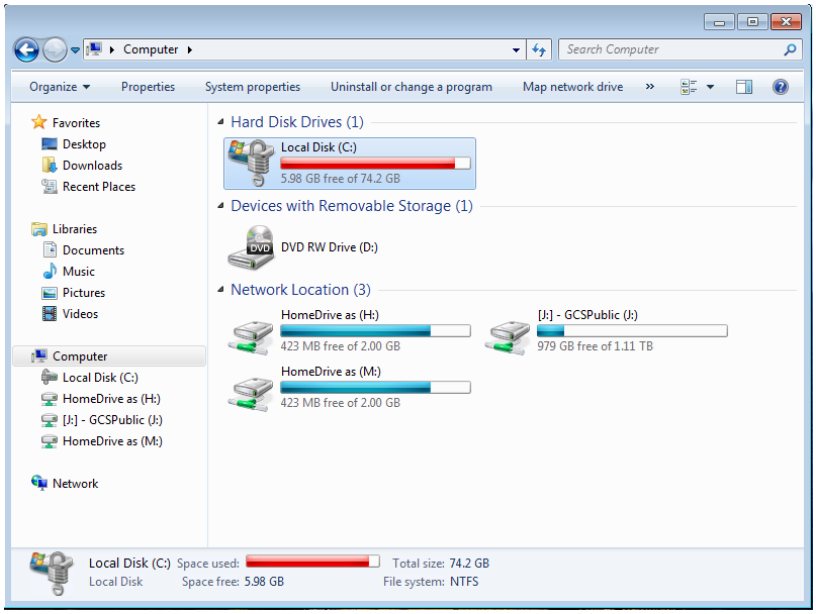


Once the recovery key is saved, the drive is ready to be encrypted. We recommend that you run the BitLocker system check, to ensure that the system can successfully use the recovery key.

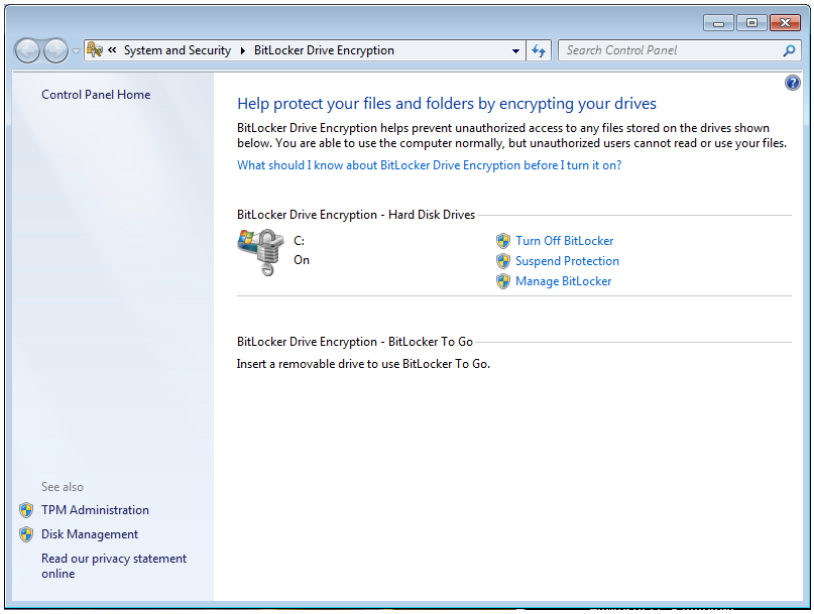


The system will then need to be restarted again, after which the encryption process begins.

Once the system has restarted, you will now notice in Windows Explorer that there is a ***padlock*** on the drive, which denotes that BitLocker is tuned on for this drive.



In the BitLocker Drive Encryption control panel, you'll see that the drive is Encrypting. Once completed, the BitLocker control panel will confirm that ***BitLocker is on***.



You'll be able to use the system whilst the drive is being encrypted, however whilst this is in progress, it may be sluggish, and then return to normal once the encryption process is complete (which could be a few hours, or longer, so consider letting it run overnight). Thereafter, BitLocker should have no noticeable effect on system performance.

Advanced management

The command line tool provides further information about the system's disks and their BitLocker status, as well as allowing you to control other aspects of disk encryption. We can use it to also monitor the disc encryption progress, shown below via the command, **manage-bde -status**. For more functionality see the output from the command **manage-bde -?**.

NOTE: You require local admin rights to run manage-bde commands.