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.

System System Info Processor Info Memory Info PCI Info Date/Time Boot Sequence HDD Boot Sequence Parimee TPM Security Off On board Devices This field controls the TPM security device. Video On = TPM security device is On Off = TPM security device is Off curitu ecurry dmin Password ystem Password prive O Password The factory default setting is **Off** sswor Chang Chassis Intrus Intrusion Aler TPM Security TPM Activation No Execute Power Management Maintenance POST Behavior Press **Left/Right** arrows to change setting Press **Enter** when done modifying this field Press **Esc** to cancel modification

Activate TPM

E-Sustem 🖪								
System Info	TPM Activation							
Processor Info								
Memory Info								
PCI Info	Activate Deactivate (Clear)							
Date/Time								
Boot Sequence								
HDD Boot Sequence								
🕀 – Drives								
🕀-Onboard Devices	This field can be used to enable/activate, deactivate/disable, or clear							
∲−Video	ownership of the integrated TPM security device. Physical presence is							
Ģ−Security	implied when accessing this field.							
Admin Password								
System Password	Activate = TPM security will be enabled and activated							
Drive O Password	Deactivate = TPM security will be deactivated and disabled							
Drive 1 Password	Clear = TPM security ownership data will be cleared							
Drive 2 Password								
Password Changes								
Chassis Intrusion								
Intrusion Alert								
TPM Security								
TPM Activation								
No Execute								
🛨 Power Management								
🕀 – Maintenance								
D T Of Blatt	to always setting							
Press Left/Right arrows to change setting								
Press Ener when done modification								
rress LSC to cancer muc	The feat for							

Enable 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!

🚱 🎭 BitLocker Drive Encryption (C:)	x
How do you want to store your recovery key? A recovery key is different from your PIN or Startup key. It is used to access your files and folders if a problem with your computer prevents you from doing so.	
Save the recovery key to a USB flash drive	
Save the recovery key to a file	
Print the recovery key	
What is a recovery key?	
Next Can	ncel

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.

😋 🗢 🖳 🕨 Computer 🕨	
Organize Properties	System properties Uninstall or change a program Map network drive » 🔮 🔻 🔳 🔞
 ★ Favorites ■ Desktop ▶ Downloads ③ Recent Places ② Documents > Music ≅ Pictures ⊠ Videos ★ Computer ♦ Local Disk (C:) ♀ HomeDrive as (M:) ♥ Network 	Hard Disk Drives (1) Local Disk (C:) S.98 GB free of 74.2 GB Devices with Removable Storage (1) DVD RW Drive (D:) Network Location (3) HomeDrive as (H:) Y 423 MB free of 2.00 GB Y 123 MB free of 2.00 GB Y
Local Disk (C:) Spa Local Disk Spi	ce used: Total size: 74.2 GB ace free: 5.98 GB File system: NTFS

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*.

									- 0	×
	🚫 🗢 🏘 « System and Security	 BitLocke 	r Drive Encryption		•	4 7	Search Control Pa	nel		٩
	Control Panel Home									0
		Help protect your files and folders by encrypting your drives								
		BitLocker Drive Encryption helps prevent unauthorized access to any files stored on the drives show below. You are able to use the computer normally, but unauthorized users cannot read or use your								
		What should I know about BitLocker Drive Encryption before I turn it on?								
		BitLocker Drive Encryption - Hard Disk Drives								
		🤷 🖉	3		🛞 Tur	rn Off	BitLocker			
			Dn		😗 Sus	spend	Protection			
		0			😗 Ma	inage	BitLocker			
		BitLocker Drive Encryption - BitLocker To Go Insert a removable drive to use BitLocker To Go.								
	See also									
0	TPM Administration									
0	Disk Management									
	Read our privacy statement online									
-										_

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.

