Encrypting with BitLocker for disk volumes under Windows 7

Summary of the contents

1. Introduction

BitLocker was introduced in Windows Vista and is also supported in Windows 7. You can use BitLocker Drive Encryption to help protect all files stored on the drives where Windows is installed (the operating system drive) as well as those on fixed data drives (internal hard drives).

BitLocker will encrypt the entire drive. The encryption is transparent to users who log on the system. That is, they can work with their files in normal way while the system performs the encryption and decryption for them automatically.

BitLocker can help block hackers from accessing the system files they rely on to discover your password or any information in the drive, even if it is removed from your computer and installed in another computer.

Files remain encrypted only while they are stored in the encrypted drive. Files copied out or transferred through network from encrypted drive are in their decrypted form.

It is very important to note that if you encrypt the operating system drive, BitLocker checks the computer during startup for any conditions that could represent a security risk (for example, a change to the BIOS or changes to any startup files). If a potential security risk is detected, BitLocker will lock the operating system drive and require a special

BitLocker recovery key to unlock it. Make sure that you create this recovery key and keep it in a safe place when you turn on BitLocker for the first time; otherwise, you could permanently lose access to your files and no one will be able to help. If your computer has the Trusted Platform Module (TPM) chip, BitLocker uses it to seal the keys that are used to unlock the encrypted operating system drive. When you start your computer, BitLocker asks the TPM for the keys to the drive and unlocks it.

If you encrypt fixed data drives, you can add additional authentication to unlock an encrypted drive with either a password or a smart card with PIN. If additional authentication is not preferred, then just set the drive to automatically unlock when you log on to the computer. If you forget the password or lose the smartcard, you also have to use the BitLocker recovery key to unlock the drive.

2. Hardware requirements for BitLocker Drive Encryption

To use BitLocker Drive Encryption, your computer has to meet certain hardware requirements. These requirements vary depending on the type of drive that you are encrypting.

To encrypt the drive that Windows is installed on (the operating system drive), BitLocker stores its own encryption and decryption key in a hardware device that is separate from your hard disk, so you must have one of the following:

- A computer with Trusted Platform Module (TPM), which is a special microchip in many computers that supports advanced security features. If your computer was manufactured with TPM version 1.2 or higher, BitLocker will store its key in the TPM.

- A removable USB memory device, such as a USB flash drive. If your computer does not have the TPM version 1.2 or higher, BitLocker will store its key on the flash drive. This option is only available if your system administrator has set up your network to allow the use of a start-up key instead of the TPM.

To turn on BitLocker Drive Encryption on the operating system drive, your computer's hard disk must:

- Have at least two partitions: a system partition (which contains the files needed to start your computer and must be at least 100 MB) and an operating system partition (which contains Windows). The operating system partition will be encrypted and the system partition will remain unencrypted so that your computer can start. If your computer does not have two partitions, BitLocker will create them for you. Both partitions must be formatted with the NTFS file system.

- Have a BIOS that is compatible with TPM or supports USB devices during computer startup.

You can also use BitLocker to encrypt fixed data drives (such as internal hard drives) by using either a password or a smartcard with PIN.

3.1 Encrypting Operating System Drive

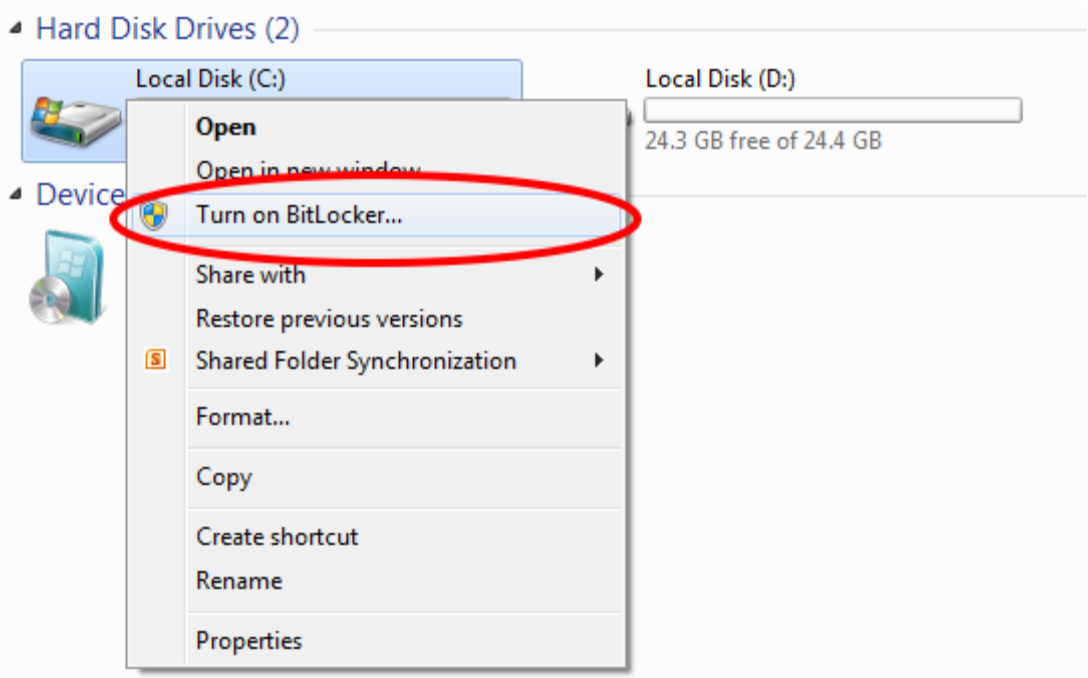
3.1.1 with TPM

On computers with a compatible TPM, startup of TPM can be configured and unlocked in one of the following four ways depending on whether additional authentication, if any, is required:

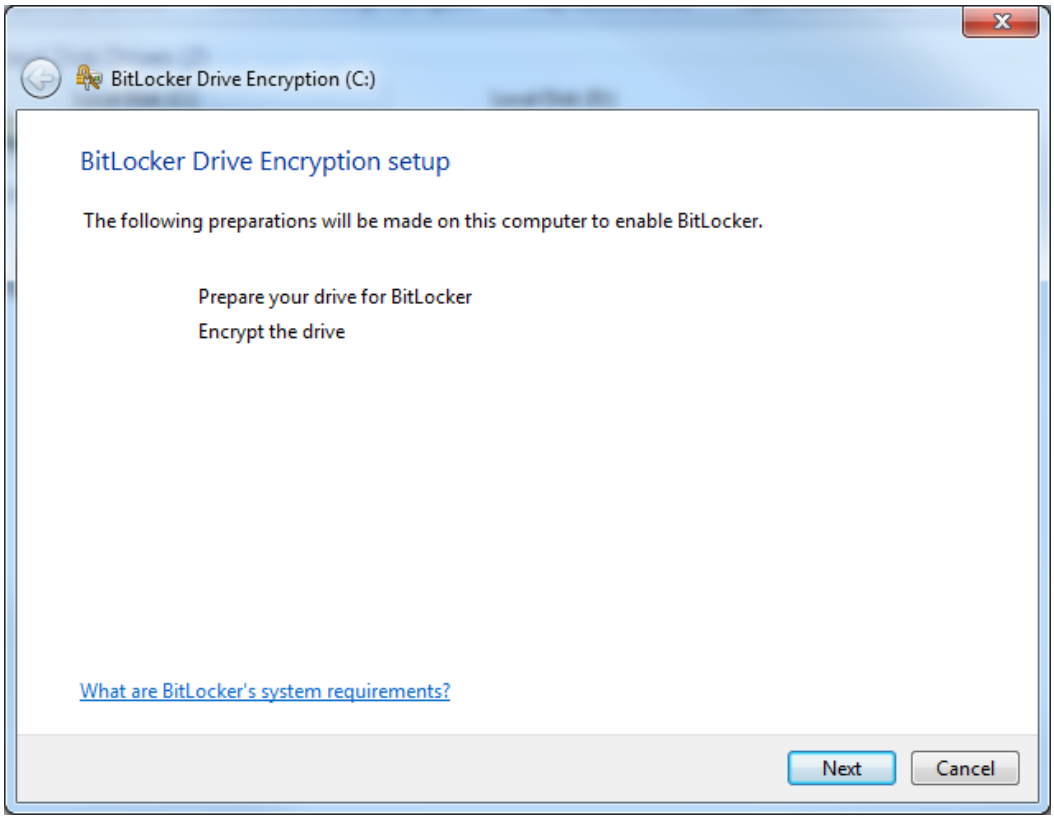
- Allow TPM only
- Allow startup key with TPM
- Allow PIN with TPM
- Allow startup key and PIN with TPM

As not each of these additional authentications is provided by default or can be user selectable, you or your administrator must allow it in group policy and configure BitLocker settings using the command-line tool first. For simplicity, some of the less common additional authentications are not shown in the examples.

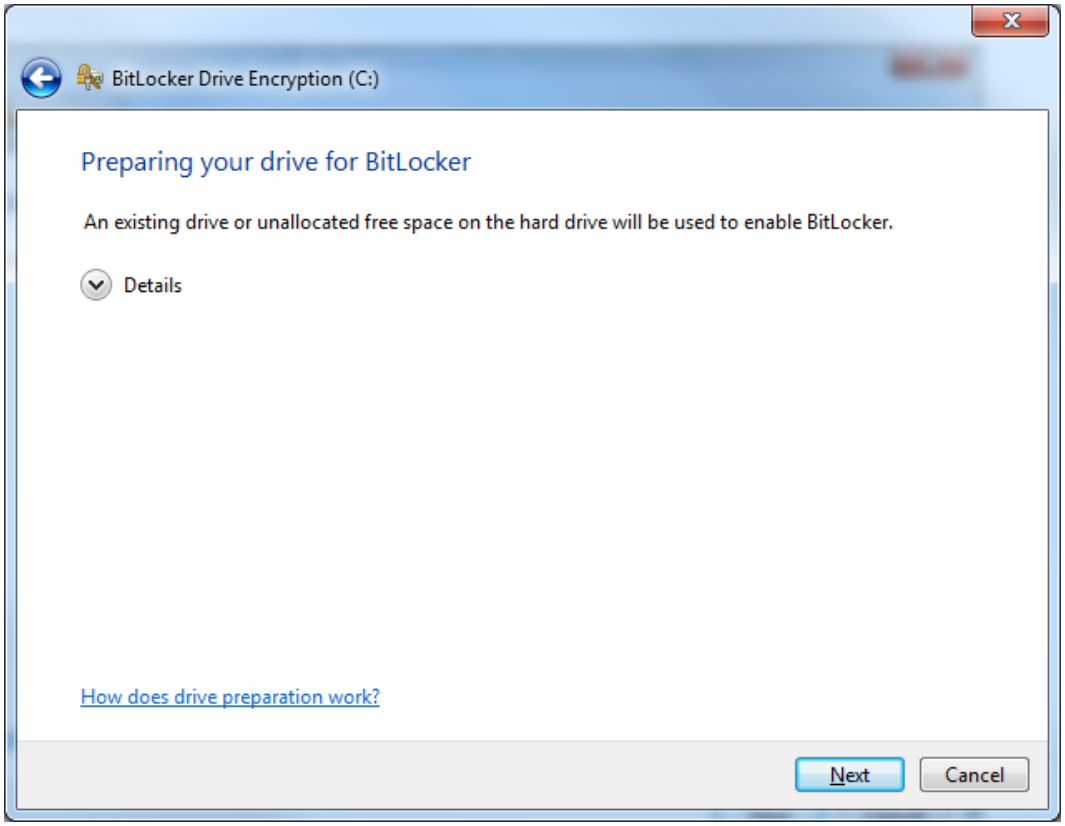
i. Right-click on the operating system drive icon and select the “Turn on BitLocker”



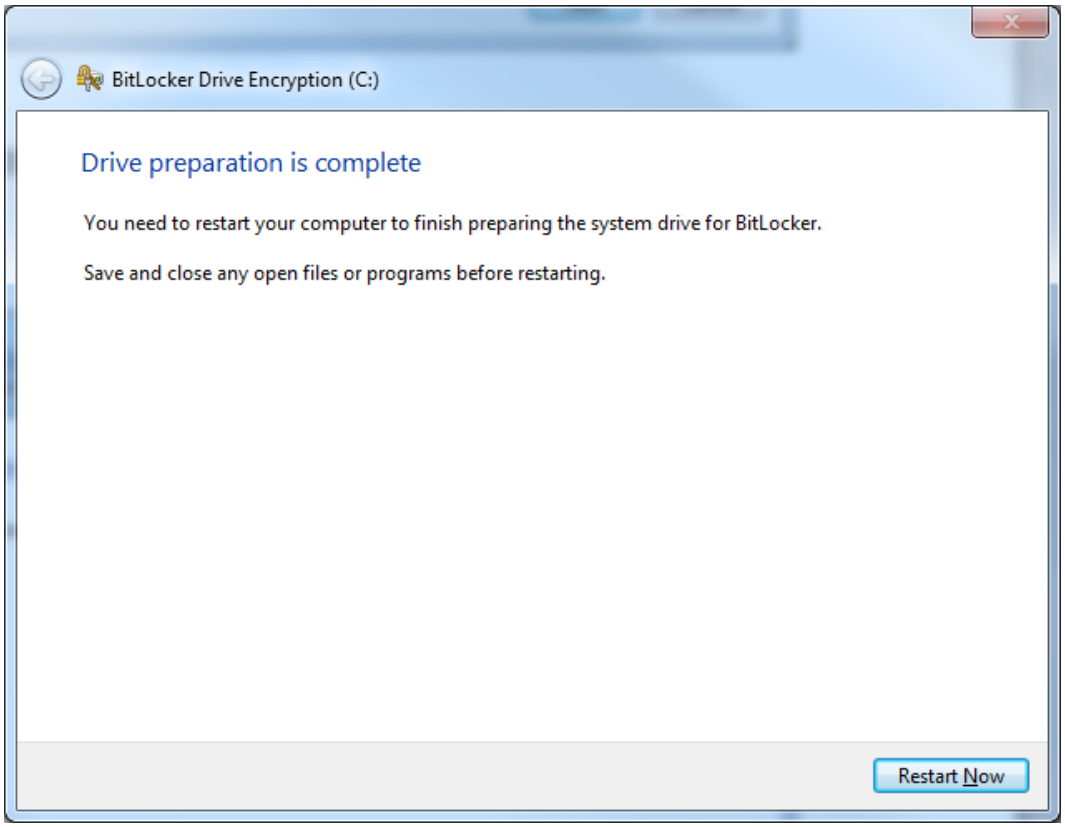
ii. Click “Next”



iii. Click “Next”

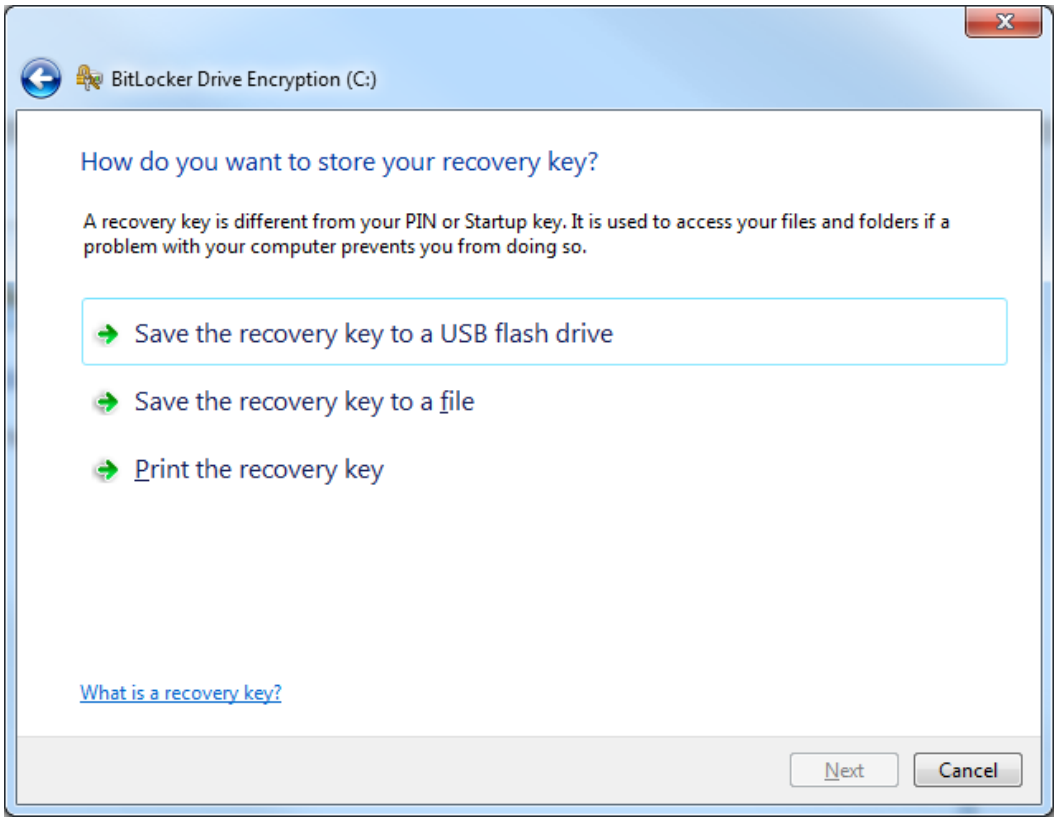


iv. Save and close any open files or programs, then click “Restart Now”

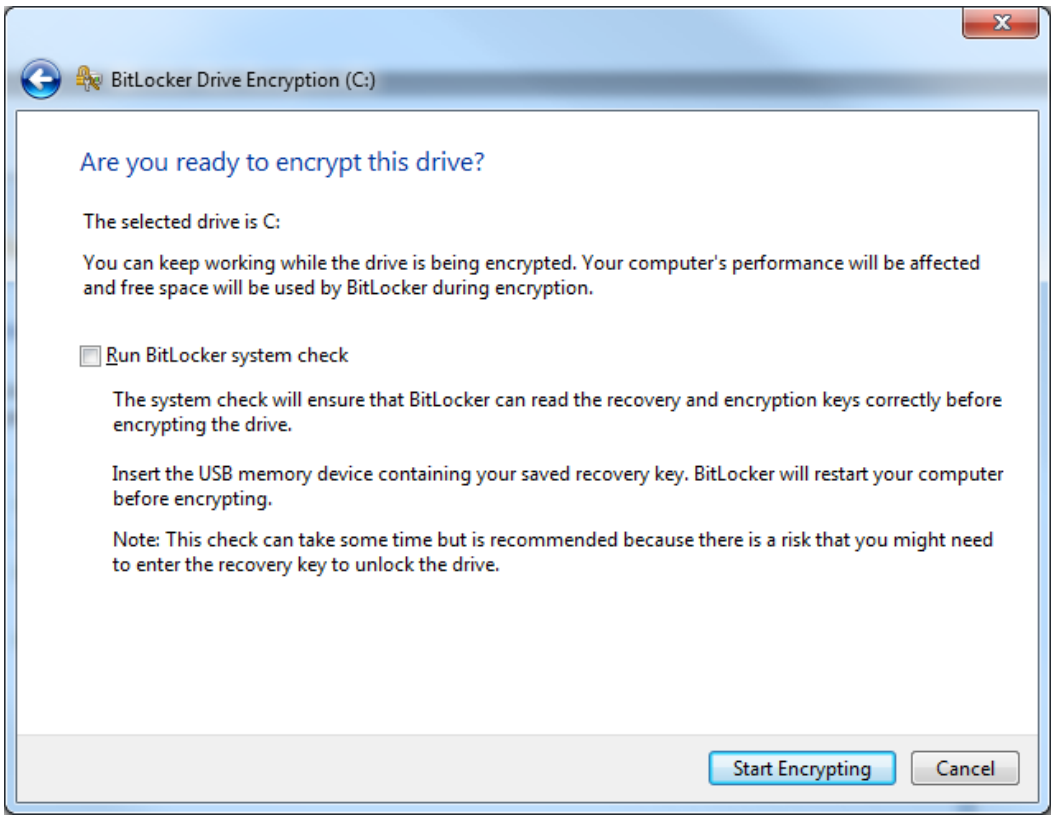


v. After the restart, click “Next”

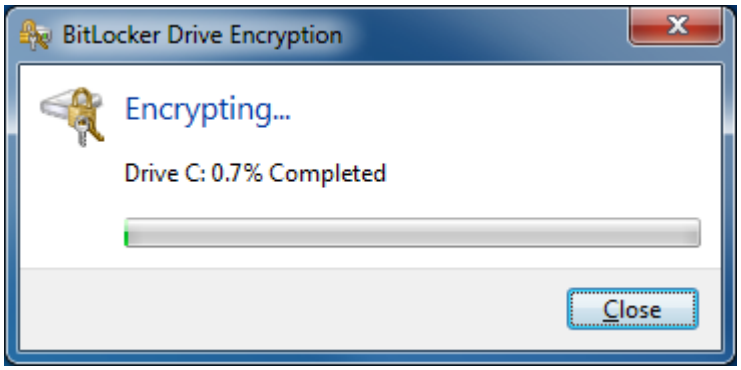
vi. Save or print the recovery key, then click “Next”



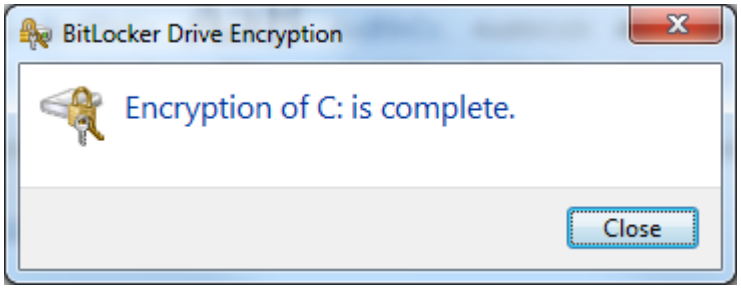
vii. Click “Start Encrypting”



viii. During the encryption process, a progress monitor will be shown. The amount of time that it will take to complete the process varies, depending mainly on the size of your drive.



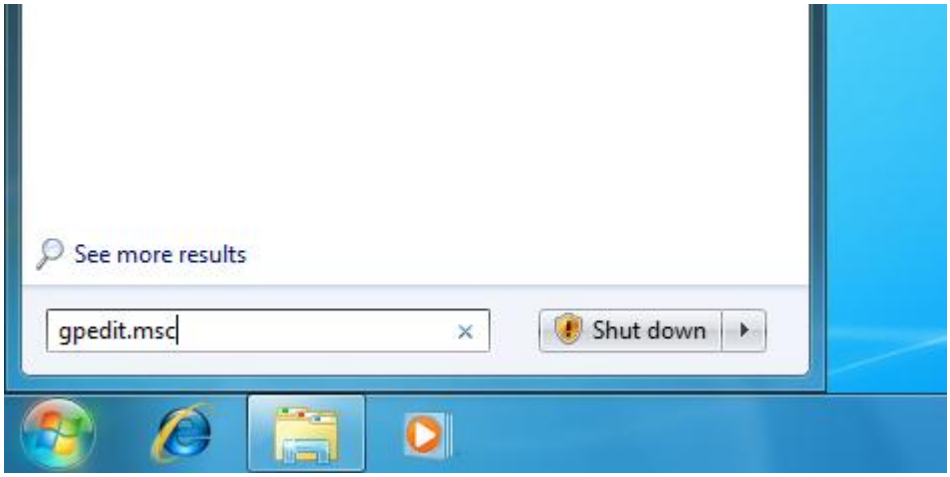
ix. Click "Close" to complete the encryption



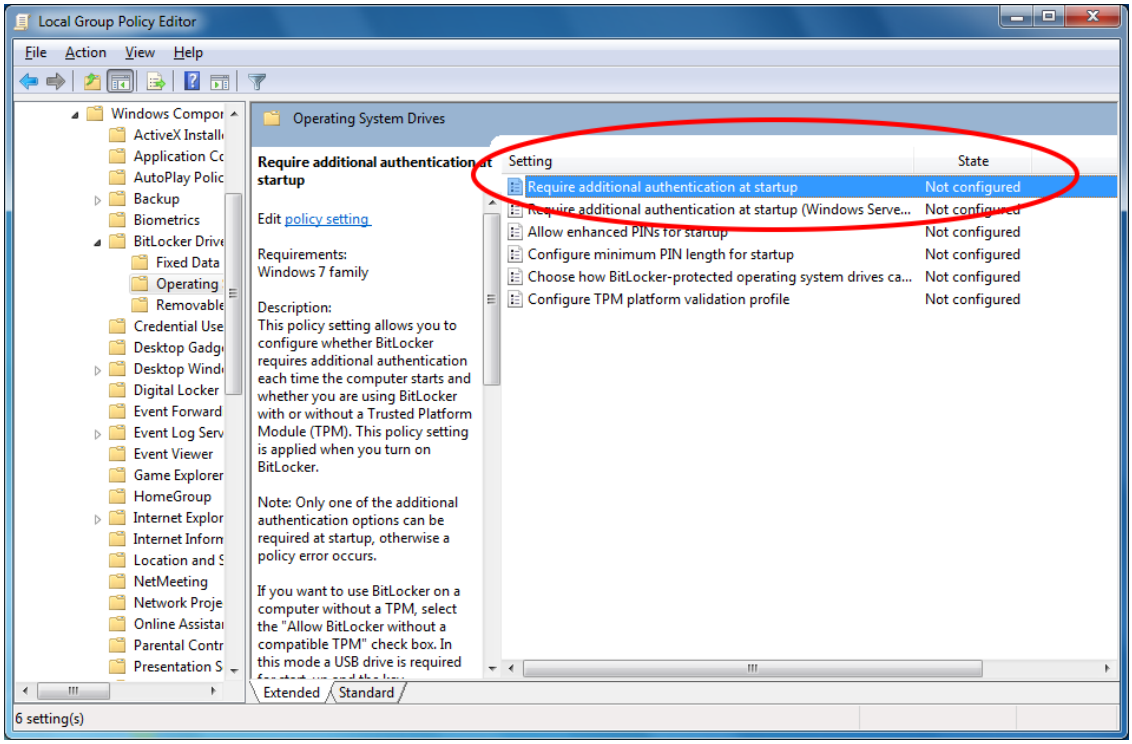
3.1.2 Without TPM

If your computer does not have a TPM, you can still use BitLocker, but you will be using the Startup-key-only authentication method. ***All of the required encryption key information is stored on a USB flash drive, which the user must insert into the computer during startup. The key stored on the USB flash drive unlocks the computer***. **Unlike using a TPM that helps protect against attacks made against the computer's critical startup process,** the Startup-key-only authentication method only encrypts the drive; it does not provide any validation of the early boot components or hardware tampering. To use this method, your computer must support the reading of USB devices in the preboot environment and you must enable this authentication method by selecting the check box ***Allow BitLocker without a compatible TPM*** in the Group Policy setting ***Require additional authentication at startup***, which is located in the following location in the Local Group Policy Editor: ***Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives***.

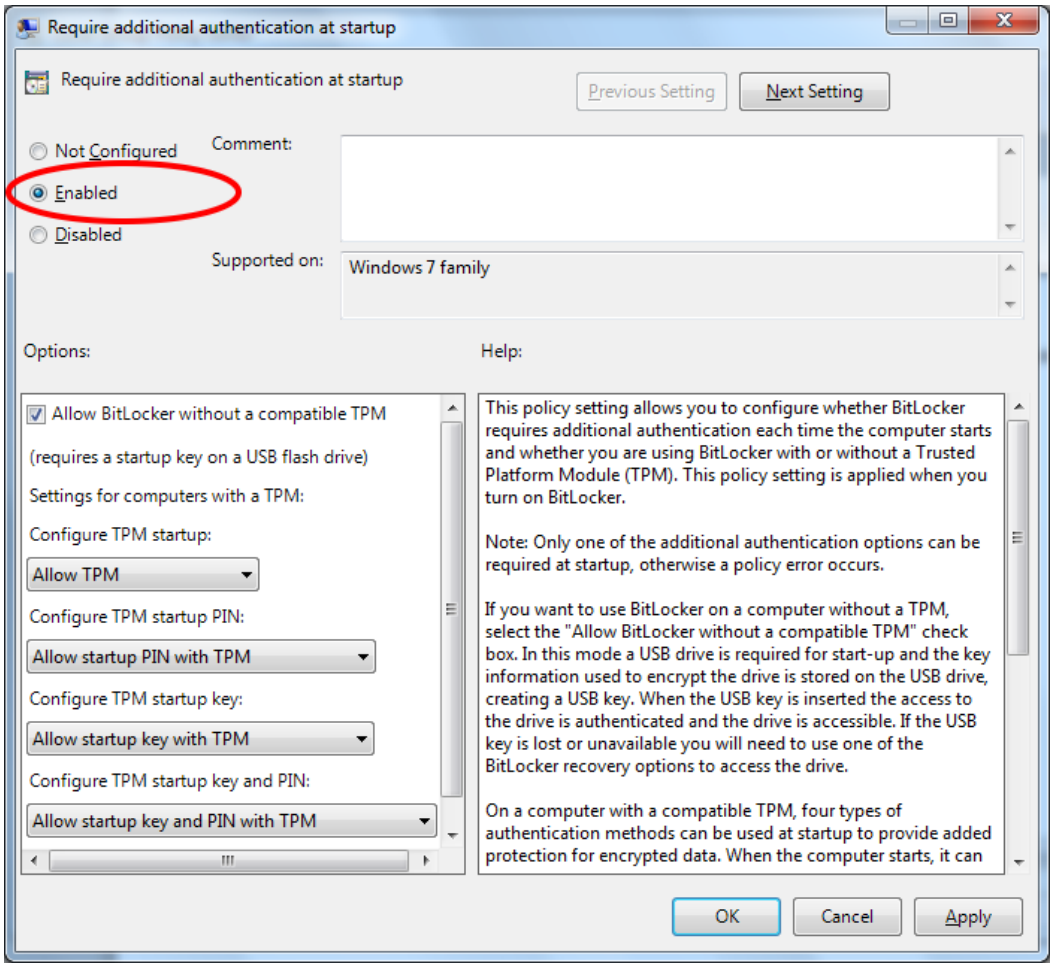
i. Enter in "gpedit.msc" in the search box of the Start menu and press Enter.



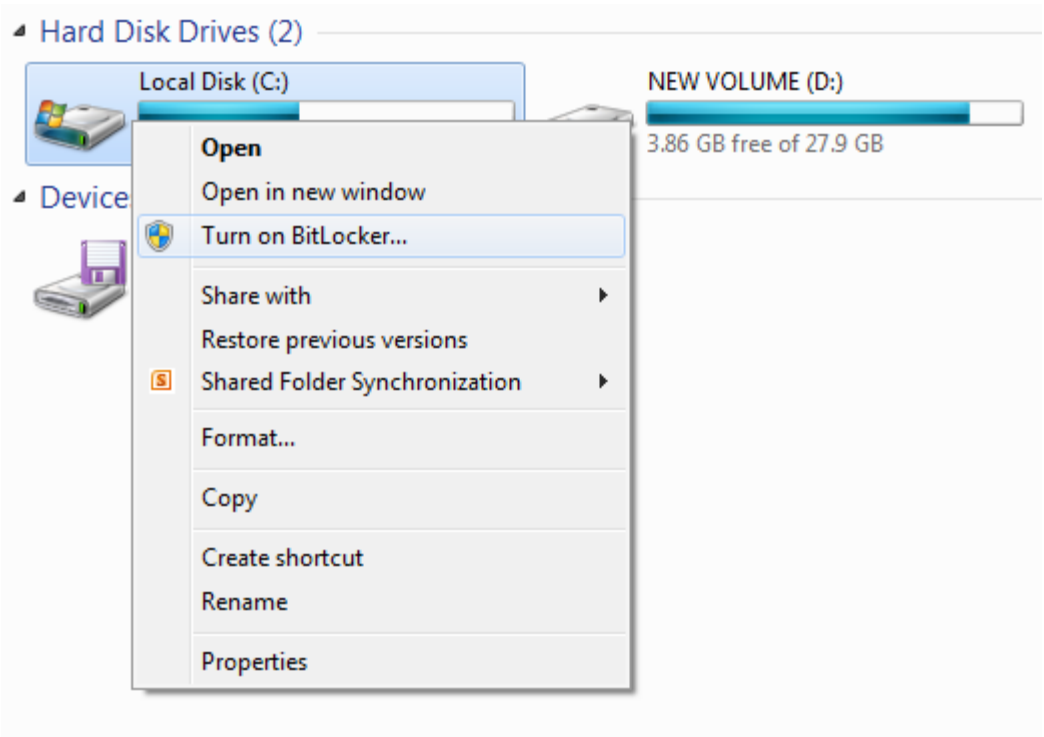
ii. Under “Local Computer Policy” , navigate to Computer Configuration \ Administrative Templates \ Windows Components \ BitLocker Drive Encryption \ Operating System Drives and click “Require additional authentication at startup”



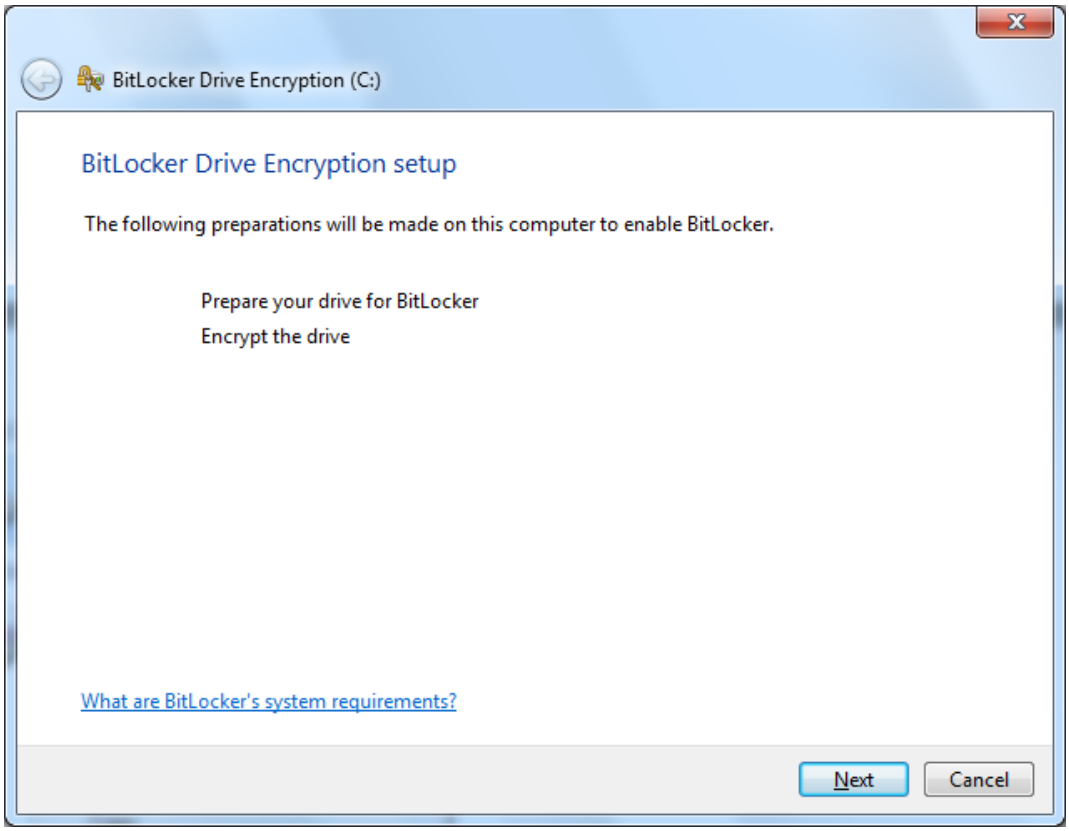
iii. Select “Enabled” and click “OK”



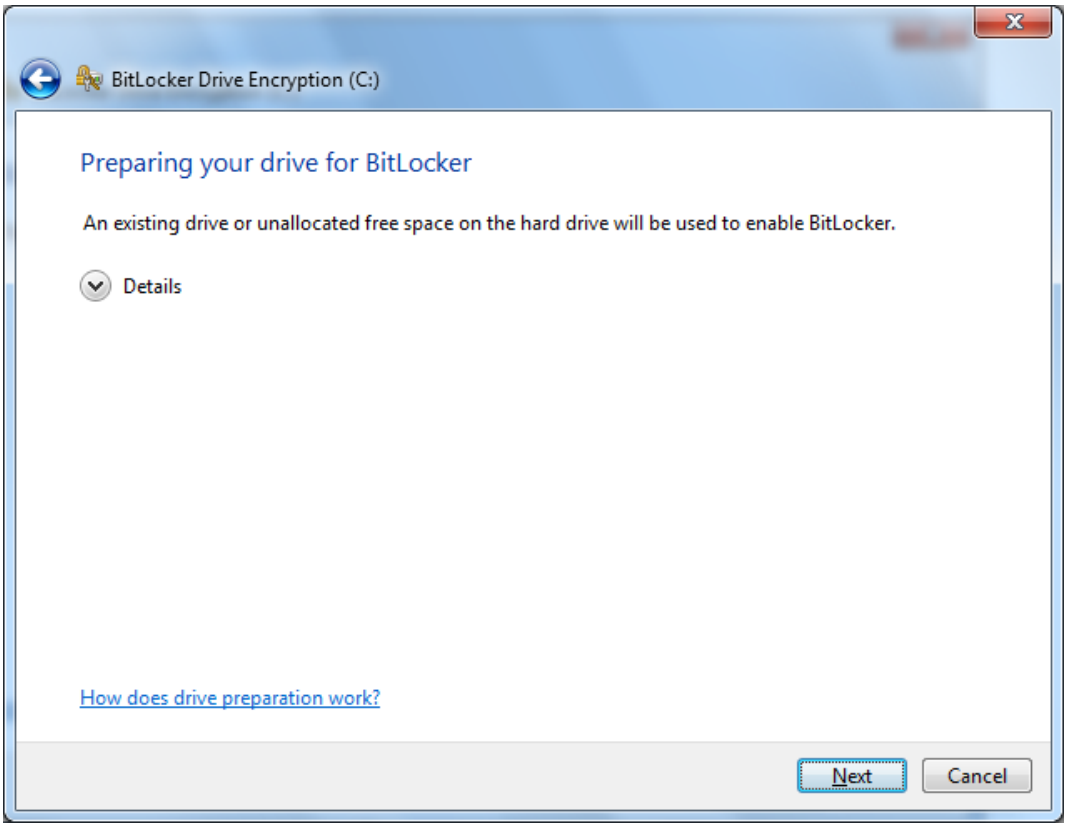
iv. Right-click on the operating system drive icon and select the “Turn on BitLocker”



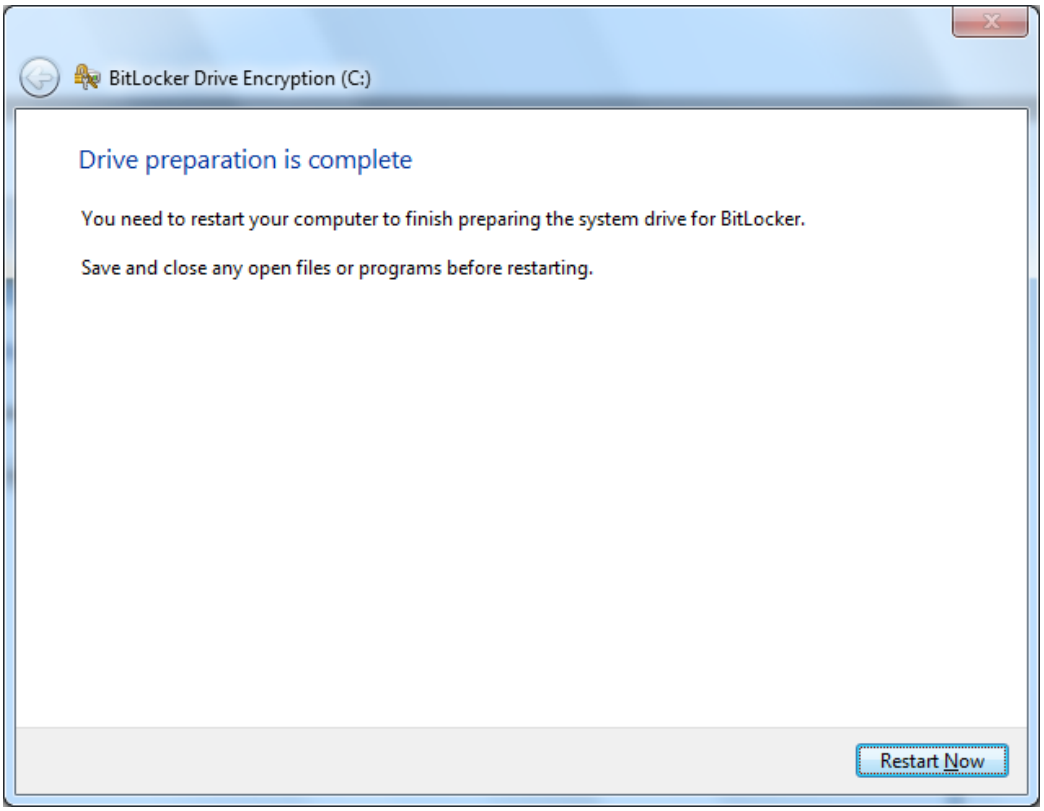
v. Click “Next”



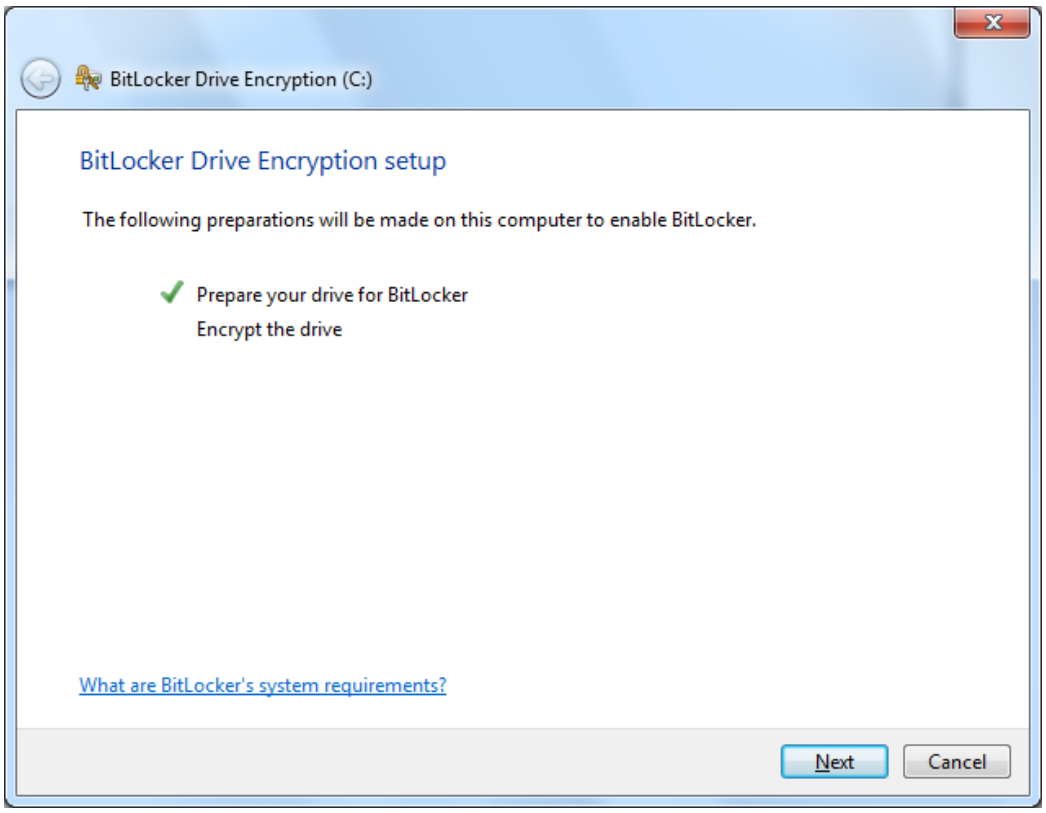
vi. Click “Next”



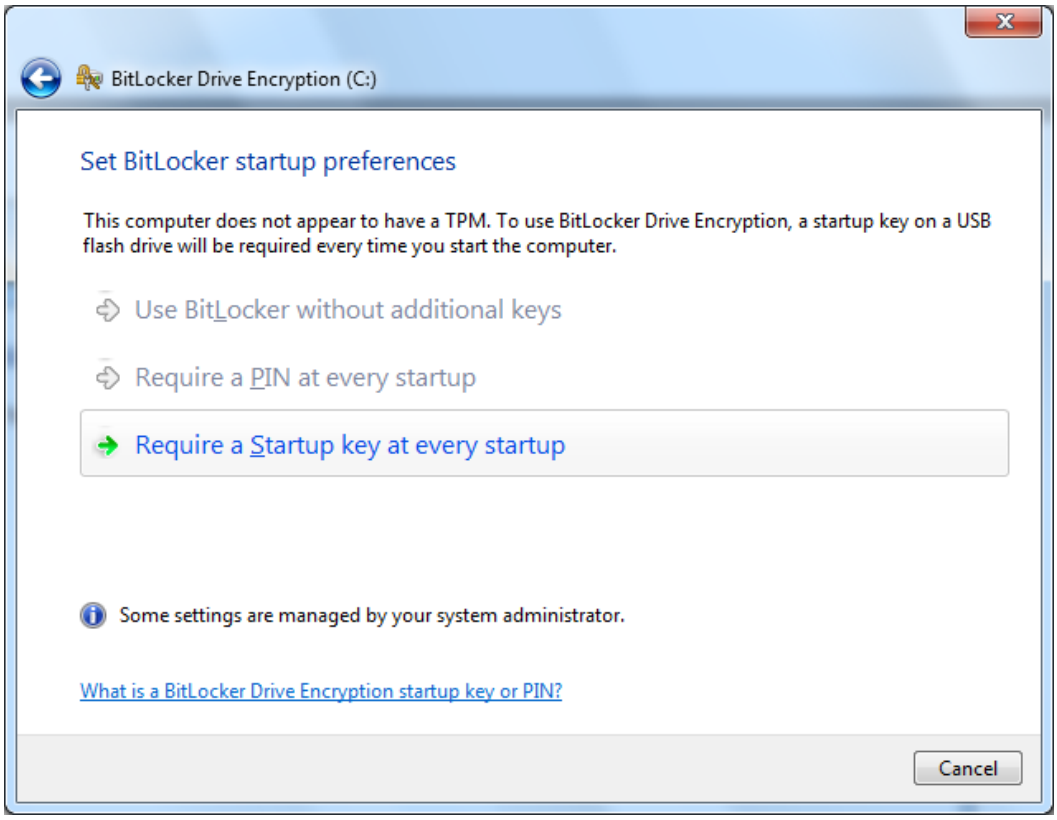
vii. Save and close any open files or programs, then click “Restart Now”



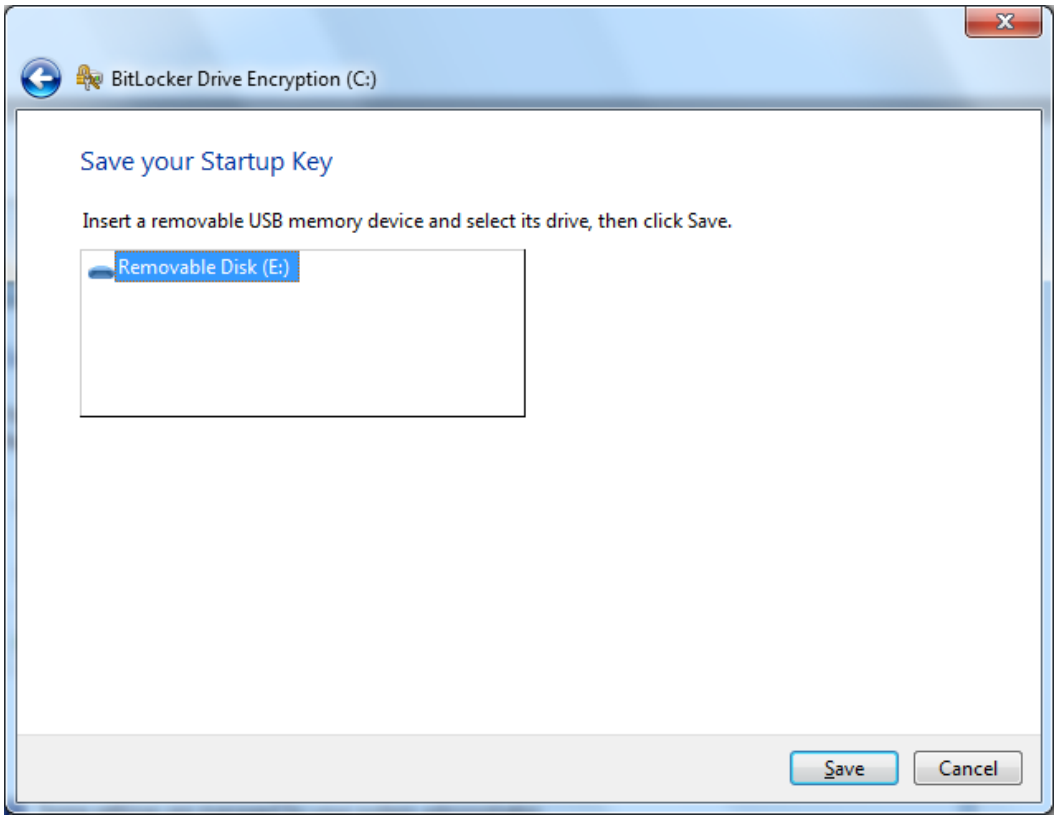
viii. After the restart, click “Next” to continue



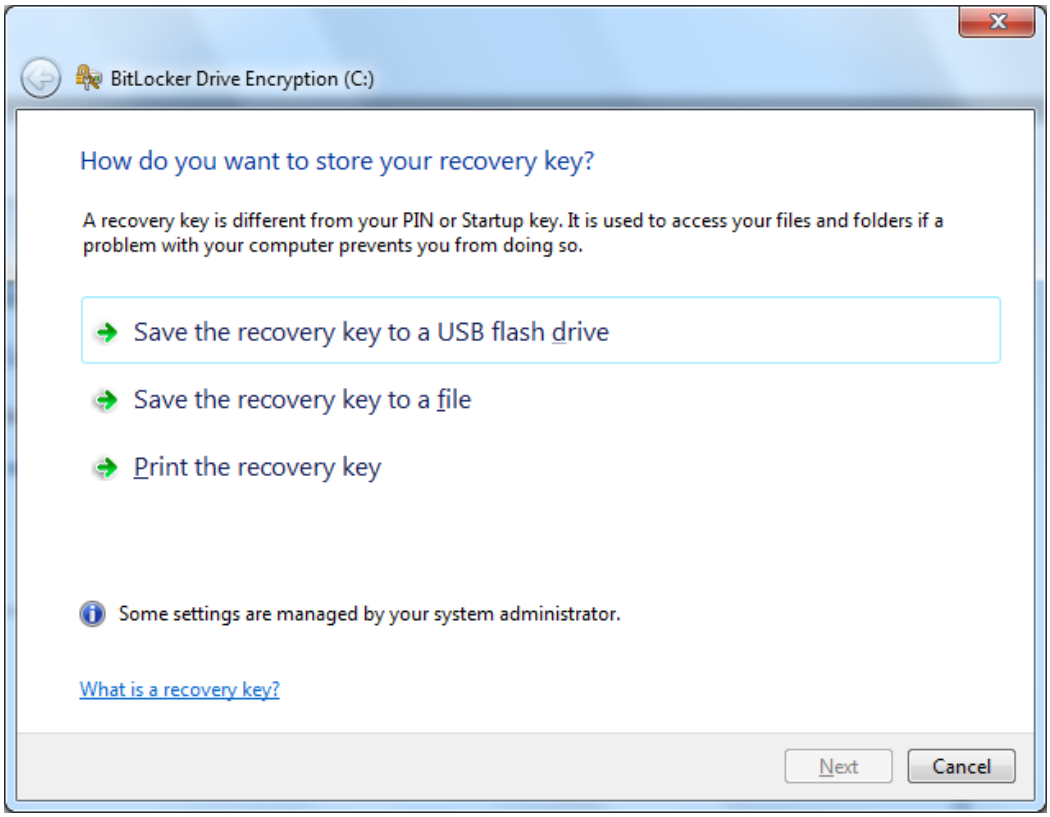
ix. Click “Require a Startup key at every startup”



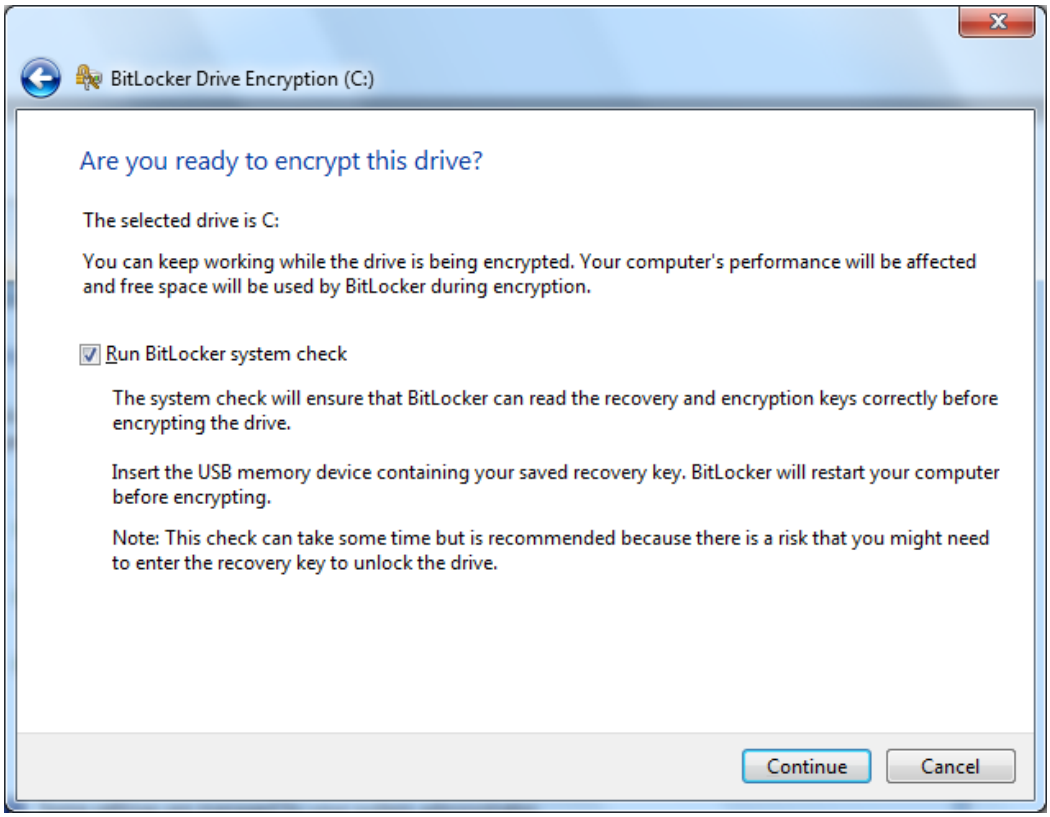
x. Insert a removable USB drive and select its drive, then click “Save”



xi. Save or print the recovery key, then click “Next”

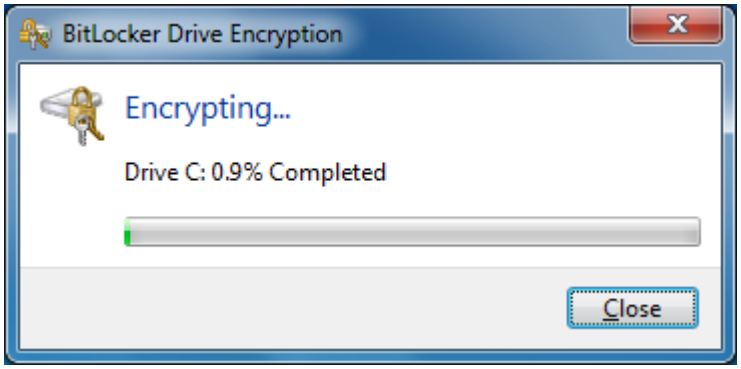


xii. Click “Continue”

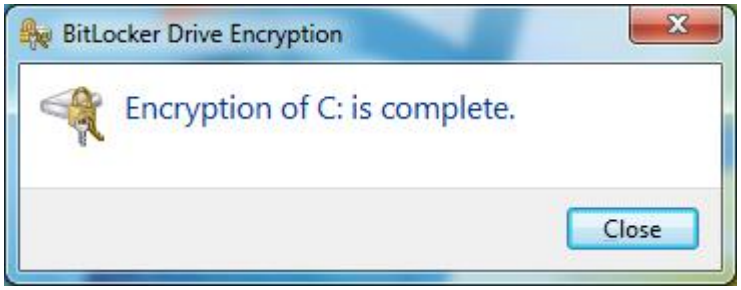


xiii. Save and close all the editing files and click “Restart Now”

xiv. The Encryption will be started after restart. During the encryption process, a progress monitor will be shown. The amount of time that it will take to complete the process varies, depending mainly on the size of your drive



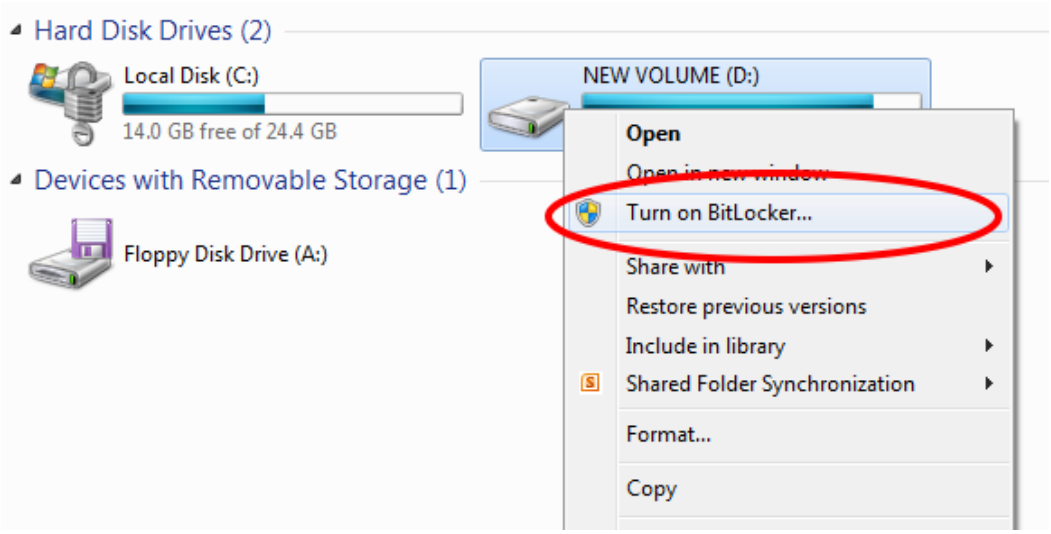
xv. Click “Close” to complete the encryption



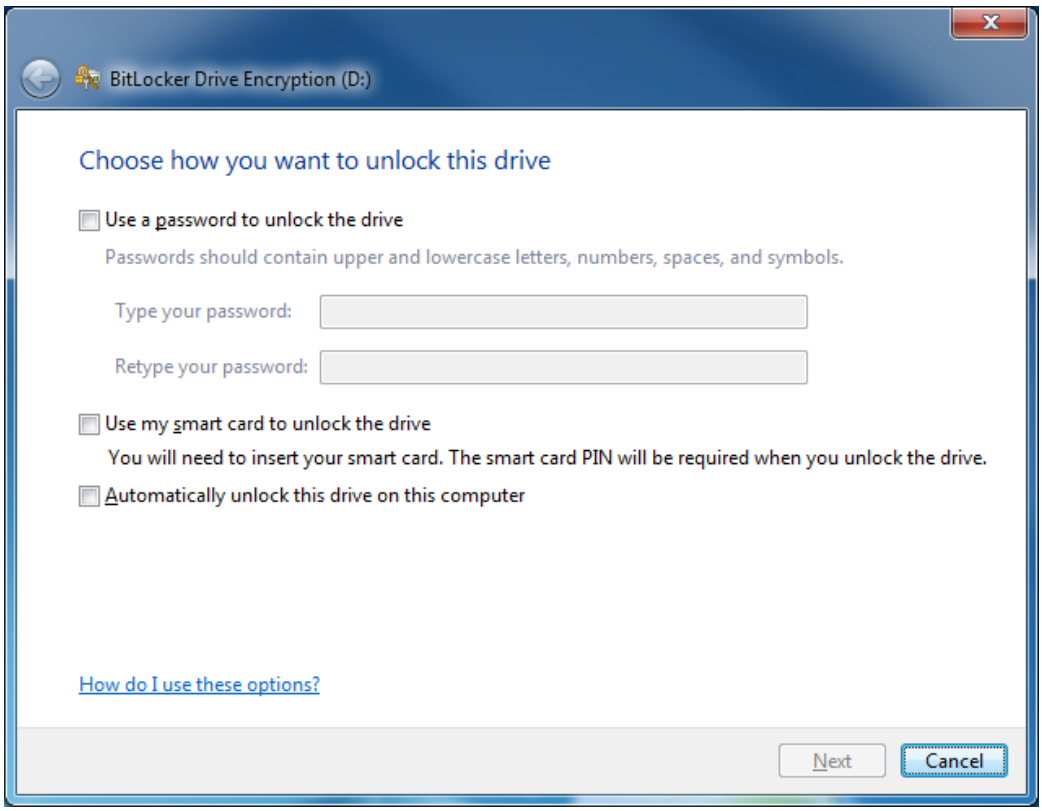
3.2 Encrypting Fixed Data Drive

In addition to encrypting fixed data drive by turning on the BitLocker, you can also specify additional authentication (using either password or smart card with PIN) to unlock the drive if so desired.

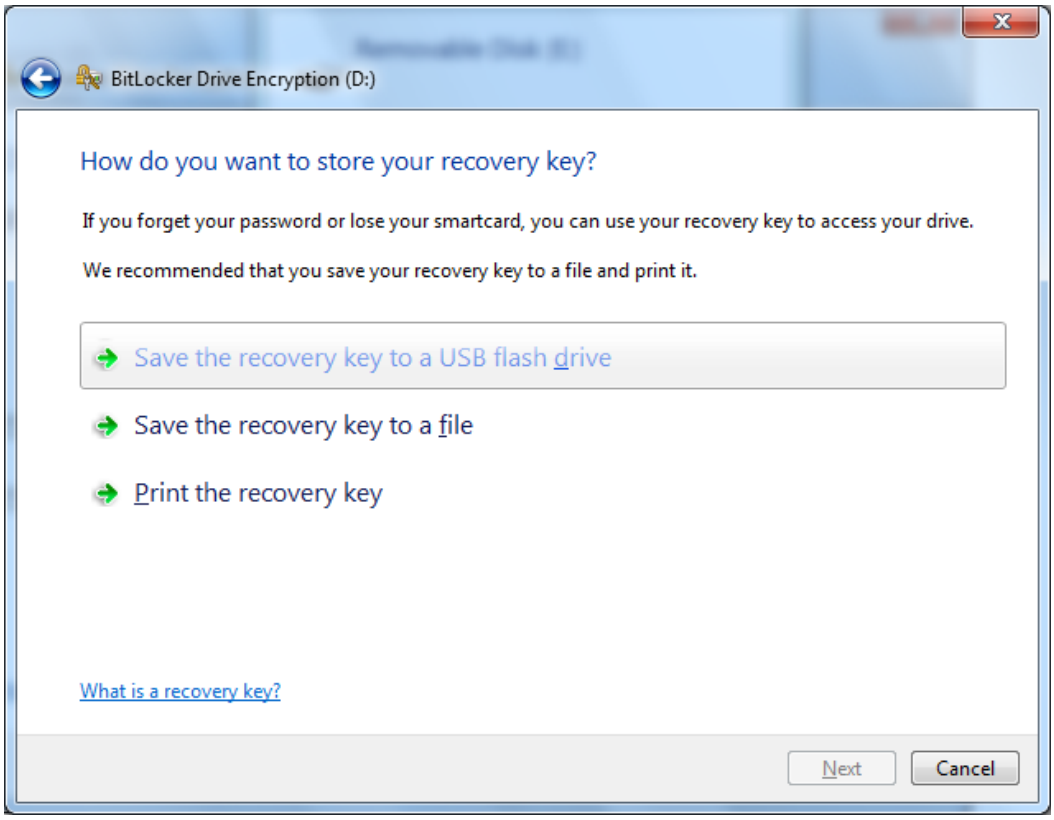
i. Right-click on the fixed data drive icon and select the “Turn on BitLocker”



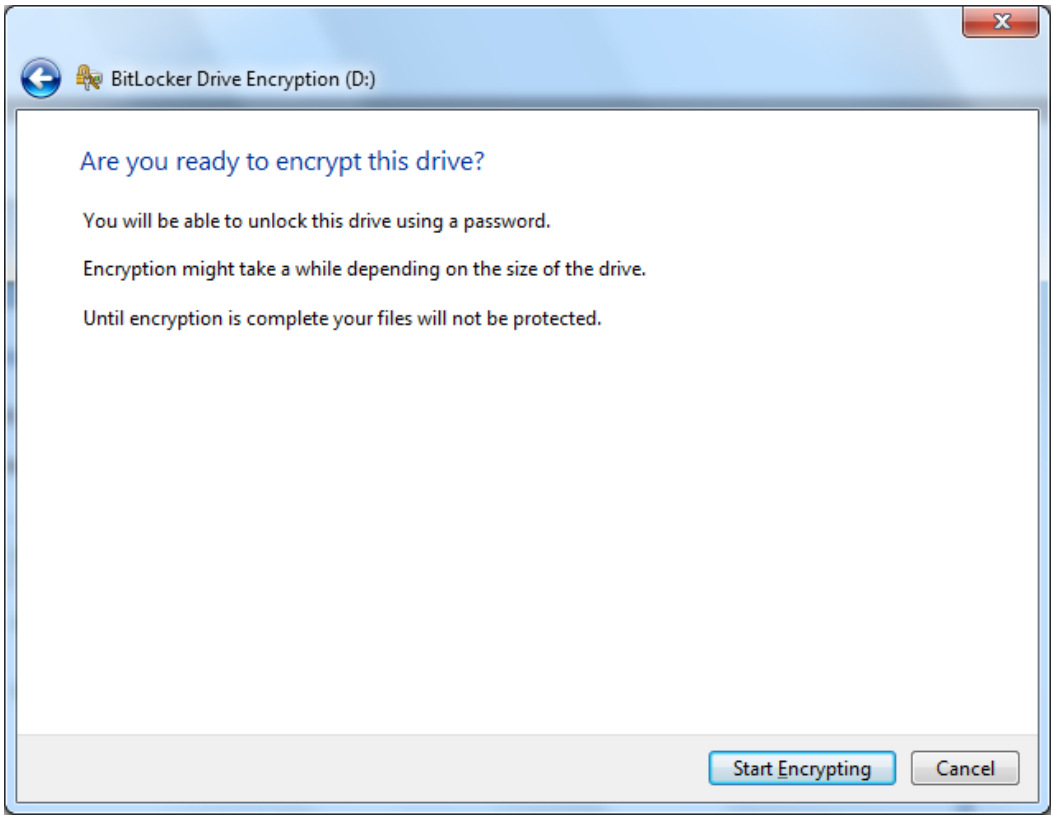
ii. Choose the method you want to unlock this drive and click “Next”



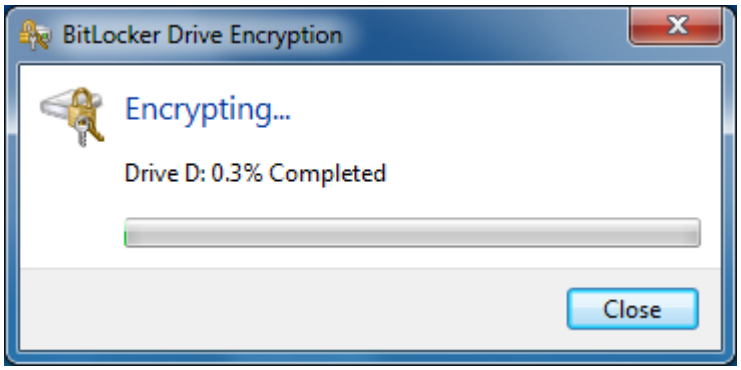
iii. Save or print the recovery key, then click “Next”



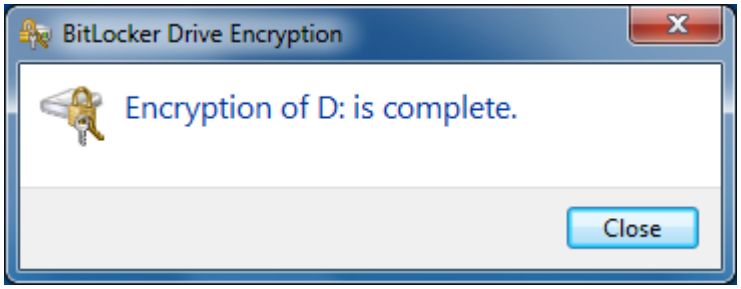
iv. Click “Start Encrypting”



v. During the encryption process, a progress monitor will be shown. The amount of time that it will take to complete the process varies, depending mainly on the size of your drive

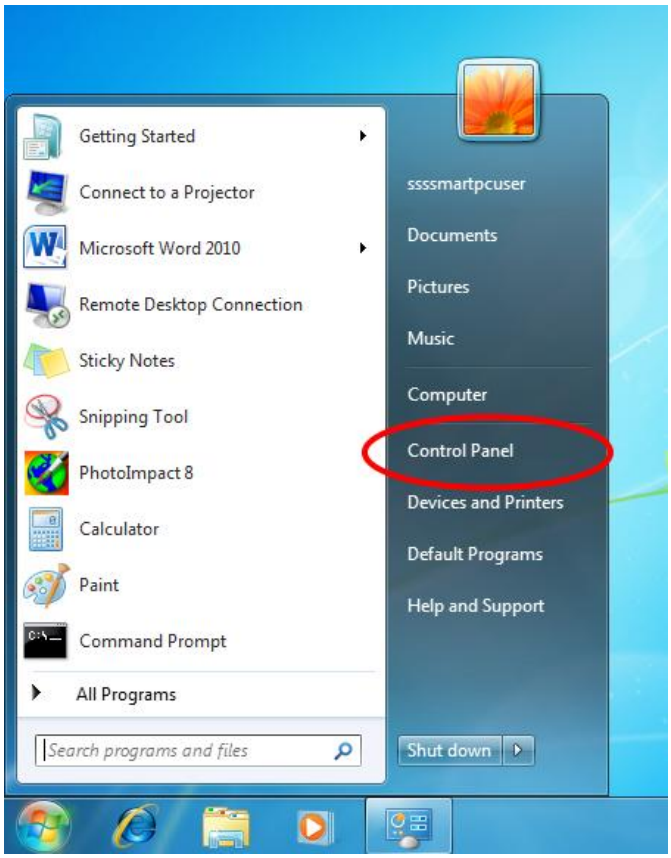


vi. Click “Close” to complete the encryption

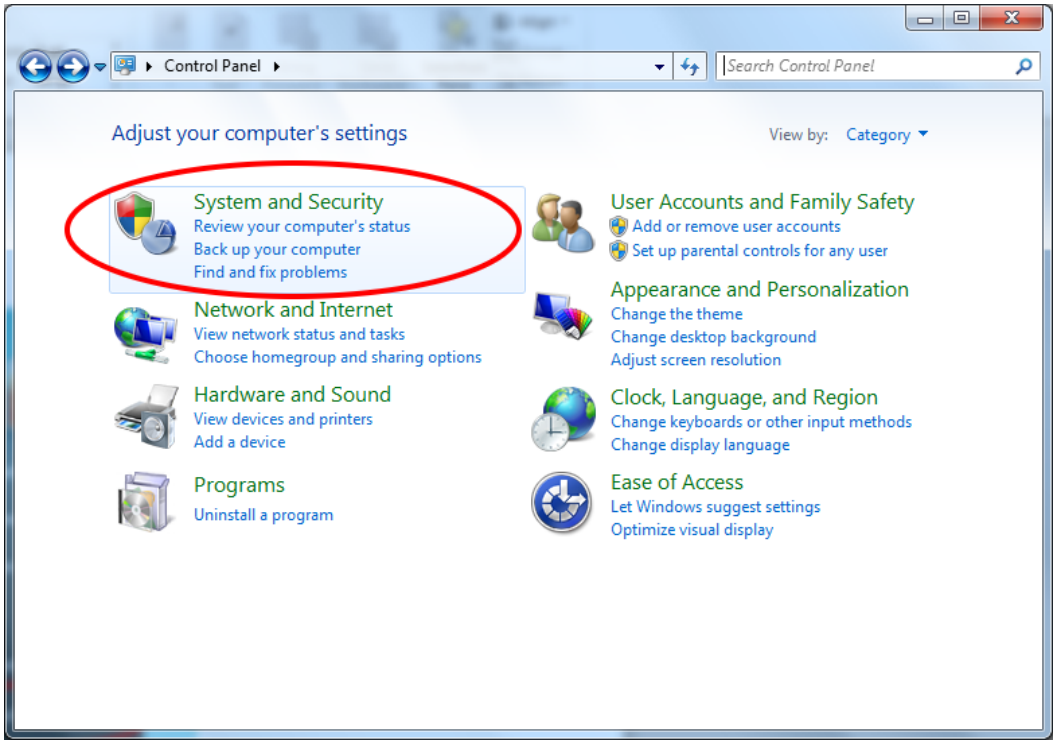


4 Remove Encryption from encrypted drive

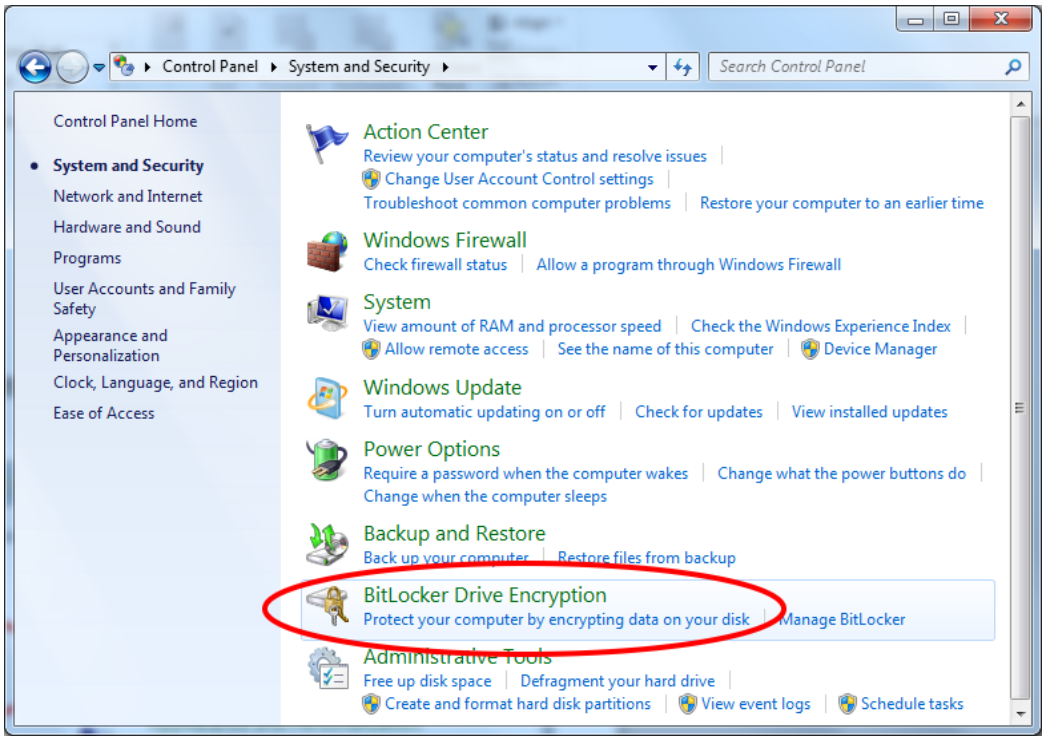
i. Open “Control Panel” from Start Menu



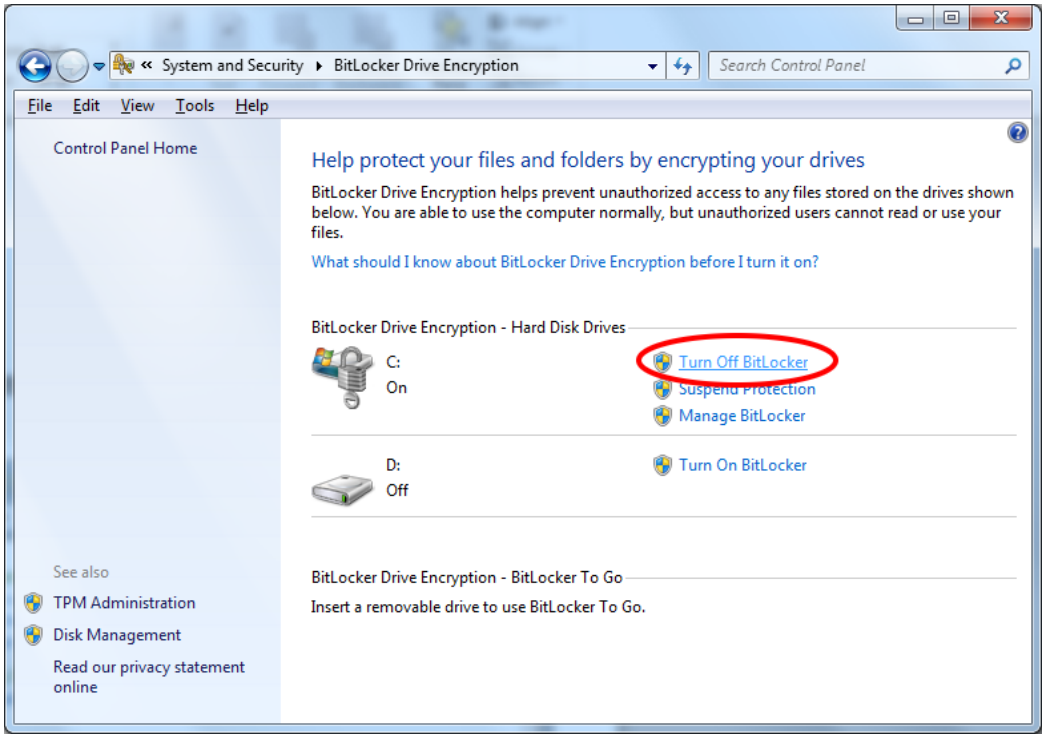
ii. Click “System and Security”



iii. Click “BitLocker Drive Encryption”

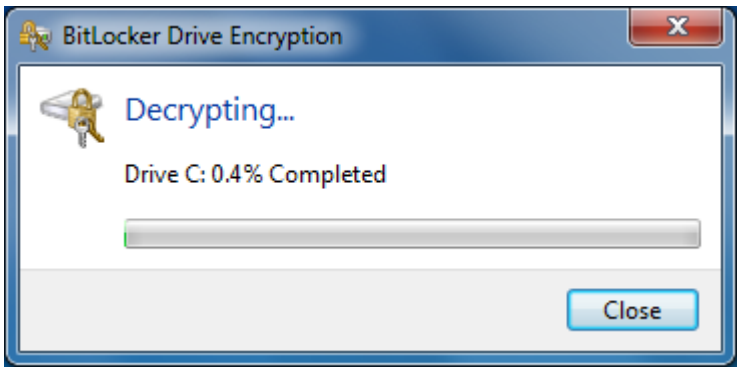


iv. Click “Turn Off BitLocker” on the drive that you want BitLocker Drive Encryption turned off

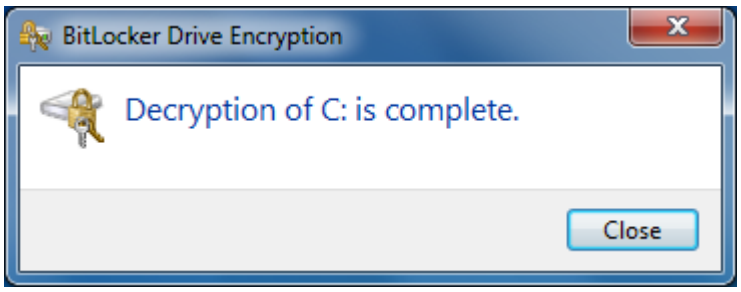


v. Click “Decrypt Drive” to start the decryption process

vi. During the decryption process, a progress monitor will be shown. The amount of time it will take to complete the process varies, depending mainly on the size of your drive



vii. Click “Close” to complete the decryption



5.1. Recovering the Encrypted Operating System Drive

BitLocker locks the computer when a disk encryption key is not available. The following is a list of likely causes:

- An error related to TPM validation occurs on an operating system drive
- The boot files are modified

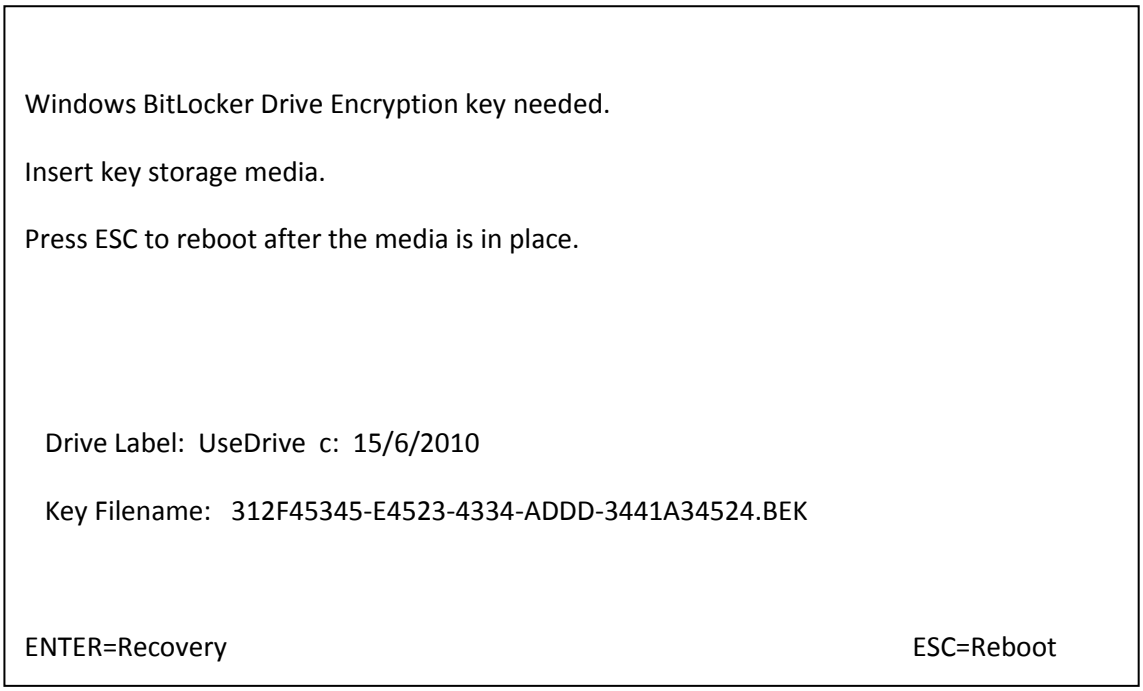
When the computer is locked by Bitlocker, it will interrupt the startup process before the operating system starts. So you must recover it by:

- Inserting the USB flash drive with the recovery key
- Or, typing the recovery key manually

5.1.1. Recovering by inserting the USB flash drive with the recovery key

i. Turn on the computer

ii. If the computer is locked, the BitLocker Drive Encryption Recovery Console will appear. You will be prompted to insert the USB flash drive that contains the recovery key.



(Example)

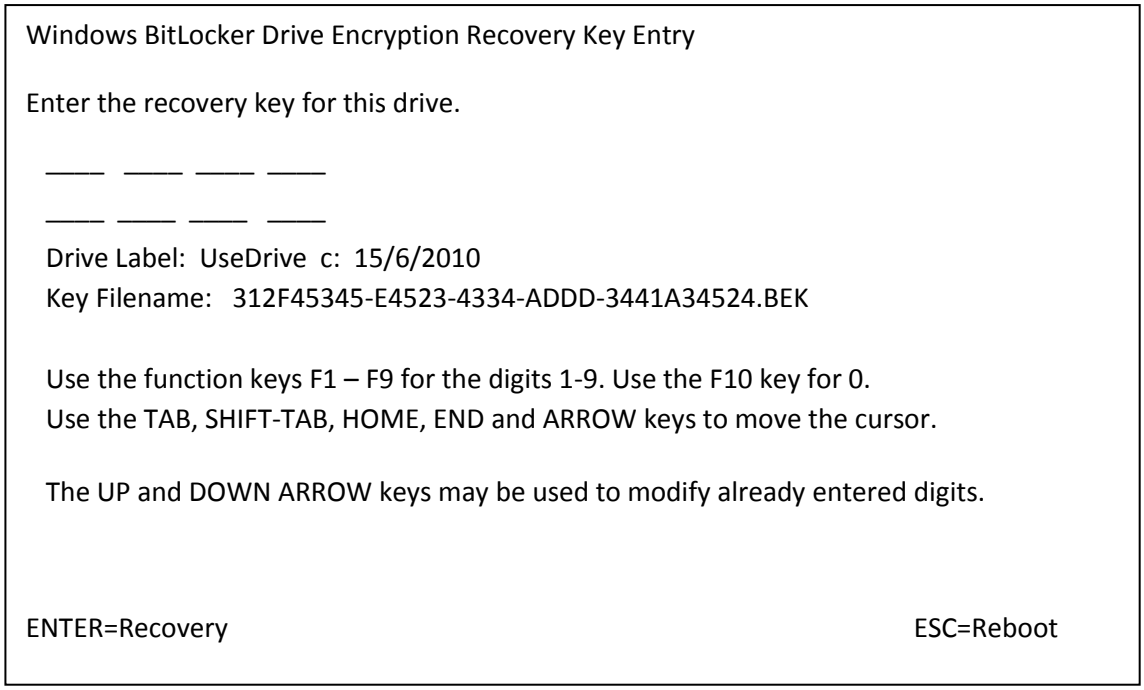
iii. Insert the USB flash drive with the recovery password, and then press ESC. Your computer will restart automatically.

5.1.2 Recovering by typing the recovery key

i. Turn on the computer

ii. If the computer is locked, the BitLocker Drive Encryption Recovery Console will appear. You will be prompted to insert the USB flash drive that contains the recovery key.

iii. Press ENTER. You will be prompted to enter the recovery key. Type the 48-digit recovery key, and then press ENTER.



(Example)

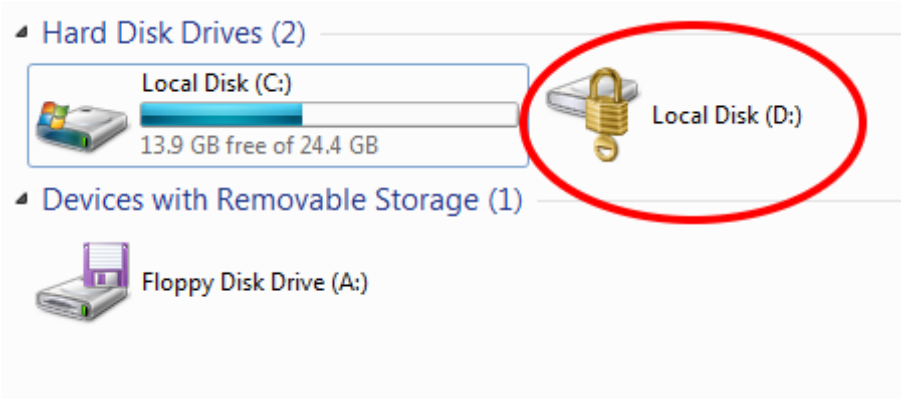
5.2. Recovering the Encrypted Fixed Data Drive

If you forget the password of the encrypted fixed data drive, you should unlock the drive by:

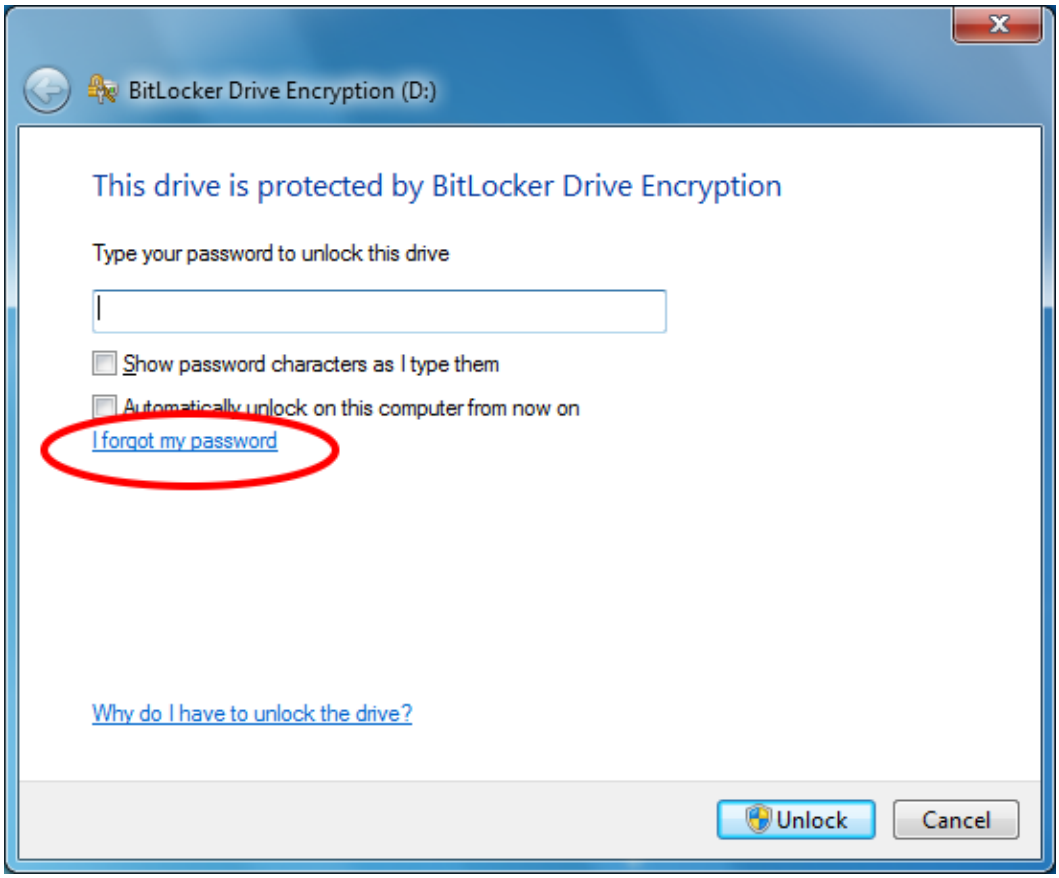
- Inserting the USB flash drive with the recovery key, or
- Typing the recovery key

5.2.1 Recovering by inserting the USB flash drive with the recovery key

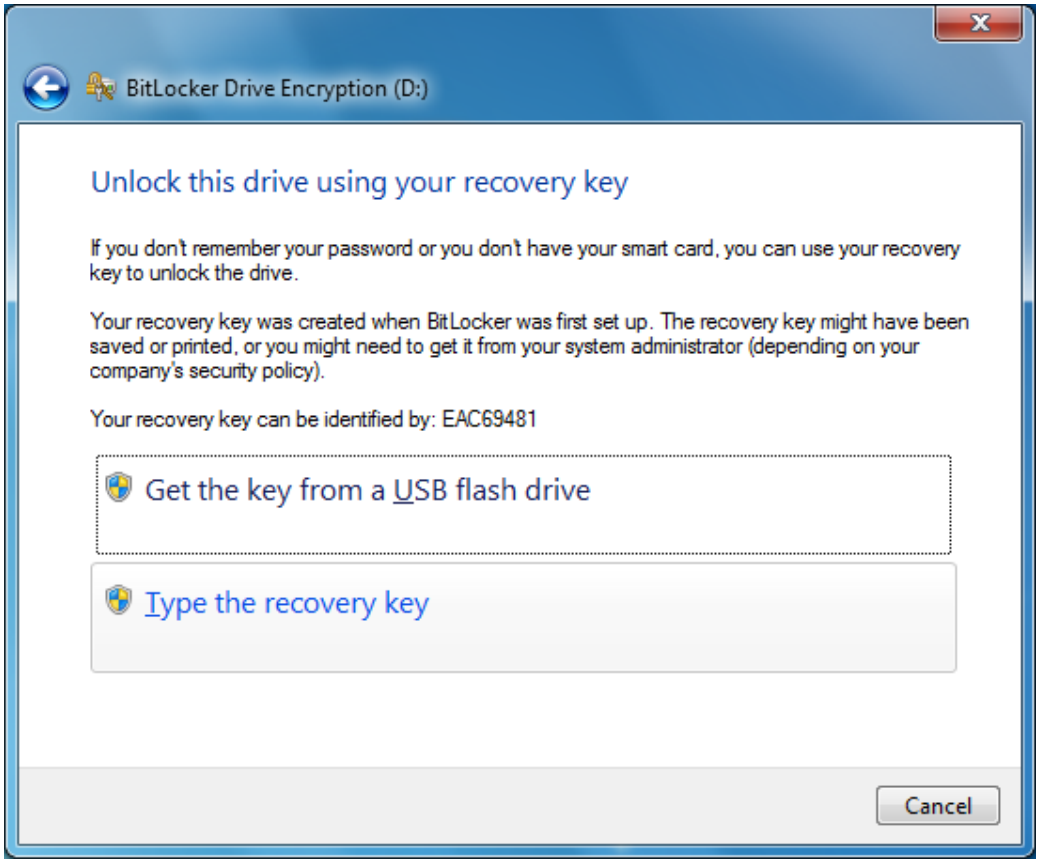
i. Double-click the encrypted fixed data drive



ii. Click “I forgot my password”



iii. Plug the USB flash drive that saved the recovery key and click “Get the key from a USB flash drive”


BitLocker Drive Encryption (D:)
Unlock this drive using your recovery key
If you don't remember your password or you don't have your smart card, you can use your recovery key to unlock the drive.
Your recovery key was created when BitLocker was first set up. The recovery key might have been saved or printed, or you might need to get it from your system administrator (depending on your company's security policy).
Your recovery key can be identified by: EAC69481
Get the key from a USB flash drive
Type the recovery key
Cancel

5.2.2 Recovering by typing the recovery key

i. Follow the step i. & ii. of 5.2.1

ii. Click “Type the recovery key”

Enter the recovery key and click “Next”