# Encrypting with BitLocker for disk volumes under Windows 7

# Summary of the contents

- 1 Introduction
- 2 Hardware requirements for BitLocker Driver Encryption
- 3 Encrypting drive
  - 3.1 Operating System Drive
    - 3.1.1 With TPM
    - 3.1.2 Without TPM
  - 3.2 Fixed Data Drive
- 4 Removing encryption from encrypted drive
- 5 Recovering encrypted drive
  - 5.1 Recovering the Encrypted Operating System Drive
    - 5.1.1 by inserting the USB flash drive with the recovery key
    - 5.1.2 by typing the recovery key
  - 5.2 Recovering the Encrypted Fixed Data Drive
    - 5.2.1 by inserting the USB flash drive with the recovery key
    - 5.2.2 by typing the recovery key

#### 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"

⊿ Ha	ard D	lisk L	Drives (2)		
		Loca	l Disk (C:)		Local Disk (D:)
			Open in new window		24.3 GB free of 24.4 GB
- 0	evice	۲	Turn on BitLocker	$\supset$	
			Share with Restore previous versions	•	
		s	Shared Folder Synchronization	· ·	
			Сору		
			Create shortcut Rename		
			Properties		

# ii. Click "Next"

		x
	BitLocker Drive Encryption (C:)	
· ۱	BitLocker Drive Encryption setup	
	The following preparations will be made on this computer to enable BitLocker.	
	Prepare your drive for BitLocker	
	Encrypt the drive	
	What are Bitl ocker's system requirements?	
	white one one offer a system requirements.	
	Next Can	cel

# iii. Click "Next"

		x
G 🎨 BitLocker Drive Encryption (C:)	-	
Preparing your drive for BitLocker		
An existing drive or unallocated free space on the hard drive will be used to enable BitLocke	er.	
✓ Details		
How does drive preparation work?		
Next	Car	ncel

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

🕞 🏘 BitLocker Drive Encryption (C:)	
Drive preparation is complete	
You need to restart your computer to finish preparing the system drive for BitLocker.	
Save and close any open files or programs before restarting.	
	Restart <u>N</u> ow

v. After the restart, click "Next"

r

	x
🕞 🎭 BitLocker Drive Encryption (C:)	
BitLocker Drive Encryption setup	
The following preparations will be made on this computer to enable BitLocker.	
Prepare your drive for BitLocker	
Encrypt the drive	
What are BitLocker's system requirements?	
Next Can	icel

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

		x
$\bigcirc$	RitLocker Drive Encryption (C:)	
	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	
	$\Rightarrow$ Save the recovery key to a <u>file</u>	
	Print the recovery key	
	<u>What is a recovery key?</u>	
	Next Ca	incel

vii. Click "Start Encrypting"

General BitLocker Drive Encryption (C:)
Are you ready to encrypt this drive?
The selected drive is C:
You can keep working while the drive is being encrypted. Your computer's performance will be affected and free space will be used by BitLocker during encryption.
Run BitLocker system check
The system check will ensure that BitLocker can read the recovery and encryption keys correctly before encrypting the drive.
Insert the USB memory device containing your saved recovery key. BitLocker will restart your computer before encrypting.
Note: This check can take some time but is recommended because there is a risk that you might need to enter the recovery key to unlock the drive.
Start Encrypting Cancel

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.

Re BitLo	cker Drive Encryption
	Encrypting Drive C: 0.7% Completed
	<u>Close</u>

ix. Click "Close" to complete the encryption

Ne BitLo	Real BitLocker Drive Encryption				
R	Encryption of C: is complete.				
		Close			

# 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.

See more results			
gpedit.msc	×	🕖 Shut down	
🤭 🖉 🛅	0		

 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"

sequire additional authentication at startup			x
Require additional authentication at startup	)	Previous Setting	
<ul> <li>Not <u>Configured</u> Comment:</li> <li><u>Enabled</u></li> </ul>			*
Disabled Supported on: Windo	ws 7 fam	ily	*
Options:		Help:	
<ul> <li>Allow BitLocker without a compatible TPM (requires a startup key on a USB flash drive)</li> <li>Settings for computers with a TPM:</li> <li>Configure TPM startup:</li> <li>Allow TPM          <ul> <li>Configure TPM startup PIN:</li> <li>Allow startup PIN with TPM              </li> <li>Configure TPM startup key:</li> <li>Allow startup key with TPM              </li> <li>Configure TPM startup key and PIN:</li> </ul> </li> </ul>		This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker. Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs. If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode a USB drive is required for start-up and the key information used to encrypt the drive is stored on the USB drive, creating a USB key. When the USB key is inserted the access to the drive is authenticated and the drive is accessible. If the USB key is lost or unavailable you will need to use one of the BitLocker recovery options to access the drive. On a computer with a compatible TPM, four types of authentication methods can be used at startup to provide added protection for encrypted data. When the computer starts, it can	E
		OK Cancel <u>A</u> pply	

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

# v. Click "Next"

BitLocker Drive Encryption (C:)	
BitLocker Drive Encryption setup	
The following preparations will be made on this computer to enable BitLocker.	
Prepare your drive for BitLocker	
Encrypt the drive	
What are Ritl ocker's system requirements?	
mile die die de beere system requirements:	
Next	Cancel

# vi. Click "Next"

See State Contraction (C:)
Preparing your drive for BitLocker
An existing drive or unallocated free space on the hard drive will be used to enable BitLocker.
How does drive preparation work?
Next Cancel

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

🕞 🏘 BitLocker Drive Encryption (C:)	x
Drive preparation is complete	
You need to restart your computer to finish preparing the system drive for BitLocker.	
Save and close any open files or programs before restarting.	
Re	start <u>N</u> ow

# viii. After the restart, click "Next" to continue

	×
BitLocker Drive Encryption (C:)	
BitLocker Drive Encryption setup	
The following preparations will be made on this computer to enable BitLocker.	
Prepare your drive for BitLocker	
Encrypt the drive	
What are BitLocker's system requirements?	
Next	Cancel

ix. Click "Require a Startup key at every startup"

	BitLocker startup preferences
This flash	computer does not appear to have a TPM. To use BitLocker Drive Encryption, a startup key on a US drive will be required every time you start the computer.
Ŷ	Use Bit <u>L</u> ocker without additional keys
¢	Require a <u>P</u> IN at every startup
•	Require a <u>S</u> tartup key at every startup
<b>()</b> S	Some settings are managed by your system administrator.

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

	BitLocker Drive Encryption (C;)	x
	Save your Startup Key Insert a removable USB memory device and select its drive, then click Save.	
0		
	<u>Save</u> Cance	2

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

🕞 🏘 BitLocker Drive Encryption (C:)	×
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	
$\bigcirc$ Save the recovery key to a <u>file</u>	
Print the recovery key	
Some settings are managed by your system administrator.	
What is a recovery key?	
Next Ca	ncel

# xii. Click "Continue"

$\Theta$	BitLocker Drive Encryption (C:)
	Are you ready to encrypt this drive?
	The selected drive is C:
	You can keep working while the drive is being encrypted. Your computer's performance will be affected and free space will be used by BitLocker during encryption.
	The system check will ensure that BitLocker can read the recovery and encryption keys correctly before encrypting the drive.
	Insert the USB memory device containing your saved recovery key. BitLocker will restart your computer before encrypting.
	Note: This check can take some time but is recommended because there is a risk that you might need to enter the recovery key to unlock the drive.
	Continue Cancel

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

🎭 BitLo	ocker Drive Encryption
The computer must be restarted	
Insert the USB memory device containing the recovery key.	
	Restart now Restart later

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

💫 BitLocker Drive Encryption 📃 💌			
R	Encrypting Drive C: 0.9% Completed		
	Close		

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"

🕞 🏤 BitLocker Drive Encryption (D:)
Choose how you want to unlock this drive
Use a password to unlock the drive
Passwords should contain upper and lowercase letters, numbers, spaces, and symbols.
Type your password:
Retype your password:
Use my smart card to unlock the drive
You will need to insert your smart card. The smart card PIN will be required when you unlock the drive.
Automatically unlock this drive on this computer
How do I use these options?
<u>N</u> ext Cancel

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

G 🏀 BitLocker Drive Encryption (D:)	
How do you want to store your recovery key? If you forget your password or lose your smartcard, you can use your recovery key t	to access your drive.
We recommended that you save your recovery key to a file and print it.	
Save the recovery key to a USB flash <u>d</u> rive	
Save the recovery key to a <u>file</u>	
Print the recovery key	
What is a recovery key?	
	Next Cancel

iv. Click "Start Encrypting"

0	Real BitLocker Drive Encryption (D:)	
	Are you ready to encrypt this drive? You will be able to unlock this drive using a password. Encryption might take a while depending on the size of the drive. Until encryption is complete your files will not be protected.	
	Start Encrypting Car	ncel

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 <u>Remove Encryption from encrypted drive</u>

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

RitLocker Drive Encryption			
R	Decrypting Drive C: 0.4% Completed		
	Close		

vii. Click "Close" to complete the decryption



# 5.1. <u>Recovering the Encrypted Operating System Drive</u>

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. <u>Recovering by inserting the USB flash drive with the recovery key</u>

- 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.

Windows BitLocker Drive Encryption key needed.				
Insert key storage media.				
Press ESC to reboot after the media is in place.				
Drive Label: UseDrive c: 15/6/2010				
Key Filename: 312F45345-E4523-4334-ADDD-3441A34524.BEK				
ENTER=Recovery	ESC=Reboot			

#### (Example)

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

# 5.1.2 <u>Recovering by typing the recovery key</u>

- 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 48digit recovery key, and then press ENTER.

Windows BitLocker Drive Encryption Recovery Key Entry		
Enter the recovery key for this drive.		
 Drive Label: UseDrive c: 15/6/2010 Key Filename: 312F45345-E4523-4334-ADDD-3441A34524.BEK		
Use the function keys F1 – F9 for the digits 1-9. Use the F10 key for 0. Use the TAB, SHIFT-TAB, HOME, END and ARROW keys to move the cursor.		
The UP and DOWN ARROW keys may be used to modify already entered digits.		
ENTER=Recovery ESC	=Reboot	

(Example)

# 5.2. <u>Recovering the Encrypted Fixed Data Drive</u>

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

- Hard Disk Drives (2)
   Local Disk (C:)
   13.9 GB free of 24.4 GB
   Devices with Removable Storage (1)
   Floppy Disk Drive (A:)
- ii. Click "I forgot my password"

🕞 🎭 BitLocker Drive Encryption (D:)
This drive is protected by BitLocker Drive Encryption
Type your password to unlock this drive
Show password characters as I type them
Automatically unlock on this computer from now on <u>I forgot my password</u>
Why do I have to unlock the drive?
Cancel

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

G	RitLocker 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
	♥ <u>Type</u> the recovery key
	Cancel

# 5.2.2 <u>Recovering by typing the recovery key</u>

- i. Follow the step i. & ii. of 5.2.1
- ii. Click "Type the recovery key"

🚱 🎭 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
left the key from a <u>U</u> SB flash drive
Ivpe the recovery key
Cancel

# Enter the recovery key and click "Next"

	×
G & BitLocker Drive Encryption (D:)	
Enter your recovery key	
Type your BitLocker recovery key:	
More information	
	Next Cancel