CYBERDEFENSE

۶.

BitLocker Disk Encryption Guide for Windows 10 Pro



Contents

How to use BitLocker Drive Encryption on Windows 10	2
What is Full Disk Encryption?	2
Why use full disk encryption?	2
Things to Know Before You Begin	2
How to check if your device has a TPM chip	2
How to ensure you can turn on BitLocker without TPM	3
How to turn on BitLocker on the operating system drive	5
BitLocker Drive Encryption options	11
How to turn on BitLocker To Go	12
Quick access to manage your BitLocker drive	16



How to use BitLocker Drive Encryption on Windows 10

This guide explains the process for activating BitLocker encryption on Windows 10 to protect your data.

What is Full Disk Encryption?

Full disk encryption is the process of making data unreadable by anyone without proper authorization. It is important to note that encryption is only as strong as the user account password used to authenticate to the system. As a result, using a long complex password is highly recommended.

Windows 10 includes BitLocker Drive Encryption, which is a built-in feature that makes it easy and convenient to encrypt your computer's hard drive and removable media (such as USB storage devices) to protect your organizations sensitive data.

Why use full disk encryption?

Most companies deal with customer information or other sensitive data on computer systems. Employing full disk encryption to protect this data from unauthorized access provides assurance that private information stays private in the event of loss or theft.

In this guide, we'll walk you through the steps to set up BitLocker Drive Encryption on your PC to secure sensitive information.

Things to Know Before You Begin

- BitLocker Drive Encryption is available only on Windows 10 Pro and Windows 10 Enterprise.
- Please ensure the laptop OS has been updated.
- Your PC's hard drive must contain two partitions: a system partition, which contains the necessary files to start Windows, and the partition with the operating system. If your computer does not meet the requirements, BitLocker will create them for you. Additionally, the hard drive partitions must be formatted with the NTFS file system.
- Depending on the amount of data and the size of the hard drive, the behind the scene encryption process can be time-consuming.
- Make sure to keep your computer connected to an uninterrupted power supply throughout the entire process. Abrupt loss of power, such as a power outage and/or depletion of battery power can result in total loss of data. Please plan accordingly.

Important: While BitLocker is a stable feature on Windows 10, any significant change made to your computer has its risks.

How to check if your device has a TPM chip

1. Use the keyboard shortcut, **Windows key + X** to open the Power User menu and select Device Manager.



2. Expand **Security devices**. If you have a TPM chip, you should see an item that reads **Trusted Platform Module** with the version number.



Note: Verify that your computer has a TPM chip version 1.2 or later to support hardware-based encryption with BitLocker.

Alternatively, you can also check your PC manufacturer's support website to find out if your device includes the security chip, and for instructions to enable the chip in the BIOS (if applicable).

How to ensure you can turn on BitLocker without TPM

If your computer doesn't include a Trusted Platform Module chip, you won't be able to turn on BitLocker on Windows 10. In this is your case, you can still use encryption, but you'll need to use the Local Group Policy Editor to enable additional authentication at startup.

- 1. Use the keyboard shortcut **Windows key + R** to open the Run command, type **gpedit.msc**, and click **OK**.
- 2. Under Computer Configuration, expand Administrative Templates.
- 3. Expand Windows Components.
- 4. Expand BitLocker Drive Encryption and Operating System Drives.
- 5. On the right side, double-click **Require additional authentication at startup**.



Local Group Policy Editor

Local Computer Policy	Setting	State
Computer Configuration	Allow network unlock at startup	Not configured
> 🧾 Software Settings	Allow Secure Boot for integrity validation	Not configured
> 🛗 Windows Settings	Require additional authentication at startun	Enabled
 Administrative Templates 	Require additional authentication at startup Windows Serve	Not configure
> 🧮 Control Panel	Disallow standard uses from changing the DIN or personal	Not configured
> 📔 Network	E Disallow standard users from changing the Pilv of password	Not configured
Printers	Enable use of BitLocker authentication requiring preboot ke	Not configure
Server	Allow enhanced PINs for startup	Not configured
Start Menu and Taskbar	Configure minimum PIN length for startup	Not configure
> 🗾 System	Configure use of hardware-based encryption for operating s	Not configure
✓ I Windows Components	Enforce drive encryption type on operating system drives	Not configure
ActiveX Installer Service	Configure use of passwords for operating system drives	Not configure
Add features to Windows 10	Choose how BitLocker-protected operating system drives ca	Not configure
App Package Deployment	Configure TPM platform validation profile for BIOS-based fi	Not configure
App Privacy	Configure TPM platform validation profile (Windows Vista,	Not configure
🧮 App runtime	Configure TPM platform validation profile for native UEFI fir	Not configure
Application Compatibility	Configure pre-boot recovery message and URL	Not configure
AutoPlay Policies	Reset platform validation data after BitLocker recovery	Not configure
> 🧮 Biometrics	Use enhanced Boot Configuration Data validation profile	Not configure
✓ I BitLocker Drive Encryption		
Fixed Data Drives		
C Operating System Drives		
Removable Data Drives		
Cloud Content		
Credential User Interface	, <	

- 6. Select Enabled.
- 7. Make sure to check the "Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)" option.

×

8. Click OK to complete this process.



support@corvidcd.com

support.corvidcyberdefense.com



How to turn on BitLocker on the operating system drive

- 1. Use the keyboard shortcut Windows key + X to open the Power User menu and select Control Panel.
- 2. Click System and Security.
- 3. Click BitLocker Drive Encryption.



4. Under BitLocker Drive Encryption, click Turn on BitLocker.

BitLocker Drive Encryption			- 0	×
🗧 🚽 👻 🛧 🏘 > Control Pan	el $ ightarrow$ System and Security $ ightarrow$ BitLocker Drive Encryption $ ightarrow$	õ	Search Control Panel	P
Control Panel Home	BitLocker Drive Encryption Help protect your files and folders from unauthorized access by protecting	g you	r drives with BitLocker.	
	Operating system drive			
	C: BitLocker off		0	
	Fixed data drives]		
	Removable data drives - BitLocker To Go			
	SanDisk (E:) BitLocker off		\odot	
	Turn on BitLocker			
See also	~			
TPM Administration				
Disk Management				

5. Choose how you want to unlock your drive during startup: **Insert a USB flash drive** or **Enter a password**. For the purpose of the guide, select **Enter a password** to continue.



	BitLocker Drive Encryption (C:)
(Choose how to unlock your drive at startup
() Some settings are managed by your system administrator.
and	To help keep your data more secure, you can have BitLocker prompt you to enter a password or insert a USB flash drive each time you start your PC.
	\rightarrow Insert a <u>U</u> SB flash drive
	→ Enter a pass <u>w</u> ord

6. Enter a password that you'll use every time you start Windows 10 to decrypt the drive. Then click **Next** to continue. (Make sure to create a strong password mixing uppercase, lowercase, numbers, and symbols.)

BitLocker Drive Encryption (C:)	
Create a password to unlock this drive	
You should create a strong password that uses uppercase and lowercase letters, numbers, symbols, and spaces.	
Enter your password	
•••••	
Reenter your p <u>a</u> ssword	

Tips for creating a strong password.	
Next Cance	1

- 7. You will be given the choices to save a recovery key to regain access to your files in case you forget your password. Options include:
 - Save to your Microsoft account
 - Save to a USB flash drive
 - Save to a file



• Print the recovery key

Select the option that is most convenient for you (we recommend a dedicated USB that is stored is a safe), and save the recovery key in a safe and secure place.

8. Click **Next** to continue.

How do you w	ant to back up	your recovery k	ey?	
Some settings	are managed by yo	our system administra	tor.	
A recovery key car It's a good idea to	h be used to access y have more than one	your files and folders e and keep each in a	if you're having problems safe place other than your l	unlocking your F PC.
\rightarrow Save to y	our <u>M</u> icrosoft a	ccount		
\rightarrow Save to a	<u>U</u> SB flash drive	e		
→ Save to a	file			
$\rightarrow \underline{P}$ rint the	recovery key			
What is a recovery	key?			

- 9. Select the encryption option that best suits your scenario:
 - Encrypt used disk space only (faster and best for new PCs and drives)
 - Encrypt entire drive (slower but best for PCs and drives already in use)



We bicocke bive cheryphon (C)
Choose how much of your drive to encrypt
If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.
If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected—even data that you deleted but that might sti contain retrievable info.
Encrypt used disk space only (faster and best for new PCs and drives)
O Encrypt entire drive (slower but best for PCs and drives already in use)

10. Choose New encryption mode (best for fixed drives on this device)

On Windows 10 version 1511, Microsoft introduced support for <u>XTS-AES encryption algorithm</u>. This new encryption method provides additional integrity support and protection against new attacks that use manipulating cipher text to cause predictable modifications in clear text. BitLocker supports 128-bit and 256-bit XTS AES keys.

11. Click **Next** to continue.



12. Make sure to check the **Run BitLocker system check** option, and click **Continue**.





- 13. Finally, restart your computer to begin the encryption process.
- 14. On reboot, BitLocker will prompt you to enter your encryption password to unlock the drive. Type the password and press **Enter**.

Enter the password to u	nlock this drive	
Press Enter to continue		
Press Esc for BitLocker r		

After rebooting, you'll notice that your computer will quickly boot to the Windows 10 desktop. However, if you go to **Control Panel > System and Security > BitLocker Drive Encryption**, you'll see that BitLocker is still encrypting your drive. Depending on the option you selected and the size of the drive, this process can take a significant amount of time, but you'll still be able to work on your computer. We strongly recommend leaving your computer overnight to avoid disrupting the encryption process.



BitLocker Drive Encryption						1
- 🛶 🔹 🛧 🎭 > Control Pane	> System and Security > BitLocker Drive Encry	/ption v	õ	Search Control Panel		P
Control Panel Home	BitLocker Drive Encryption Help protect your files and folders from unautho	rized access by protectin	ig you	r drives with BitLocker.		
	Operating system drive					
	C: BitLocker Encrypting			\odot		
		 Back up your recover Change password Remove password Turn off BitLocker 	ry key			
	Fixed data drives					
	Removable data drives - BitLocker To	Go				
	SanDisk (E:) BitLocker off			\odot		
See also	New Volume (F:) BitLocker off			\odot		
TPM Administration						
Disk Management						
Privacy statement						

Once the encryption process completes, the drive level should read **BitLocker on**.

g BitLocker Drive Encryption				
🛧 🏘 > Contro	ol Panel > System and Security > BitLocker Drive	e Encryption 🗸 🗸	Search Control Panel	۶
Control Panel Home	BitLocker Drive Encryption Help protect your files and folders from un	nauthorized access by protectin	g your drives with BitLocker.	
	Operating system drive			
	C: BitLocker on		\odot	
		 Suspend protection Back up your recover, Change password Remove password Turn off BitLocker 	y key	
	Fixed data drives			
	Removable data drives - BitLock	er To Go		
See also	SanDisk (E:) BitLocker off		\odot	
TPM Administration Disk Management	New Volume (F:) BitLocker off		\odot	

You can verify that BitLocker is turned on by the lock icon on the drive when you open This PC on File Explorer.



■ 🖸 🛄 = Thi	iis PC View				-	
← → ~ ↑ 💻	> This PC			5	Search This PC	٩
 ← → ~ ↑ ← → ~ ↑ ✓ Quick access Desktop ↓ Downloads ⊘ Documents ⊘ Pictures ♪ Music ⊗ Videos ⊗ OneDrive ② This PC ⇒ New Volume (F ⊘ Network 	F)	ders (6) Desktop Music vices and drives (3) Local Disk (C:) 15.9 GB free of 29.5 GB	Documents Pictures DVD Drive (D:)		Search This PC Downloads Videos New Volume (F:) 1.98 GB free of 1.99 GB	<i>م</i>

BitLocker Drive Encryption options

When BitLocker is enabled on your main hard drive, you'll receive a few additional options, including:

- **Suspend protection:** When you're suspending protection your data won't be protected. Typically, you would use this option when applying a new operating system, firmware, or hardware upgrade. If you don't resume the encryption protection, BitLocker will resume automatically during the next reboot.
- **Back up your recovery key:** If you lose your recovery key, and you're still signed into your account, you can use this option to create a new backup of the key with the options mentioned on **step 6**.
- **Change password:** You can use this option to create a new encryption password, but you'll still need to supply the current password to make the change.
- **Remove password:** You can't use BitLocker without a form of authentication. You can remove a password only when you configure a new method of authentication.
- **Turn off BitLocker:** In the case, you no longer need encryption on your computer, BitLocker provides a way to decrypt all your files. However, make sure to understand that after turning off BitLocker your sensitive data will no longer be protected. In addition, decryption may take a long time to complete its process depending on the size of the drive, but you can still use your computer.



How to turn on BitLocker To Go

BitLocker is not an encryption feature that you can enable globally on every drive connected to your computer at once. It has two parts: you can use **BitLocker Drive Encryption** to encrypt your sensitive data on the main hard drive of your PC, and then you can use **BitLocker To Go**. This last feature will help you to use encryption on removable drives and secondary hard drives connected to your computer.

To turn on BitLocker To Go on a removable drive do the following:

- 1. Connect the drive you want to use with BitLocker.
- 2. Use the Windows key + X keyboard shortcut to open the Power User menu and select Control Panel.
- 3. Click System and Security.
- 4. Click BitLocker Drive Encryption.



- 5. Under BitLocker To Go, expand the drive you want to encrypt.
- 6. Click the Turn on BitLocker link.



BitLocker Drive Encryption			- c	
🗧 🚽 👻 🛧 🏘 > Contro	I Panel > System and Security > BitLocker Drive Encryption	v Ö	Search Control Panel	,
Control Panel Home	BitLocker Drive Encryption			
	Help protect your files and folders from unauthorized access by prot	ecting yo	ur drives with BitLocker.	
	Operating system drive			
	C: BitLocker on		\odot	
	Fixed data drives			
	Removable data drives - BitLocker To Go			
	SanDisk (E:) BitLocker off		0	
	Turn on BitLock	er]	
	New Volume (F:) BitLocker off		\odot	
See also				
TPM Administration				
Disk Management				
Privacy statement				

- 1. Check the **Use a password to unlock the drive option**, and create a password to unlock the drive. (Make sure to create a strong password mixing uppercase, lowercase, numbers, and symbols.)
- 2. Click **Next** to continue.

Use a password to unloc	k the drive
Enter your password	un upper case and lower case letters, numbers, spaces, and symbols.
<u>R</u> eenter your password	•••••
Use my smart card to un	lock the drive
You II need to insert you	r smart card. The smart card PIN Will be required when you unlock the driv

- 3. You will be given the choices to save a recovery key to regain access to your files in case you forget your password. Options include:
 - Save to your Microsoft account
 - Save to a file



• Print the recovery

Select the option that is most convenient for you, then click **Next**.

鞭 BitLocker Drive Encryption (F:)				
How do you want to back up your recovery key?				
If you forget your password or lose your smart card, you can use your recovery key to access your drive				
\rightarrow Save to your <u>M</u> icrosoft account				
\rightarrow Save to a file				
\rightarrow Print the recovery key				
What is a recovery key?				
	2			

- 4. Choose the encryption option that best suits your scenario:
 - Encrypt used disk space only (faster and best for new PCs and drives)
 - Encrypt entire drive (slower but best for PCs and drives already in use)

	>
-	RitLocker Drive Encryption (C:)
	Choose how much of your drive to encrypt
	If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.
	If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected–even data that you deleted but that might still contain retrievable info.
	Encrypt used disk space only (faster and best for new PCs and drives)
	○ Encrypt entire drive (slower but best for PCs and drives already in use)
	Next



5. Select Compatible mode, which is best for drives that can be moved from this device. "Compatible mode," will ensure you can unlock the drive if you move it to another computer running a previous version of the Windows operating system.



6. Click Start encrypting to finish the process.



When encrypting a storage device try to start with an empty removable media, as it'll speed up the process, then new data will encrypt automatically.



In addition, similar to BitLocker Drive Encryption, you will get the same additional options using BitLocker To Go, plus a few more, including:

- Add smart card: This option will allow you to configure a smart card to unlock the removable drive.
- **Turn on auto-unlock:** Instead of having to type a password every time you re-connect the removable drive, you can enable auto-unlock to access your encrypted data without entering a password.

BitLocker Drive Encryption			>		
🗧 🚽 👻 🛧 🎭 > Contro	I Panel > System and Security > BitLocker	Drive Encryption v 🖏 Searc	h Control Panel 🔎		
Control Panel Home	BitLocker Drive Encryption		at Patentee		
	help protect your files and folders from unauthorized access by protecting your drives with bitcocker.				
	Operating system drive				
	C: BitLocker on		\odot		
	Fixed data drives				
	Removable data drives - BitL	ocker To Go			
	SanDisk (E:) BitLocker on		\odot		
	6	Back up your recovery key			
		Change password Remove password			
		Add smart card			
		Turn on auto-unlock Turn off BitLocker			
	New Volume (F:) BitLocker o	off	\odot		
See also					
TPM Administration					
Disk Management					
Privacy statement					

Quick access to manage your BitLocker drive

Whether you turn on BitLocker for your system hard drive or removable drive, you can always get quick access to the BitLocker settings for a particular drive using the following steps:

- 1. Use the keyboard shortcut **Windows key + E** to open File Explorer.
- 2. Click **This PC** from the left pane.
- 3. Right-click the encrypted drive and select Manage BitLocker.



I I I I I I I I I I I I I I I I I I I	Drive Tools This PC View Manage		- □ × ~ 0
← → • ↑ 💻 י	This PC	v ک	Search This PC 🔎
 Quick access Desktop Downloads Documents Pictures Music 	Folders (6) * Desktop * Music	Documents	Downloads Vídeos
Videos ConeDrive This PC New Volume (F	Devices and drives (3) Coal Disk (C) Open Open in new window Pin to Quick access Change BitLocker password Manage BitLocker	DVD Drive (D:)	New Volume (F:) 1.98 GB free of 1.99 GB
	Scan with Windows Defender Share with > Restore previous versions Pin to Start Format Copy Create shortcut		
	Rename Properties		