Procedure for BitLocker to Go in Windows 10

Table of Contents

Proce	edure for BitLocker to Go in Windows 10	1
١.	What is BitLocker to Go?	1
١١.	Requirement for BitLocker to Go	1
111.	Using BitLocker to Go to Encrypt the USB device	2
IV.	Accessing USB device protected by BitLocker to Go	8
V.	Step to recover BitLocker to Go with Recovery Key if you forget the password	9
VI.	Reminder for Password and Recovery Key	10

I. What is BitLocker to Go?

Microsoft BitLocker To Go is BitLocker Drive Encryption on removable data drives. It can be used to encrypt:

- USB flash drives
- SD cards
- External hard disk drives
- Other drives that are formatted by using the NTFS, FAT16, FAT32, or exFAT file system.

Reference: <u>https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-to-go-faq</u>

II. Requirement for BitLocker to Go

BitLocker is not available on Windows 10 Home Edition. You need to use either Windows 10 Pro, Education or Enterprise Edition. It also needs a system partition that is:

- Must be configured as the active partition.
- Must not be encrypted or used to store user files.
- Must have at least 100 megabytes (MB) of space.
- Must have at least 50 MB of free space.

There is no official support of non-Windows Based OS (include MacOS and Linux base OS) to access USB drive protected by BitLocker to Go.

Reference: <u>https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/bitlocker-</u> <u>drive-encryption#bitlocker-drive-encryption-partitioning-requirements</u>

III. Using BitLocker to Go to Encrypt the USB device

- 1. Insert a USB devices
- 2. Open "File Explorer"; select "This PC" and then select the USB device.



3. Select the "Drive Tools" Menu and click BitLocker, if the BitLocker icon is disabled, please contact your system administrator.



5		<i>,</i> 1				
💻 🛃 🔚 🖛	Manage	This PC		—	\Box \times	
File Computer View	Drive Tools				~ (?
\leftarrow \rightarrow \checkmark \uparrow \blacksquare \rightarrow This PC	2	~	ට 🔎 Search This PC			
	Foldors (7)					,
🗸 🖈 Quick access	rolders (7)			_		
E Des				×		
🕂 Doʻ 🔶 🛛 🏘 BitLocker I	Drive Encryption (I	E:)				
🖆 Doi						
Pic Starting Bit	tLocker					
> 💻 This Please wait w	hile Bitl ocker initi	alizes the drive				
> USB	ine bitebeker inte	anzes the drive.		_		
Neta 🔥 Don't rem	nove vour drive du	ring BitLocker setup.				
	,,	,				
						_
Wheet are Did.						
<u>vvnat are BitLo</u>	ocker's system req	uirements:				
				Cancel		
10 items 1 item selected				Cancer	8== 6	
io items i item selected					•	-

5. After selecting "Turn on BitLocker", please wait for BitLocker initializes

6. After initializes, please check "Use a password to unlock this drive"

		\times
~	RitLocker Drive Encryption (E:)	
	Change have seen to be a ship drive	
	choose now you want to unlock this drive	
	Use a password to unlock the drive	
	Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.	
	Enter your password	
	Reenter your password	
	Use my smart card to unlock the drive	
	You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.	
	Next Cancel	

7. Please set a password following the on-screen instructions

		×
÷	Real BitLocker Drive Encryption (E:)	
	Choose how you want to unlock this drive	
	Use a password to unlock the drive	
	Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.	
	Enter your password	
	Reenter your password	
	Use my smart card to unlock the drive	
	You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.	
	Next Cance	

8. After input the password, please select "Save to a file" with recovery key or Print the recovery key.

It is recommended not to save the Recovery key to USB device.

				×		
←	🏘 BitLocker Drive Encryption (E:)					
	How do you want to back up yo	our recovery key?				
	 Some settings are managed by your 	system administrator				
	If you forget your password or lose your					X
		Rave BitLocker recover	ry key as			×
	ightarrow Save to a file	← → ~ ↑ □ >	This PC > Desktop	ٽ ~	Search Desktop	
	ightarrow Print the recovery key	Organize 🔻 New fo	lder			• • •
		✓	Name	^	Date modified	Туре
		Desktop 🤉	t	No items match ye	our search.	_
		🕹 Downloads 🦻	e			
		Documents 🤅	e .			
		E Pictures	d.			
	How can I find my recovery key later?	> 💻 This PC				
		> 👝 USB Drive (E:)				
		> 🍠 Network				
			٢			>
		File name: Bitl	Locker Recovery Key 4EFCB4	A2-B83D-48D4-803D-0	83425C3747C	~
		Save as type: Tex	t Files (*.txt)			~
		∧ Hide Folders			Save Car	ncel

9. Please choose how much of your drive to encrypt and click "Next". Recommend to use "Encrypt entire drive" for better encrypt security.

	X
~	litLocker Drive Encryption (E:)
	Choose how much of your drive to engrypt
	choose now 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 Cancel
	×
←	Ritl ocker Drive Encryption (Fr)
1	- Breecker Bille Enclyption (L)
	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 Pitl ocker on a DC or drive that's already in use, consider once uting the entire drive
	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.
	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.
	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. O Encrypt used disk space only (faster and best for new PCs and drives) Encrypt entire drive (clower but best for PCs and drives already in use)
	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. O 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)
	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. O Encrypt used disk space only (faster and best for new PCs and drives) Incrypt entire drive (slower but best for PCs and drives already in use)
	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. O Encrypt used disk space only (faster and best for new PCs and drives)
	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. O 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)
	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)
	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)
	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. O Encrypt used disk space only (faster and best for new PCs and drives) Incrypt entire drive (slower but best for PCs and drives already in use)
	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. O Encrypt used disk space only (faster and best for new PCs and drives) I Encrypt entire drive (slower but best for PCs and drives already in use)
	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)

10. Click "Start encrypting" to encrypt the USB device.

ess the protected data on the USB device!		
New BitLocker Drive Encryption (E:)		×
Are you ready to encrypt this drive?		
You'll 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 won't be protected.		
	Start encrypting	Cancel
	Rest contract of the cost devices Rest between the cost devices Are you ready to encrypt this drive? You'll 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 won't be protected.	Start encryption

Please keep your Password and Recovery key carefully! If you lost both, there is no way to

11. BitLocker Drive Encryption start and please wait for complete. If you need to remove the USB device while it is still encrypting, please click "Pause" encryption before Ejecting it. It will continue the encryption process next time you insert it to the PC.

BitLock	er Drive Encryption				
	Encrypting				
6	Drive E: 0.8% Completed				
			Pause		
A Pa th	ause encryption before removin e drive could be damaged.	BitLock	er Drive Encryp	tion	×
M	lanage BitLocker	R	Encryption	of E: is complete.	
					Close
					Close
		Manag	e BitLocker		

- IV. Accessing USB device protected by BitLocker to Go
 - 1. Insert the USB devices
 - 2. Open "File Explorer"; select "This PC" and then double-click the encrypted USB device.



3. Please enter the password as instructed in the Pop-up Windows

BitLocker (E:)	
Enter password to unlock this drive.	
More options	
	Unlock

4. The USB Drive and the icon changed to unlock status and you can access the USB device as usual.



You can use BitLocker icon under "Drive Tools" Tab to manage BitLocker of your USB device.



- V. Step to recover BitLocker to Go with Recovery Key if you forget the password
 - 1. Insert a USB devices
 - 2. Open "File Explorer"; select "This PC" and then double-click the encrypted USB device.



3. Click "More Option" in the Pop-up Windows

BitLocker (E:)	
Enter password to unlock this drive.	
More options	
Unlock	

4. Select "Enter recovery key"

BitLocker (E:)
Enter password to unlock this drive.
Fewer options
Enter recovery key
Automatically unlock on this PC
Unlock

 Please enter the recovery key saved/printed when encrypting the USB device and then click "Unlock"



6. Please use "Change password/PIN" of "BitLocker" under "Drive Tools" Tab to change the password.



VI. Reminder for Password and Recovery Key

Please keep your password and recovery key safe. If you forget password and lost the recovery key, <u>ALL</u> <u>Data will be lost in the USB device because it is not possible to unlock the encrypted USB device!</u>