Procedure for BitLocker to Go in Windows 10

Table of Contents

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

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: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/bitlocker-drive-encryption#bitlocker-drive-encryption-partitioning-requirements
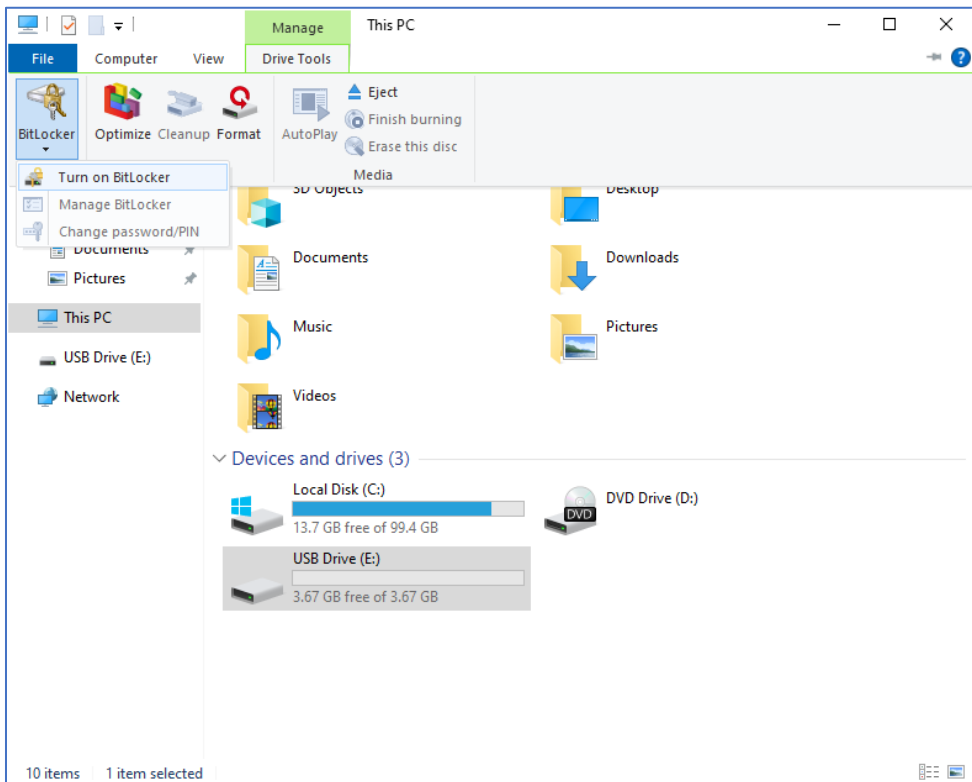
III. Using BitLocker to Go to Encrypt the USB device

1. Insert a USB devices
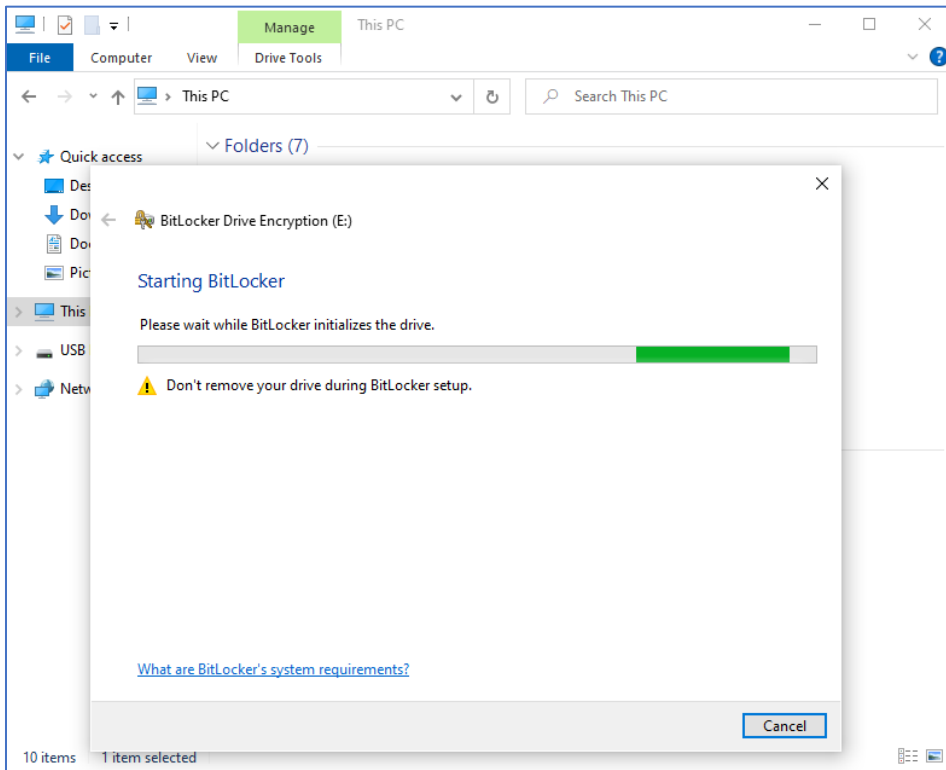2. Open "File Explorer"; select "This PC" and then select the USB device.
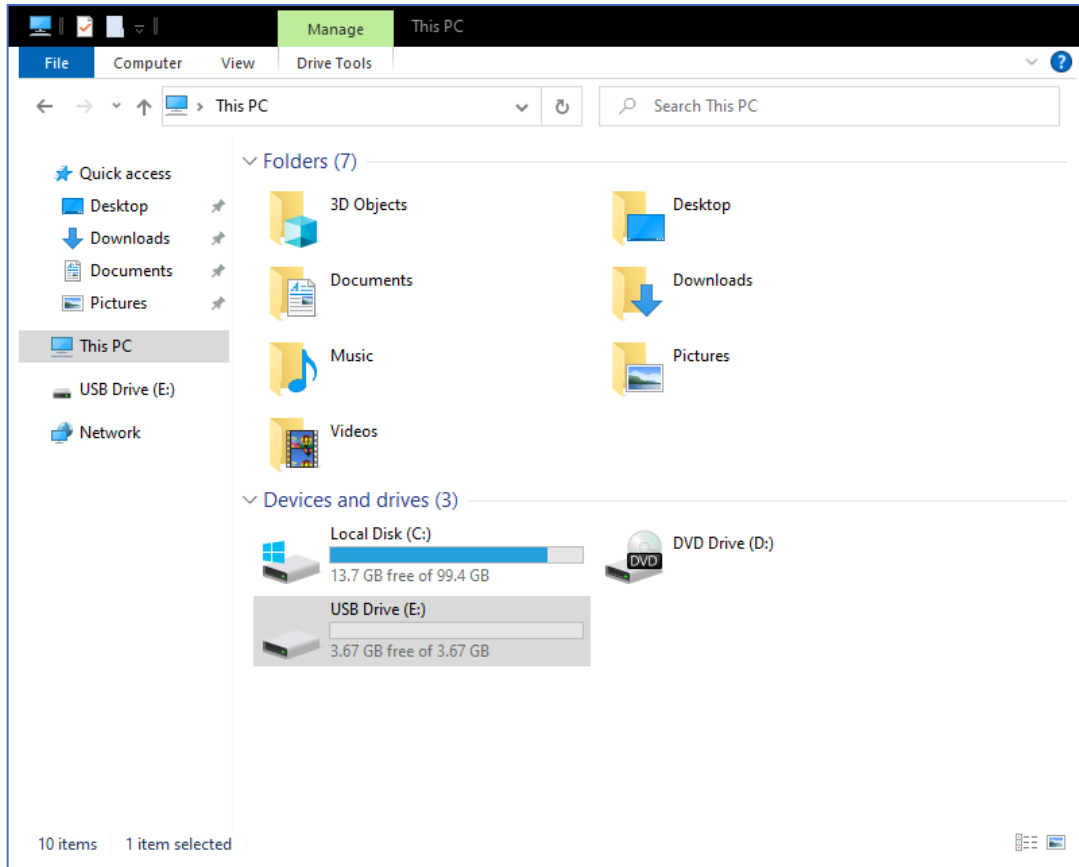
3. Select the "Drive Tools" Menu and click BitLocker, if the BitLocker icon is disabled, please contact your system administrator.
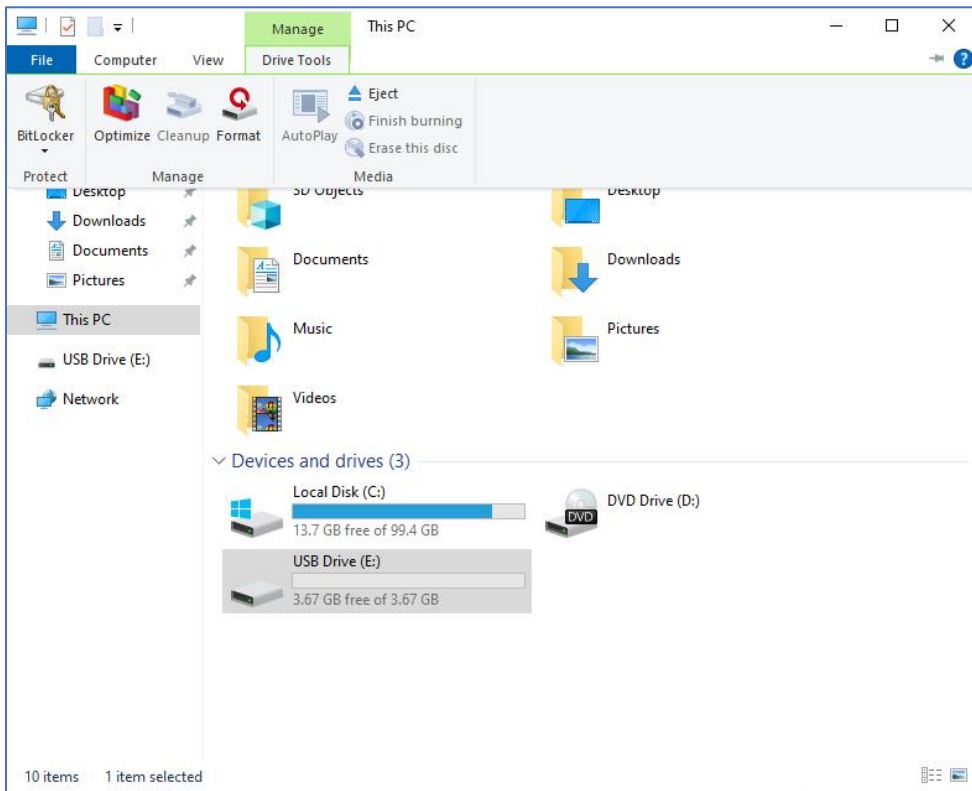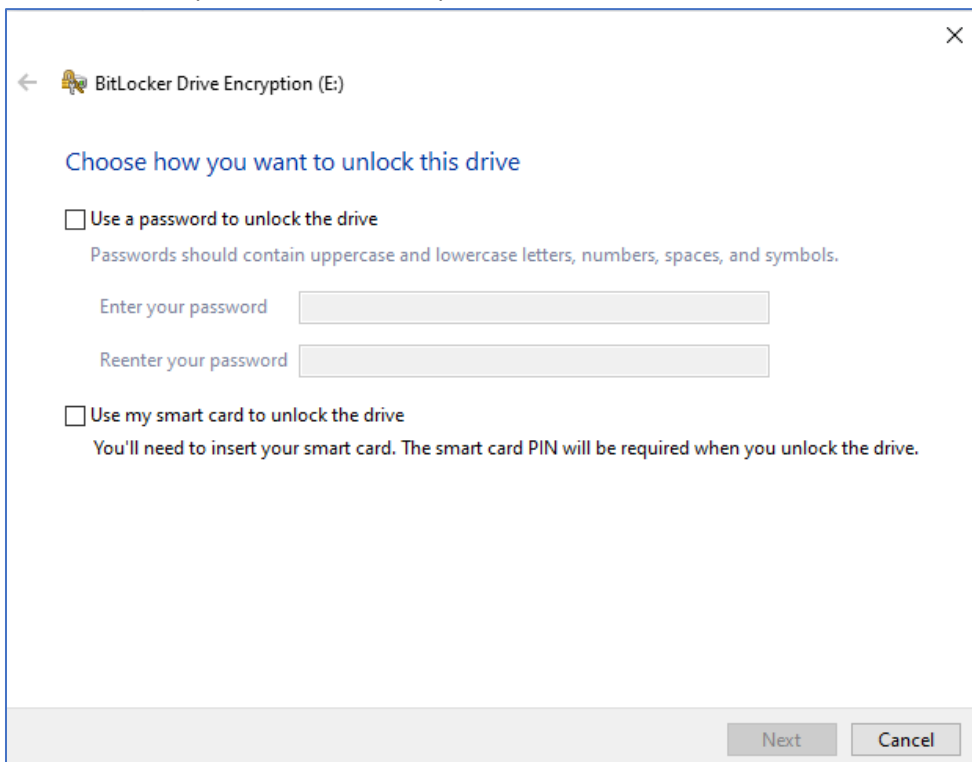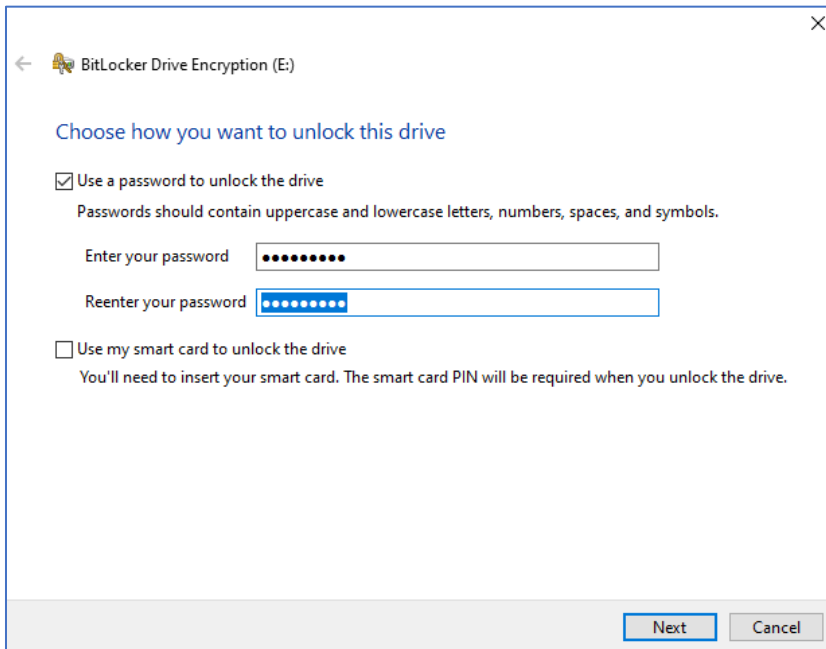

4. Select "Turn on BitLocker"

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

6. After initializes, please check "Use a password to unlock this drive"
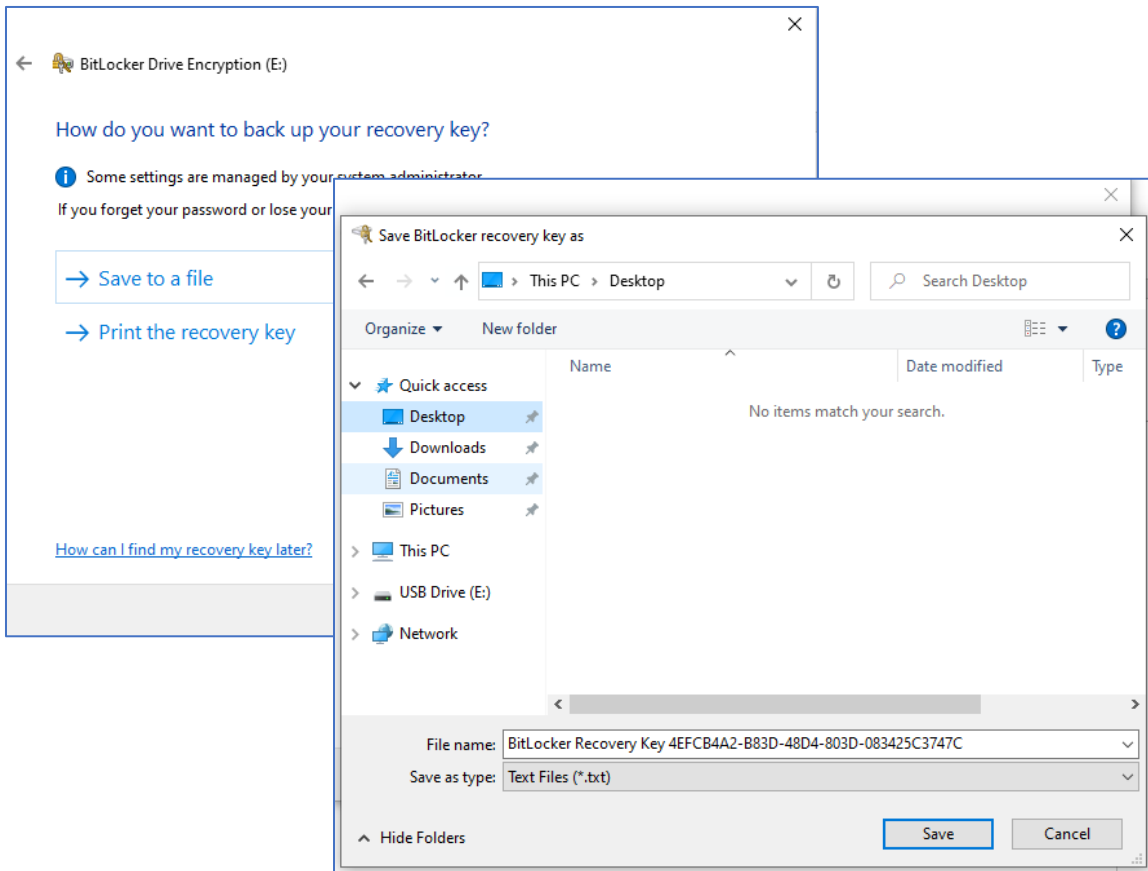
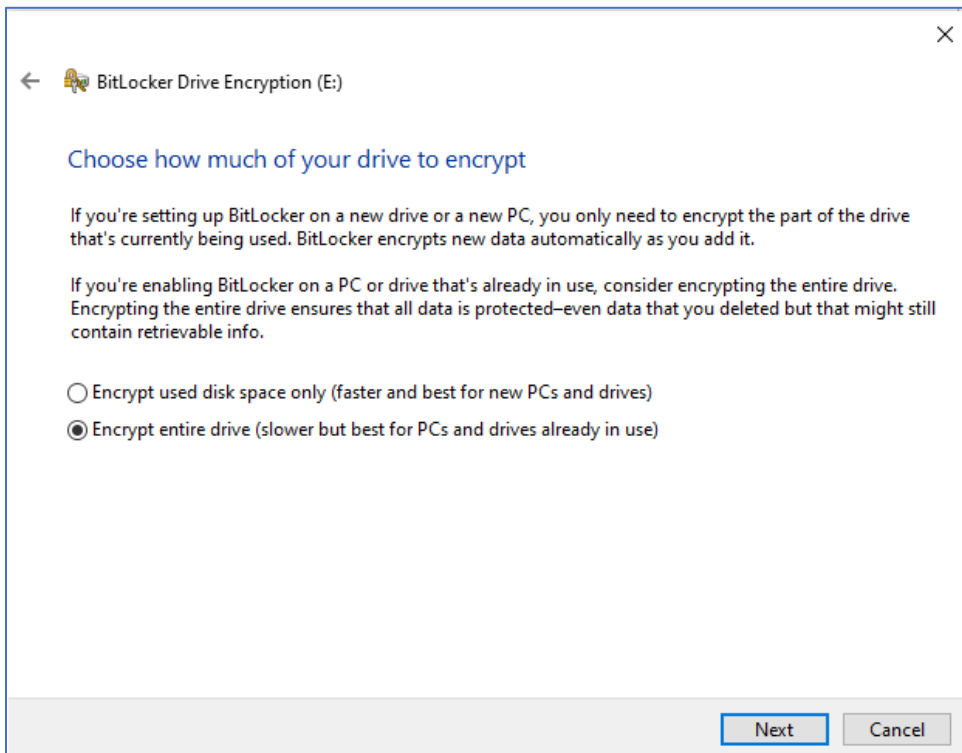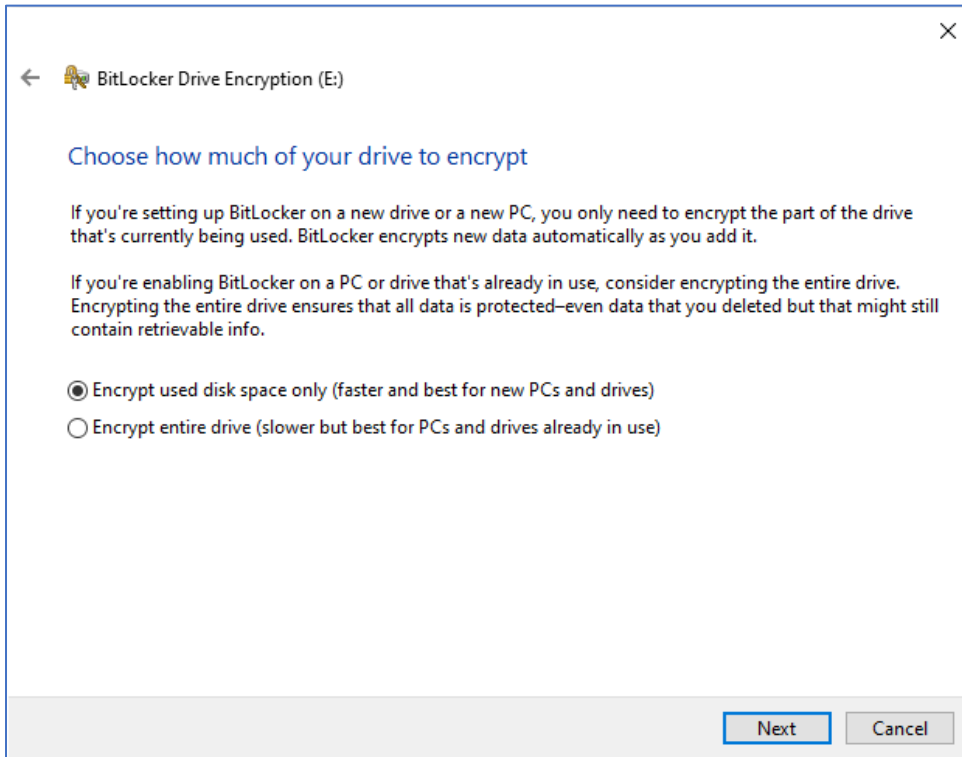7. Please set a password following the on-screen instructions

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.

9. Please choose how much of your drive to encrypt and click "Next". Recommend to use "Encrypt entire drive" for better encrypt security.
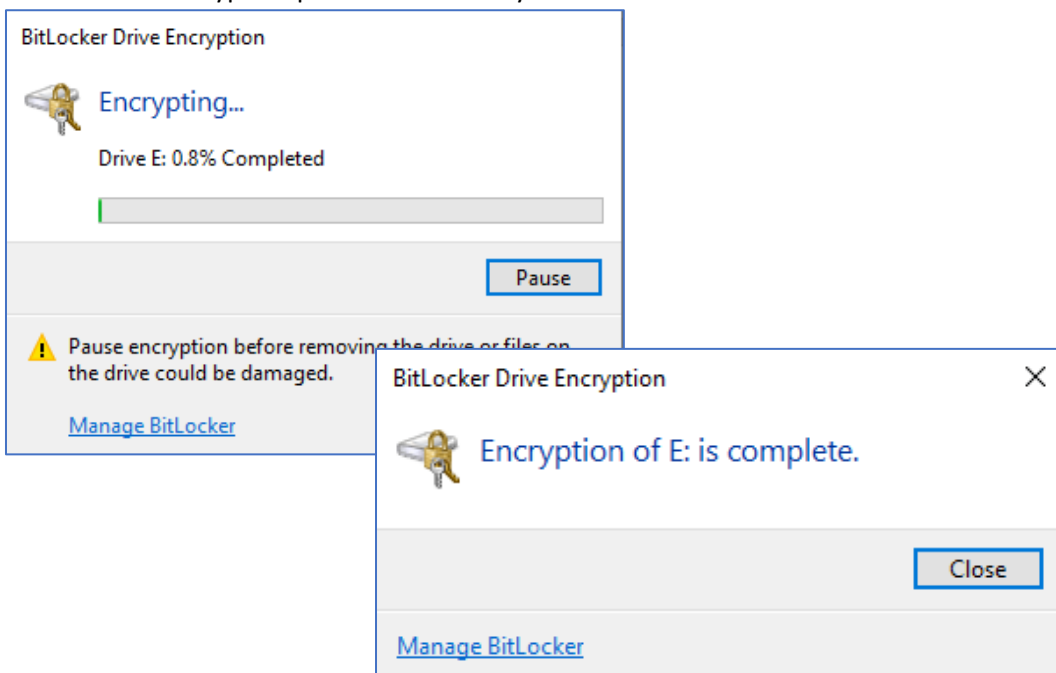
10. Click "Start encrypting" to encrypt the USB device.
    Please keep your Password and Recovery key carefully! If you lost both, there is no way to access the protected data on the USB device!
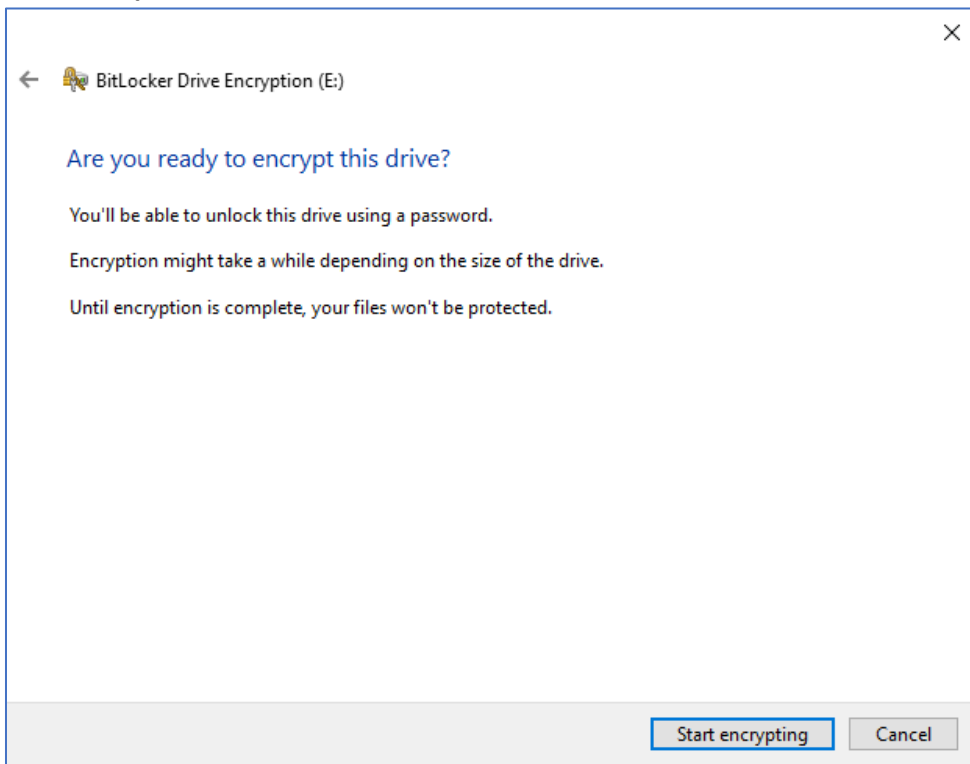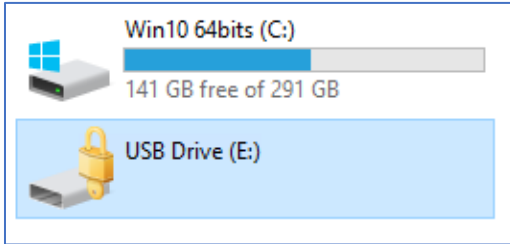

11. BitLocker Drive Encryption start and please wait for complete. If you need to remove the USB device while it is still encrypting, please click "Pause" encryption before Ejecting it. It will continue the encryption process next time you insert it to the PC.
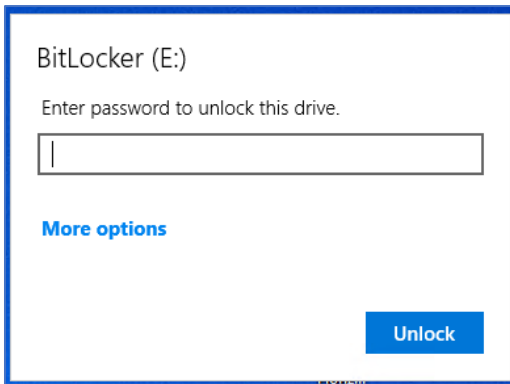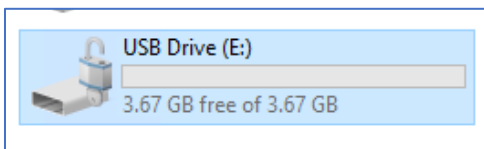
1. Insert the USB devices
2. Open "File Explorer"; select "This PC" and then double-click the encrypted USB device.
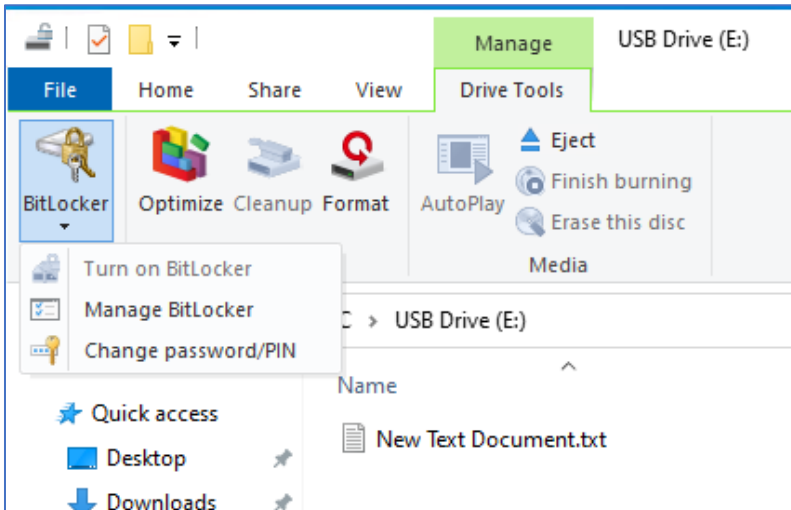

3. Please enter the password as instructed in the Pop-up Windows

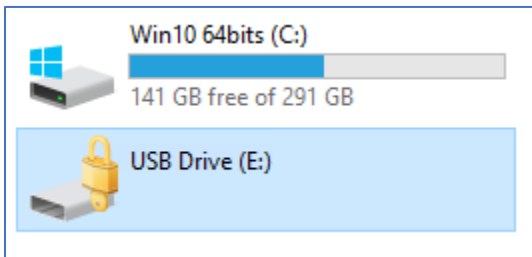4. The USB Drive and the icon changed to unlock status and you can access the USB device as usual.

You can use BitLocker icon under "Drive Tools" Tab to manage BitLocker of your USB device.
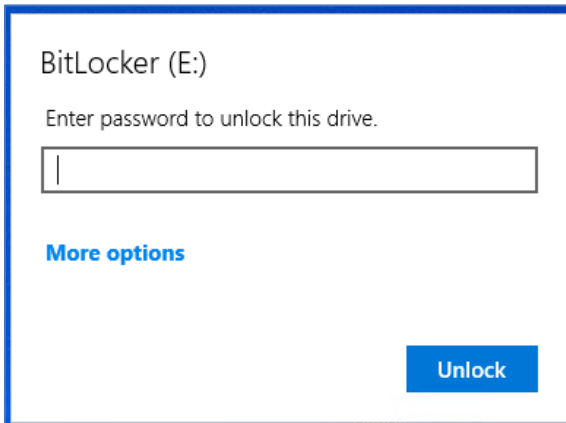
V. Step to recover BitLocker to Go with Recovery Key if you forget the password
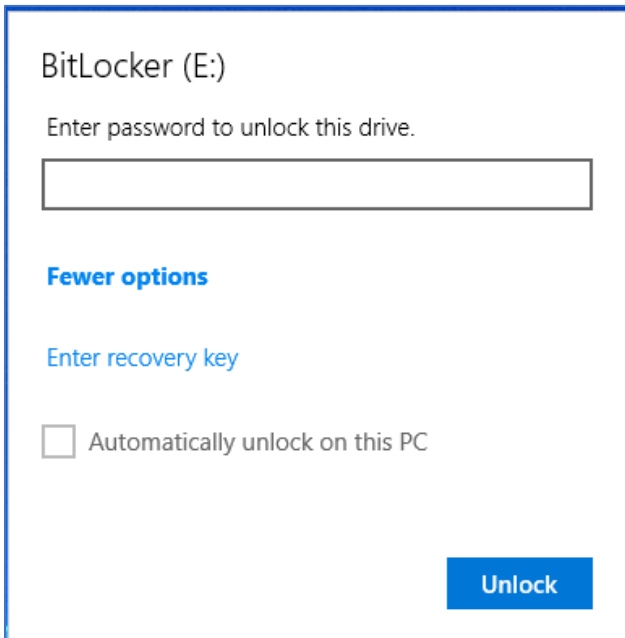
1. Insert a USB devices
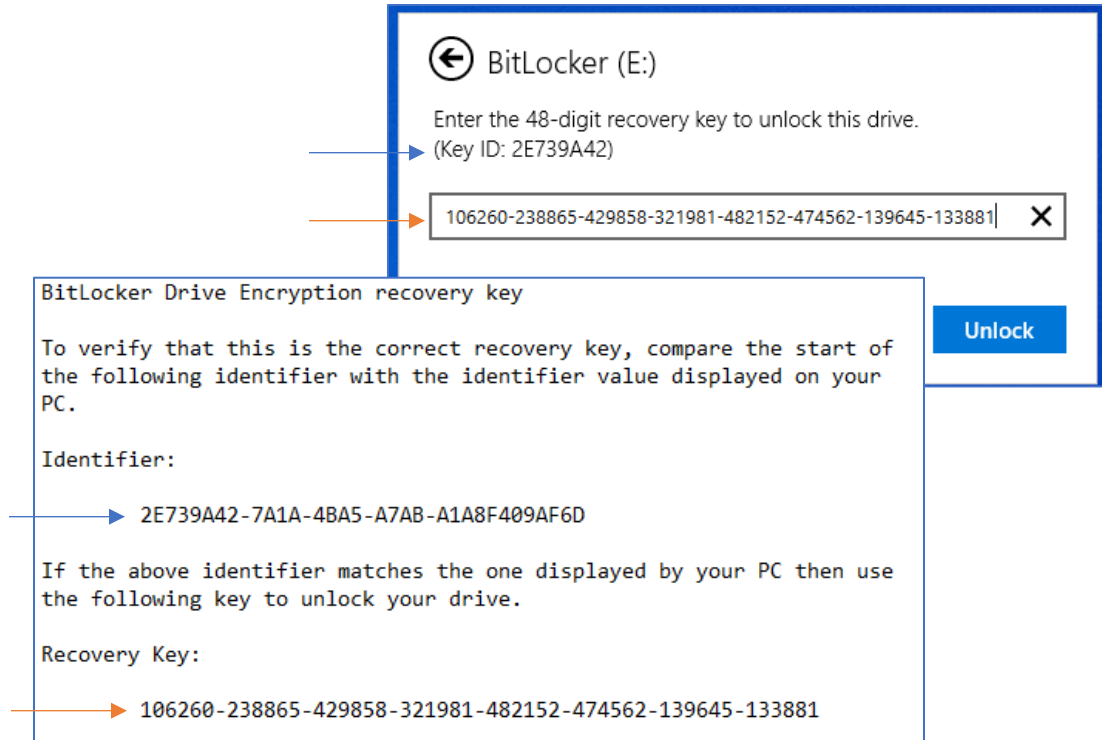2. Open "File Explorer"; select "This PC" and then double-click the encrypted USB device.

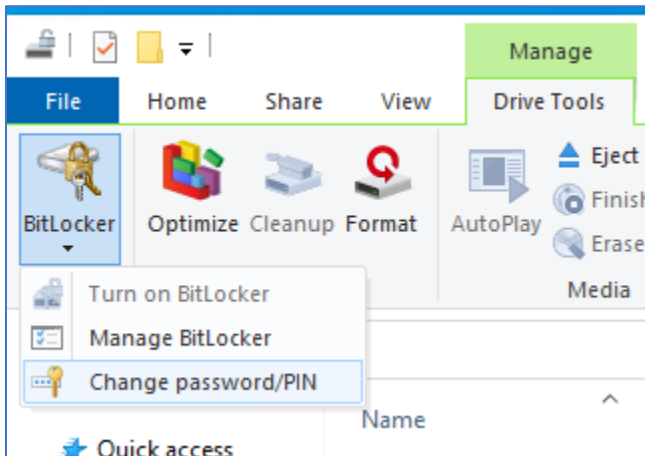3. Click "More Option" in the Pop-up Windows

4. Select "Enter recovery key"

5. 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, **ALL Data will be lost in the USB device because it is not possible to unlock the encrypted USB device!**