Encrypting with BitLocker To Go for removable devices under Windows 10

(BitLocker To Go User Guide)

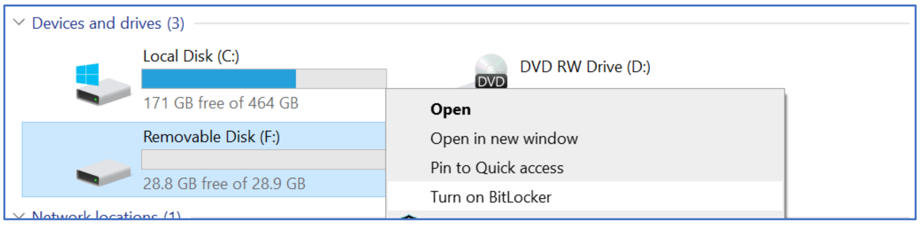
1. Introduction

BitLocker To Go —a feature of Windows 10— is a full-disk encryption protection technology for removable storage devices that are connected to one of the USB ports on your computer (referred as either USB drive or drive hereafter).

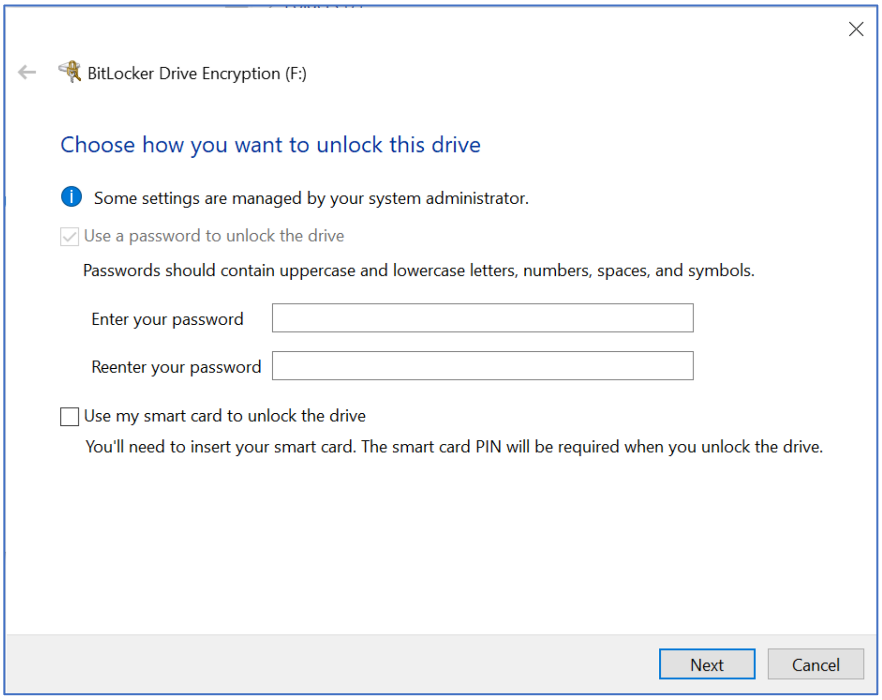
Basically, BitLocker To Go allows you to encrypt a USB drive and restrict access with a password. When you connect the encrypted USB drive to a Windows 10 computer, you will be prompted for the password and upon successfully entering it, you can read and write to the drive as usual.

2. Turning on BitLocker To Go for a USB Drive

i. Go to “This PC” and select the USB Drive you want to encrypt, right click and select “turn on BitLocker”.



ii. Once the initialization process is completed, BitLocker To Go will prompt you to set up a password that is used to unlock the drive.



BitLocker Drive Encryption (F:)

Choose how you want to unlock this drive

Some settings are managed by your system administrator.

☑ Use a password to unlock the drive

Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.

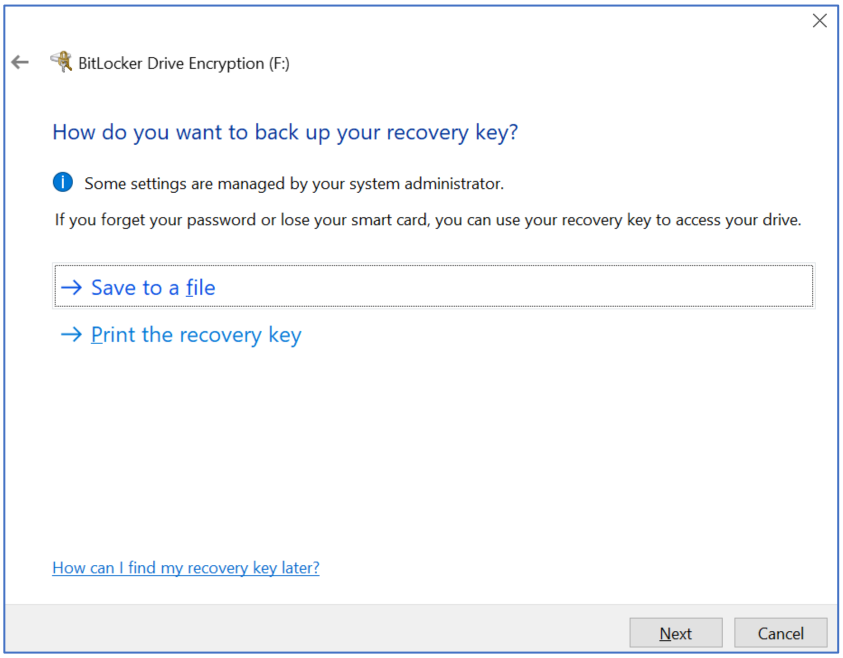
Enter your password

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.

iii. After setting up a password, BitLocker To Go will prompt you to store or print the recovery key that is used to unlock the drive, in case you forget the password one day.



BitLocker Drive Encryption (F:)

How do you want to back up your recovery key?

Some settings are managed by your system administrator.

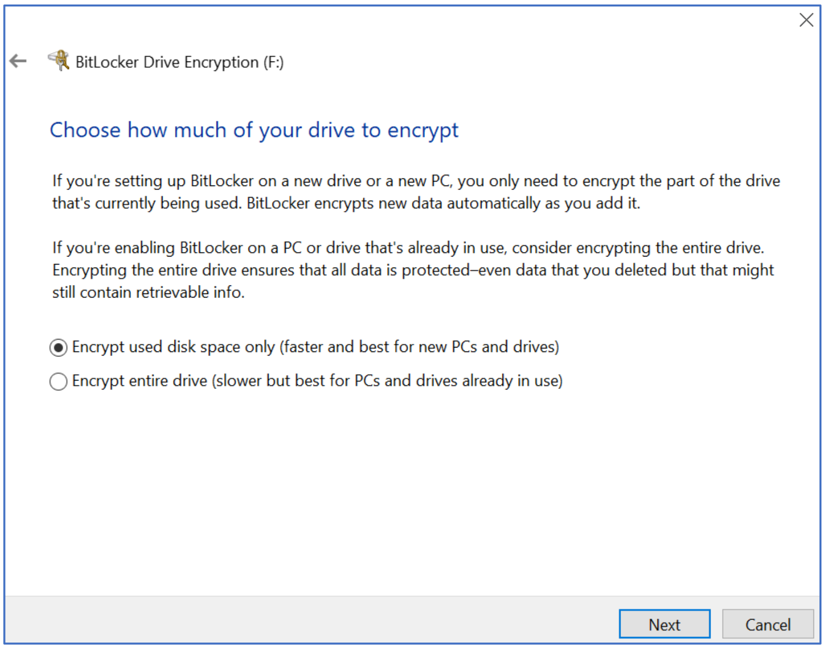
If you forget your password or lose your smart card, you can use your recovery key to access your drive.

→ Save to a file

→ Print the recovery key

How can I find my recovery key later?

iv. You will be prompted to start the encryption process.



BitLocker Drive Encryption (F:)

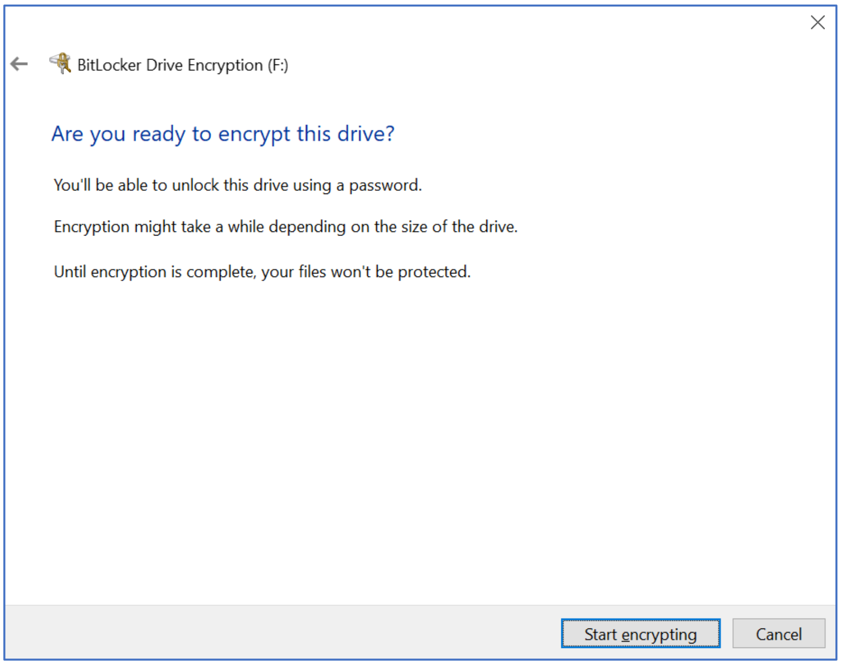
Choose how much of your drive to encrypt

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)



BitLocker Drive Encryption (F:)

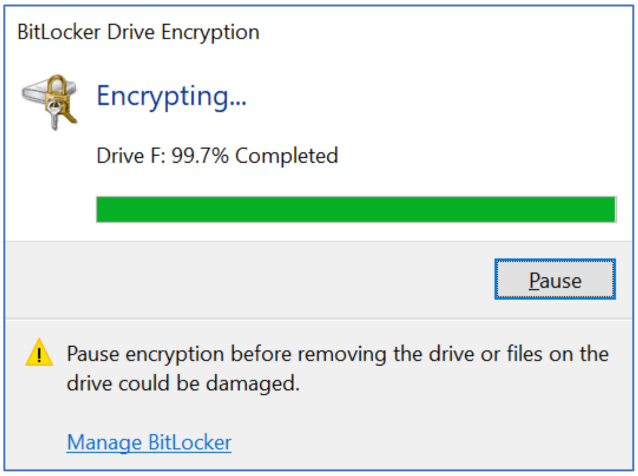
Are you ready to encrypt this drive?

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.

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.

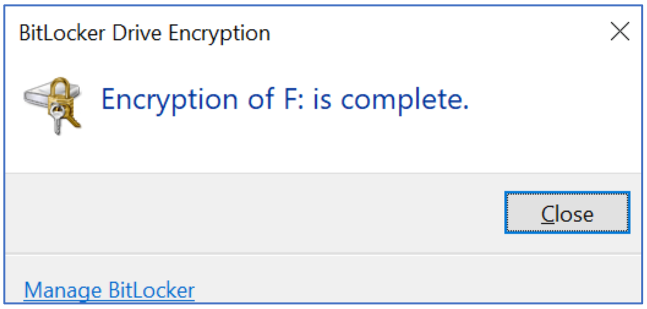

BitLocker Drive Encryption

Encrypting...

Drive F: 99.7% Completed

⚠ Pause encryption before removing the drive or files on the drive could be damaged.

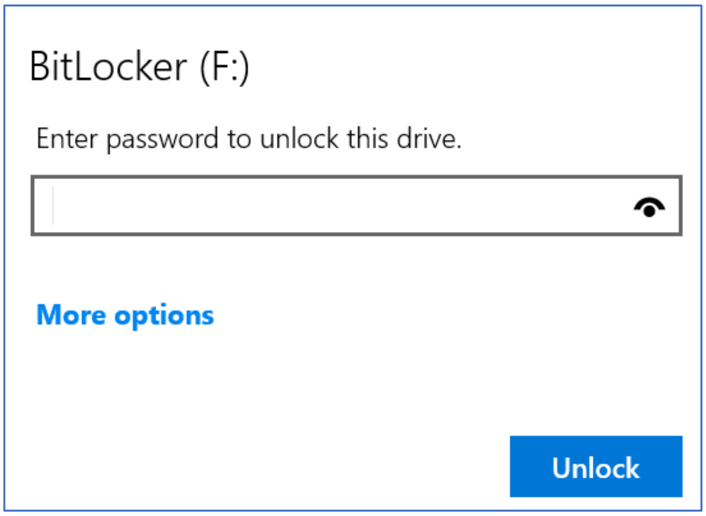
vi. Once the encryption is complete, BitLocker To Go displays a confirmation dialog box and a lock icon will be shown on the Drive.


BitLocker Drive Encryption

Encryption of F: is complete.

3. Accessing a BitLocker To Go encrypted drive in Windows 10

When a BitLocker To Go encrypted drive is plugged in any Windows 10 system, a dialog window will appear, informing you that the drive is protected by BitLocker Drive Encryption and waiting for you to enter the password.

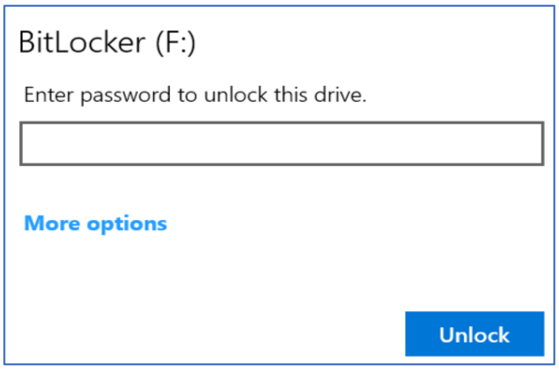


After typing the password and clicking the Unlock button, you will be able to access the drive and its content as usual.

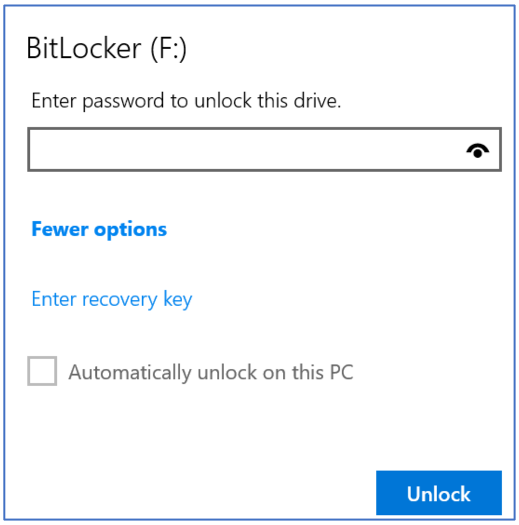
4. Recovering the encrypted USB drive using BitLocker recovery key

If you forget the password of the encrypted drive, the BitLocker recovery key saved or printed in 2 (iii) above will help you unlock the drive and create a new password for the drive.

i. Plug the encrypted USB drive in Windows 10 and click "More options"



ii. Enter the BitLocker recovery key and click "Unlock"

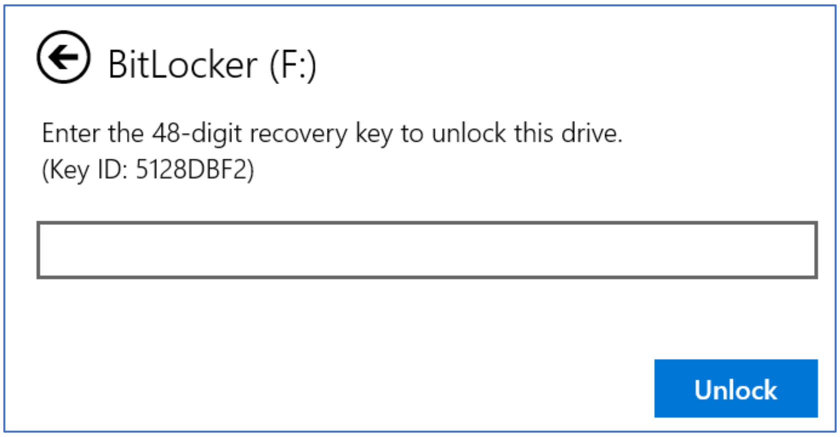


BitLocker (F:)

Enter password to unlock this drive.

iii. Enter the BitLocker recovery key and click “Unlock”

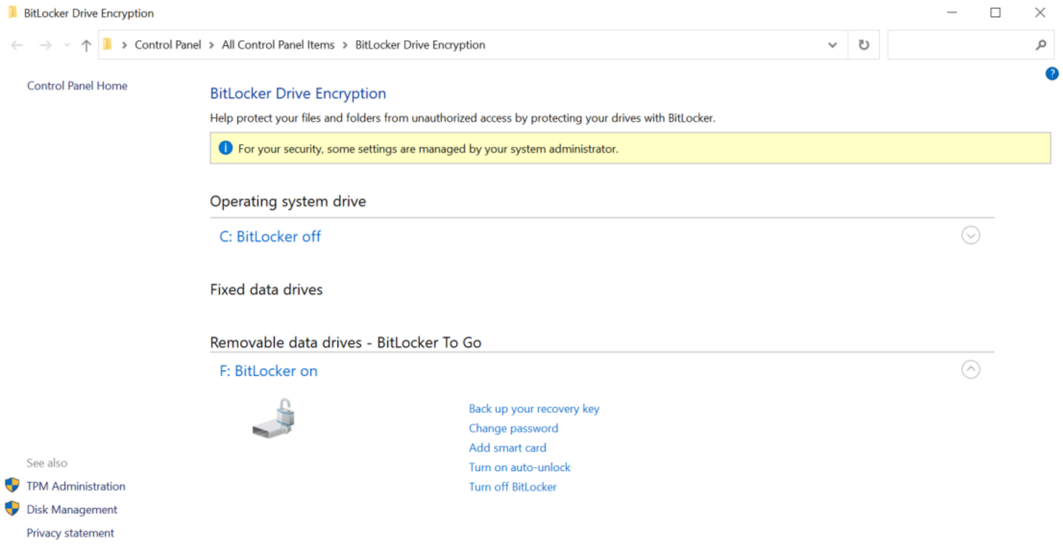
If you have saved the recovery key in a file, you can simply copy and paste it; otherwise, you have to enter the long key carefully.



BitLocker (F:)

Enter the 48-digit recovery key to unlock this drive.
(Key ID: 5128DBF2)

iv. Click “This PC”, highlight the removable drive and right click “Manage BitLocker”


BitLocker Drive Encryption
Control Panel > All Control Panel Items > BitLocker Drive Encryption
Control Panel Home
See also
TPM Administration
Disk Management
Privacy statement

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

For your security, some settings are managed by your system administrator.

Operating system drive

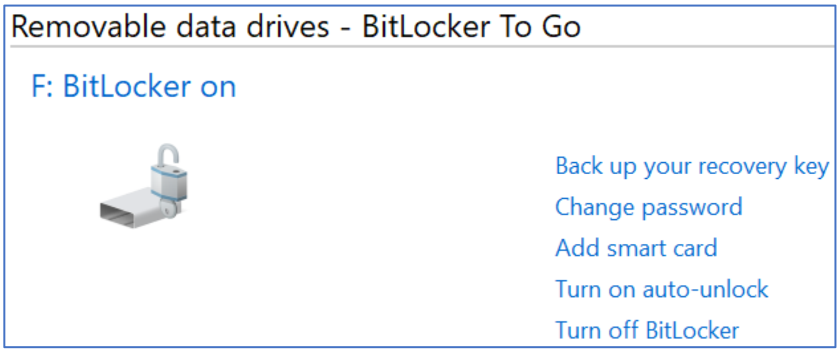
C: BitLocker off

Fixed data drives

Removable data drives - BitLocker To Go

F: BitLocker on

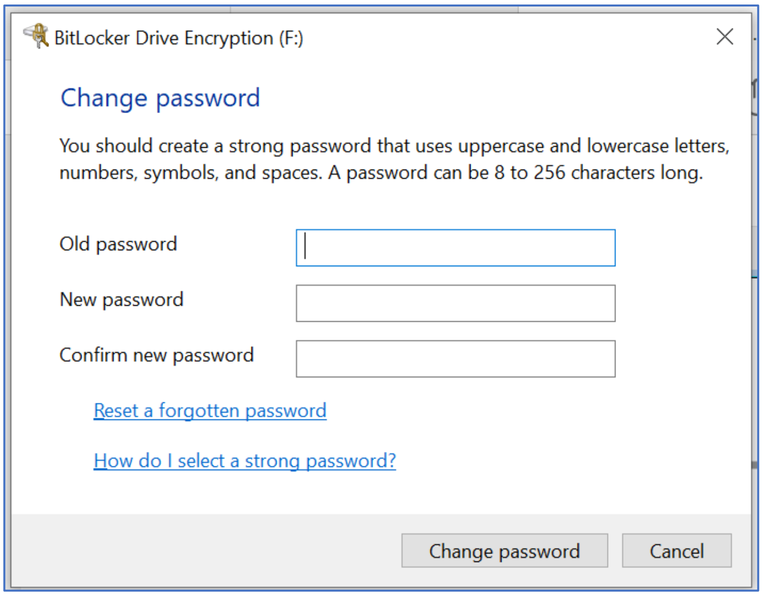
v. Click “Change password”



Removable data drives - BitLocker To Go

F: BitLocker on

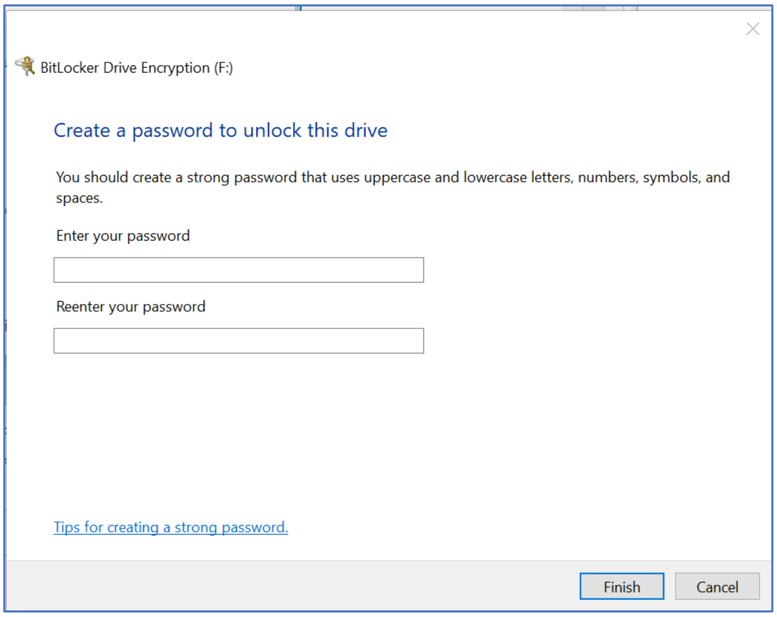
5. Forgetting both the password and the recovery key


BitLocker Drive Encryption (F:)

Change password

You should create a strong password that uses uppercase and lowercase letters, numbers, symbols, and spaces. A password can be 8 to 256 characters long.

If you forget your old password, click the “Reset a forgotten password” and then create a new password and then click finish


BitLocker Drive Encryption (F:)

Create a password to unlock this drive

You should create a strong password that uses uppercase and lowercase letters, numbers, symbols, and spaces.

If you have lost both the password and the recovery key, you will lose your data forever as you cannot unlock the drive. Therefore, you are recommended to memorize the password and keep the printed or saved recovery key in a safe place.