CORVID

CYBERDEFENSE

BitLocker Disk Encryption Guide for Windows 10 Pro

Contents

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

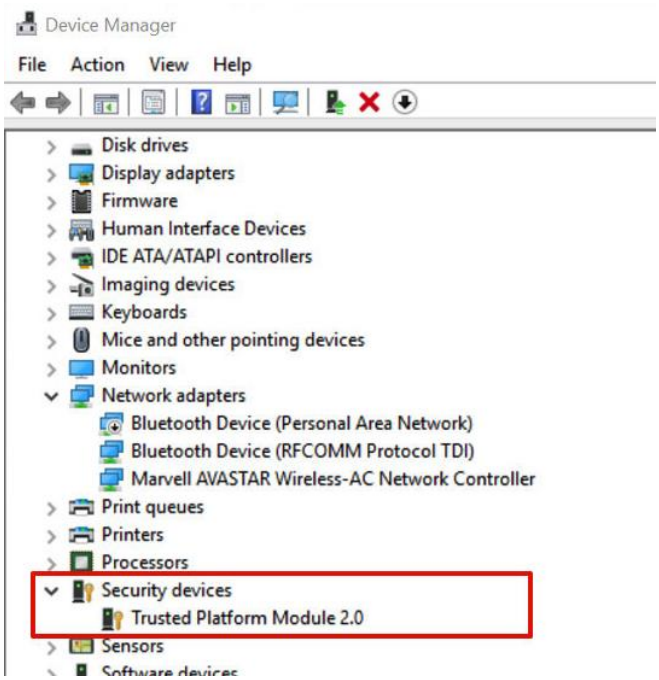
- BitLocker Drive Encryption is available only on Windows 10 Pro and Windows 10 Enterprise.
- Please ensure the laptop OS has been updated.
- Your PC's hard drive must contain two partitions: a system partition, which contains the necessary files to start Windows, and the partition with the operating 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.



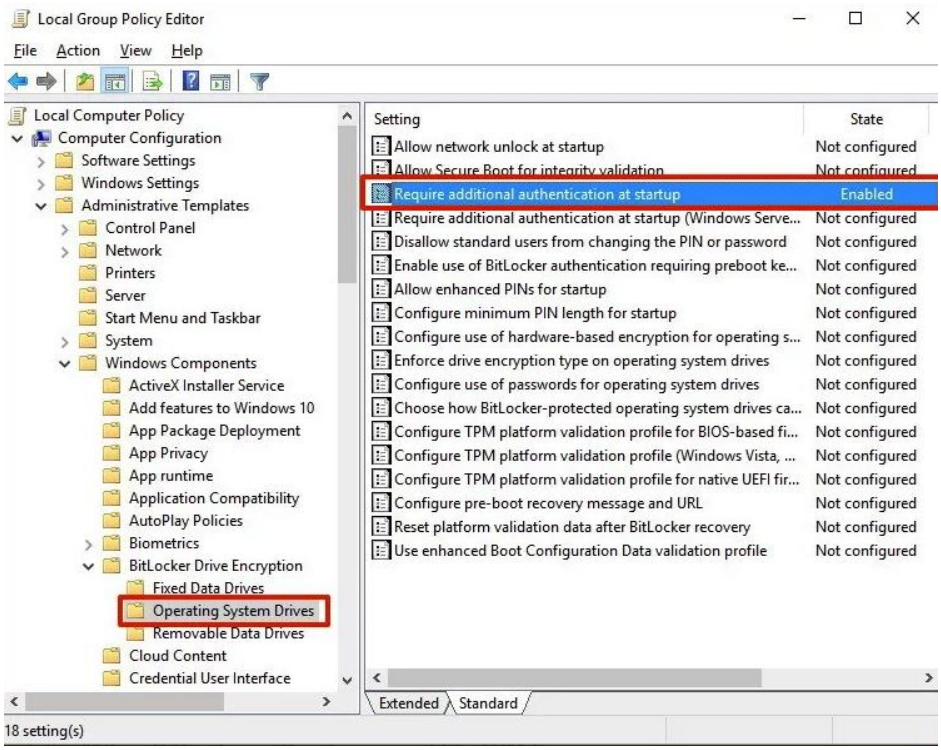
Note: Verify that your computer has a TPM chip version 1.2 or later to support hardware-based encryption with BitLocker.

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).

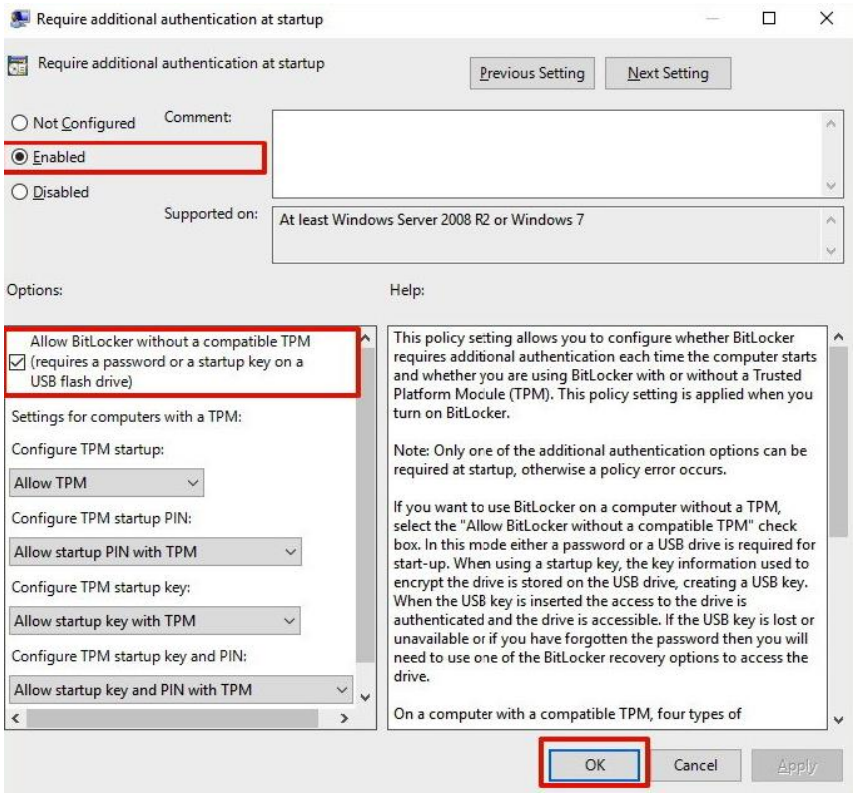
How to ensure you can turn on BitLocker without TPM

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**.

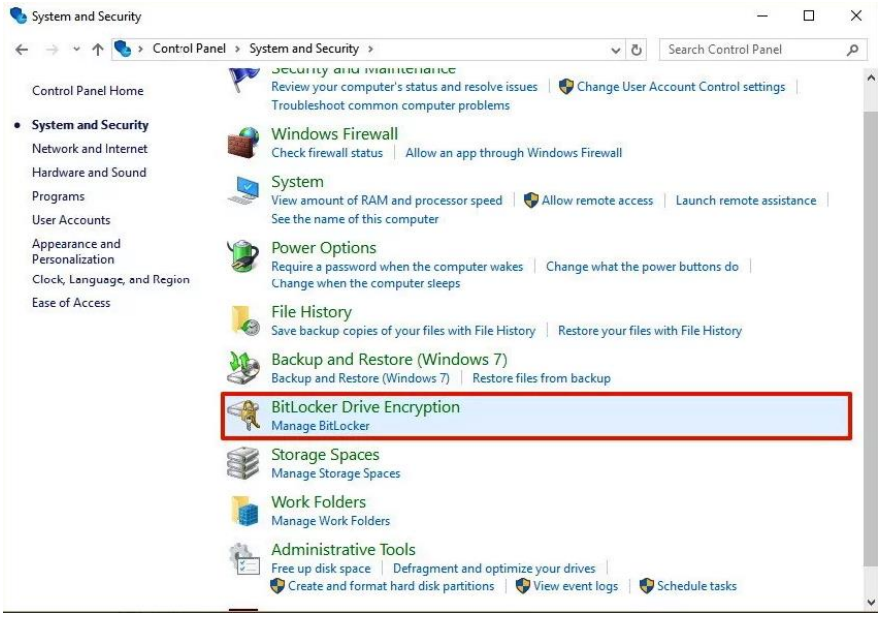


6. Select **Enabled**.
7. Make sure to check the **"Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)"** option.
8. Click **OK** to complete this process.

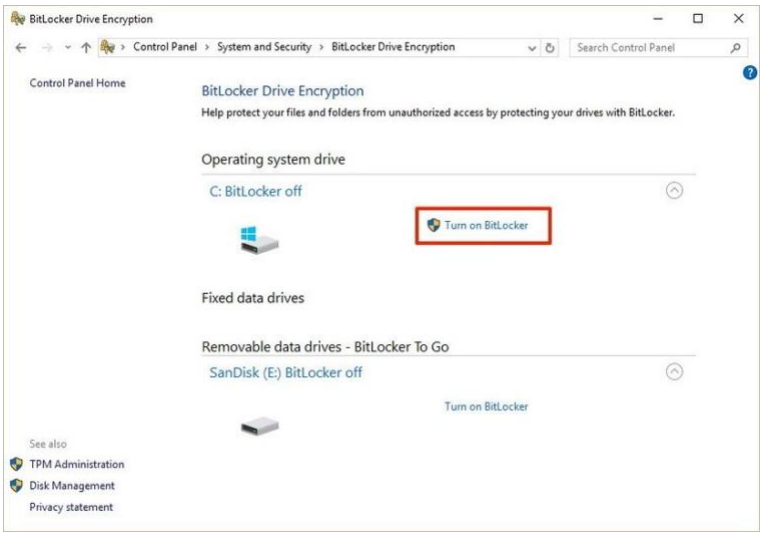


How to turn on BitLocker on the operating system drive

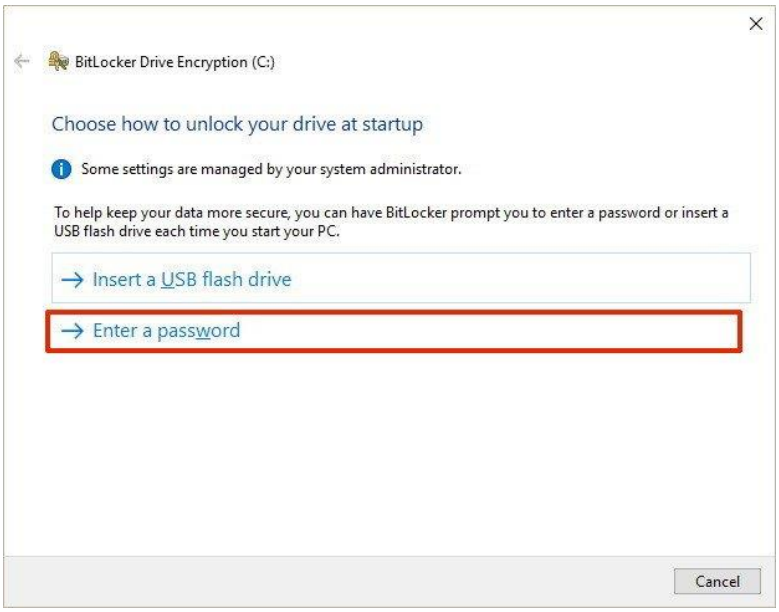
1. Use the keyboard shortcut **Windows key + X** to open the Power User menu and select **Control Panel**.
2. Click **System and Security**.
3. Click **BitLocker Drive Encryption**.



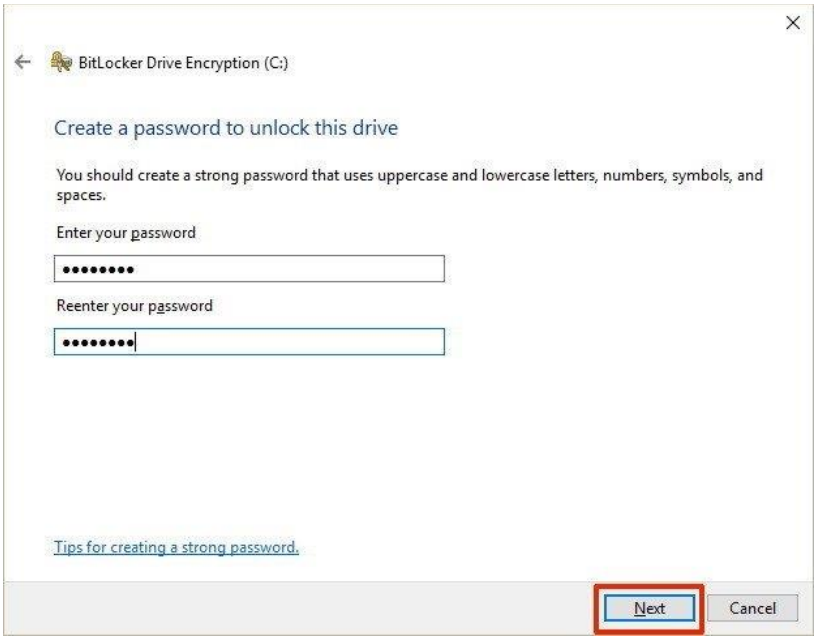
4. Under BitLocker Drive Encryption, click **Turn on BitLocker**.



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.



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.)



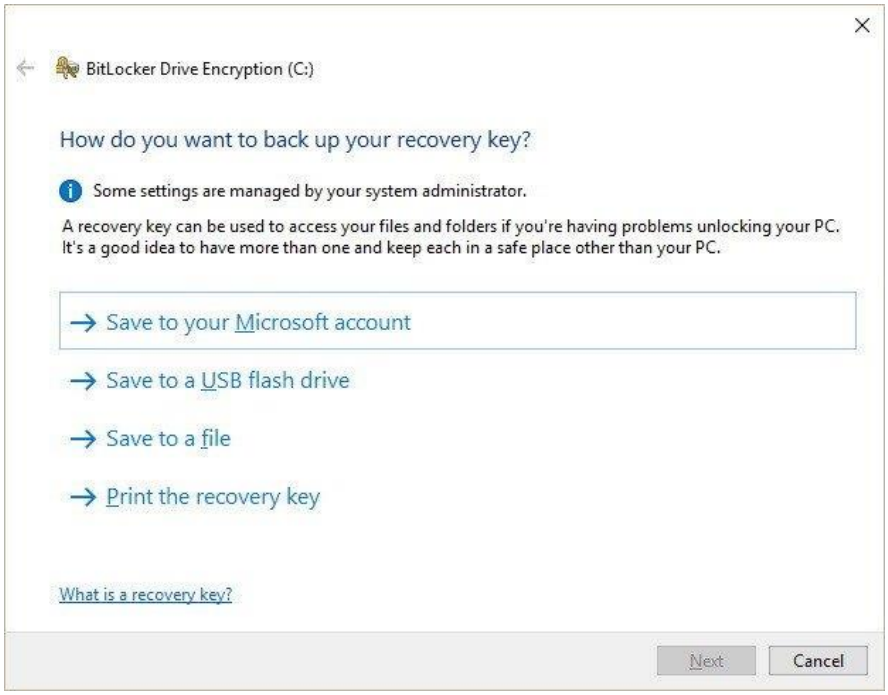
7. You will be given the choices to save a recovery key to regain access to your files in case you forget your password. Options include:

   - Save to your Microsoft account
   - Save to a USB flash drive
   - Save to a file

- Print the recovery key

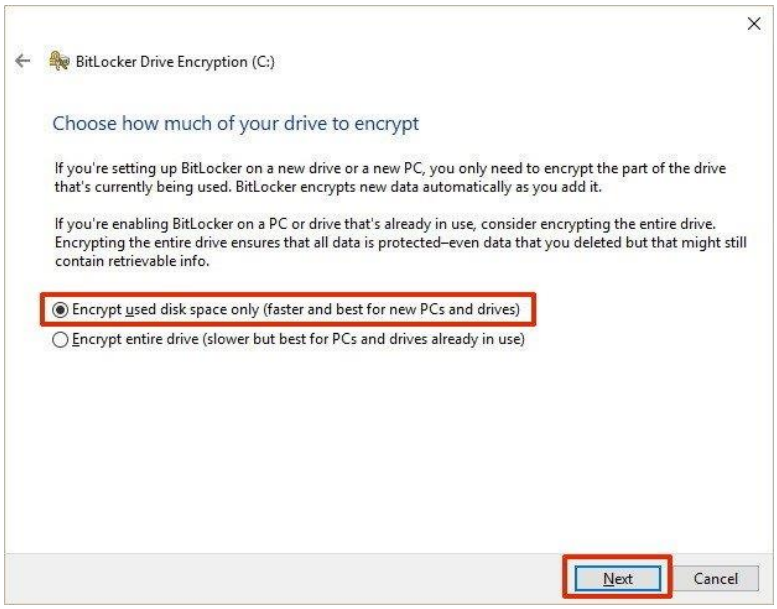
Select the option that is most convenient for you (we recommend a dedicated USB that is stored is a safe), and save the recovery key in a safe and secure place.

8. Click **Next** to continue.



9. Select the encryption option that best suits your scenario:

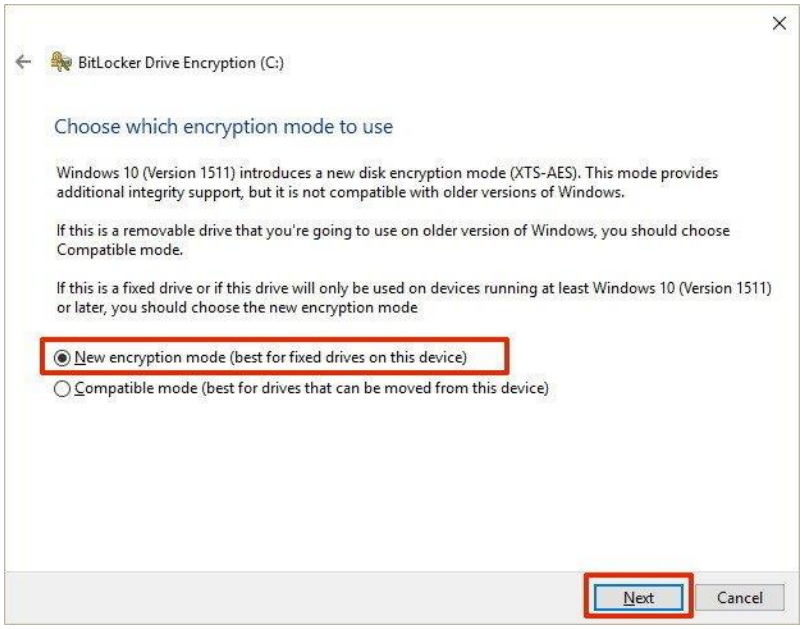
- Encrypt used disk space only (faster and best for new PCs and drives)
- Encrypt entire drive (slower but best for PCs and drives already in use)



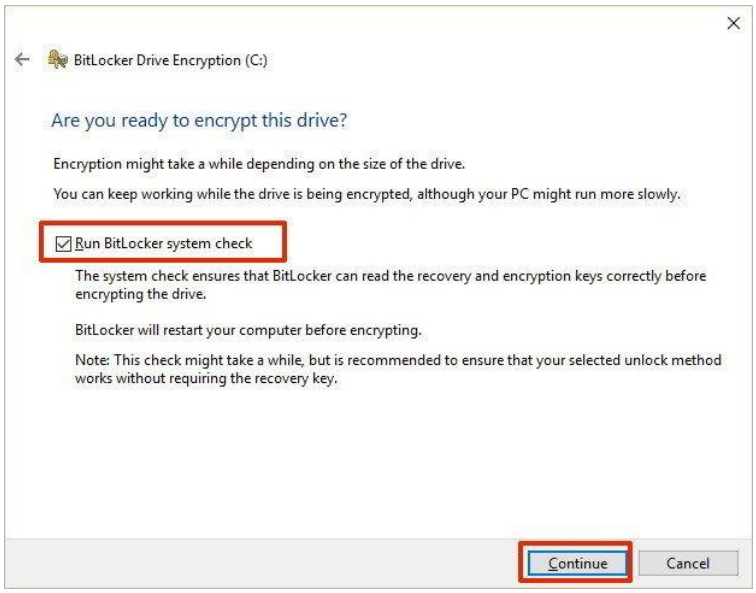
10. Choose **New encryption mode** (best for fixed drives on this device)

    On Windows 10 version 1511, Microsoft introduced support for XTS-AES encryption algorithm. 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.

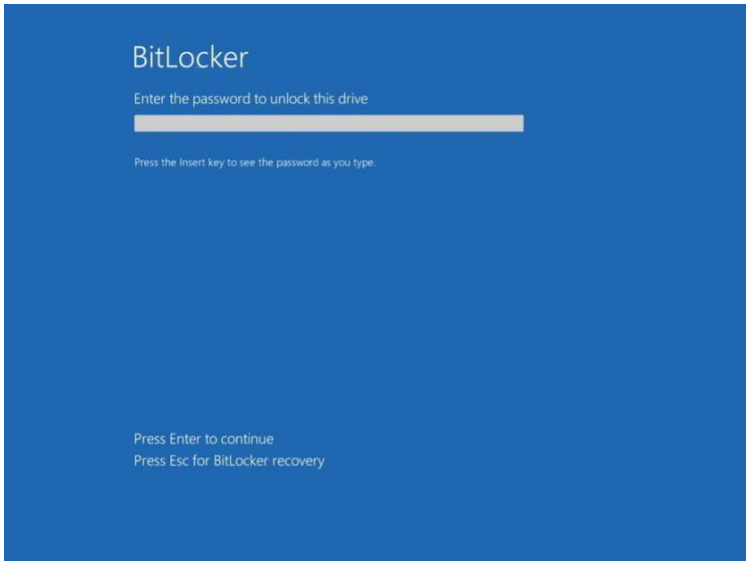
11. Click **Next** to continue.



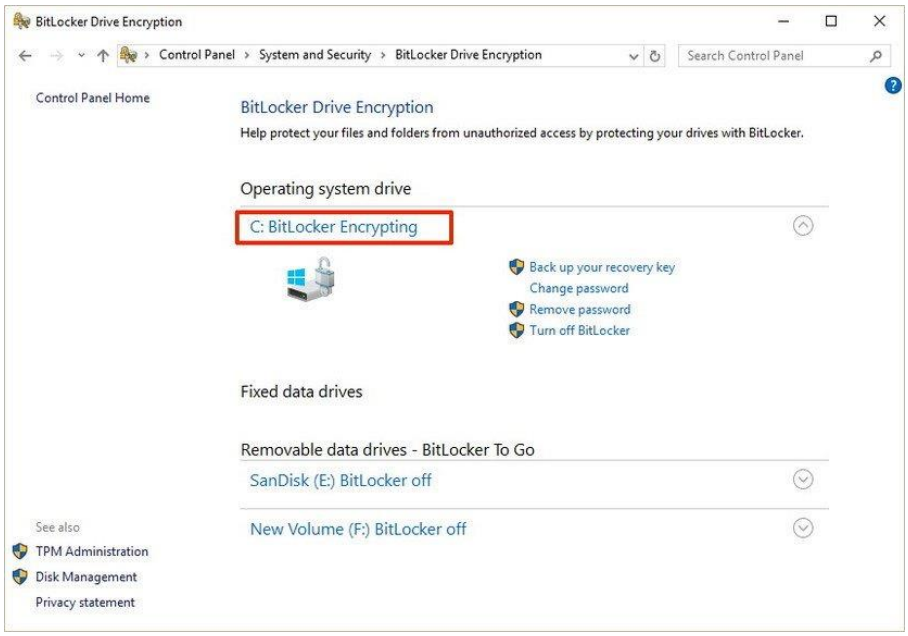
12. Make sure to check the **Run BitLocker system check** option, and click **Continue**.



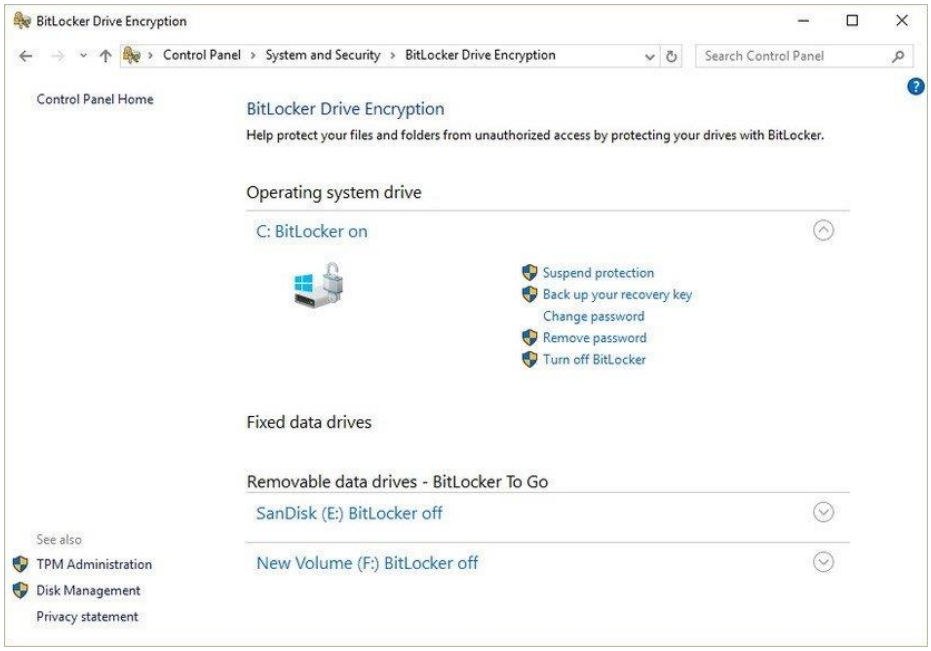
13. Finally, restart your computer to begin the encryption process.
14. On reboot, BitLocker will prompt you to enter your encryption password to unlock the drive. Type the password and press **Enter**.



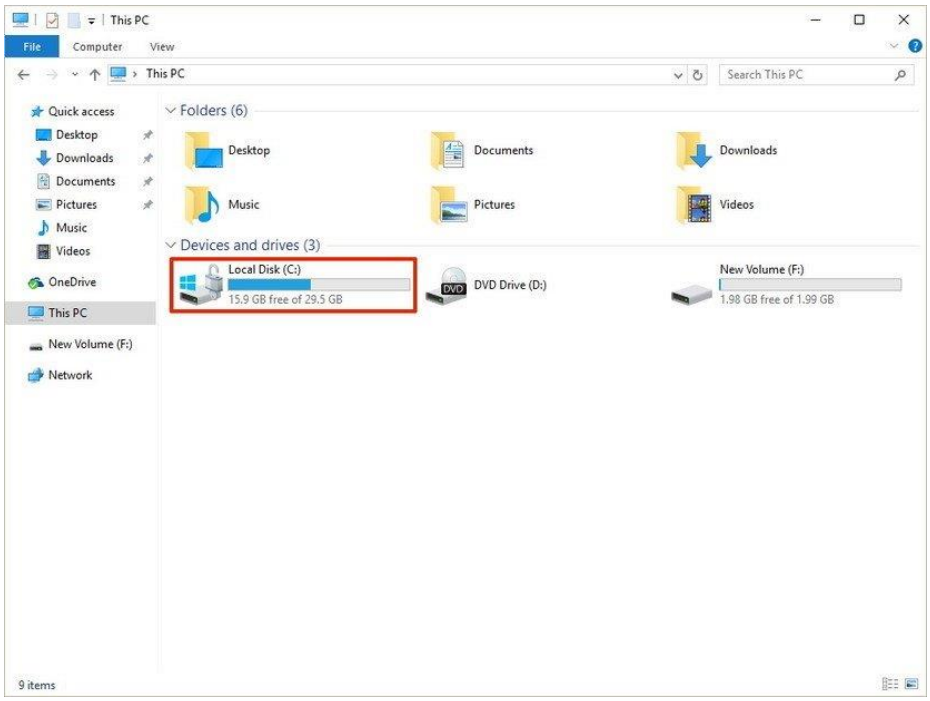
After rebooting, you'll notice that your computer will quickly boot to the Windows 10 desktop. However, if you go to **Control Panel > System and Security > BitLocker Drive Encryption**, you'll see that BitLocker is still encrypting your drive. Depending on the option you selected and the size of the 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.



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



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



BitLocker Drive Encryption options

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

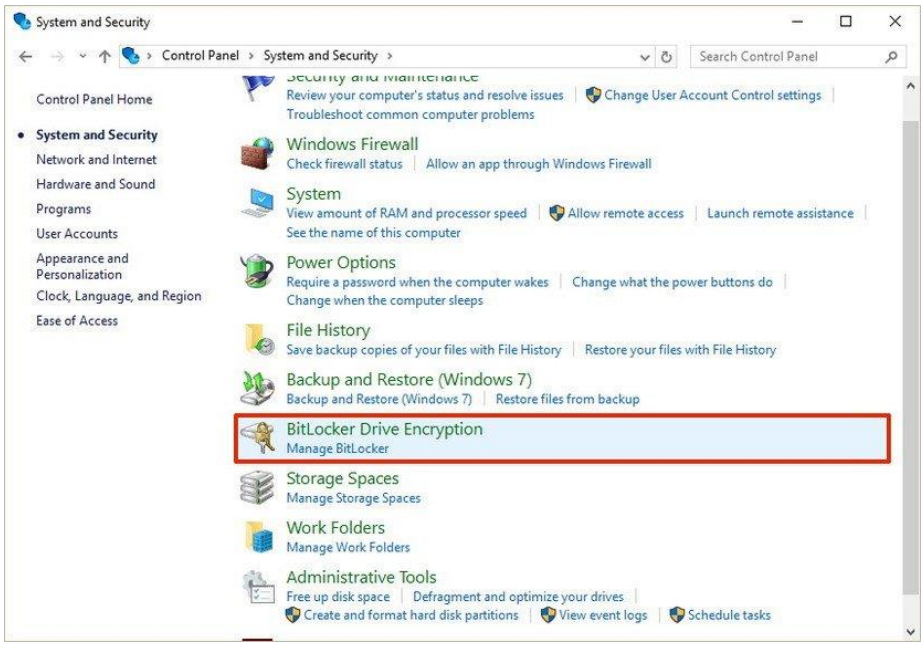
- **Suspend protection:** When you're suspending protection your data won't be protected. Typically, you would use this option when applying a new operating system, firmware, or hardware upgrade. If you don't resume the encryption protection, BitLocker will resume automatically during the next reboot.
- **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

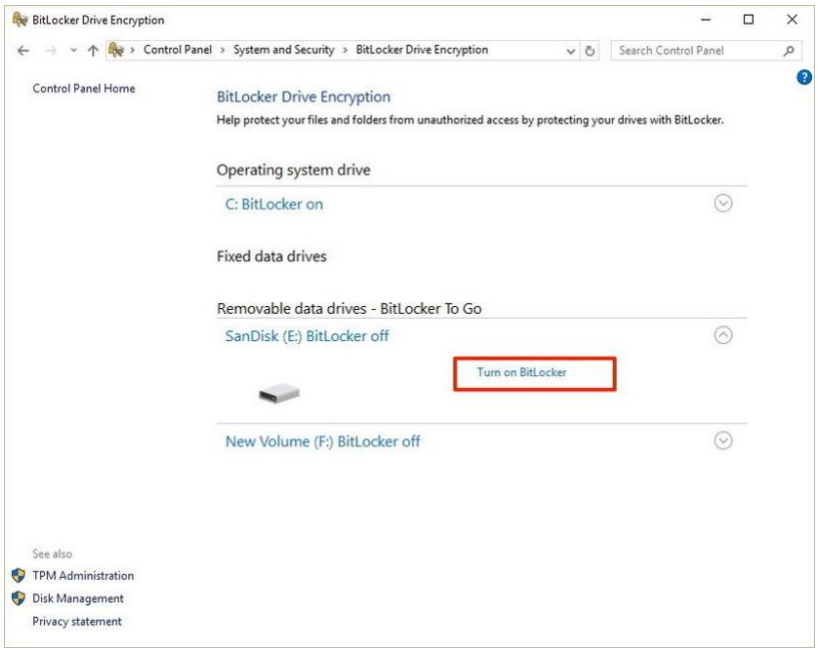
BitLocker is not an encryption feature that you can enable globally on every drive connected to your computer at once. It has two parts: you can use **BitLocker Drive Encryption** to encrypt your sensitive data on the main hard drive of your PC, and then you can use **BitLocker To Go**. This last feature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

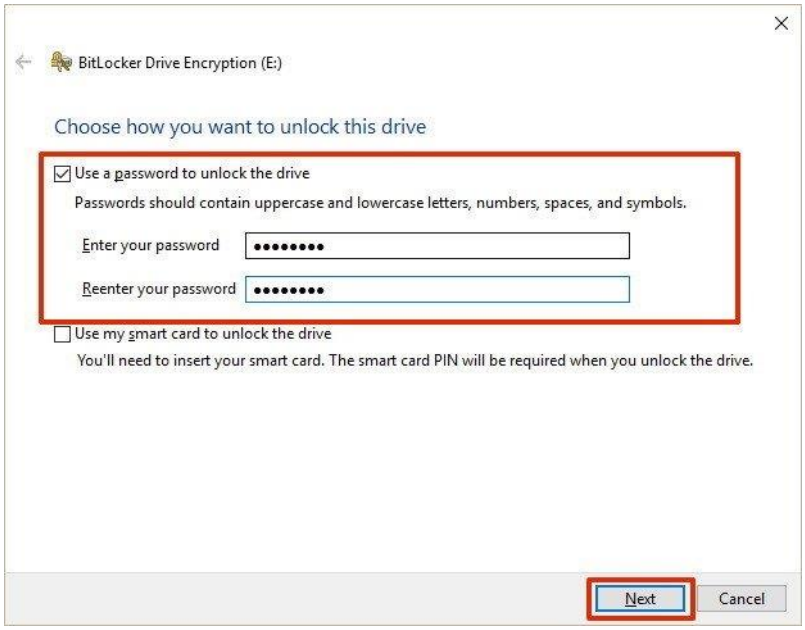
1. Connect the drive you want to use with BitLocker.
2. Use the **Windows key + X** keyboard shortcut to open the Power User menu and select **Control Panel**.
3. Click **System and Security**.
4. Click **BitLocker Drive Encryption**.



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



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.

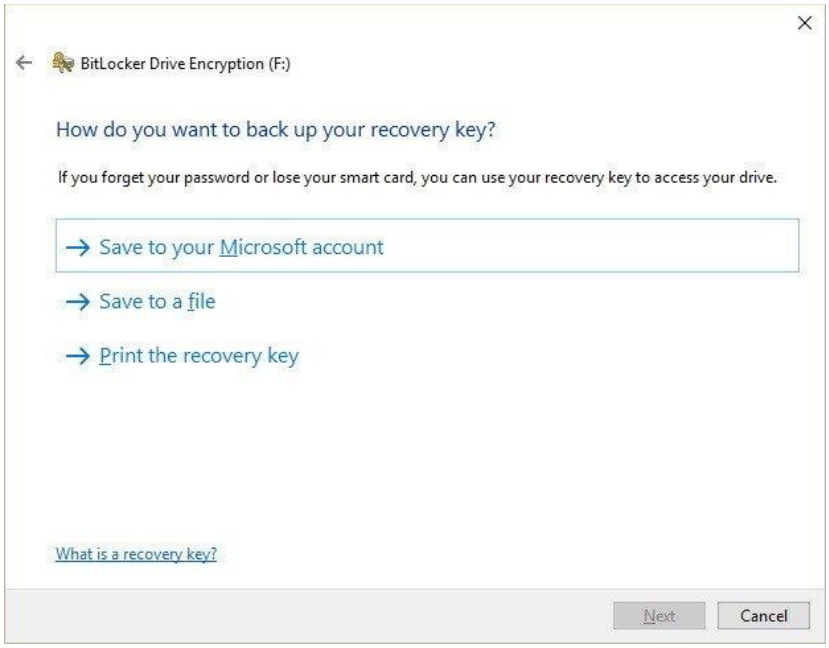


3. You will be given the choices to save a recovery key to regain access to your files in case you forget your password. Options include:

    - Save to your Microsoft account
    - Save to a file

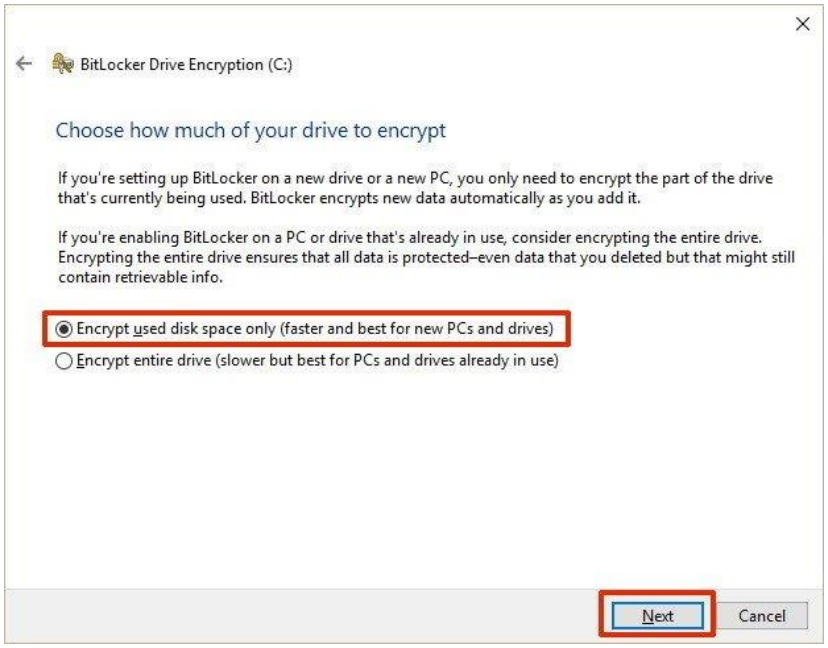
- Print the recovery

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

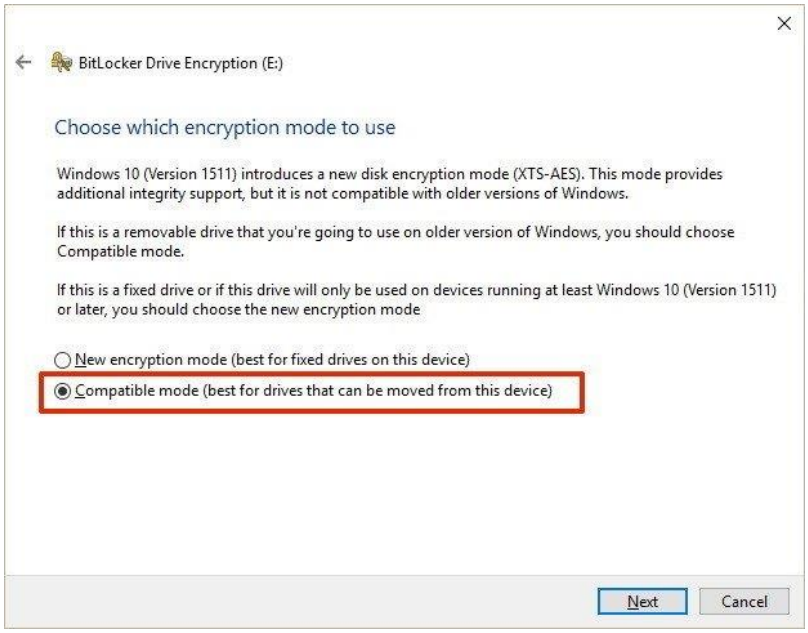


4. Choose the encryption option that best suits your scenario:

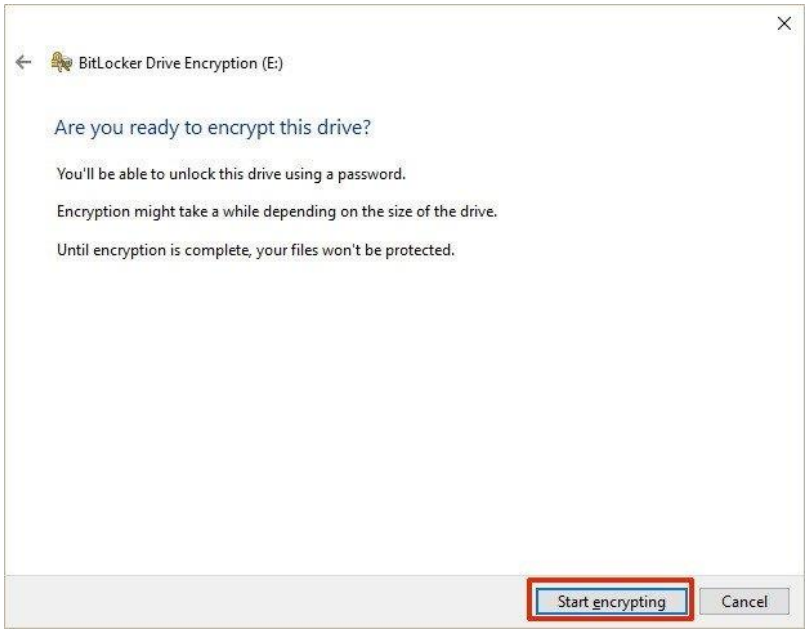
- Encrypt used disk space only (faster and best for new PCs and drives)
- Encrypt entire drive (slower but best for PCs and drives already in use)



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.



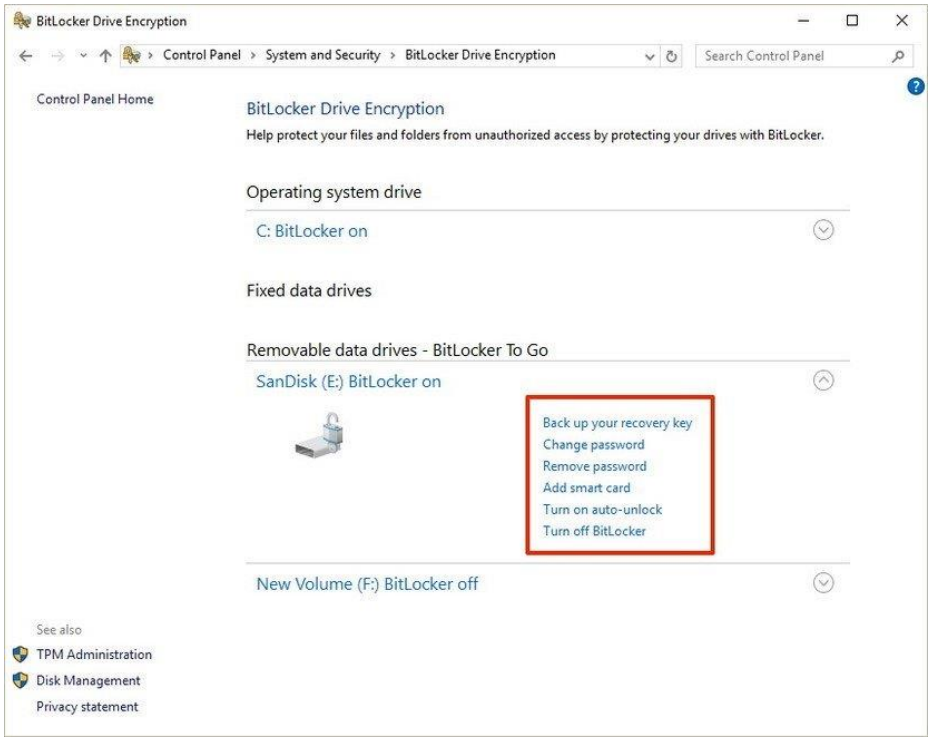
6. Click **Start encrypting** to finish the process.



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:

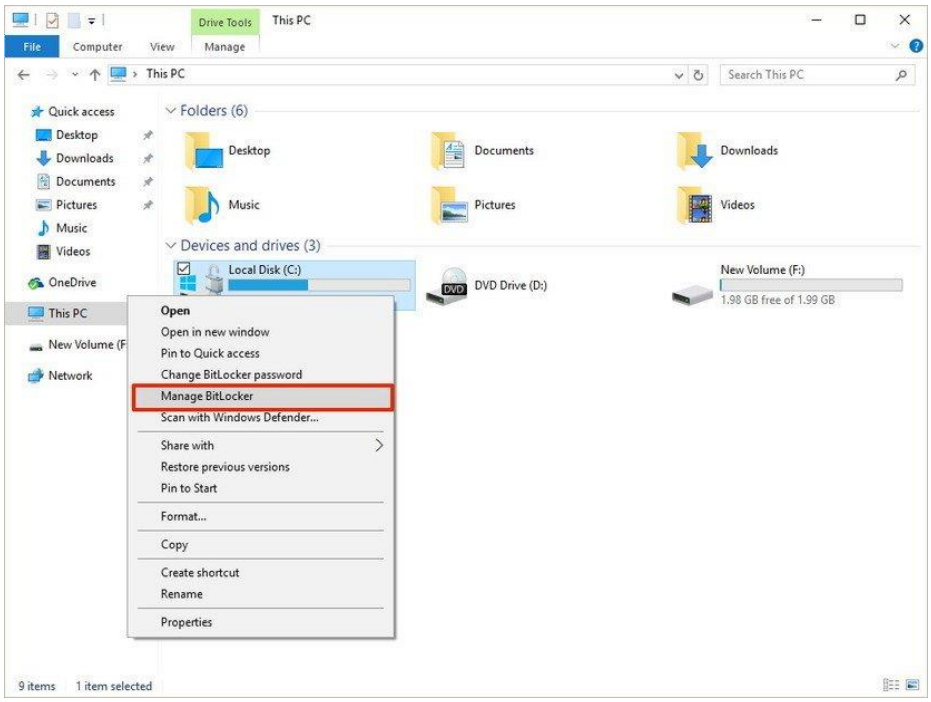
- **Add smart card:** This option will allow you to configure a smart card to unlock the removable drive.
- **Turn on auto-unlock:** Instead of having to type a password every time you re-connect the removable drive, you can enable auto-unlock to access your encrypted data without entering a password.



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**.


Drive Tools
This PC
File
Computer
View
Manage
This PC
Search This PC
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
New Volume (F
Network
Folders (6)
Desktop
Documents
Downloads
Music
Pictures
Videos
Devices and drives (3)
Local Disk (C:)
DVD Drive (D:)
New Volume (F:)
1.98 GB free of 1.99 GB
Open
Open in new window
Pin to Quick access
Change BitLocker password
Manage BitLocker
Scan with Windows Defender...
Share with
Restore previous versions
Pin to Start
Format...
Copy
Create shortcut
Rename
Properties
9 items
1 item selected