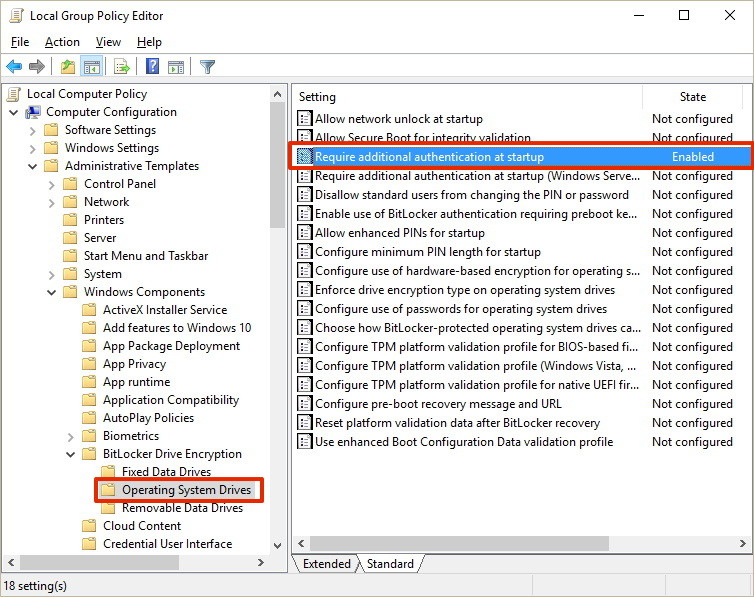
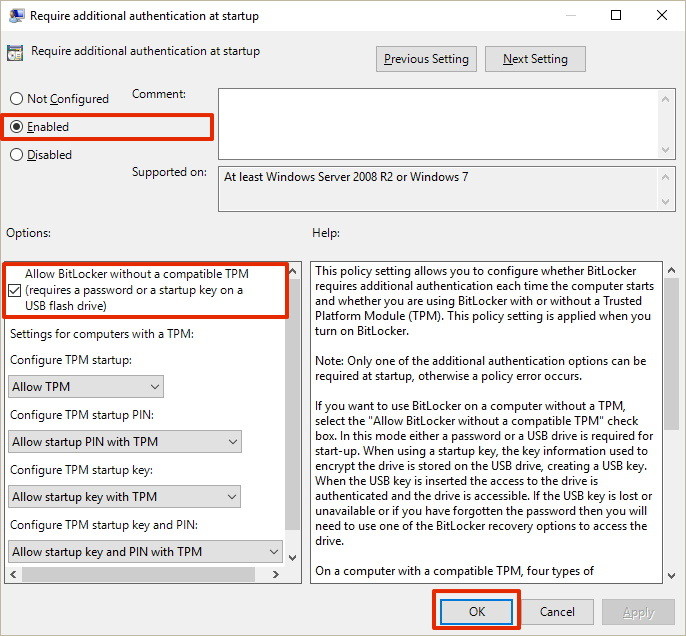
1. Use the **Windows key + R** keyboard shortcut to open the Run command, type **gpedit.msc**, and click **OK**.
2. Under Computer Configuration, expand **Administrative Templates**.
3. Expand **Windows Components**.
4. Expand **BitLocker Drive Encryption** and **Operating System Drives**.
5. On the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

[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2016/06/additional-authentication-bitlocker.jpg?itok=zSxfcC7o)

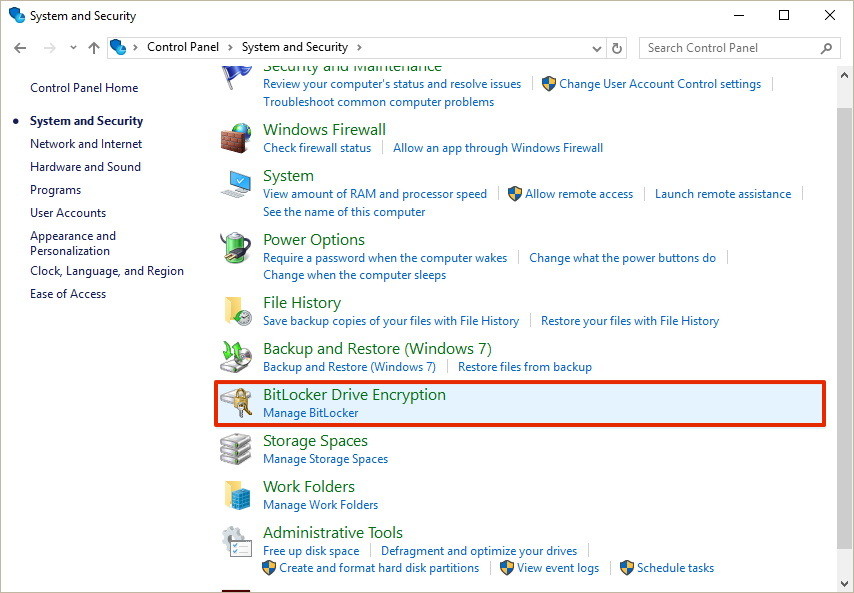
1. Select **Enabled**.
2. Make sure to check the **"Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)"** option.
3. Click **OK** to complete this process.

[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2016/06/gpedit-authentication-startup-bitlocker.jpg?itok=GOqBlFT1)

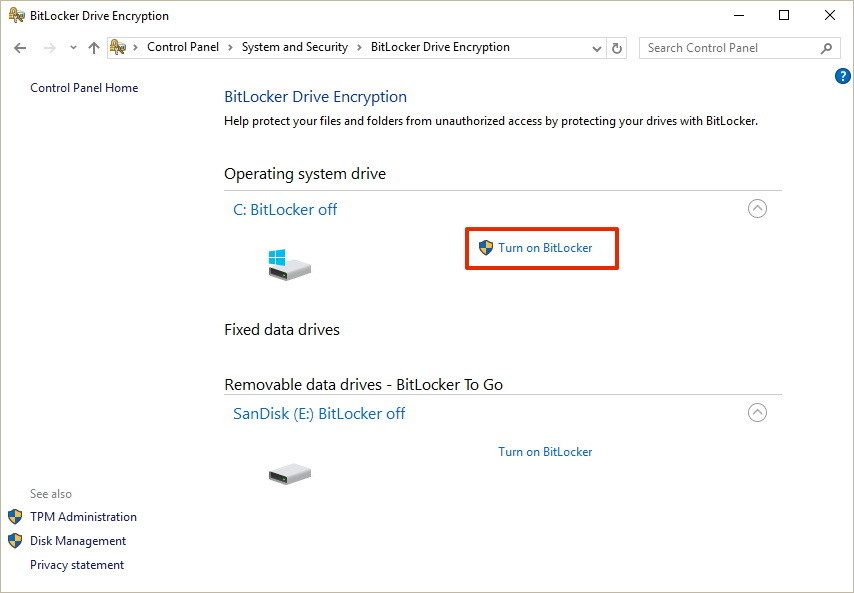
How to turn on BitLocker on the Operating system drive

Once you made sure BitLocker can be properly enabled on your computer, follow these steps:

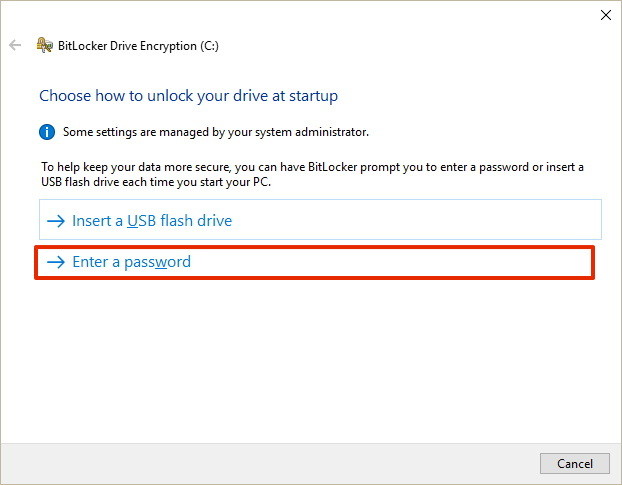
1. Use the **Windows key + X** keyboard shortcut to open the Power User menu and select **Control Panel**.
2. Click **System and Security**.
3. Click **BitLocker Drive Encryption**.

[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2016/06/bitlocker-drive-encryption-windows-10.jpg?itok=c8D3w3Ft)

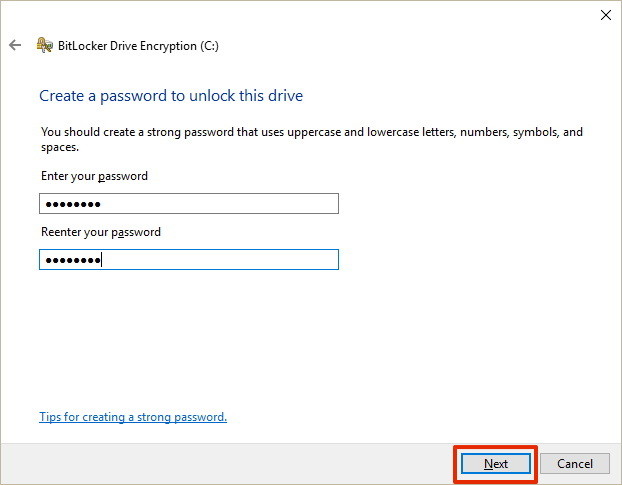
1. Under BitLocker Drive Encryption, click **Turn on BitLocker**.

[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2016/06/turnon-bitlocker-windows-10.jpg?itok=1fflD7sw)

1. 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.

[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2016/06/choose-unlock-option.jpg?itok=nnYSEW2a)

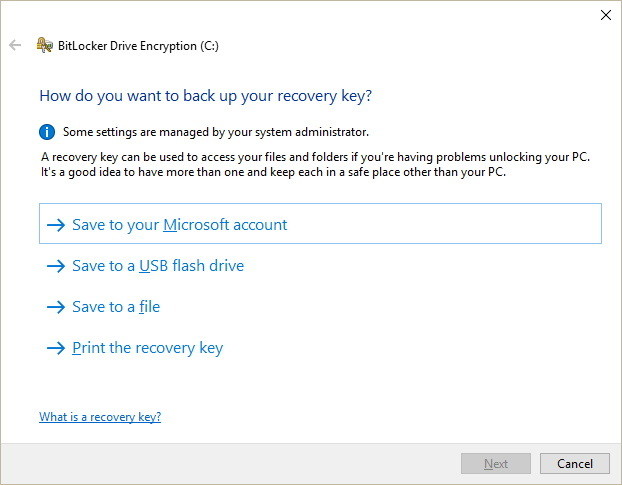
1. Enter a password that you'll use every time you boot Windows 10 to unlock the drive, and click **Next** to continue. (Make sure to create a strong password mixing uppercase, lowercase, numbers, and symbols.)

[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2016/06/create-bitlocker-password.jpg?itok=sBLucivN)

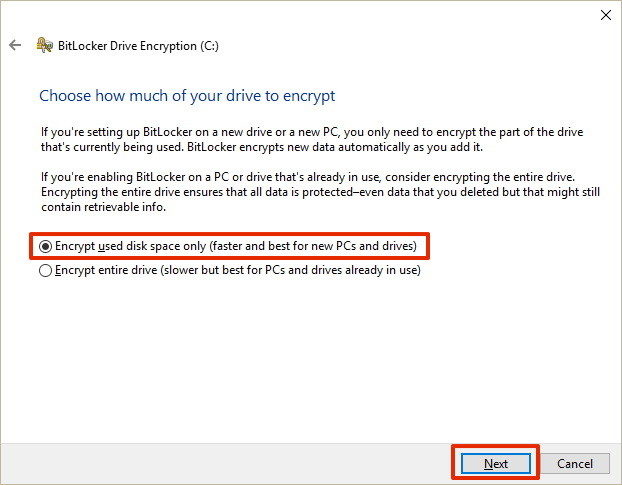
1. You will be given the choices to save a recovery key to regain access to your files in case you forget your password. Options include:
   * Save to your Microsoft account
   * Save to a USB flash drive
   * Save to a file
   * Print the recovery

Select the option that is most convenient for you, and save the recovery key in a safe place.

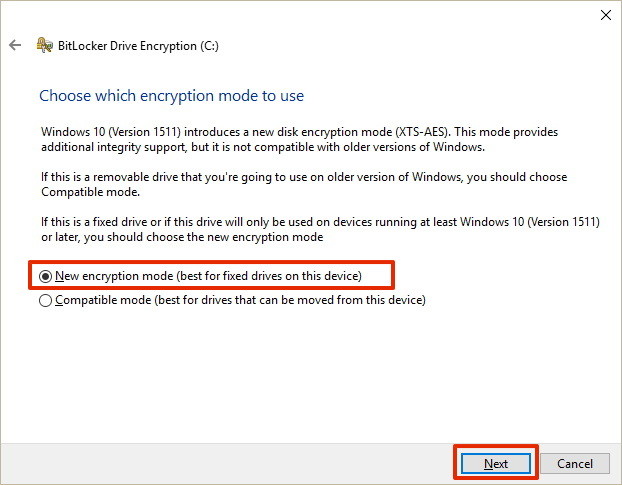
1. Click **Next** to continue.

[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2016/06/bitlocker-recovery-key-options.jpg?itok=-SXHpWcp)

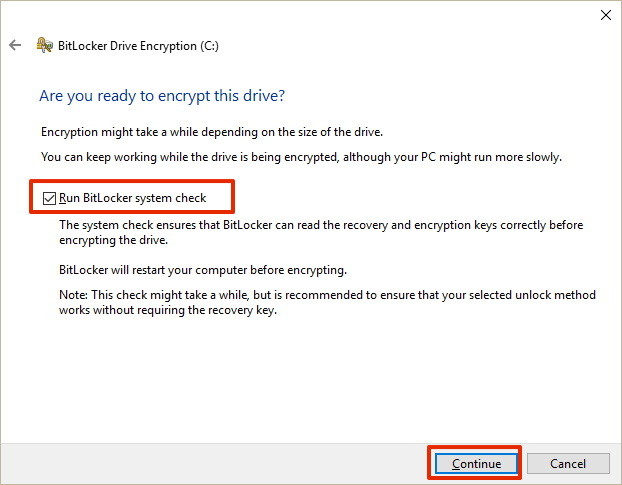
1. Select the encryption option that best suits your scenario:
   * Encrypt used disk space only (faster and best for new PCs and drives)
   * Encrypt entire drive (slower but best for PCs and drives already in use)

[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2016/06/how-encrypt-drive-bitlocker.jpg?itok=FChAlG8s)

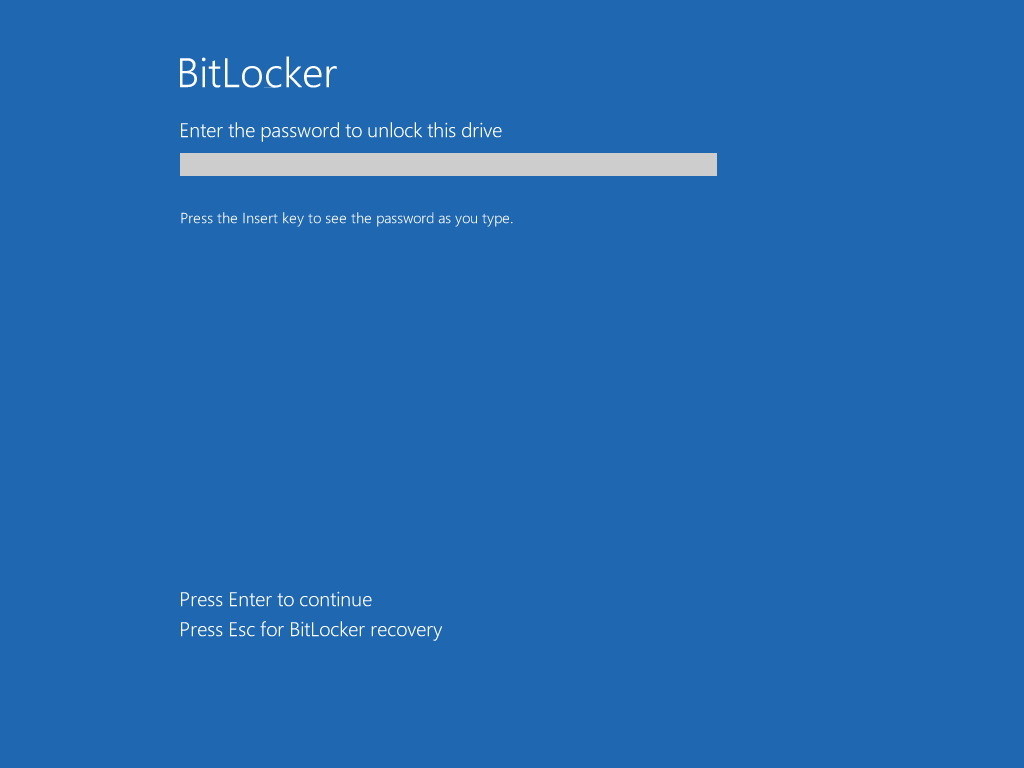
1. Choose between the two encryption options:
   * New encryption mode (best for fixed drives on this device)
   * Compatible mode (best for drives that can be moved from this device)
2. Click **Next** to continue.

[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2016/06/encryption-mode-bitlocker.jpg?itok=Ik2yR-VL)

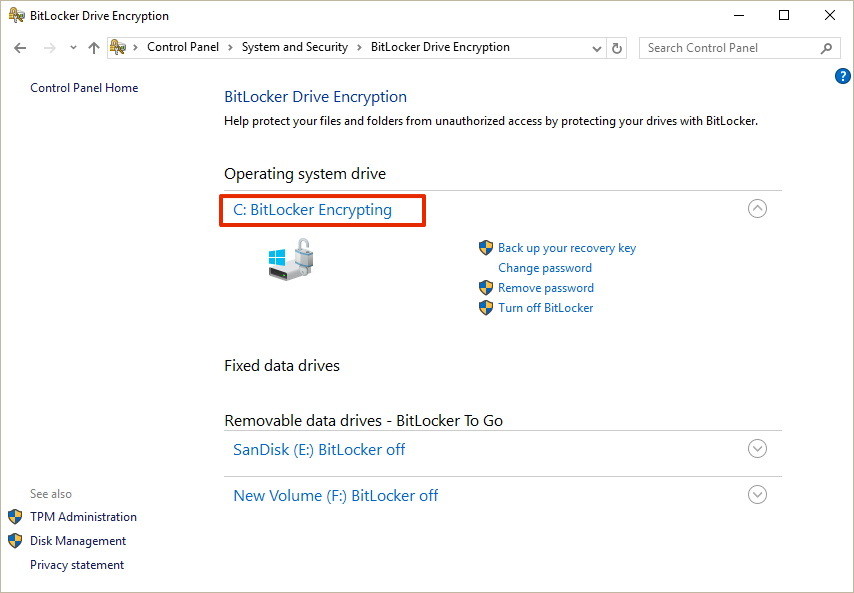
1. Make sure to check the **Run BitLocker system check** option, and click **Continue**.

[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2016/06/encrypt-drive-bitlocker-windows-10.jpg?itok=DKIZ_XjF)

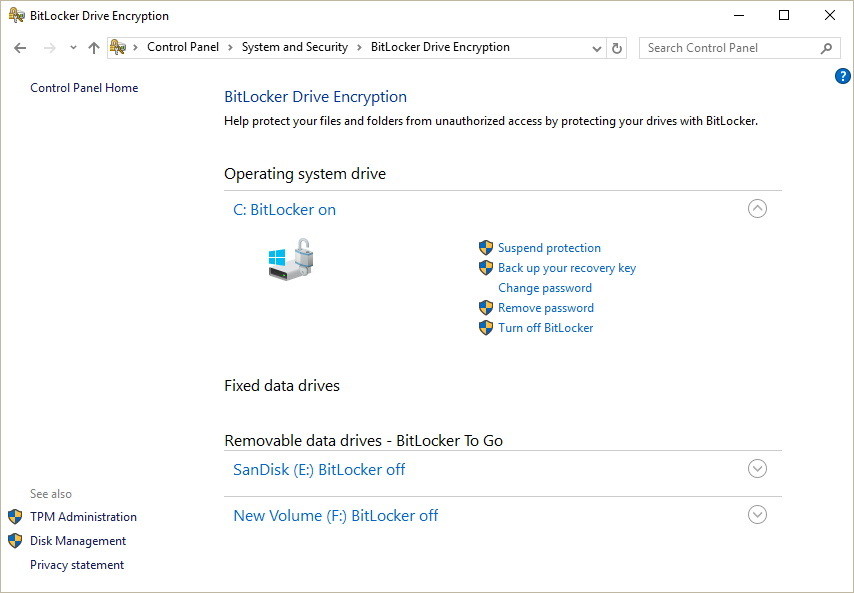
1. Finally, restart your computer to begin the encryption process.
2. On reboot, BitLocker will prompt you to enter your encryption password to unlock the drive. Type the password and press **Enter**.

[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2016/06/bitlocker-password-startup.jpg?itok=0dbSOR_x)

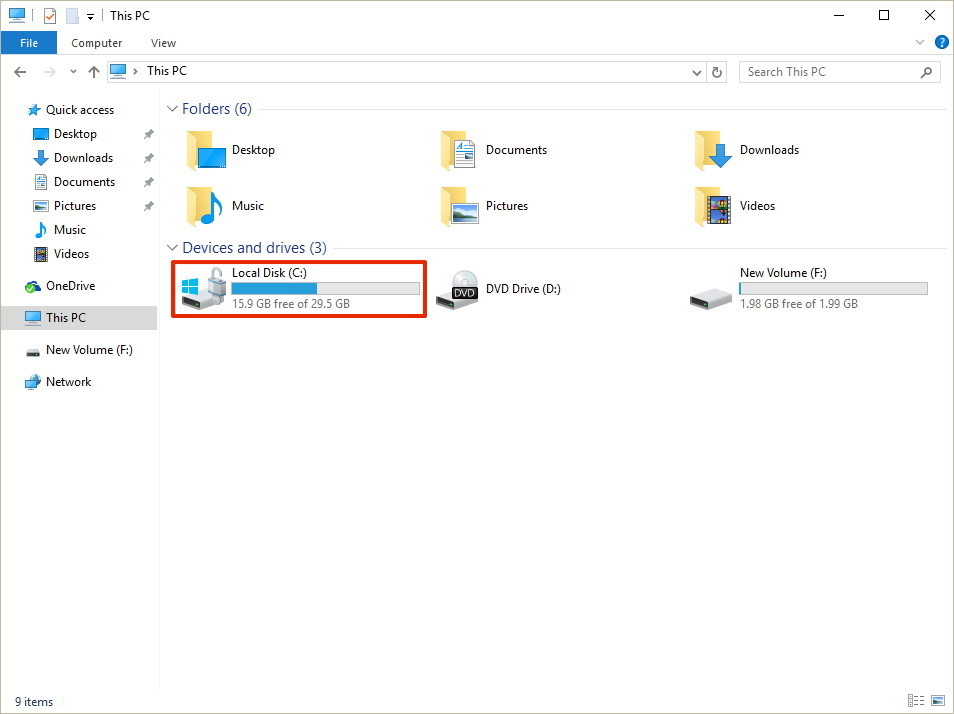
After rebooting, you'll notice that your computer will quickly boot to the Windows 10 desktop. However, if you go to **Control Panel > System and Security > BitLocker Drive Encryption**, you'll see that BitLocker is still encrypting your drive. Depending on the option you selected and the size of the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

[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2016/06/bitlocker-encrypting-windows-10.jpg?itok=uB7VjuIA)

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

[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2016/06/bitlocker-on-windows-10-options.jpg?itok=QHeSg-vk)

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

[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2016/06/drive-bitlocker-enabled-icon-windows-10.jpg?itok=RCWzDAiM)

BitLocker Drive Encryption options

When BitLocker is enabled on your main hard drive, you'll get 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.