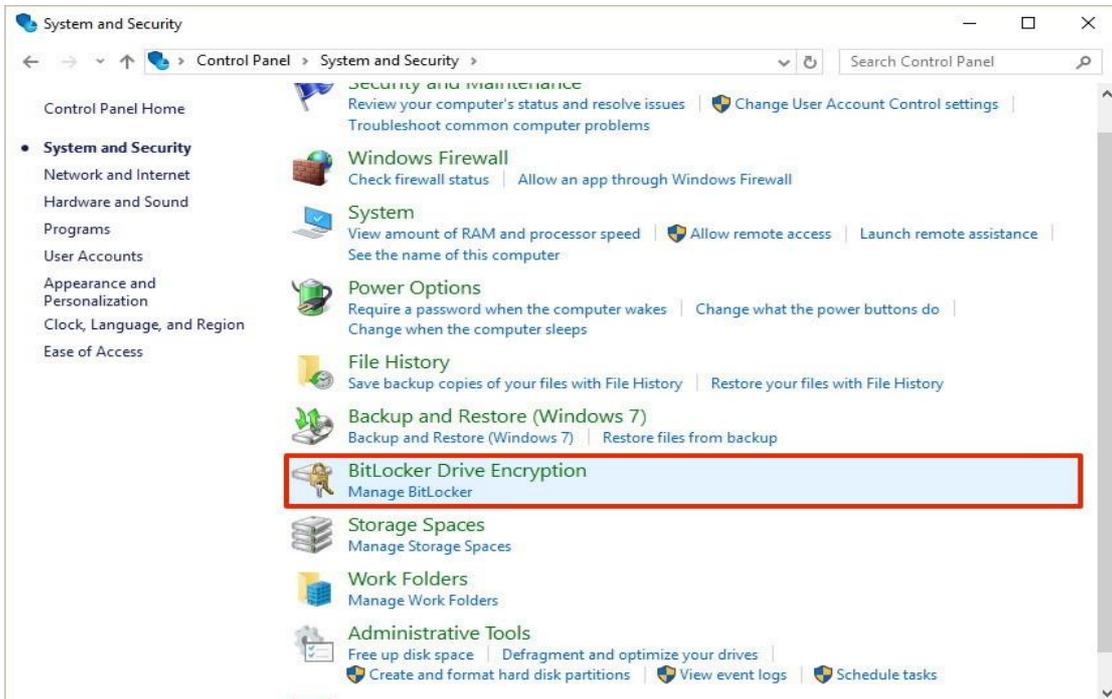


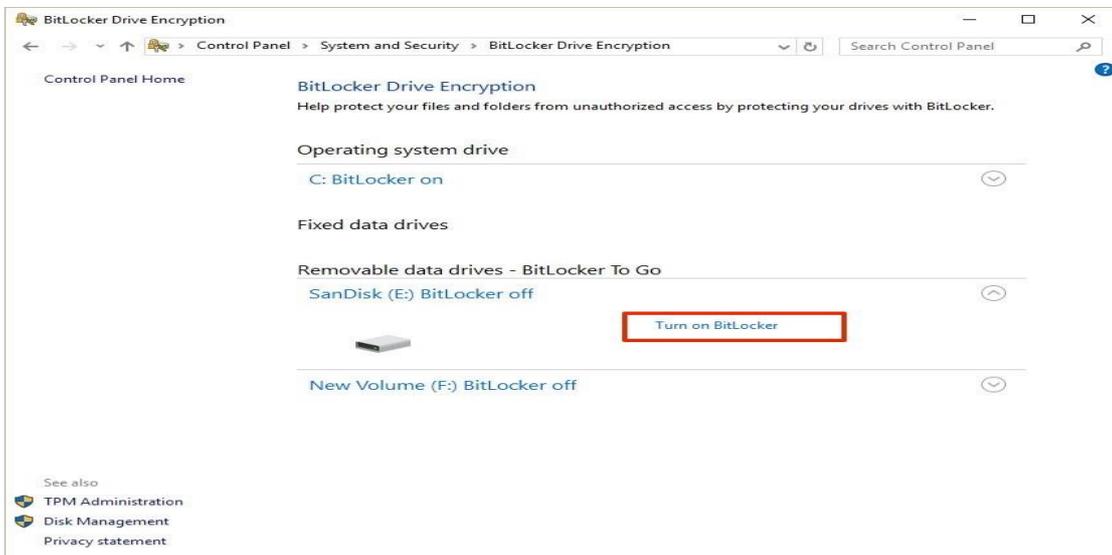


To turn on BitLocker To Go on a removable drive do the following:

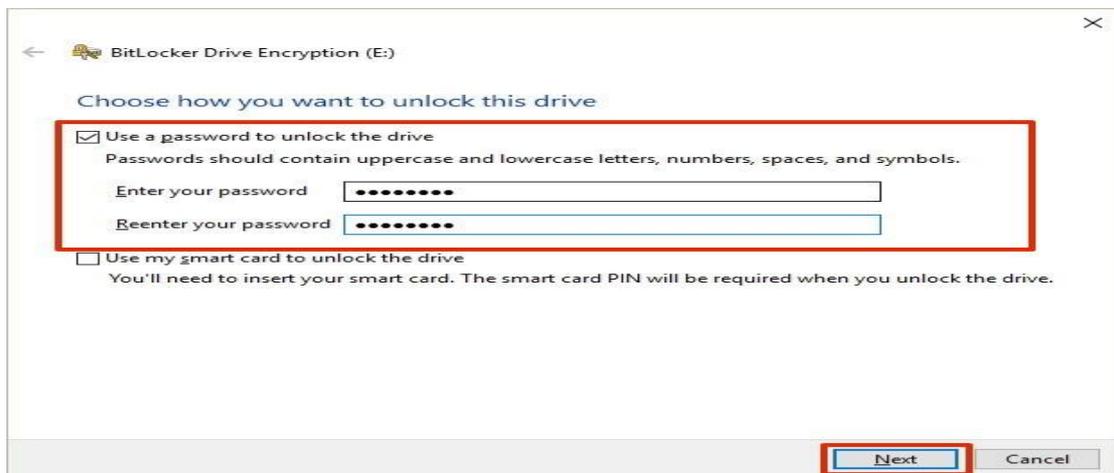
1. Connect the drive you want to use with BitLocker.
2. Use the **Windows key + X** keyboard shortcut to open the Power User menu and select **Control Panel**.
3. Click **System and Security**.
4. Click **BitLocker Drive Encryption**.



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



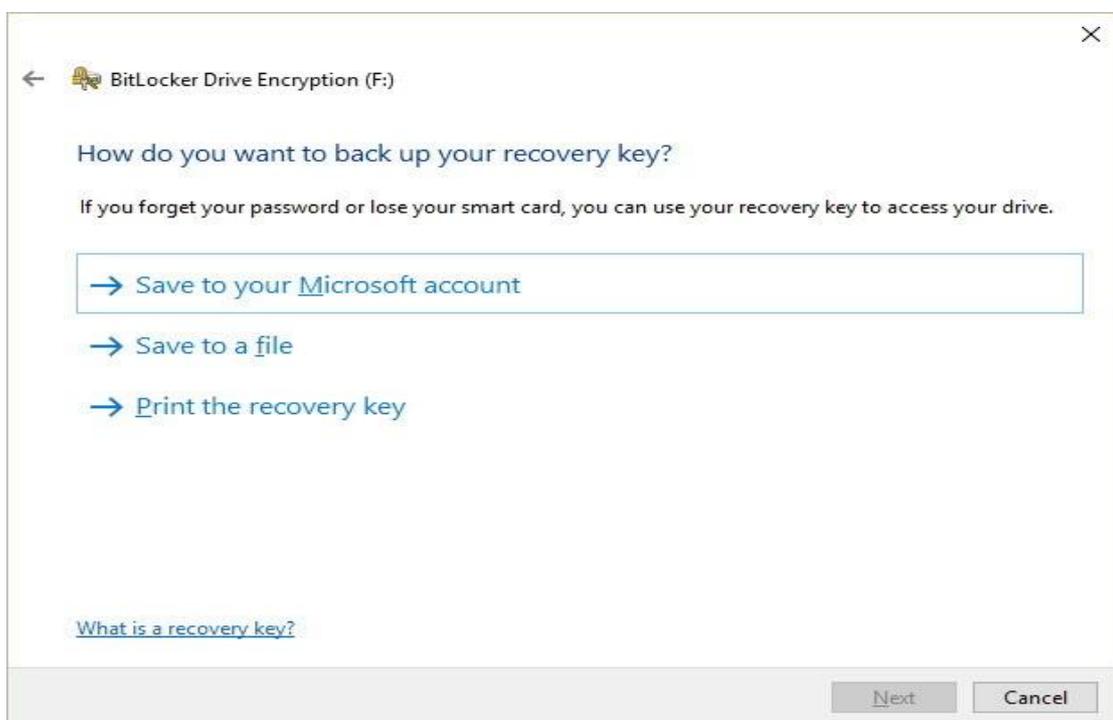
7. Check the **Use a password to unlock the drive option**, and create a password to unlock the drive. (Make sure to create a strong password mixing uppercase, lowercase, numbers, and symbols.)
8. Click **Next** to continue.



The screenshot shows the BitLocker Drive Encryption (E:) dialog box. The title bar reads "BitLocker Drive Encryption (E:)". The main heading is "Choose how you want to unlock this drive". There are two radio button options. The first option, "Use a password to unlock the drive", is selected and highlighted with a red box. Below it, a note states "Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols." There are two password input fields: "Enter your password" and "Reenter your password", both containing seven dots. The second option, "Use my smart card to unlock the drive", is unselected. Below it, a note states "You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive." At the bottom right, there are "Next" and "Cancel" buttons, with the "Next" button highlighted by a red box.

9. 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

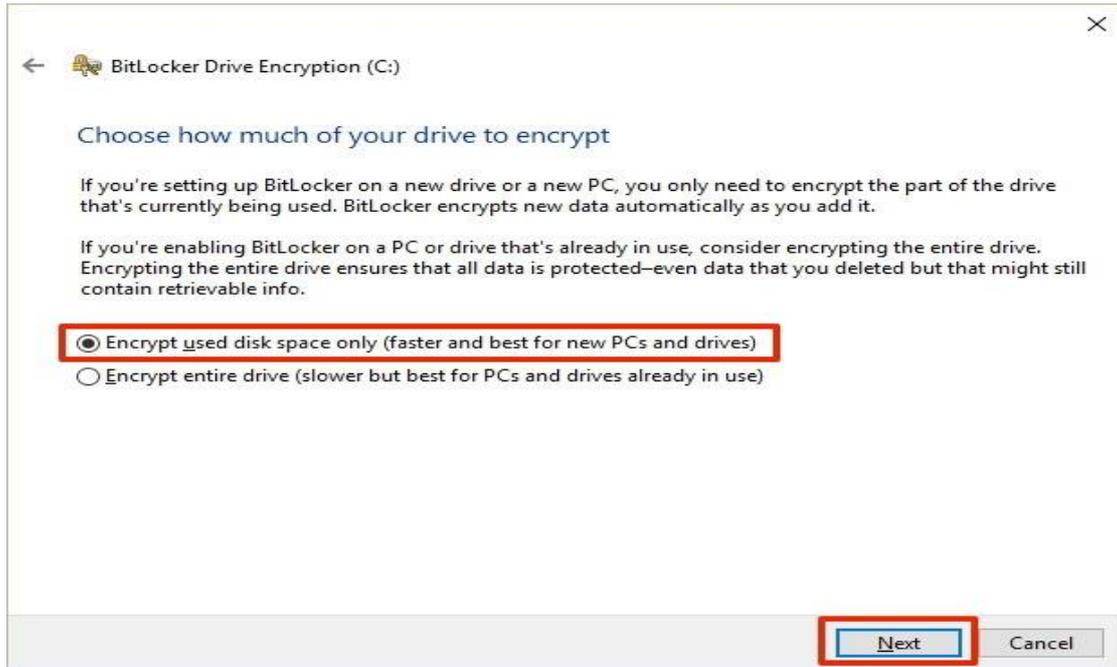
Select the option that is most convenient for you, and click **Next**.



The screenshot shows the BitLocker Drive Encryption (F:) dialog box. The title bar reads "BitLocker Drive Encryption (F:)". The main heading is "How do you want to back up your recovery key?". Below it, a note states "If you forget your password or lose your smart card, you can use your recovery key to access your drive." There are three radio button options, each with a blue arrow icon to its left. The first option, "Save to your Microsoft account", is selected and highlighted with a blue box. The other two options, "Save to a file" and "Print the recovery key", are unselected. At the bottom left, there is a link "What is a recovery key?". At the bottom right, there are "Next" and "Cancel" buttons.

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

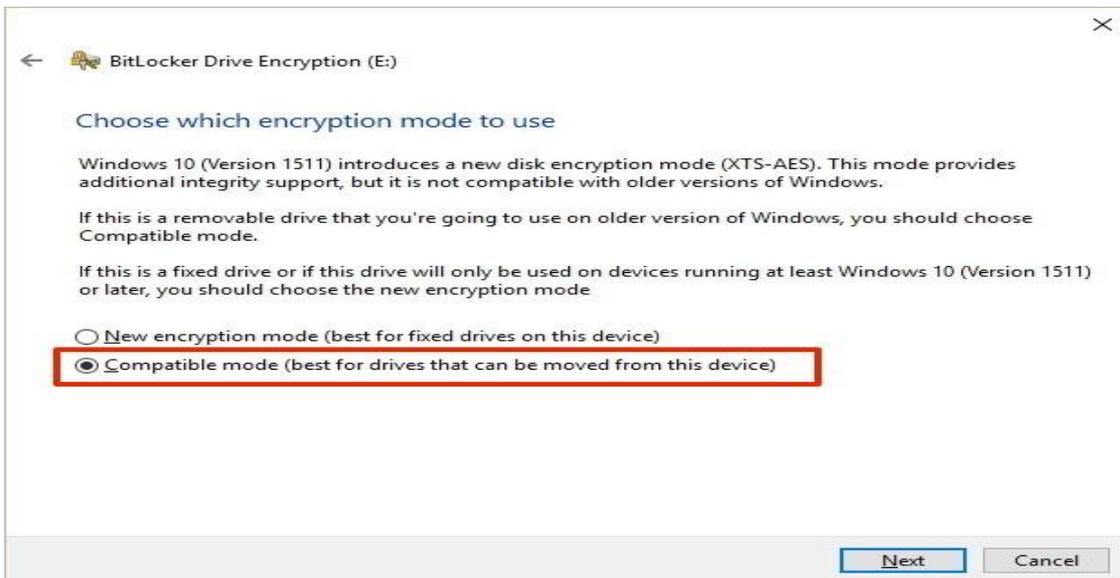
- Encrypt used disk space only (faster and best for new PCs and drives)
- Encrypt entire drive (slower but best for PCs and drives already in use)



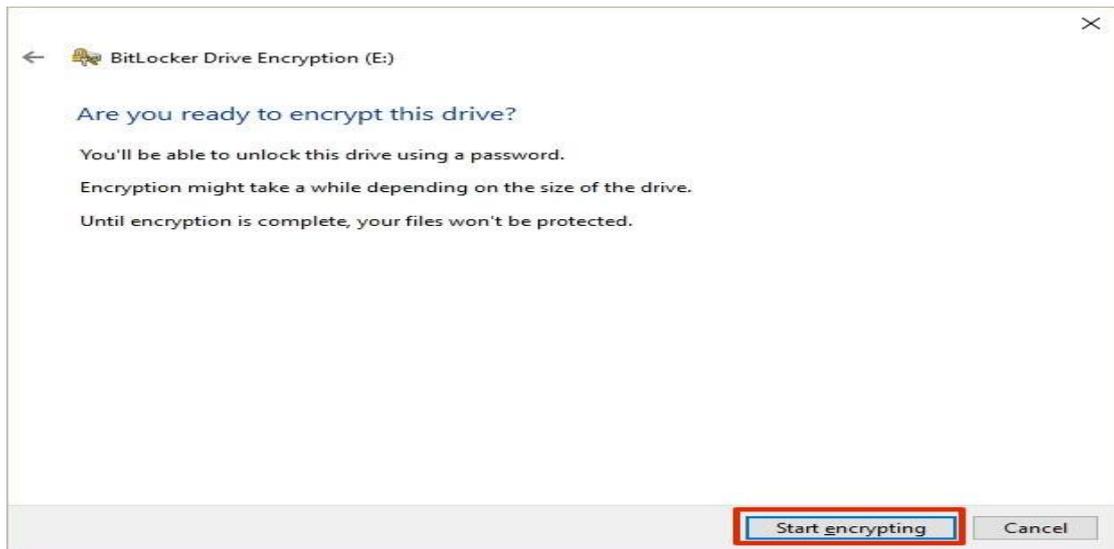
11. Select between the two encryption options:

- New encryption mode (best for fixed drives on this device)
- Compatible mode (best for drives that can be moved from this device)

In this step is recommended that you select the "Compatible mode," as it will ensure you can unlock the drive if you move it to another computer running a previous version of the operating system.



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



When encrypting a storage try to start with an empty removable media, as it'll speed up the process, then new data will encrypt automatically.