

BitLocker Encryption for USB Drives

BitLocker is a security feature. The purpose of BitLocker is to encrypt your data. This is extremely necessary for any data that is not to be shared with other persons. This will prevent anyone from being able to access your files. In order to have access to your files, you will need to provide a secure password. This password should be unique only to you. More information is provided below on how to make a unique password in step 2. During this process, step 3 offers the option to save a recovery key. The recovery key is 48 characters long and consist of numbers and letters. This key will be saved to Active Directory and allow the IS Department to access your USB/External drive should you forget your password. To get started I would recommend encrypting the USB/External drive BEFORE adding any files. Once the drive is encrypted and you enter your password it will function as any other USB/External drive. So you may add, edit, or delete your files as you normally would. If you have any trouble following this guide or have any questions please do not hesitate to contact the IS department.

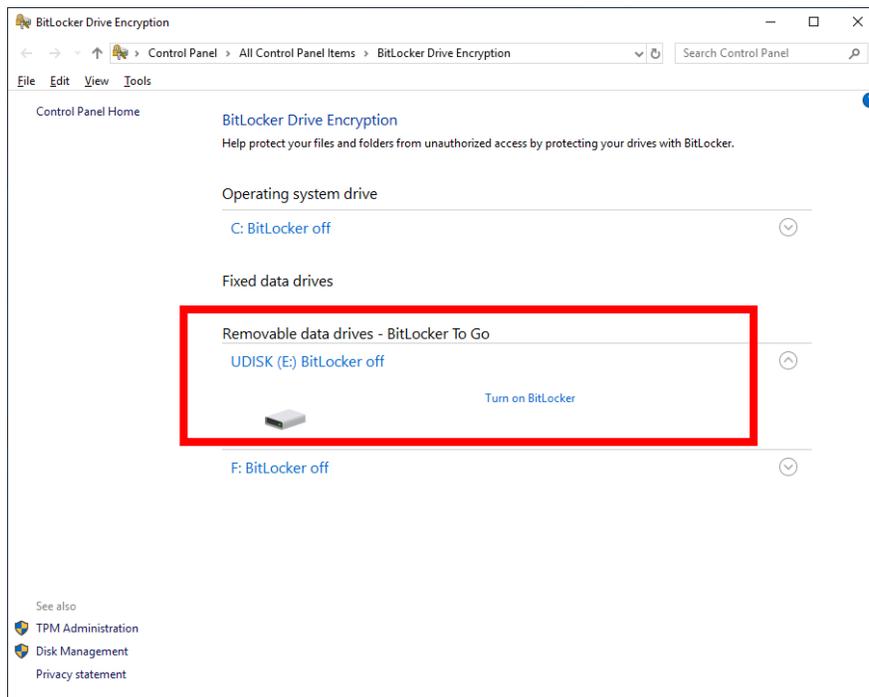
You will need a USB or External drive in order to successfully complete this process.

Multiple ways to navigate to BitLocker:

1. Control Panel → System & Security → BitLocker Drive Encryption
2. Search bar → type in "BitLocker" → Manage BitLocker

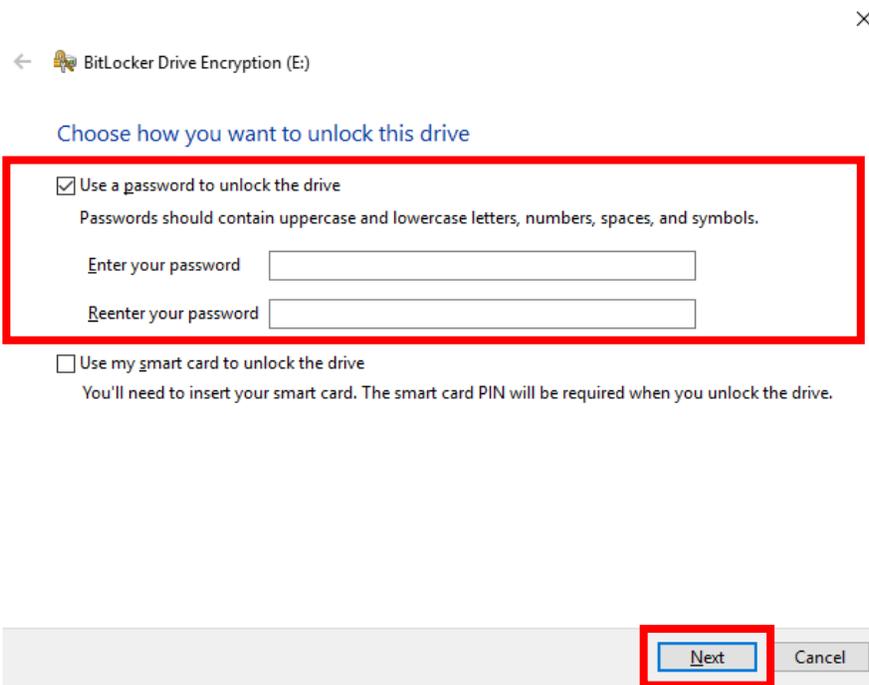
Steps to encrypt your USB drive:

Step 1:



Click "Turn on BitLocker"

Step 2:

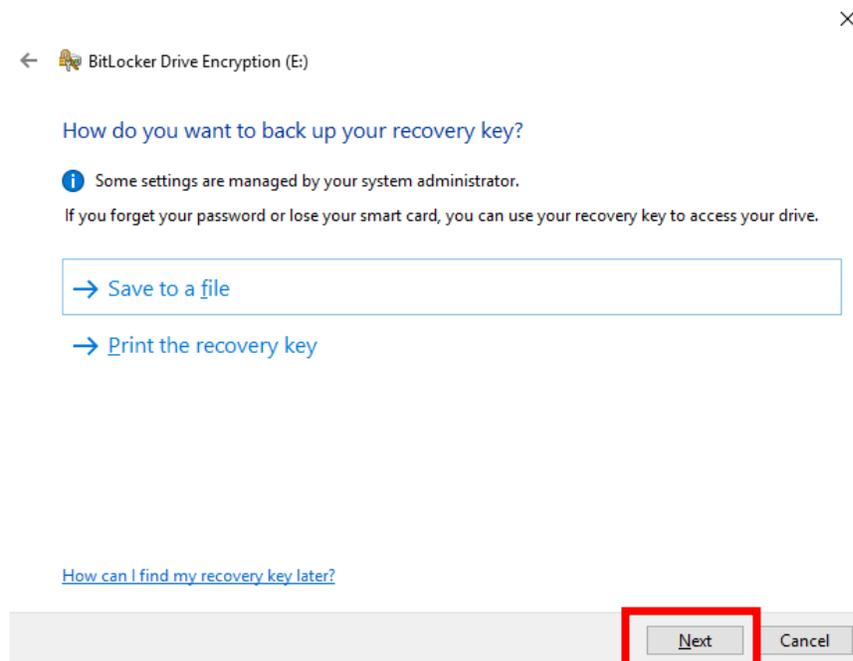


Check the "Use a password to unlock the drive" and enter your password.

The Do's and Don'ts for creating a password.

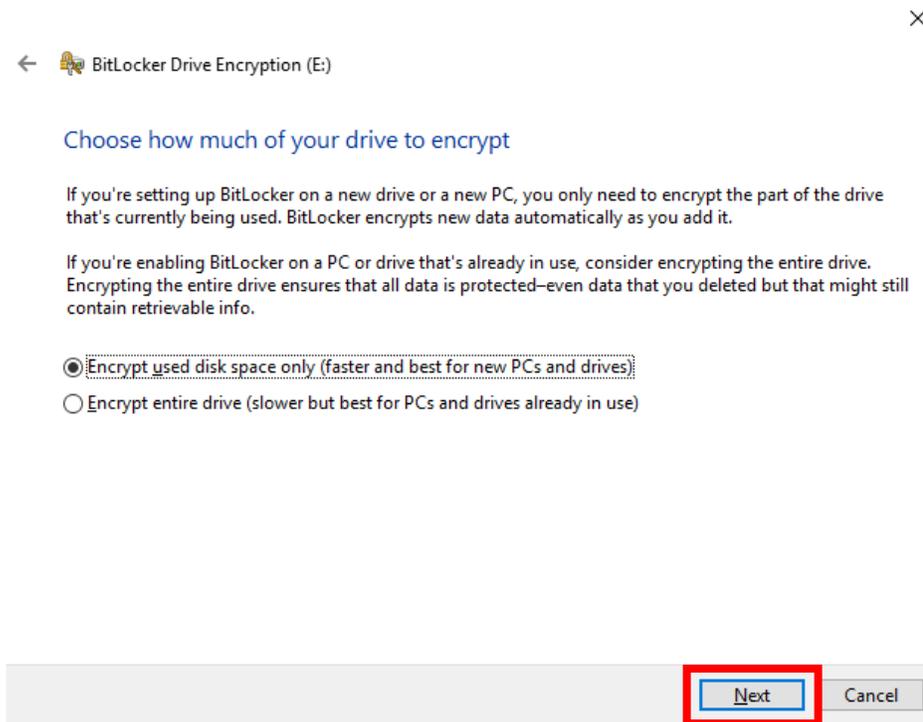
Do	Don't
Do make the new password significantly different from previous passwords.	Don't use the same password for different accounts.
Do use a sentence or phrase converted into a string of initials, numbers, and symbols.	Don't use a single word for your password like "password," "monkey," or "sunshine."
Do make your password hard to guess even if someone knows a lot about you (avoid names and birthdays of your family or your favorite band).	Don't use common passwords like "password," "iloveyou," or "12345678."

Step 3:



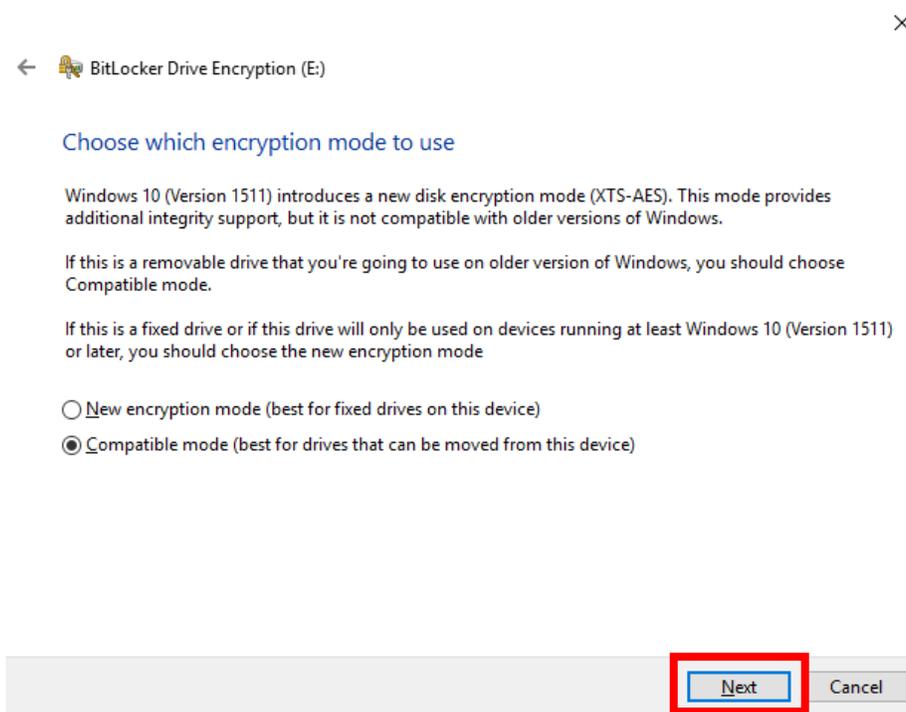
This is a great option to use for personal use but for work just select click "Next".

Step 4:



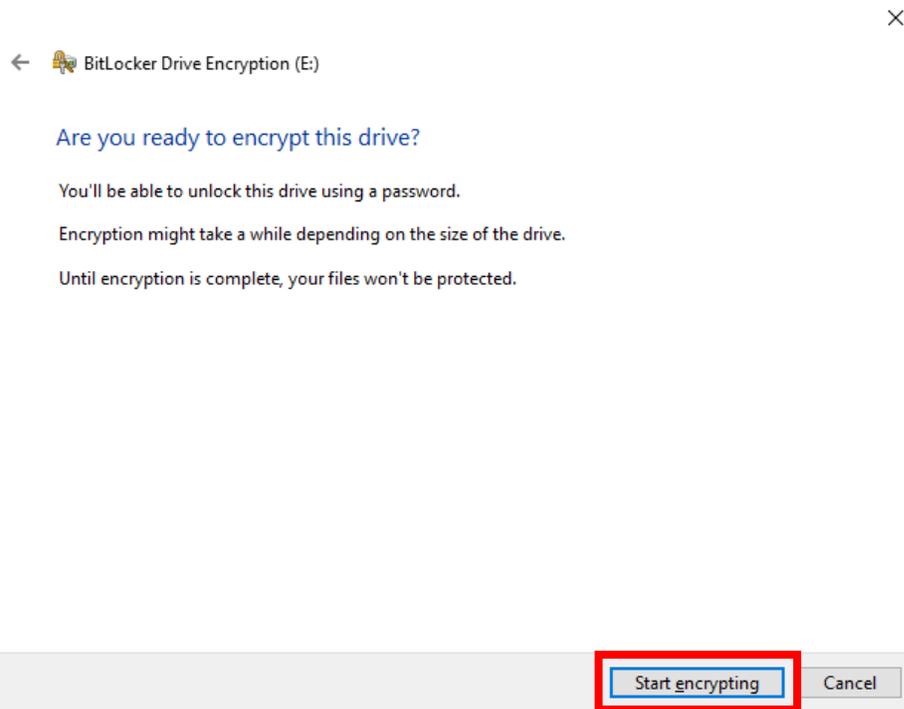
Keep the default selection and select "Next".

Step 5:



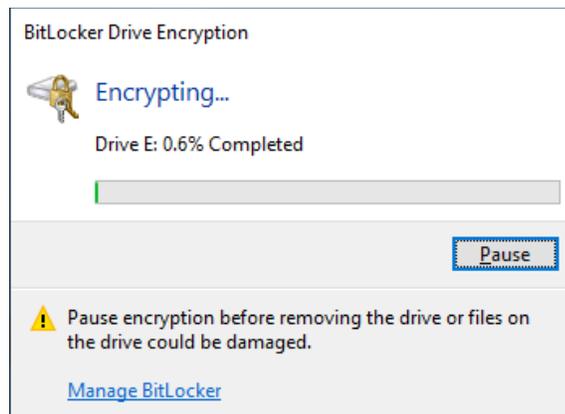
Keep the default selection and select "Next".

Step 6:



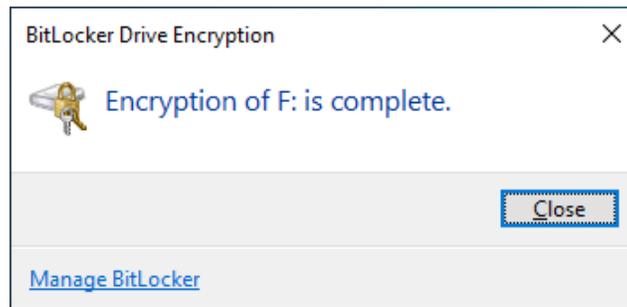
Click "Start encrypting".

Step 7:



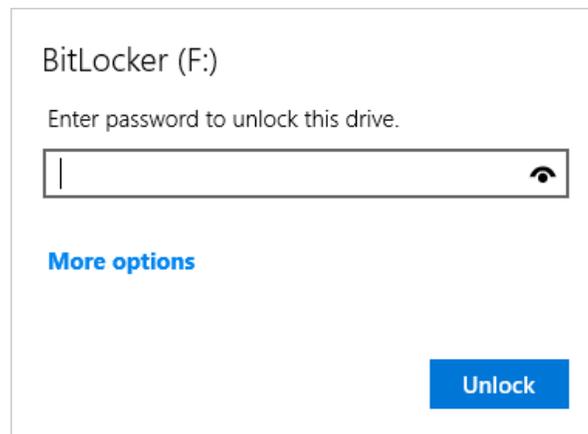
This screen just let's you know the status of the encryption.

Step 8:



Once the USB drive is connected to the computer.

Navigate to the USB drive and click on it. You will be prompted to enter the password you created during setup. You will have to do this every time you connect this USB to any computer.



Once the password is entered successfully, you will have access to your files.