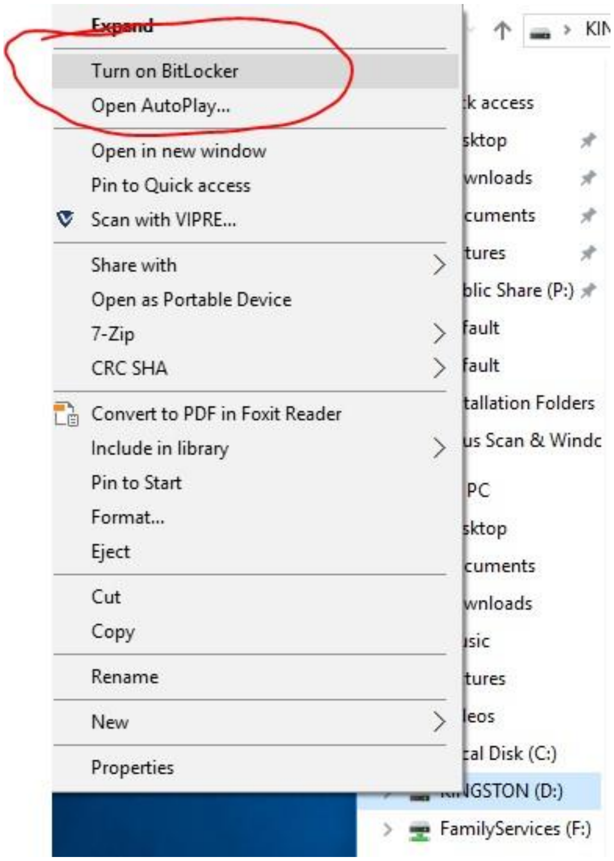
How to Encrypt a USB using BitLocker

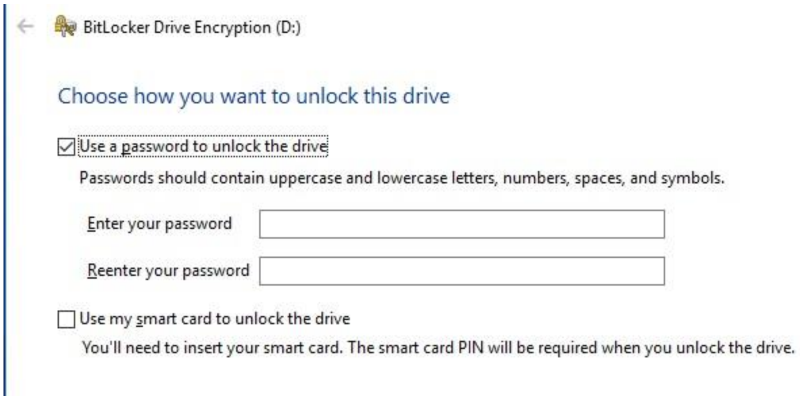
1. Insert USB

2. Open **File Explorer** and **Right Click** the USB and then select "**Turn on Bitlocker"**



3. BitLocker will Initialize the drive.

4. It will then prompt you for a password. This can be anything you decide.



BitLocker Drive Encryption (D:)

Choose how you want to unlock this drive

☑ Use a password to unlock the drive

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

Enter your password

Reenter your password

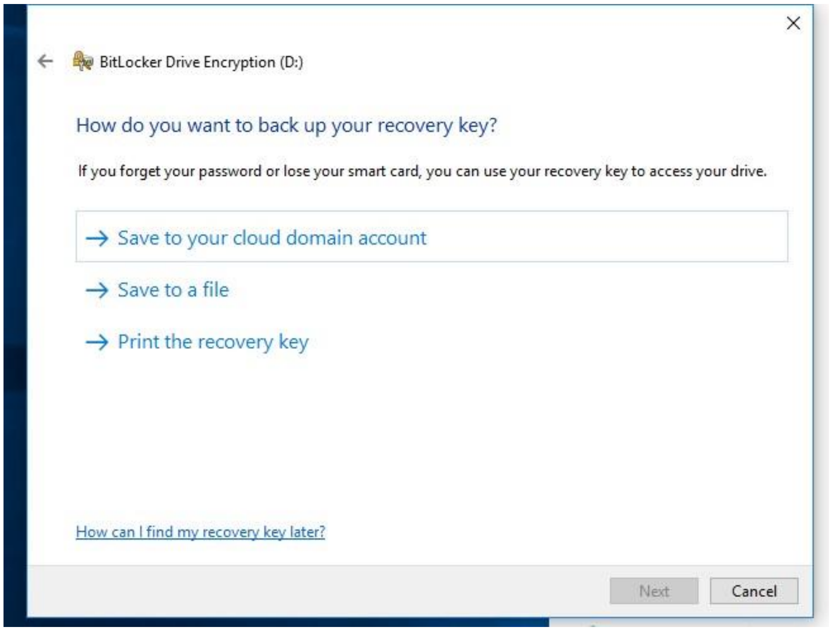
□ Use my smart card to unlock the drive

You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.

5. You will then get a prompt about the recovery key. The recovery key is used in case you do not remember the password. We recommend two options you can choose from. After you have made a choice, click Next.

    - <u>Save to a file:</u> This will provide a text document that includes an **Identifier** and a **Key**. The Identifier is essentially the ID of the USB drive. They key is what you use to unlock it. With this option you will need to save this somewhere that you can refer to in the event you forget the password.

    - <u>Print the recovery key:</u> This will basically print the same information that comes in the "Save to a file" option. Instead of saving this on your computer or server you will have a paper copy instead.



BitLocker Drive Encryption (D:)

How do you want to back up your recovery key?

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

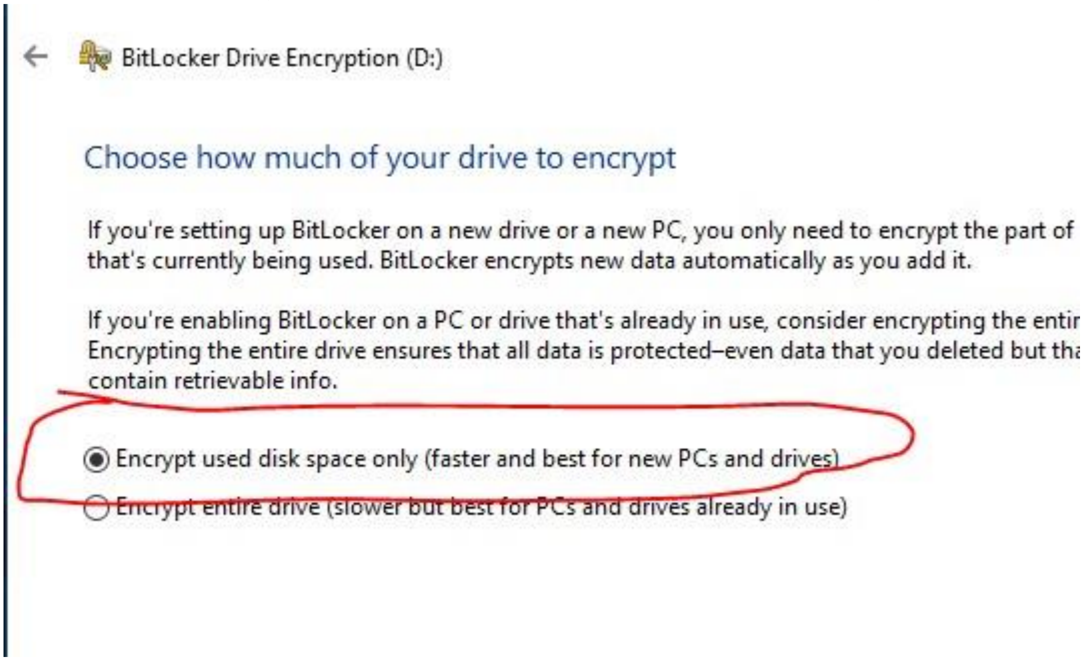
→ Save to your cloud domain account

→ Save to a file

→ Print the recovery key

How can I find my recovery key later?

6. This is where you choose how much to encrypt. Select “**Encrypt used disk space only (faster and best for new PCs and drives)**. This will only encrypt the space being used. As you add more to the drive, it will become encrypted. **Click Next.** NOTE: If you choose to encrypt the entire drive, it will take a really long time because it will encrypt all the space not being used.



BitLocker Drive Encryption (D:)

Choose how much of your drive to encrypt

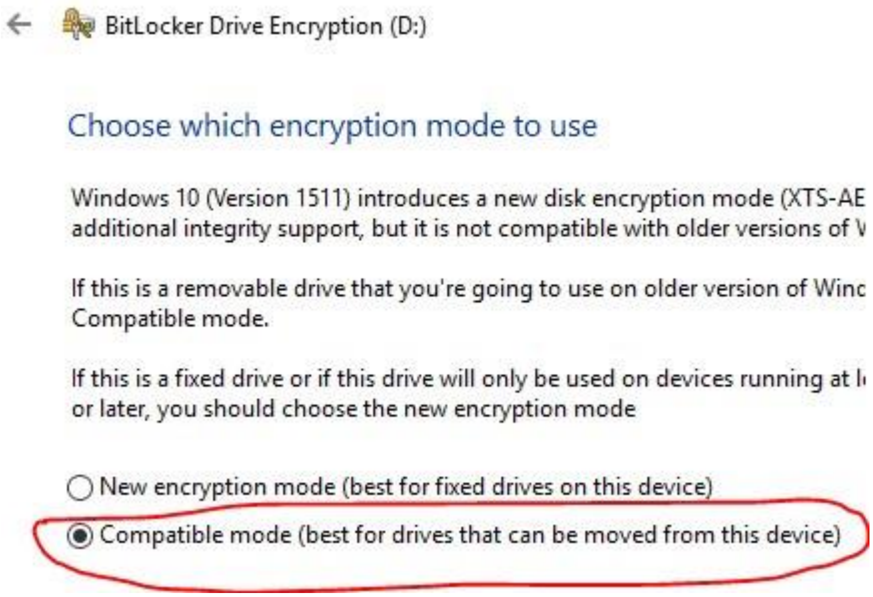
If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of that's currently being used. BitLocker encrypts new data automatically as you add it.

If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entir Encrypting the entire drive ensures that all data is protected–even data that you deleted but tha 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)

7. Next, select “**Compatible mode (best for drives that can be moved from this device)**



BitLocker Drive Encryption (D:)

Choose which encryption mode to use

Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AE additional integrity support, but it is not compatible with older versions of V

If this is a removable drive that you're going to use on older version of Winc Compatible mode.

If this is a fixed drive or if this drive will only be used on devices running at l or later, you should choose the new encryption mode

○ New encryption mode (best for fixed drives on this device)

● Compatible mode (best for drives that can be moved from this device)

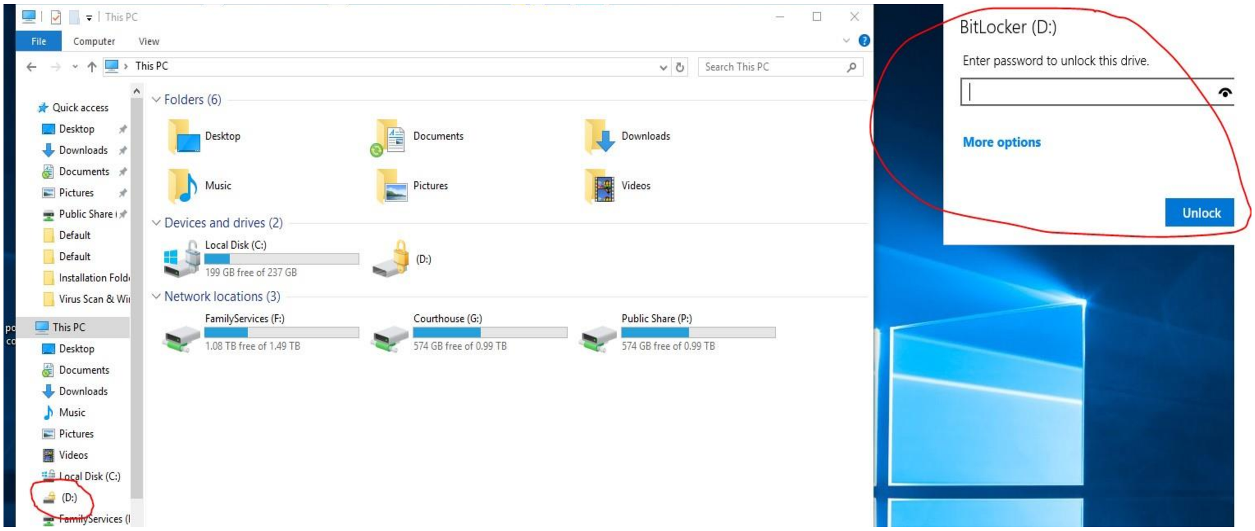
8. Click **Start Encrypting.** The drive will start encrypting, wait until it is finished. **DO NOT REMOVE THE DRIVE UNTIL IT IS FINISHED.**

9. After it is done, click **Close**

10. Now you can add the files you need to the USB.

11. To test. Remove the USB, wait 10 seconds, plug it back in.

12. Open **File Explorer** and click on your USB. It should prompt you to enter the password you created earlier. Type in your password and click **Unlock**



BitLocker (D:)

Enter password to unlock this drive.

13. You should have unlocked your USB and be able to add and remove files from it.