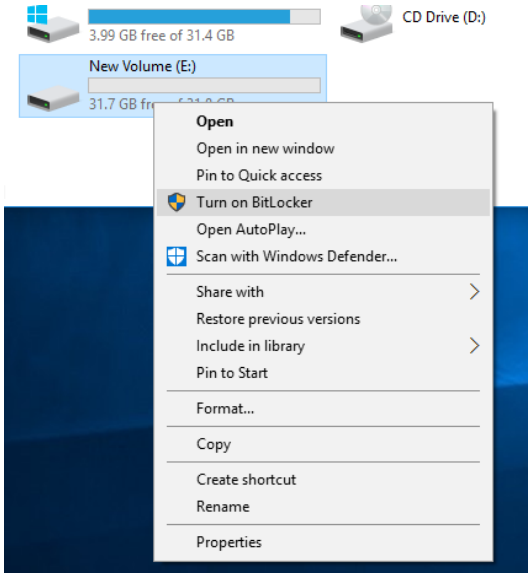
Encrypting Portable Storage (Windows 10)

1. Plug in your portable device (ex: USB key).

2. Right click on the drive you want to encrypt and click **Turn on BitLocker**



3. **Choose how you want to unlock this drive**
   Select **Use a password to unlock the drive** to unlock the drive. Enter a password that is not easy for others to guess. You will need this password to access the drive in the future. Click **Next** to continue.

4. **How do you want to back up your recovery key?**
   You will need to save a copy of the recovery key to a location. Follow the steps to save to the selected location. Once saved, click Next to continue.

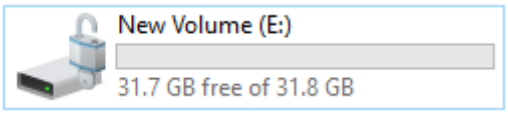
5. **Choose how much of your drive to encrypt**
   If you are encrypting a device that is already empty, choosing the first option to encrypt used disk space only is the best option. However, if you have been using a device for a period of time with pre-existing data, it is recommended to choose the option to **encrypt entire drive**. Click Next to continue.

6. **Choose which encryption mode to use**
   It is recommended to use the **New encryption mode** as this will provide highest protection for your data.

7. **Are you ready to encrypt this drive?**
   Click **Start Encrypting**. Depending on which option you chose in step 4 will depend on how long it will take to finish encrypting the device.

8. Once your device is encrypted, it will show a padlock identifying the data is encrypted. If the padlock is open, the data is accessible. If the padlock is locked, your data is protected and not accessible until unlocked.

   This drive below is encrypted and unlocked.



   The next drive is encrypted and locked, protecting it from unauthorized access.