LANDER UNIVERSITY

Information Technology Services
http://www.lander.edu/its
help@lander.edu
864.388.8234

USB Drive Encryption using BitLocker

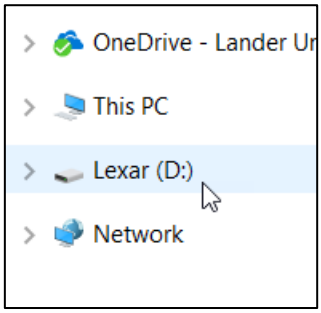
Due to their portability, USB drives are a convenient way to transport digital files. Their small size also makes them more susceptible to theft or loss. Regardless of the type of data you store on USB drives, BitLocker (available on any Lander computer running Windows 7 or later) can be used to encrypt these portable drives and protect your data from unauthorized access.

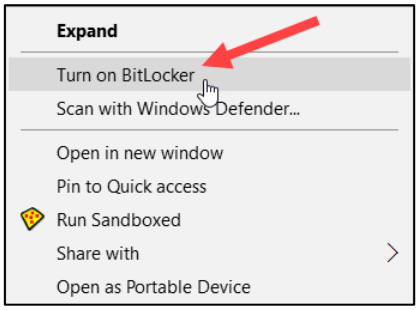
Notes:

1. **The drive encryption process may take 30 to 60 minutes or more. Do not disconnect or remove the drive until this process is finished.**
2. **USB drives encrypted with Windows BitLocker will not be accessible on any device running macOS (Apple computers such as MacBooks or iMacs).**

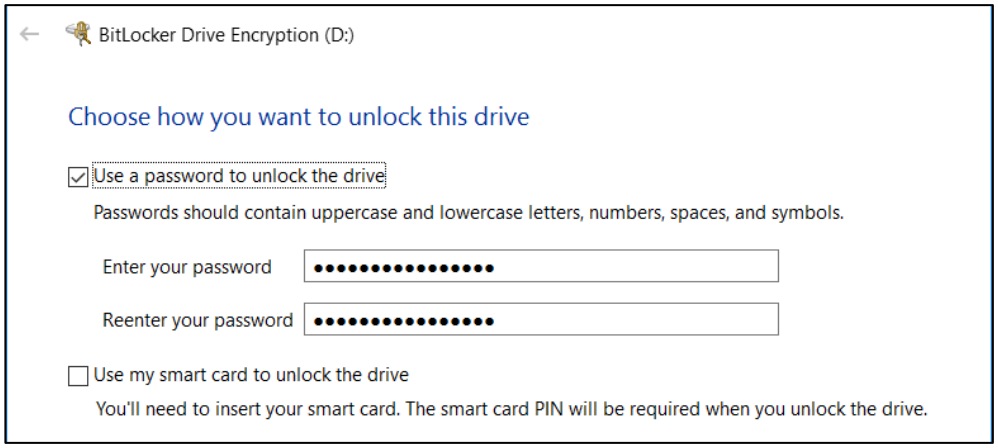
How to Encrypt a USB Drive

1. After inserting your USB drive into your Lander computer, open File Explorer (yellow folder icon) and locate your USB drive in the list on the left. Typically, USB drives are named after their manufacturer (in this case, "Lexar").
2. Right-click your USB drive and select "Turn on BitLocker".

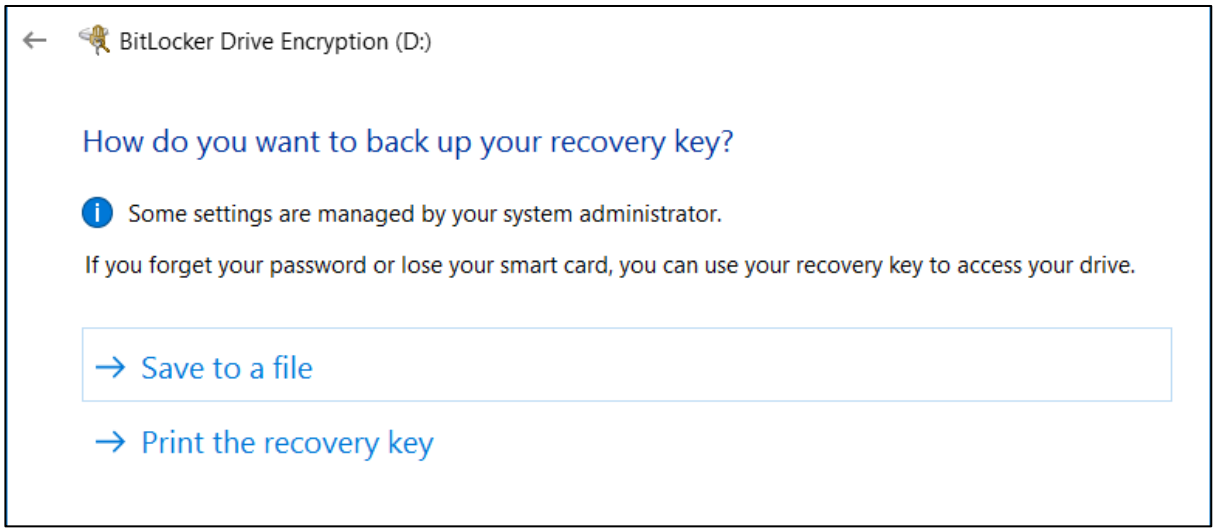




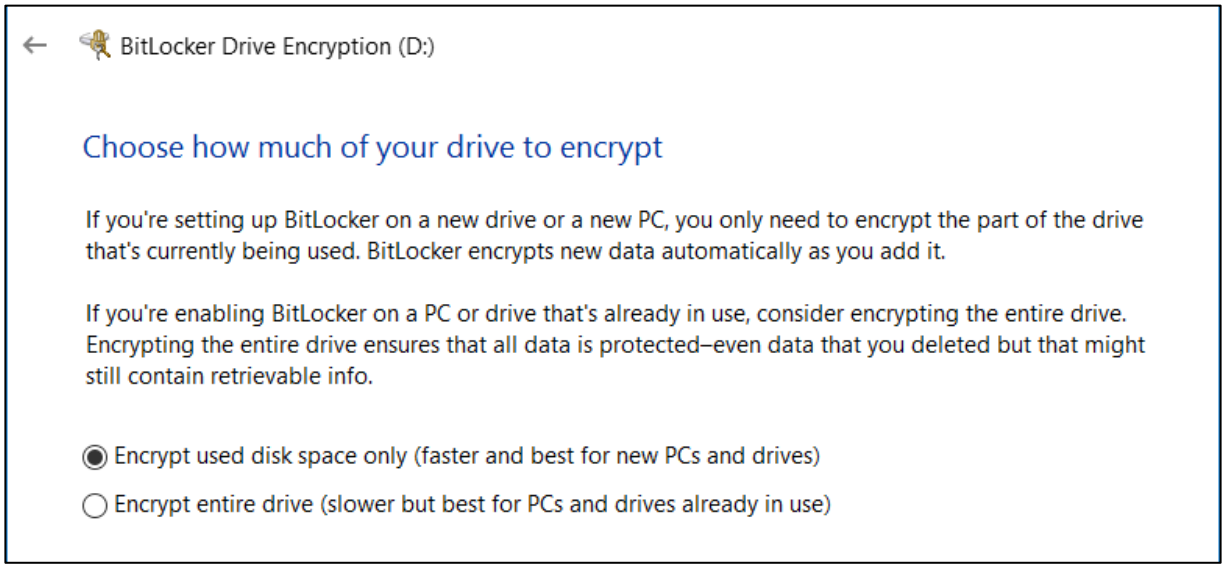
3. Once BitLocker Drive Encryption launches, select "Use a password to unlock the drive". Choose a strong password and enter it twice.



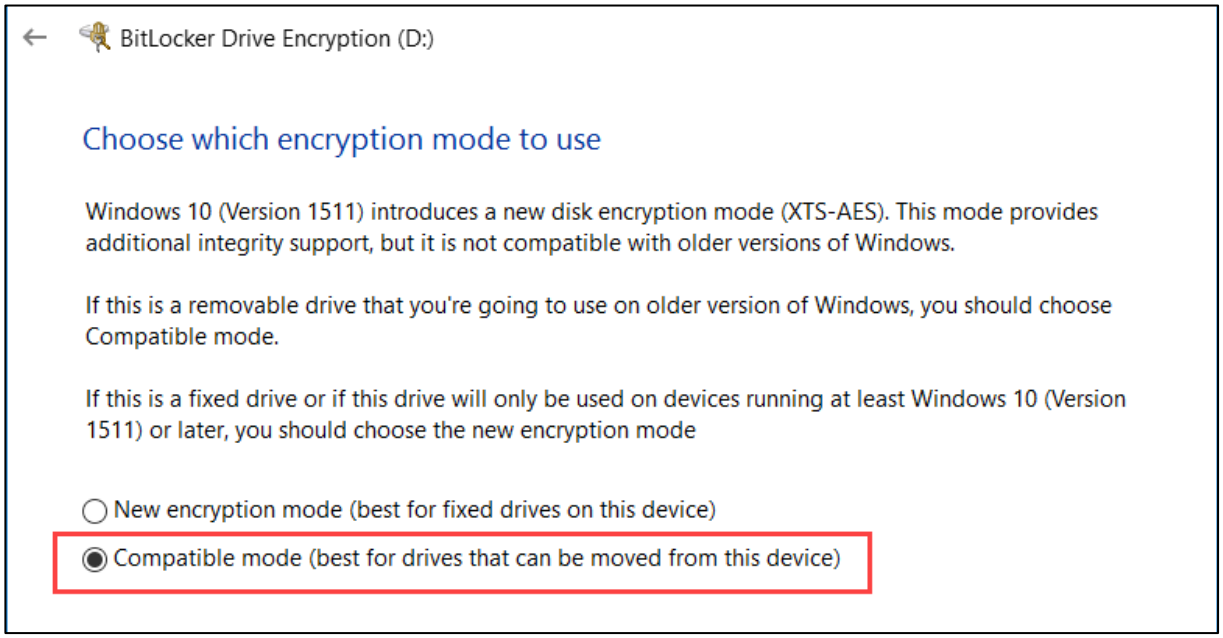
4. A recovery key will be used to access your USB drive in the event that you forget your password. You can choose one or both of the options provided. “Save to a file” will save the recovery key in a text file on your computer. “Print the recovery key” will allow you to print a physical copy of your key. Choose “Next” when finished.



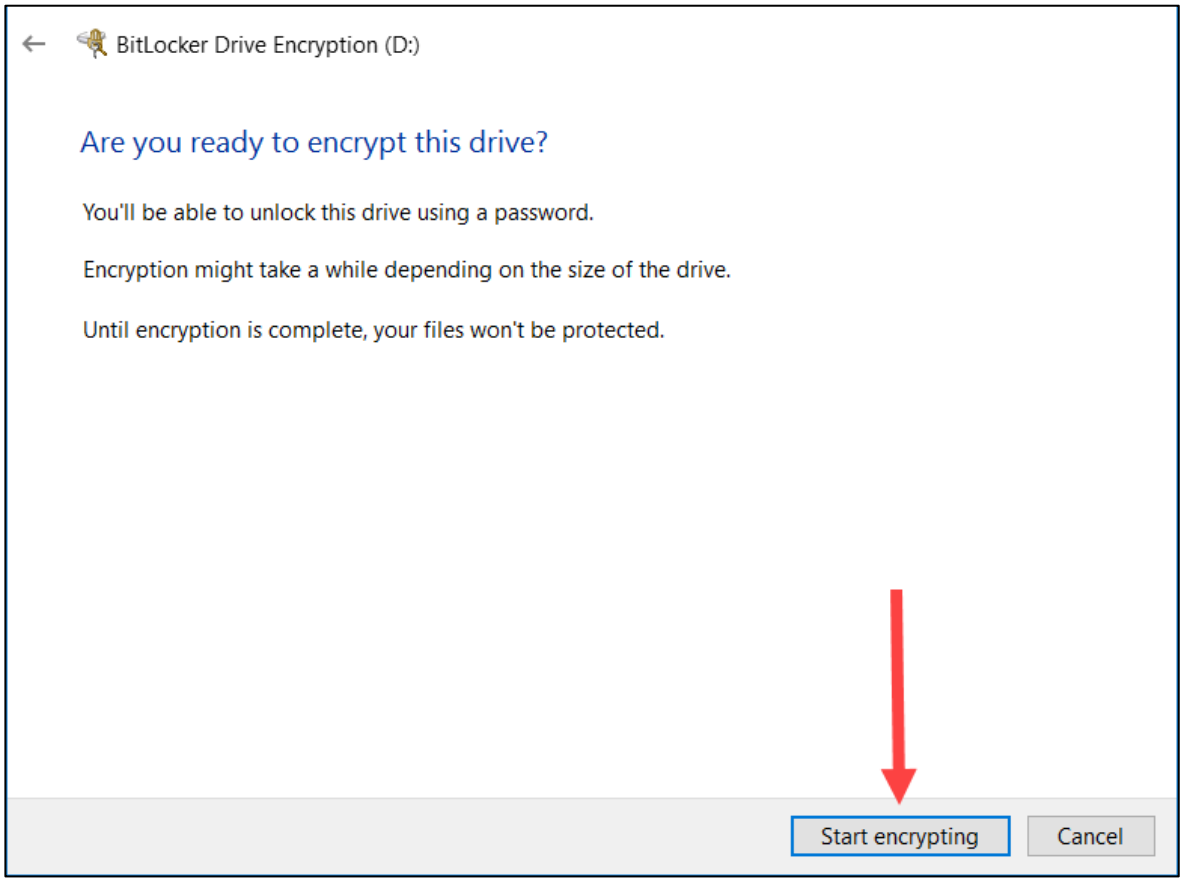
5. The next step will depend on the status of your USB drive:
    a. If your drive is new or unused, select “Encrypt used disk space only”.
    b. If your drive already has files on it, select “Encrypt entire drive”.



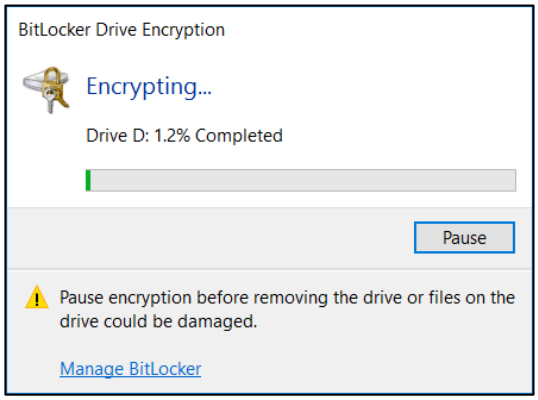
6. Since this is a portable drive that will be used on multiple computers, select “Compatible mode” in the next step.

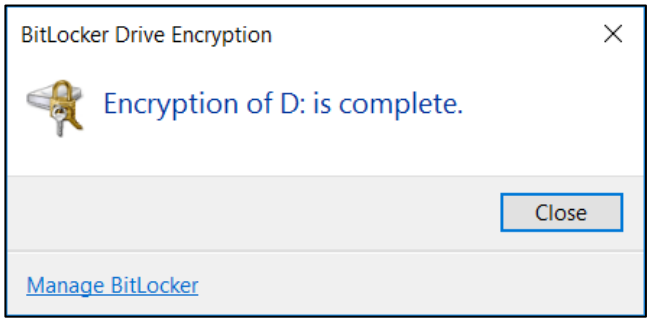


7. Select “Start encrypting”.



8. Reminder: Do not disconnect or remove the drive during the encryption process. You will be notified when the process has finished.





After Your Drive is Encrypted

- Any file or folder saved to your encrypted drive will be automatically protected – you do not have to take any additional steps when copying new files to the drive.

- When plugging your USB drive into a BitLocker-supported computer, you will be prompted to enter your encryption password in order to access any files on the drive.

- If you forget your encryption password and need assistance using the recovery key, contact the ITS Help Desk at 864-388-8234.