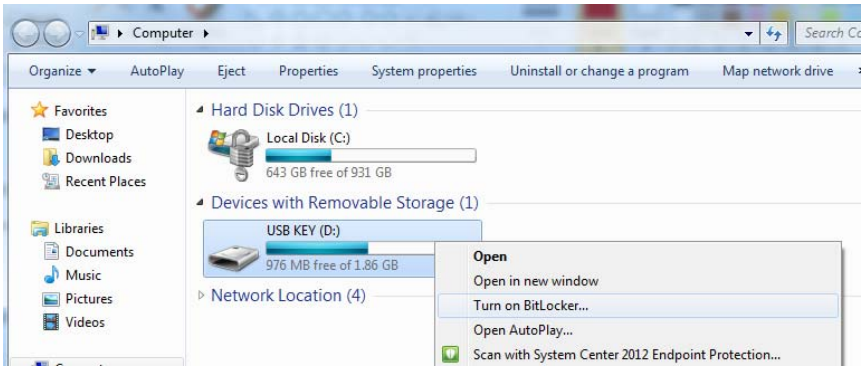
ENCRYPTING USB KEYS AND USB HARD DRIVES FOR WINDOWS 7

Encrypting allows you to protect your USB key or USB hard drive with a password of your choice. Every time you plug in an encrypted USB key/HDD into another Windows 7 PC, you will be prompted to type in the password. Once the password is typed in, you will have full access to the data on the drive. If the wrong password is typed in, the data will remain inaccessible. If you forget the password, contact I&ITS HelpDesk.

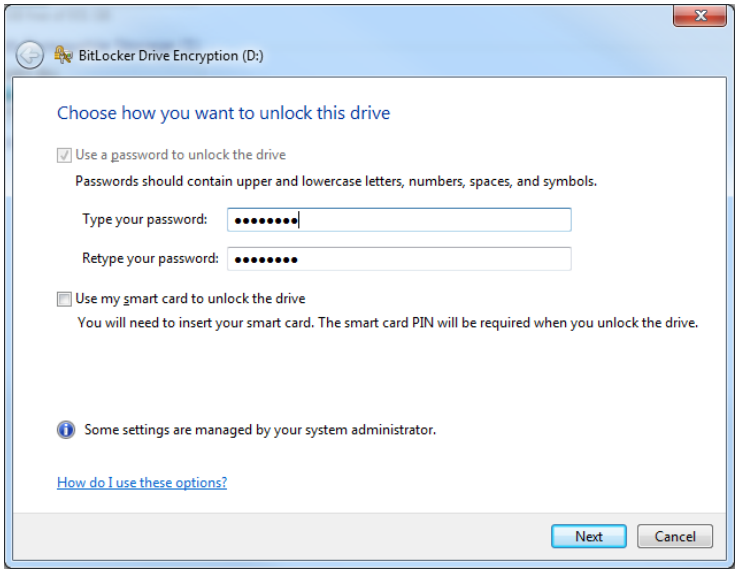
Encryption Steps:

1. Plug your USB key/hard drive into the computer then click the “Start” button and go to “Computer”.

2. Right-click the USB Key or USB Hard Drive and select “Turn on BitLocker…”



3. Pick a password, type it in twice and click next. It is best to use a secure password that contains a mix of letters, numbers and upper/lower case letters. If you intend to share this USB key/hard drive with others, do not pick the same password you currently use for your UTORid.

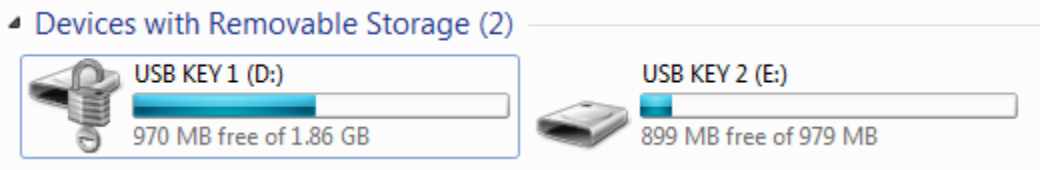


4. At the next screen, click “Start Encrypting”.

5. Wait until the drive completes the encryption.

How do you know if the drive is already encrypted?

- You will be prompted for an encryption password once you plug the drive into your computer.
- Encrypted drives will have a different icon. You will see a picture of a lock beside it.
- “USB KEY 1” is encrypted. “USB KEY 2” is **NOT** encrypted.



How do you remove encryption from the drive?

- Go to “Control Panel” > “BitLocker Drive Encryption”.
- Click “Turn Off BitLocker” next to the desired USB key/hard drive.