BitLocker to Go: Encryption for personal USB

Encryption is an effective method of protecting data stored on portable USB devices such as flash drives and external hard drives.

Encryption encodes data so that it can only be read by someone who has the right encryption key (password) to decode it. This means that if your device is lost or stolen, the information contained on it cannot be accessed by unauthorised users.

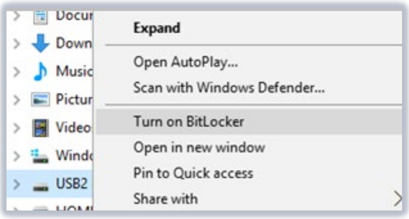
BitLocker to Go is a feature of Windows 10 (Pro and Enterprise) that allows you to easily encrypt your personal devices and prevent unauthorized access[1]. Without the encryption key, the device is inaccessible.

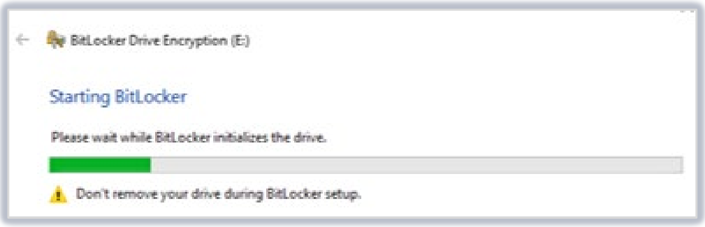
When you connect your BitLocker encrypted USB device to a Windows PC you will be prompted for your password. After entering the password correctly, you can read and write to your device as normal.

Using BitLocker on Windows 10

Encrypting a USB Flash drive

- Insert the USB drive you want to encrypt - this can be a new drive, or one that already has data stored on it.
- Open File Explorer, **right-click** on the USB drive then select **Turn on BitLocker…** from the pop-up menu.
- The BitLocker wizard launches and BitLocker prepares the USB drive for encryption.



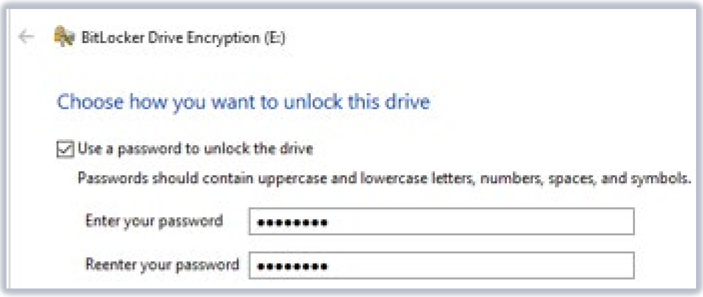

BitLocker Drive Encryption (E:)

Starting BitLocker

Please wait while BitLocker initializes the drive.

Don't remove your drive during BitLocker setup.

- After BitLocker has prepared the USB drive, the wizard prompts you to **Choose how you want to unlock the drive**.
- Tick the **Use a password to unlock the drive** checkbox and type in and retype a password, then click **Next**.


BitLocker Drive Encryption (E:)

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: ••••••••

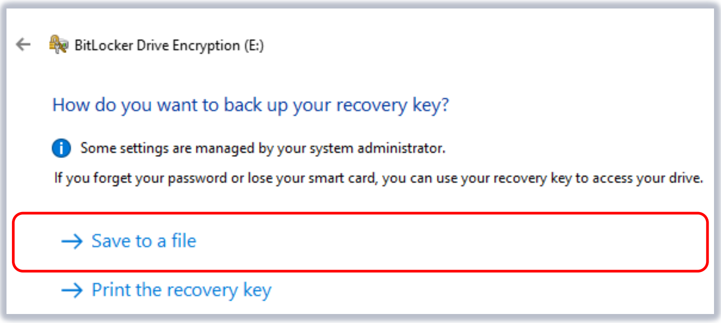
Reenter your password: ••••••••

[1] It is not possible to *encrypt* drives using BitLocker on Windows 10 Home edition. You can however unlock and use previously encrypted drives with full read/write access.

- The wizard prompts you to back up your recovery key to use in the event that you forget your password.

> **Do not save the recovery key on the USB drive you are encrypting.**
> We recommend that you store the recovery key on your personal H: drive so that it is backed up on the network.

- Click **Save to a file**. In the **Save BitLocker Recovery Key as** dialog, browse to a suitable location on your H: drive then click **Save**.



BitLocker Drive Encryption (E:)

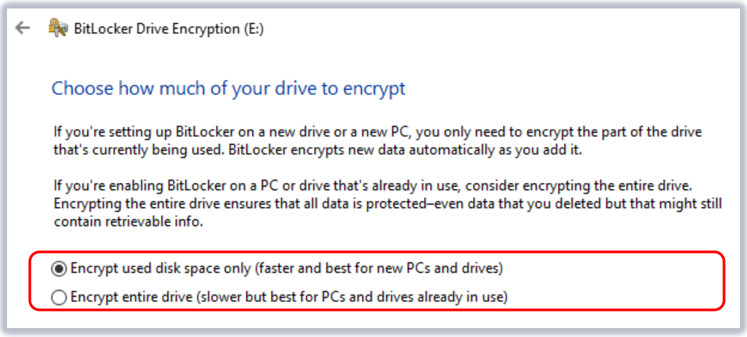
How do you want to back up your recovery key?

Some settings are managed by your system administrator.

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

- Click **Next**.
- The wizard asks how much of the drive you want to encrypt.

  You can choose to encrypt the used space only (best for a new drive) or the entire drive (best for a drive already in use).



BitLocker Drive Encryption (E:)

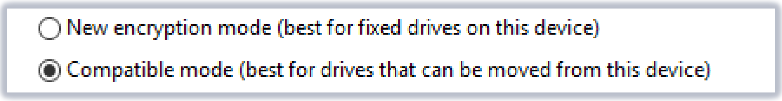
Choose how much of your drive to encrypt

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

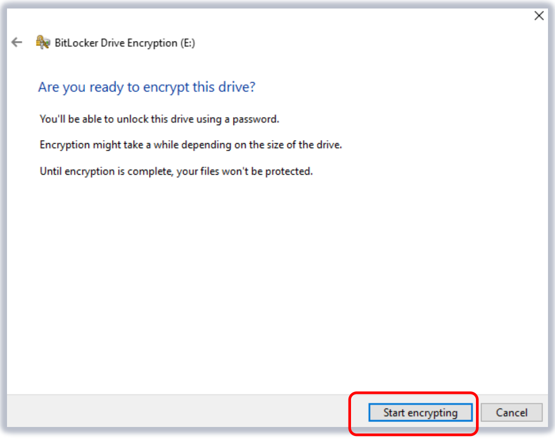
If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected–even data that you deleted but that might still contain retrievable info.

● 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)

- Click **Next**.
- As you are encrypting a USB drive leave the encryption mode set at **compatible mode** which is for drives which can be moved.



○ New encryption mode (best for fixed drives on this device)
● Compatible mode (best for drives that can be moved from this device)



BitLocker Drive Encryption (E:)

Are you ready to encrypt this drive?

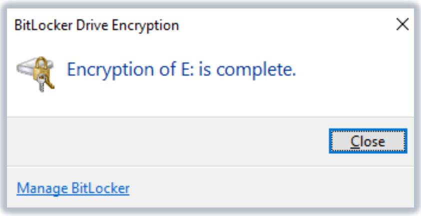
You'll be able to unlock this drive using a password.

Encryption might take a while depending on the size of the drive.

Until encryption is complete, your files won't be protected.

- Click **Next**.
- The wizard asks if you are ready to encrypt the drive.
- Click **Start Encrypting** to begin the encryption process.
- A status bar indicates progress while the USB drive is encrypting. Encryption can take several minutes if your drive contains a lot of data. For example, 2.5GB of data could take up to 10 minutes.

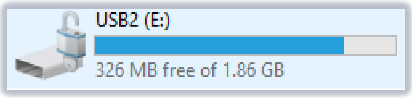
- When encryption is complete you’ll see this notification:



BitLocker Drive Encryption

Encryption of E: is complete.

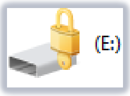
- Click **Close** to close the wizard.
- When you open File Explorer or This PC, you’ll notice that the USB drive icon has changed. The padlock indicates that the drive is now encrypted with BitLocker.
- The padlock icon is coloured **grey** – this means that the drive is **unlocked**.



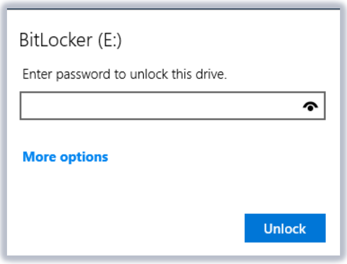
- The next time you right-click on this drive in File Explorer or This PC you will see either **Manage BitLocker** or **BitLocker Encryption Options** in the pop-up menu. (You may see both!)

  Both offer similar encryption options.

Using your encrypted flash drive in Windows 10

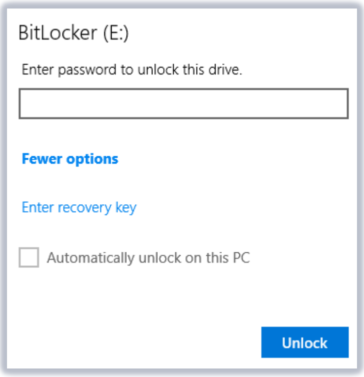


- The next time you insert your USB drive into a Windows PC you will notice that the padlock icon is coloured **gold** – this indicates that the drive is **locked**.
- When you try to open the drive, BitLocker will prompt you to enter the password you created when you encrypted the drive in order to unlock it.
- If you want, you can select to **Automatically unlock on this PC** from now on. To find this in Windows 10 click **More options**.



BitLocker (E:)

Enter password to unlock this drive.



BitLocker (E:)

Enter password to unlock this drive.

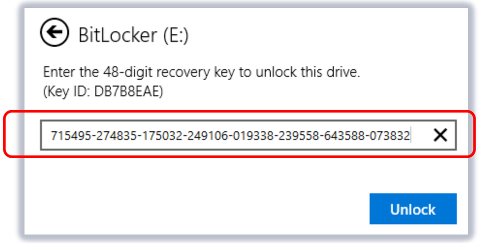
□ Automatically unlock on this PC

Forgotten your password?

If you forget the password for your encrypted USB drive, you can use the BitLocker recovery key (which you saved to your H: drive when you set up encryption) to unlock the drive and create a new password.

- Insert your USB drive into a Windows PC
- In the BitLocker wizard in Windows 10, click **More options** and then **Enter recovery key**.
- Using File Explorer or This PC , browse to the location on your H: drive where you saved the recovery key.

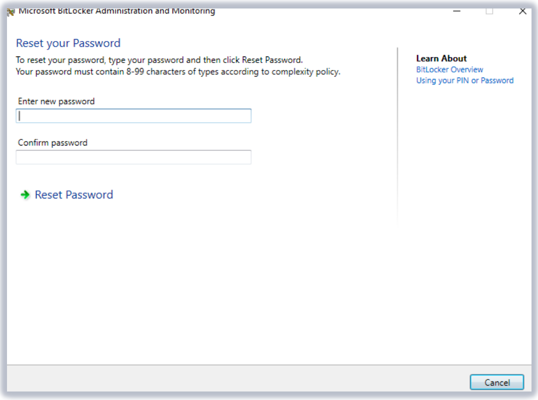
- Double-click the BitLocker Recovery Key file to open it in NotePad. Copy the **Recovery Key** code then return to the BitLocker wizard.
- Paste the text you copied into the text box and click **Unlock.**



Enter the 48-digit recovery key to unlock this drive.
(Key ID: DB7B8EAE)

715495-274835-175032-249106-019338-239558-643588-073832

- You will now have access to your drive.
- You will most likely want to reset the password to make accessing your drive easier in future. To do this right-click on the drive to bring up either **Manage Bitlocker** or **Bitlocker Encryption Options**[2].
  - From Manage Bitlocker choose **Change password**
  - From Bitlocker Encryption Options choose **Manage your Password**
- In both cases you will be prompted to enter a new password and then retype it to confirm.
- Click **Reset Password**



Microsoft BitLocker Administration and Monitoring
Learn About
BitLocker Overview
Using your PIN or Password
Reset Password
Cancel

Reset your Password

To reset your password, type your password and then click Reset Password.
Your password must contain 8-99 characters of types according to complexity policy.

Enter new password

Confirm password

- You will see a confirmation message when the password has been changed successfully.
- Next time you use your drive you will be able to unlock it with the new password.

Forgotten your password *and* lost your recovery key?

If you forget your password *and* lose your recovery key it will not be possible unlock the drive and you will lose all the data on it.

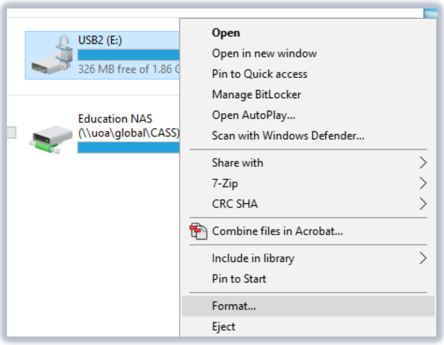
To prevent you losing your recovery key, we strongly recommend you store it on your H: drive as described above.

If you have forgotten your password and lost your recovery key but would like to *reuse* your flash drive, you can **reformat** it as below.

Note: This action will erase all data from the drive!

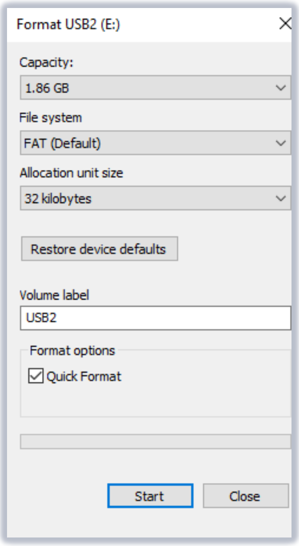
- Insert your flash drive. In This PC or File Explorer, right-click on the flash drive icon and select **Format** from the pop-up menu.

[2] If these options do not appear on your PC take your USB drive to the IT Service Desk for help changing the password.



- In the **Format** dialog, the **File system** should be the default setting **FAT**.
- Click **Start** to format the drive.

  Remember, this action will erase all data from the drive.



Format USB2 (E:)

Capacity: 1.86 GB

File system: FAT (Default)

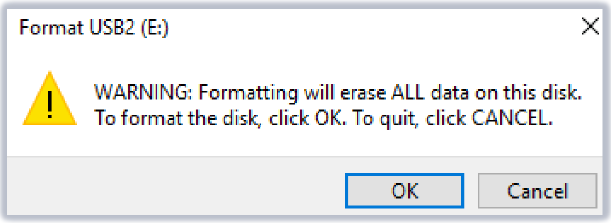
Allocation unit size: 32 kilobytes

Volume label: USB2

Format options

☑ Quick Format

- A warning will appear advising you that formatting will erase all data. Click **OK** to continue.



Format USB2 (E:)

WARNING: Formatting will erase ALL data on this disk.
To format the disk, click OK. To quit, click CANCEL.

- You will be prompted when formatting is complete. Click **OK**.

Help and Support

Use MyIT to contact the IT Service Desk: https://myit.abdn.ac.uk