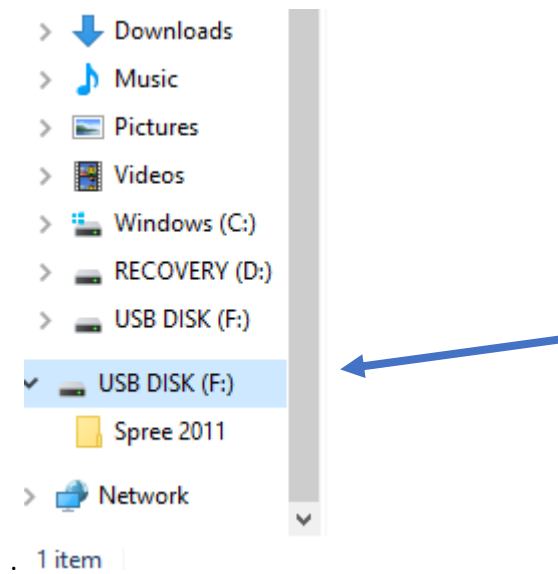
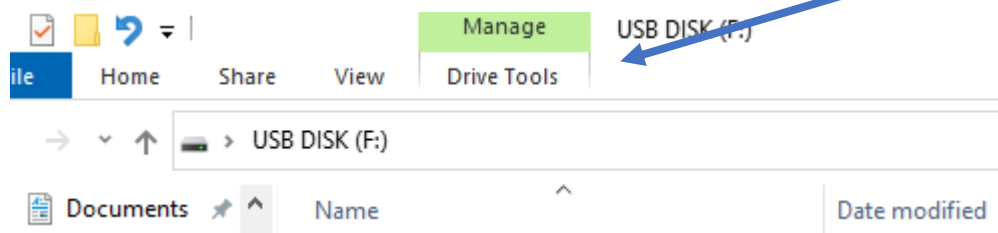


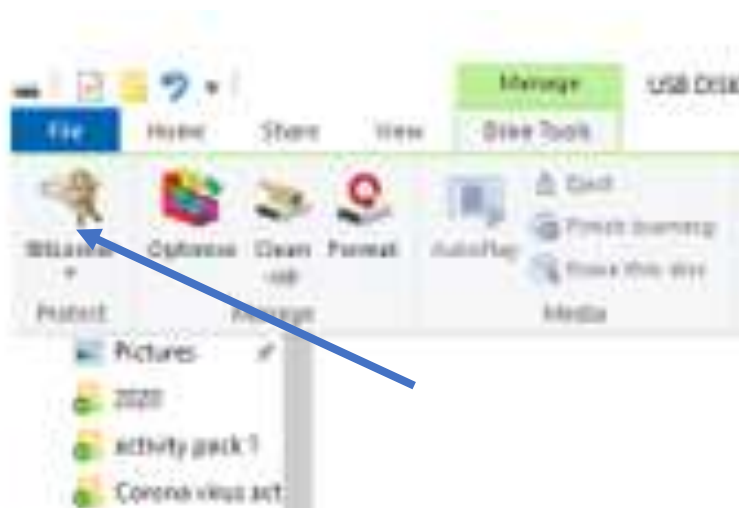
Insert the USB and open it



Open drive tools

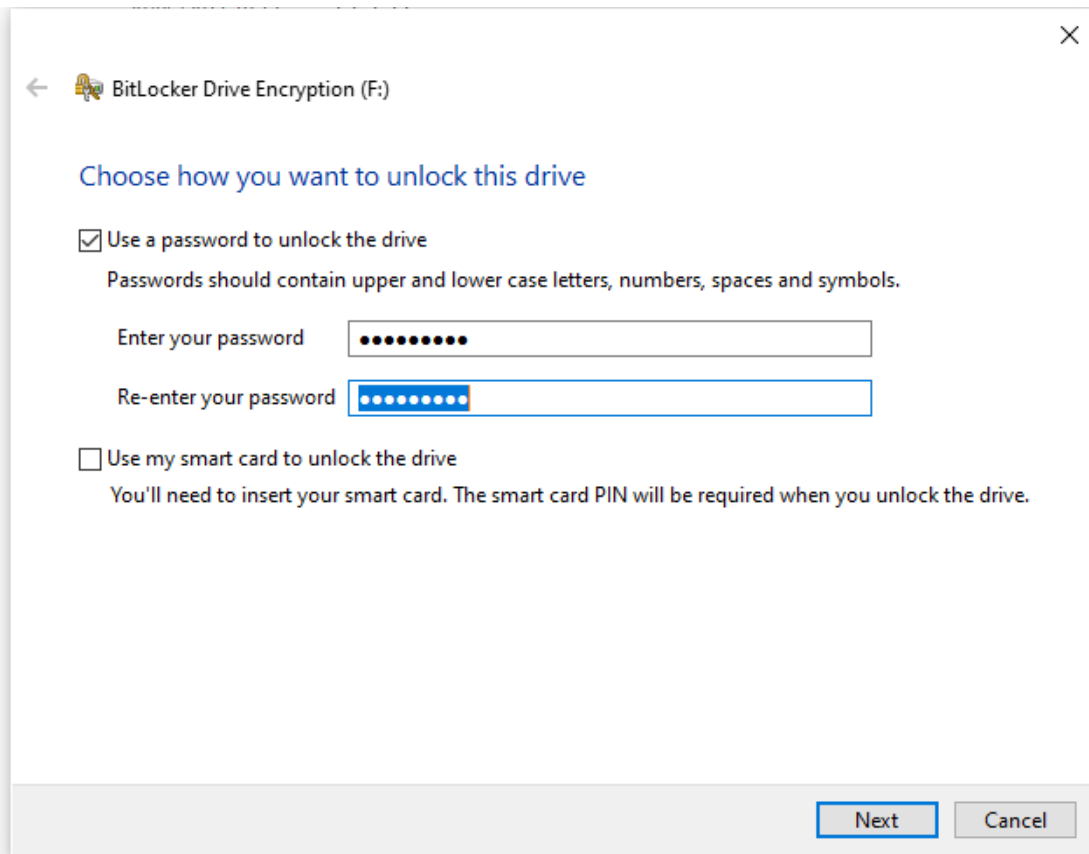


Select Bitlocker



Turn Bitlocker on

Select use password and create a password



← BitLocker Drive Encryption (F:) ×

Choose how you want to unlock this drive

Use a password to unlock the drive
Passwords should contain upper and lower case letters, numbers, spaces and symbols.

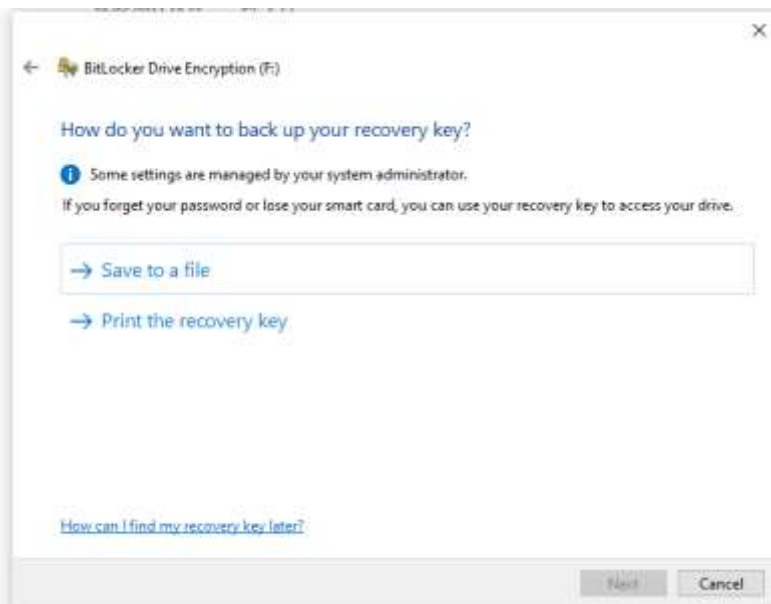
Enter your password

Re-enter 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.

Next Cancel

Choose how to save your recovery key



← BitLocker Drive Encryption (F:) ×

How do you want to back up your recovery key?

i 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.

→ Save to a file


→ Print the recovery key

[How can I find my recovery key later?](#)

Next Cancel

You can save it to your computer or print it out.

I always use the selected option here.

←  BitLocker Drive Encryption (F:)

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've deleted but that might still contain retrievable information.

- 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)

Again, I use the default option

-  BitLocker Drive Encryption (F:)

Select which encryption mode to use

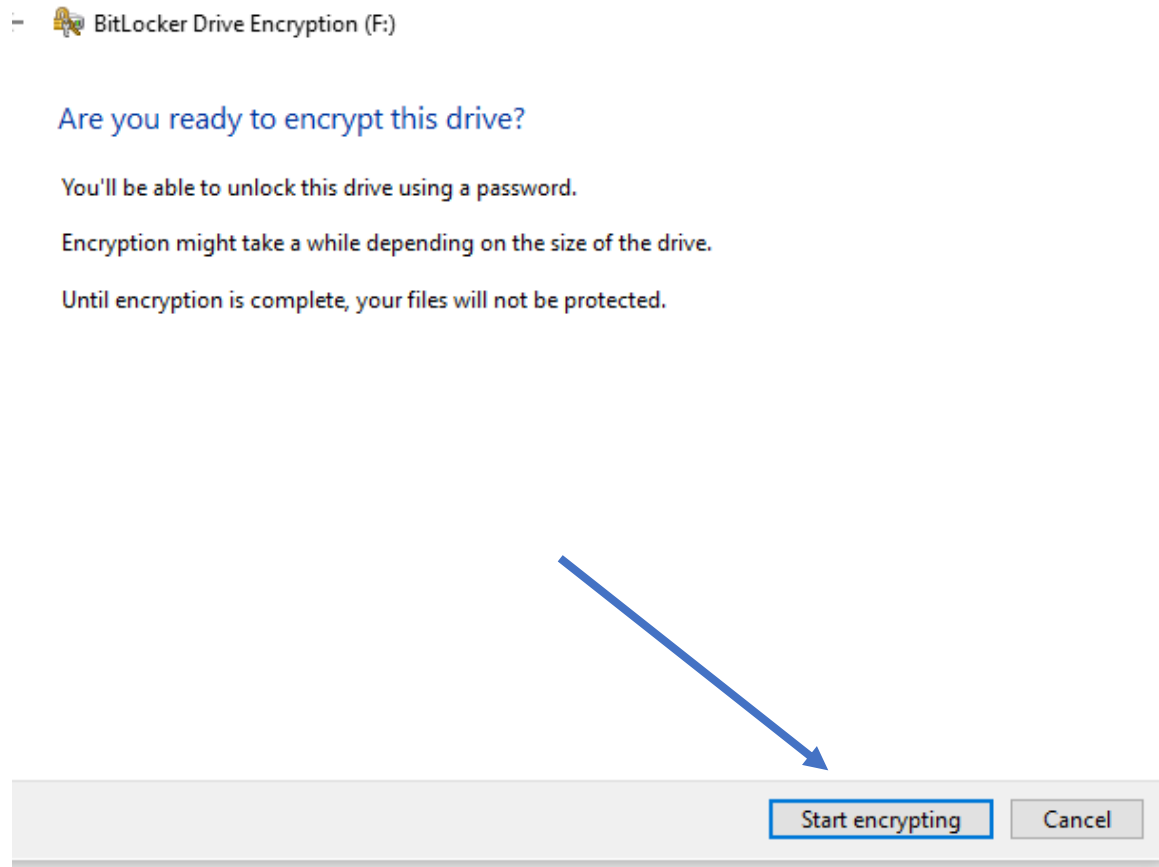
Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AES). This mode provides additional integrity support, but it is not compatible with older versions of Windows.

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

If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode

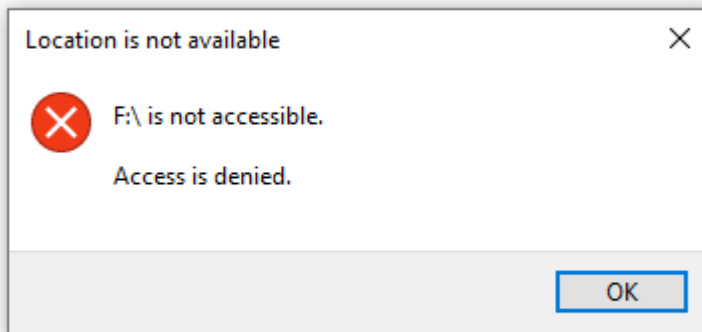
- New encryption mode (best for fixed drives on this device)
- Compatible mode (best for drives that can be moved from this device)

Follow prompts

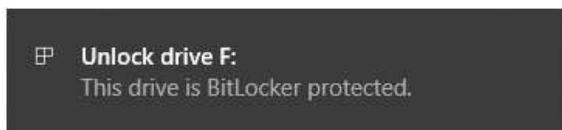


Remove USB when complete.

To open contents – insert USB



This may appear centre, but in the bottom right corner, you will get this message – click it.



This will appear top right



Insert password and click unlock and drive will open.

When using in printers etc. it may require the encryption to be removed so open drive tools again - bitlocker – manage bitlocker.

Fixed data drives

Removable data drives - BitLocker To Go

USB DISK (F:) BitLocker on



- Back up your recovery key
- Change password
- Remove password
- Add smart card
- Turn on auto-unlock
- Turn off BitLocker



Follow instruction to decrypt.