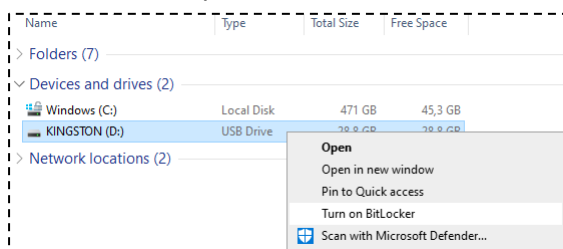
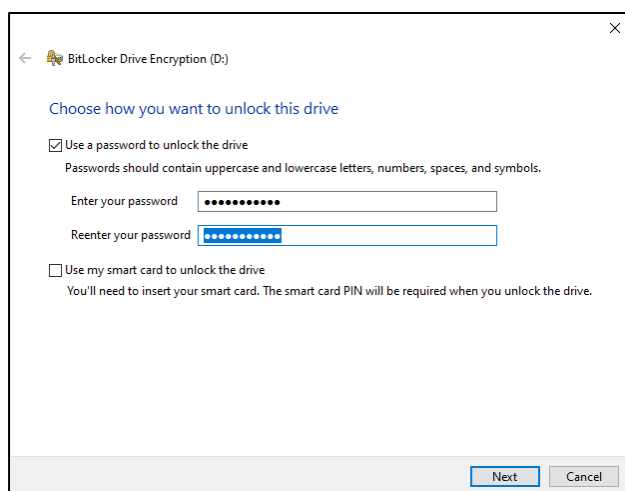


# How to protect a USB drive or a memory stick with BitLocker

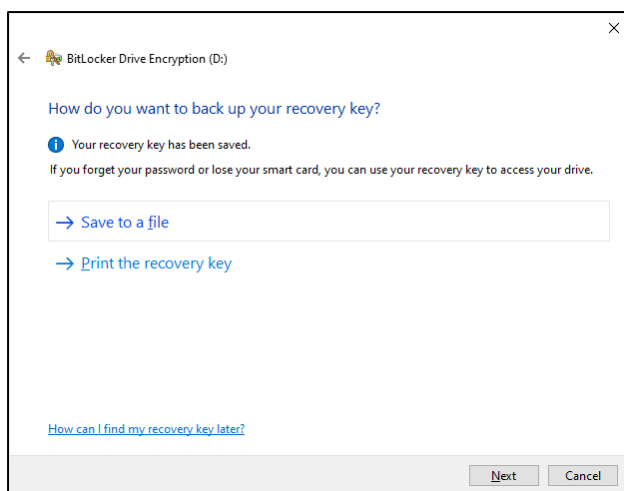
1. Plug a USB drive or a USB memory stick into a Windows computer.
2. Open File Explorer, go to My Computer and click the right mouse button on top of the USB drive. Click the option *Turn on BitLocker*.



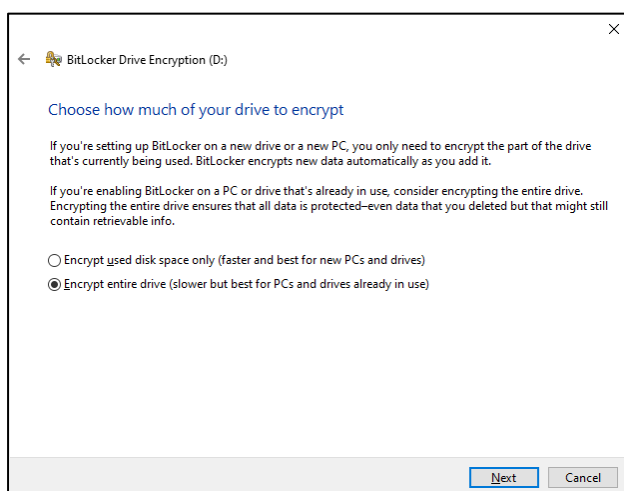
3. Define a strong password and write it down on a physical note in full or in part. More guidelines available on the page [Take control of your passwords](#) by the National Cyber Security Center. Store this note in a secure place. Write down the information in a way that makes it impossible for outsiders to determine the services that the passwords are for or the user if the note goes missing. If the password is forgotten, the encryption of the USB drive cannot be opened, and all the files stored in the drive will be permanently lost. Click *Use a password to unlock the drive* and enter the password and click *Next*.



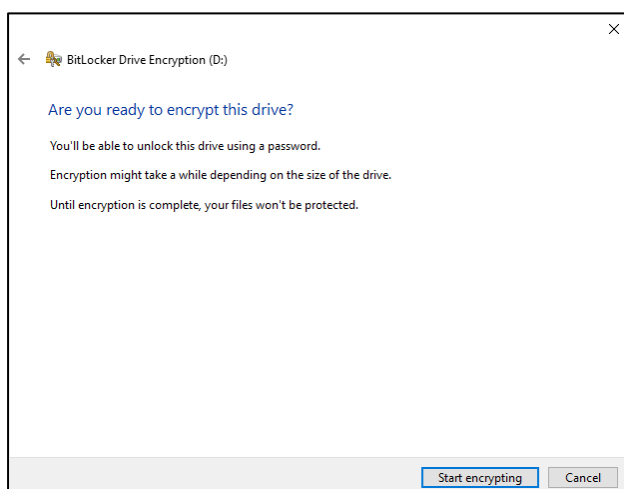
4. Next, you have the option to save a file with a recovery key that allows you to open the BitLocker encryption of a USB drive if you forget the password you just created. Saving this file is not mandatory. Since this file allows the encryption of the USB drive to be unlocked, it can only be stored in a sufficiently secure location. If you have access to the TUNI home directory on the network drive P: click *Save to a file* and save the file containing the recovery key there. This file may not be stored in an unencrypted location on your own computer, any cloud service or flash drive. Whether you save the file somewhere or not, click *Next*.



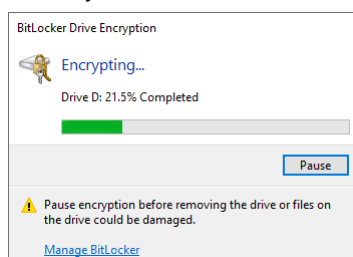
5. If the USB drive is empty, select the first choice. Otherwise select the second choice. Notice that the second choice will take a very long time even if the memory stick is empty: about 2 minutes per GB with a typical laptop and memory stick. Click *Next*.



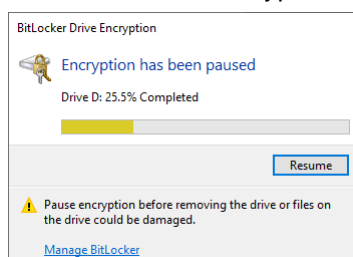
6. Click *Start encrypting*.



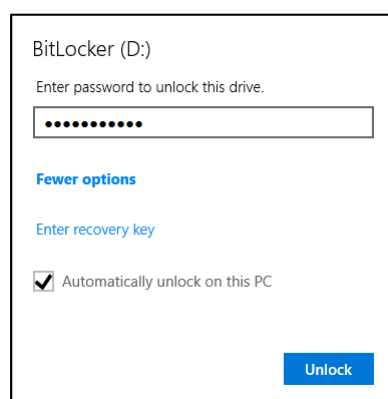
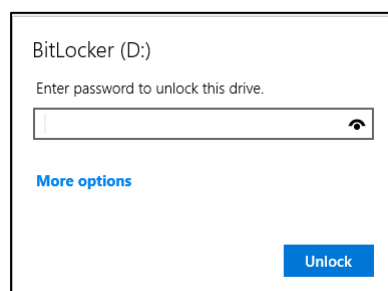
7. Wait for the encryption to finish. If you do not have now the time to wait for the encryption to finish, you can click *Pause*.



8. If you clicked Pause, the encryption will pause and then you can remove the USB drive from the computer with no harm to the data. If you remove the USB drive, you can plug it in later and continue the encryption.



9. When you plug the USB drive into a Windows computer, you will be requested to enter it's BitLocker password. If the computer you are using is your centrally maintained TUNI Windows computer, you can click *More options* and select *Automatically unlock on this PC*. If you do this, the password you enter will be stored securely into this computer so that you will not have to enter it again when plugging in this USB drive into this computer. Enter the password and click *Unlock*.



10. If the encryption was paused, you will now get to the same the window as shown in step 8 and you can click *Resume* to continue the encryption.

After these steps the USB drive is encrypted, and you can store data securely on it. Notice that for storing especially sensitive data, such as the *Special categories of data* specified in the Article 9 of the [GDPR](#), you will have to use an additional encryption software such as Cryptomator or VeraCrypt. Contact [IT Helpdesk](#) for support.