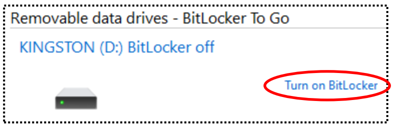
How to protect a USB drive or a memory stick with BitLocker

A USB drive or memory stick can be protected on a Windows computer using the BitLocker feature. BitLocker is Microsoft software that encrypts the USB drive or memory stick so that all files stored on it are automatically encrypted and require the password you set during the encryption process to access them.

1. Setting the encryption

1. Plug a USB drive or a USB memory stick into a Windows computer.
2. Open the Windows menu by clicking ⊞ and type *BitLocker*. Choose *Manage BitLocker*. Click *Turn on BitLocker* next to your USB disk or stick.

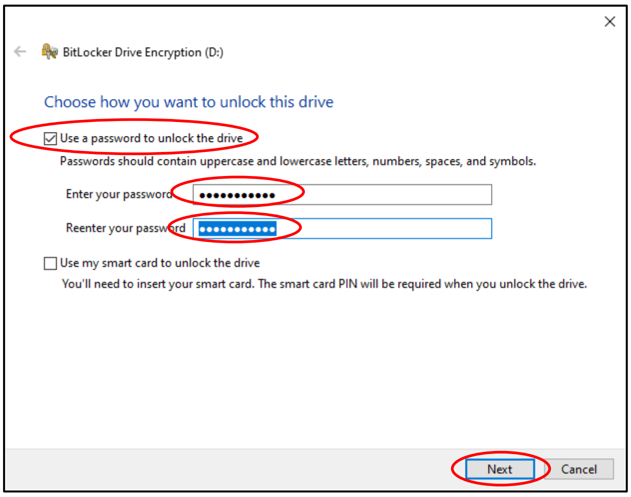


Removable data drives - BitLocker To Go

KINGSTON (D:) BitLocker off

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*.



BitLocker Drive Encryption (D:)

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 ●●●●●●●●●●●

□ 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.

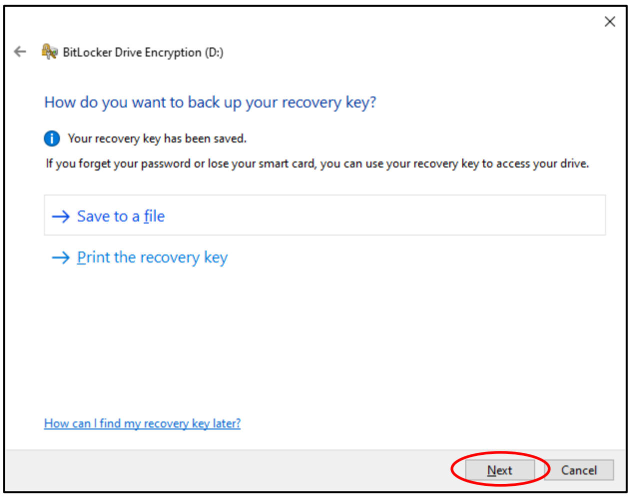
Next Cancel

4. Next, you have the option to save a file with a recovery key or print the key. That will allow you to open the BitLocker encryption of a USB drive if you forget the password you just created. Since this file allows the encryption of the USB drive to be unlocked, it can only be stored in a secure enough location. This file may not be stored in an unencrypted location on your own computer, any cloud service or flash drive.
   a. On a centrally maintained TUNI Windows computer:
      Saving this file or printing the key is mandatory. Your TUNI home directory on the network drive P: is a safe encrypted location. Outside a campus network, you can

access the P: drive by starting the TUNI VPN. Click *Save to a file* and save the file to P:.

b. On other computers:
Saving this file or printing the key is optional. If you do not have a safe encrypted storage available, it is more secure to not save the recovery key file. If you can print the recovery key on paper, do that.

5. Click *Next*.



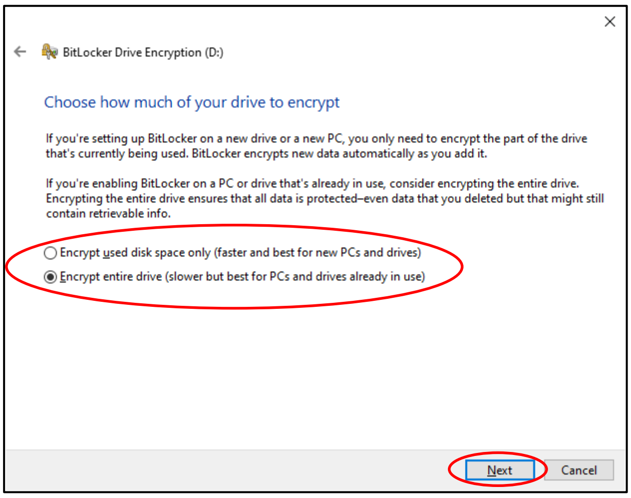
BitLocker Drive Encryption (D:)

How do you want to back up your recovery key?

Your recovery key has been saved.

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

6. 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*.



BitLocker Drive Encryption (D:)

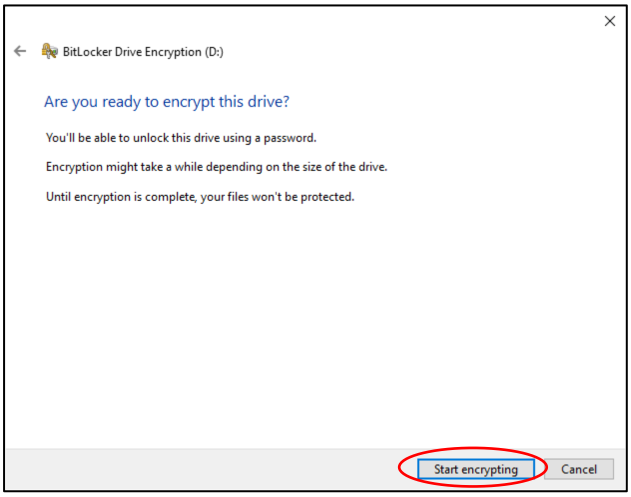
Choose how much of your drive to encrypt

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)

7. Click *Start encrypting*.



BitLocker Drive Encryption (D:)

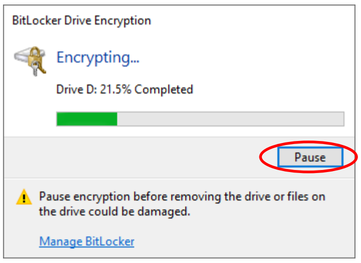
Are you ready to encrypt this drive?

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.

8. Wait for the encryption to finish. If you do not have now the time to wait for the encryption to finish and you want to continue it later, you can click *Pause*.



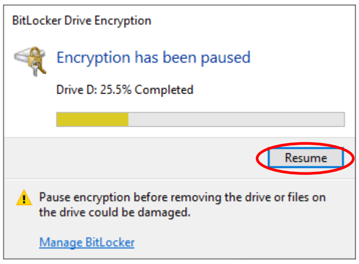
BitLocker Drive Encryption

Encrypting...

Drive D: 21.5% Completed

Pause encryption before removing the drive or files on the drive could be damaged.

9. 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 by clicking *Resume*.



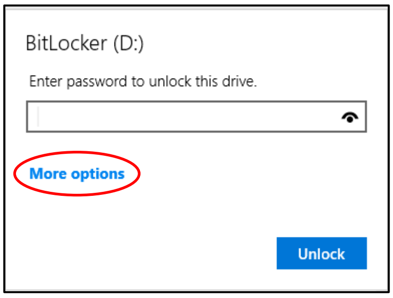
BitLocker Drive Encryption

Encryption has been paused

Drive D: 25.5% Completed

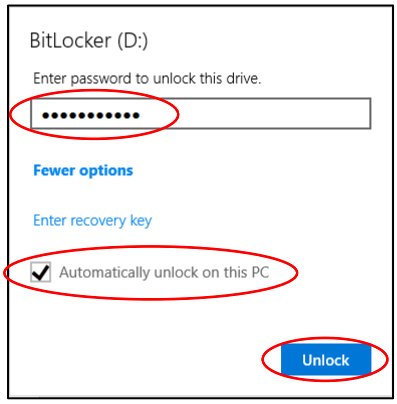
Pause encryption before removing the drive or files on the drive could be damaged.

10. 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*.



BitLocker (D:)

Enter password to unlock this drive.



BitLocker (D:)

Enter password to unlock this drive.

●●●●●●●●●●●

☑ Automatically unlock on this PC

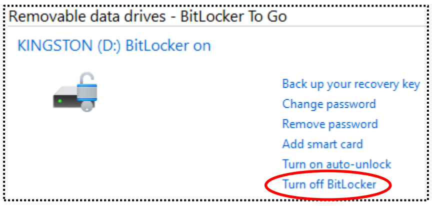
11. If the encryption was paused, you will now get to the same the window as shown in step 9 and you can click *Resume* to continue the encryption.

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.

2. Removing the encryption

With these steps you can remove the encryption you have set on the USB drive or stick.

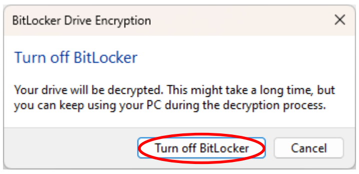
1. Open the Windows menu by clicking ⊞ and type *BitLocker*. Choose *Manage BitLocker*. Click *Turn off BitLocker* next to your USB disk or stick.



Removable data drives - BitLocker To Go

KINGSTON (D:) BitLocker on

2. Click Turn off BitLocker.

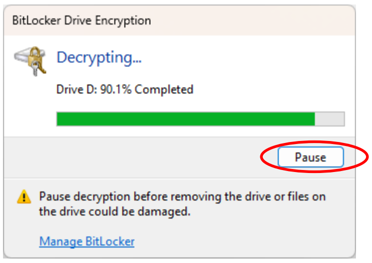


BitLocker Drive Encryption

Turn off BitLocker

Your drive will be decrypted. This might take a long time, but you can keep using your PC during the decryption process.

3. Wait for the decryption to finish. If you do not have now the time to wait for the encryption to finish and you want to continue it later, you can click *Pause*.



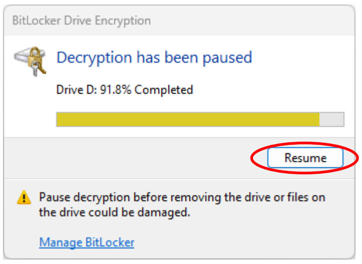
BitLocker Drive Encryption

Decrypting...

Drive D: 90.1% Completed

Pause decryption before removing the drive or files on the drive could be damaged.

4. If you clicked Pause, the decryption 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 decryption by clicking *Resume*.

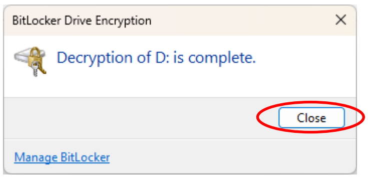


Decryption has been paused

Drive D: 91.8% Completed

Pause decryption before removing the drive or files on the drive could be damaged.

5. When the decryption is complete, the USB drive or stick is no longer encrypted and the files on it can be accessed without password. Click *Close*.



Decryption of D: is complete.