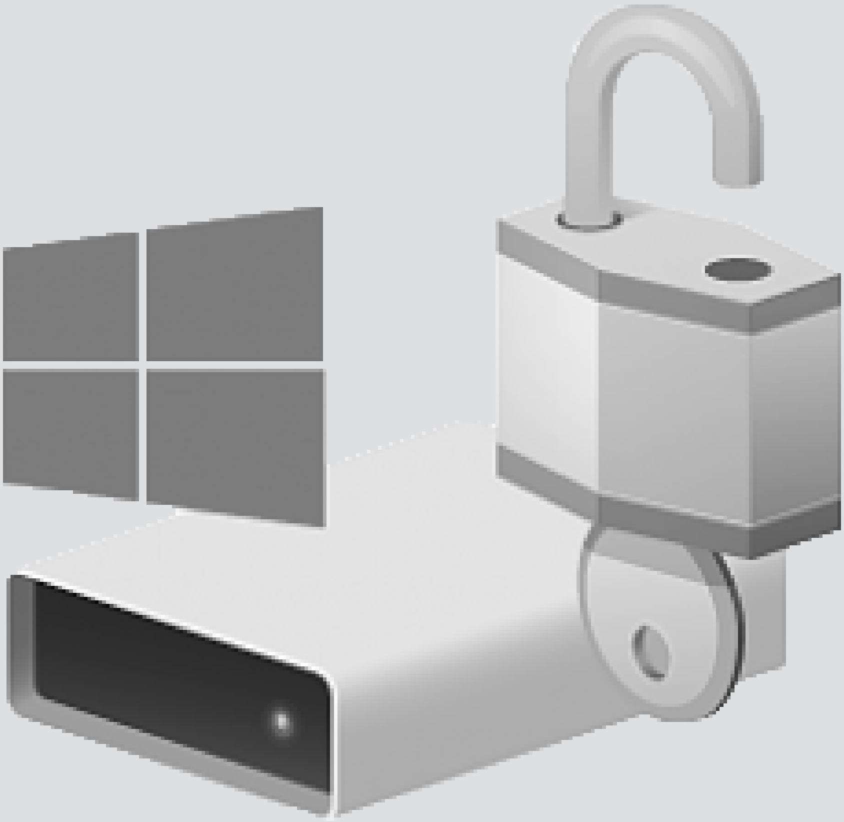
Windows



BitLocker external hard disk

For use by:	Students, Employees
Version:	1.1
Date:	26-11-2018
Owner:	ICT

TUDelft

(this page was intentionally left blank)

BitLocker on an external hard disk

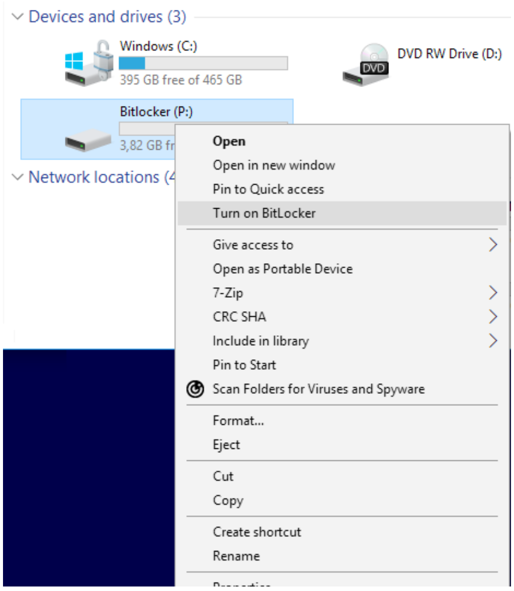
Before you begin

In this manual you can find the instructions to use BitLocker to protect your data on an external hard disk against theft. It is convenient if you have a USB-stick during the configuration.

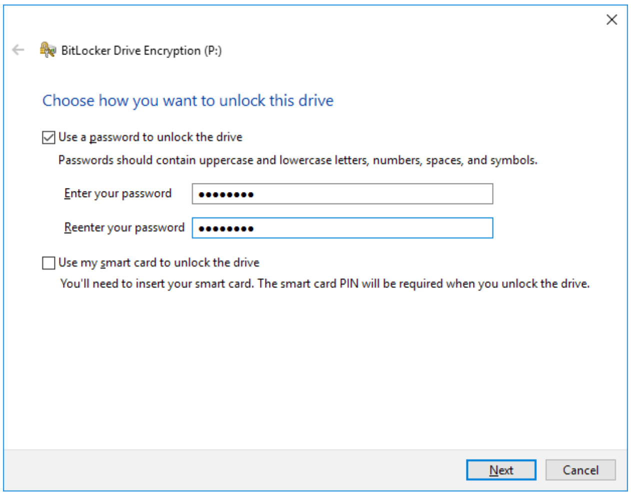
Securing our digital data is high on the agenda of the TU Delft. One of the most effective and user-friendly ways to do this, is by applying encryption on workstations (laptop/desktop). It increases the security level of your workstation and it has minimal impact for end-users.

Workstations managed by the TU Delft will be encrypted using central management. If you want to encrypt your workstation that is not managed by the TU Delft, you can do this manually. Read this instruction manual carefully and make sure you save your recovery key in a secure place where you can obtain it any time (e.g. secure cloud application such as Surfdrive). Do not save it on your local disk!

Step 1. Connect the external hard disk to the computer. Use the right mouse button to click on the external hard disk in the Windows Explorer and choose for the option "Turn on Bitlocker".



Step 2. The disk will be initialised, prior to creating a password to unlock the disk.



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 ••••••••

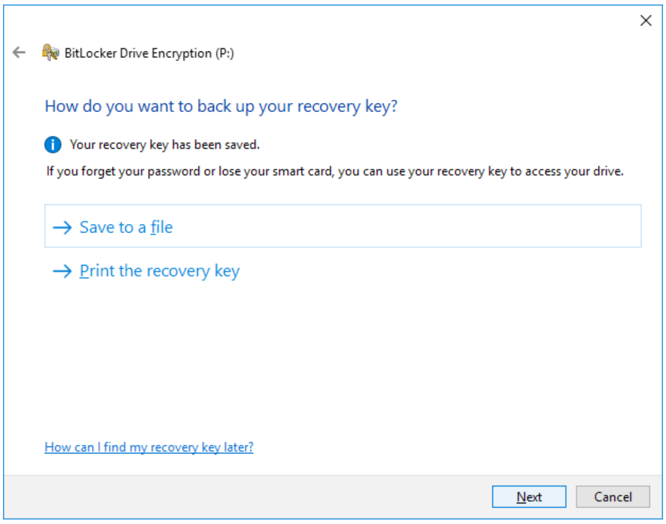
Reenter your password ••••••••

□ 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.

Step 3. Keep the recovery key in a safe place, like a USB-stick, or print it.

Using this recovery key, you are able to DECRYPT the data, without knowing the password.


BitLocker Drive Encryption (P:)

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.

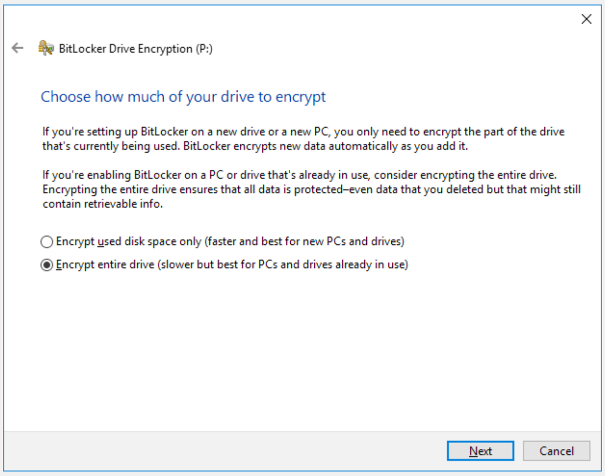
→ Save to a file
→ Print the recovery key
How can I find my recovery key later?
Next
Cancel

Step 4 is only necessary for Windows 10 users. Other users can continue with step 5.

Stap 4 is only necessary for Windows 10 users

Step 4.1. Windows 10 will ask if it should encrypt the whole disk or only the used disk space.

Choose to encrypt the whole disk.



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.

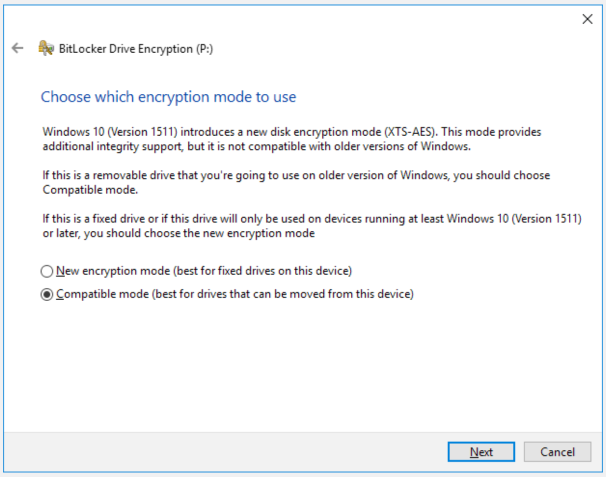
If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected–even data that you deleted but that might still contain retrievable info.

○ 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)

Step 4.2. When the disk will be used on Windows 7 systems, choose for the "Compatible mode".

If the disk only will be used on Windows 10 systems, "New encryption mode" will be a better option.



Choose 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.

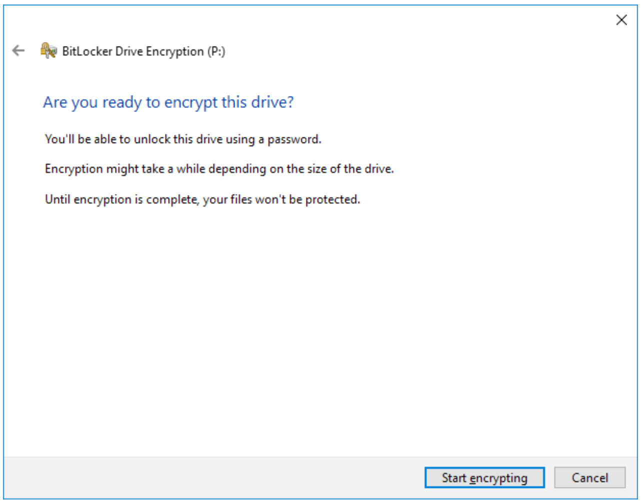
If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode

○ New encryption mode (best for fixed drives on this device)

● Compatible mode (best for drives that can be moved from this device)

Step 5. The external hard disk is ready to be encrypted.

After removing the disk, every time that the disk will be connected to this (or another) Windows-system, there will be asked for the chosen password.



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.