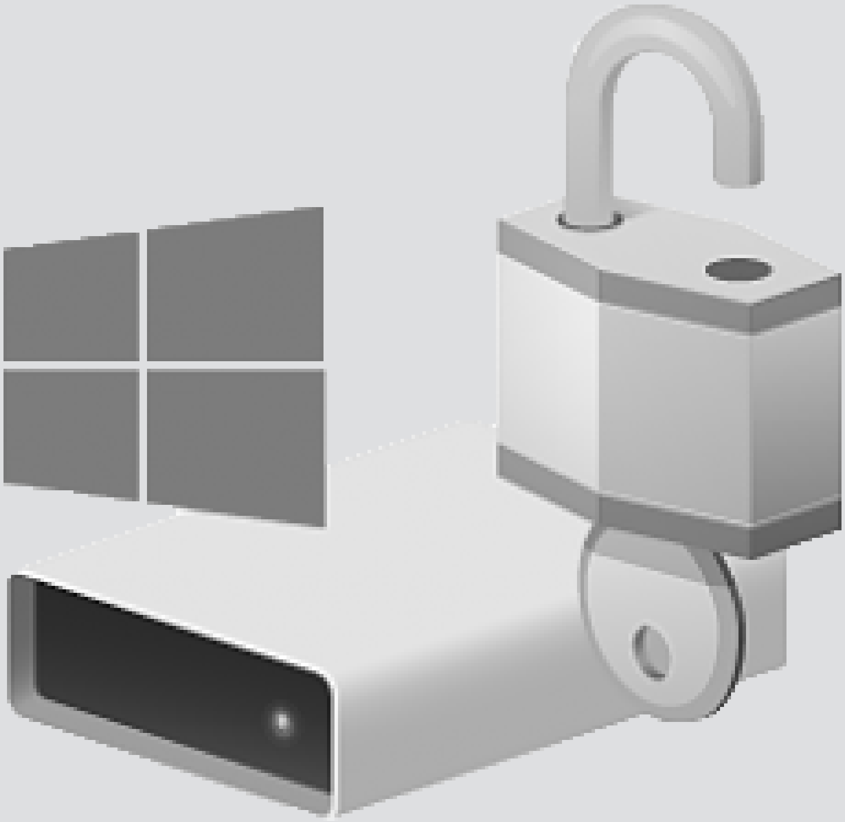
Windows



BitLocker internal 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 internal hard disk

Before you begin

In this manual you can find the instructions to use BitLocker to protect your data on your internal hard disk. To do this, you need :
- an admin account (for example: localadmin)
- a USB-stick.

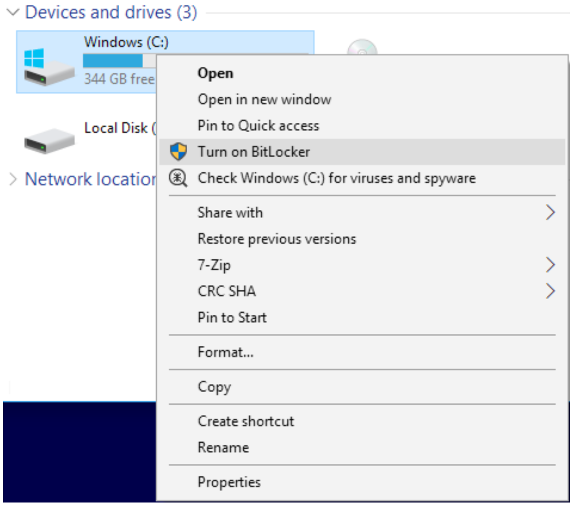
Securing our digital data is high on the agenda of the TU Delft. One of the most effective and user-friendly ways to do this, is by applying encryption on workstations (laptop/desktop). It increases the security level of your workstation and it has minimal impact for end-users.

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. Login with your NetID and open Windows Explorer.

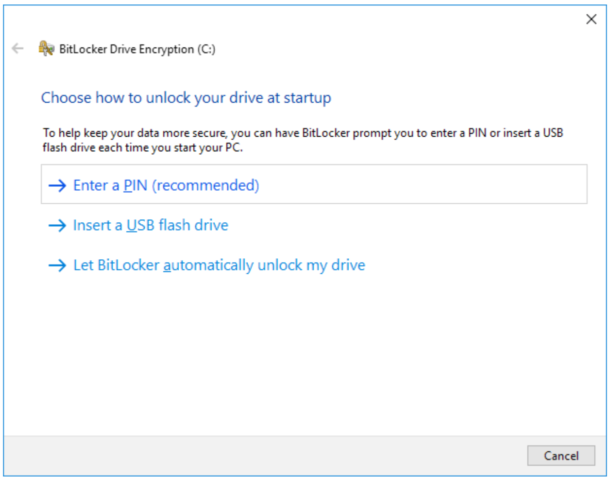
Use the right mouse button to click on the C-disk and choose the option "Turn on Bitlocker".

After filling in the admin credentials, the ability of the system is checked.



Step 2. To protect the system in a proper way, it is advised to use a PIN-code on laptops. The PIN-code will be asked prior to starting up Windows.

In some cases it may be more convenient to use no PIN-code, choose in those cases for "Let BitLocker automatically unlock my drive". (E.g. when different persons use the same desktop)



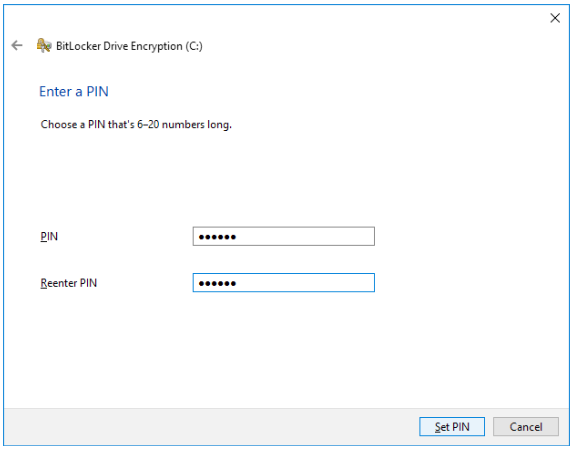
BitLocker Drive Encryption (C:)

Choose how to unlock your drive at startup

To help keep your data more secure, you can have BitLocker prompt you to enter a PIN or insert a USB flash drive each time you start your PC.

→ Enter a PIN (recommended)
→ Insert a USB flash drive
→ Let BitLocker automatically unlock my drive
Cancel

Step 3. Fill in a PIN-code (6-20 numbers).



BitLocker Drive Encryption (C:)

Enter a PIN

Choose a PIN that's 6–20 numbers long.

PIN ••••••

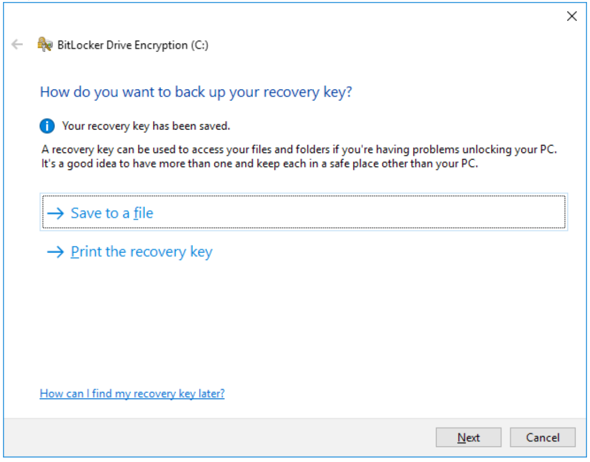
Reenter PIN ••••••

Step 4. The system will ask where it can save the recovery-key. Use a USB-stick for this.

The data can be decrypted with this recovery key when the password is unknown.

Keep the recovery key in a safe place, but not on or near your computer!

Tip: The key will be saved in a text file, this can be printed.



BitLocker Drive Encryption (C:)

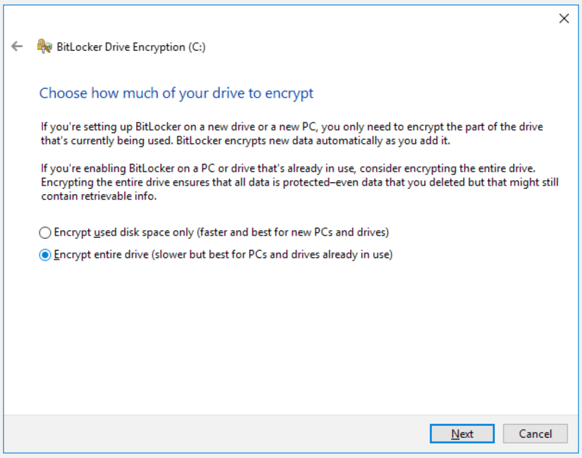
How do you want to back up your recovery key?

Your recovery key has been saved.

A recovery key can be used to access your files and folders if you're having problems unlocking your PC. It's a good idea to have more than one and keep each in a safe place other than your PC.

Step 5 is only necessary for Windows 10 users

Step 5.1. Windows 10 will ask if it should encrypt the whole disk or only the used space on the disk. Choose to encrypt the whole disk.



Choose how much of your drive to encrypt

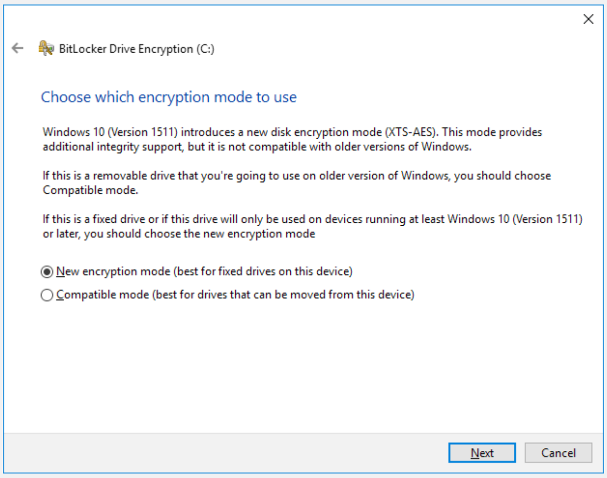
If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

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 5.2. Choose for "New encryption mode".



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.

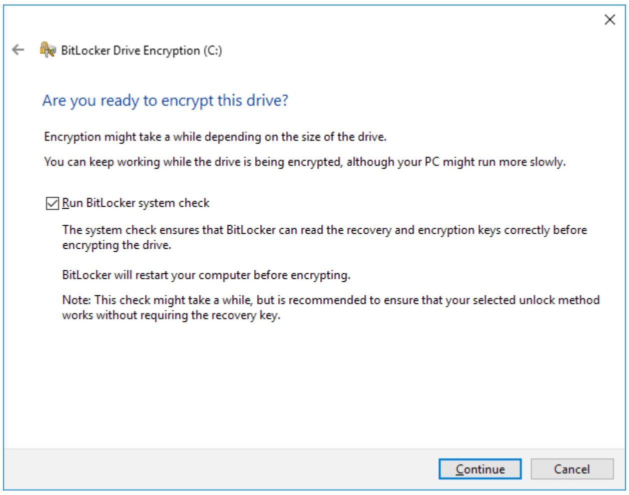
If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

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 6. Check the box of "Run BitLocker system check".



Are you ready to encrypt this drive?

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

You can keep working while the drive is being encrypted, although your PC might run more slowly.

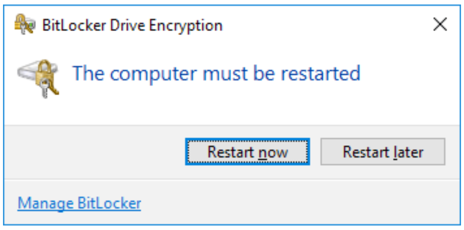
☑ Run BitLocker system check

The system check ensures that BitLocker can read the recovery and encryption keys correctly before encrypting the drive.

BitLocker will restart your computer before encrypting.

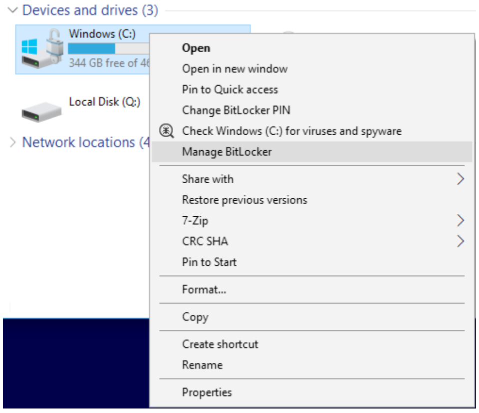
Note: This check might take a while, but is recommended to ensure that your selected unlock method works without requiring the recovery key.

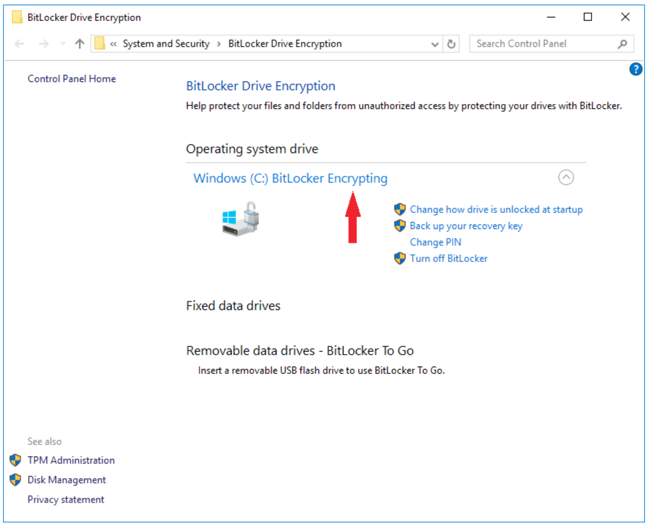
Step 7. The system requires a restart to start the encryption.



The computer must be restarted

Step 8. Windows will encrypt the C-disk after the restart (use the created PIN-code). This can take some time, depending on the type and size of the disk.
The system can be used and be restarted, but may react slower than normally.
When the encryption is finished, the system will react normally again.




BitLocker Drive Encryption
« System and Security › BitLocker Drive Encryption
Search Control Panel
Control Panel Home
Change how drive is unlocked at startup
Back up your recovery key
Change PIN
Turn off BitLocker
See also
TPM Administration
Disk Management
Privacy statement

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

Windows (C:) BitLocker Encrypting

Fixed data drives

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.