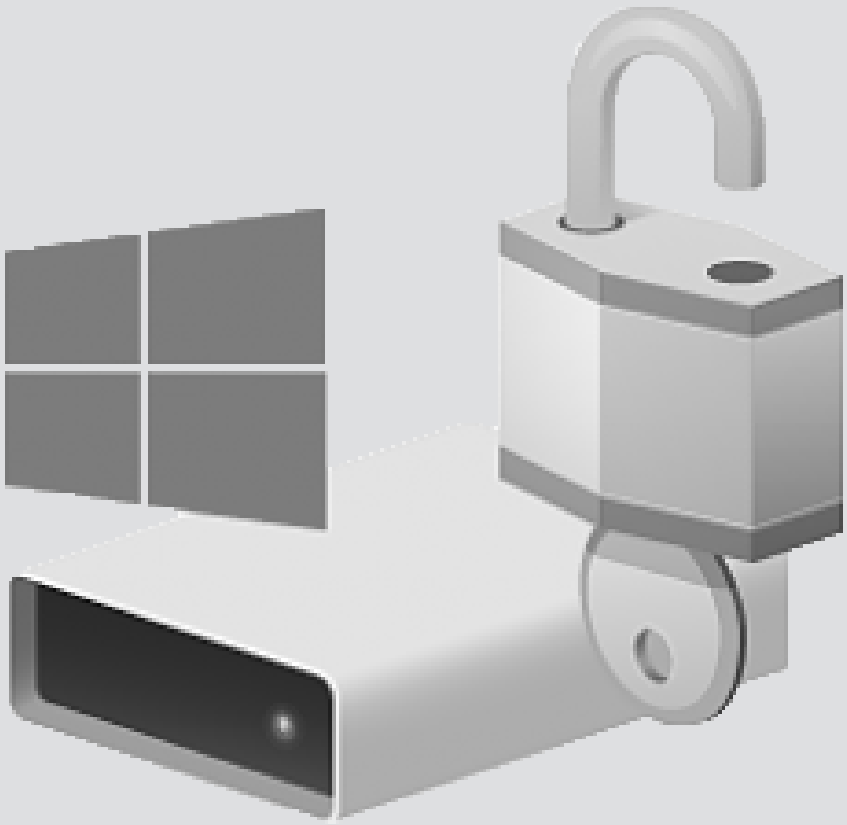
Windows



BitLocker interne harde schijf

For use by:	Students, Employees
Version:	1.1
Date:	01-12-2018
Owner:	ICT

TUDelft

(this page was intentionally left blank)

BitLocker op een interne harde schijf

Voordat je begint

In deze handleiding zijn de instructies te vinden om BitLocker te gebruiken om de data op een interne harde schijf beter te beschermen tegen diefstal. Om dit te doen moet je de beschikking hebben over:
- een admin account (bijvoorbeeld localadmin)
- een USB-stick.

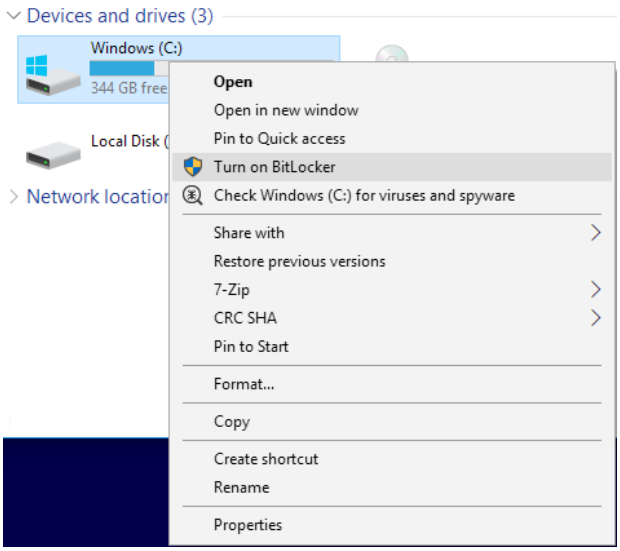
Het beschermen van digitale informatie heeft een hoge prioriteit bij de TU Delft. Een van de meest effectieve en gebruiksvriendelijke manieren om dit te doen, is door jouw werkplek (laptop of desktop) te encrypten. Dit verhoogt het beveilingsniveau van jouw werkplek en het heeft een minimale impact op jou als gebruiker.

De TU Delft draagt er zorg voor dat de door de TU Delft beheerde werkplekken encrypt worden. Als je je eigen werkplek, die niet beheerd wordt door de TU Delft, wilt encrypten kan je dit zelf handmatig uitvoeren. Lees deze handleiding rustig door en wees er zeker van dat je herstelsleutel op een veilige plek is opgeslagen, waar je op elk moment van de dag bij kan (bijvoorbeeld in een beveiligde cloud applicatie zoals Surfdrive). Sla de herstelsleutel niet op op je lokale schijf!

Stap 1. Login met je NetID en open de Windows Verkenner.

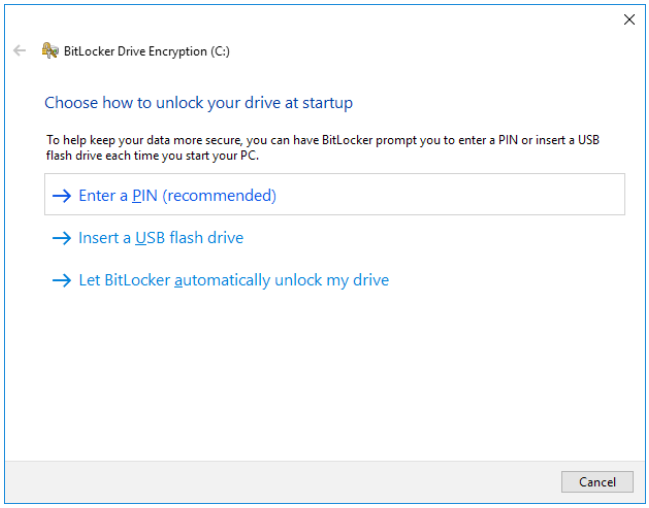
Klik met de rechter muisknop op de C-schijf en kies voor de optie “Turn on Bitlocker”.

Na invoeren van het admin-account wordt de geschiktheid van het systeem gecontroleerd.

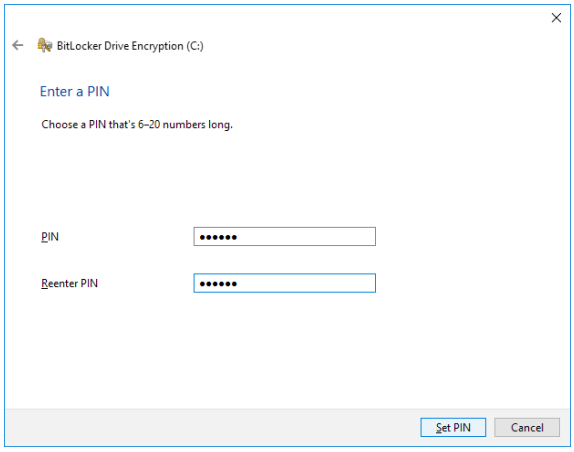


Stap 2. Om het systeem goed te beveiligen, wordt geadviseerd om een PIN-code te gebruiken op laptops. Voorafgaand aan het opstarten van Windows wordt hierom gevraagd.

Bij een desktop-systeem kan het handiger zijn om geen PIN-code in te stellen, kies dan voor “Let BitLocker automatically unlock my drive”. (Bijvoorbeeld wanneer verschillende personen het systeem gebruiken/ opstarten)



Stap 3. Voer een PIN-code in (6-20 cijfers).

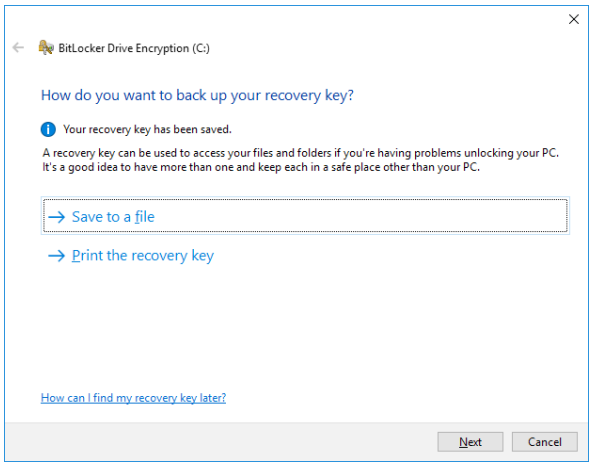


Stap 4. Het systeem vraagt waar de recovery-key kan worden opgeslagen. Gebruik hiervoor de USB-stick.

Met deze recovery key kan de data ontsleuteld worden wanneer het wachtwoord niet bekend is.

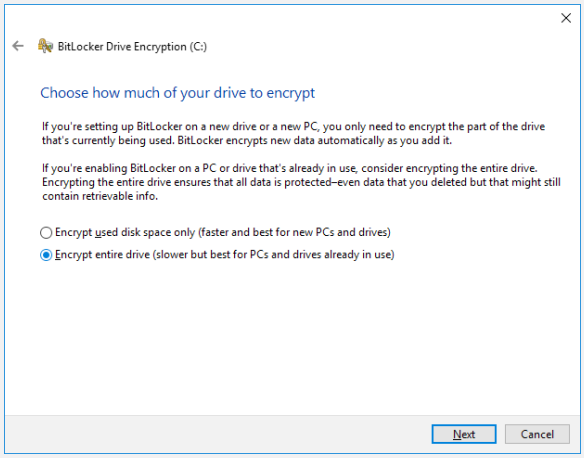
Bewaar deze recovery key goed, maar niet bij de computer!

Tip: De key wordt opgeslagen in een tekstbestand, deze kan eventueel ook worden geprint.

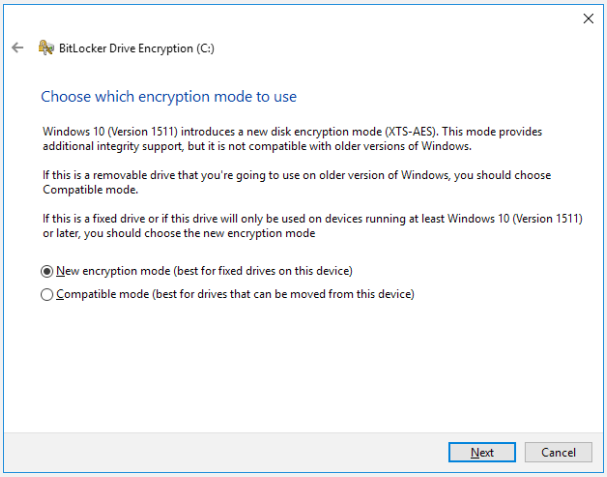


Stap 5 is alleen nodig voor Windows 10 gebruikers

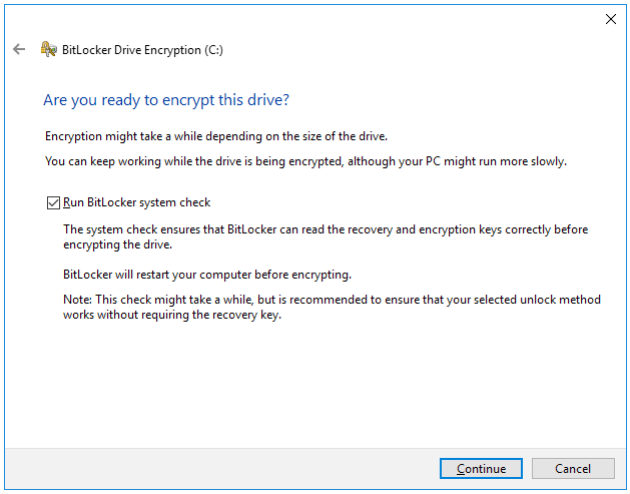
Stap 5.1. Windows 10 vraagt of de hele disk of alleen de gebruikte ruimte op de disk versleuteld moet worden. Kies hier voor het versleutelen van de hele disk.



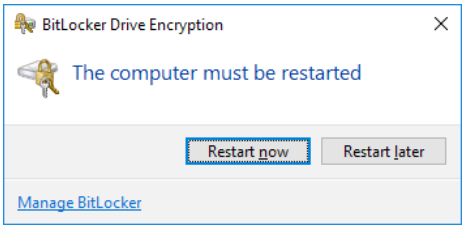
Stap 5.2. Kies voor "New encryption mode".



Stap 6. Zet het vinkje aan bij "Run BitLocker system check".



Stap 7. Het systeem geeft aan dat een herstart nodig is om de encryptie te starten.



Stap 8. Na een herstart (voer de aangemaakte PIN-code in) zal Windows de C-schijf gaan versleutelen. Dit kan afhankelijk van het soort en de omvang van de harde schijf enige tijd duren.
Het systeem kan gewoon gebruikt en herstart worden, maar kan trager reageren dan anders.

Wanneer de versleuteling klaar is, reageert het systeem weer normaal.