

Windows: Externe USB drive versleutelen

Om te voorkomen dat belangrijke of persoonlijke gegevens op uw USB-drive in verkeerde handen vallen, kunt u de bestanden eenvoudig versleutelen met een wachtwoord. Windows, macOS en Linux hebben daarvoor een ingebouwde encryptiefunctie. Deze ingebouwde encryptie werkt op alle computers met hetzelfde besturingssysteem. Na de versleuteling kan alleen degene die over het juiste wachtwoord beschikt de gegevens lezen en bewerken. Deze quick reference beschrijft hoe u encryptie instelt onder Windows.

LET OP: Het ISSC kan u niet helpen met ontsleutelen van uw bestanden als u het wachtwoord bent vergeten.

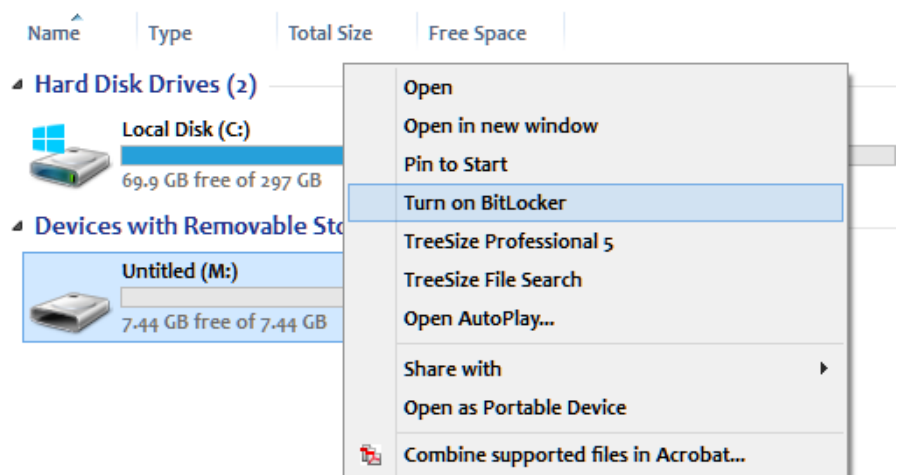
Microsoft Windows BitLocker

BitLocker is de in Windows ingebouwde versleutelingssoftware. De software is beschikbaar op de ISSC Windows werkplek en Windows Pro, Ultimate, Enterprise of Education versies sinds 2010.

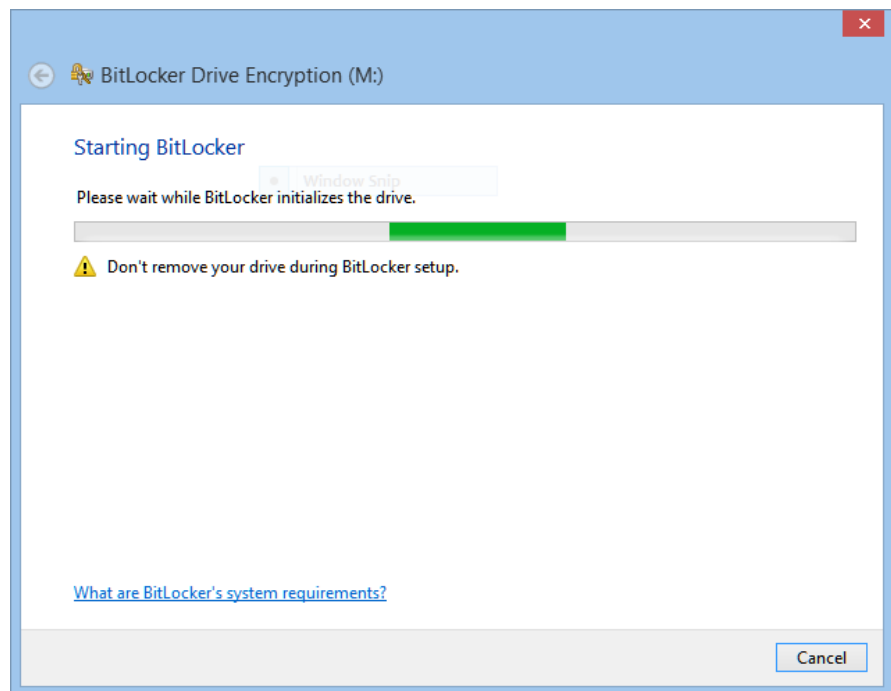
Een USB-drive die met BitLocker werd gecodeerd is ook te lezen op computers met een Home versie van Windows 7, 8, 8.1 of 10. Oudere Windows versies kunnen een BitLocker gecodeerde USB drive ook lezen met BitLocker to Go (<https://support.microsoft.com/en-us/kb/970401>).

Deze uitleg gebruikt schermafbeeldingen uit de Engelstalige Windows 8, maar onder andere Windows versies werkt het op soortgelijke manier.

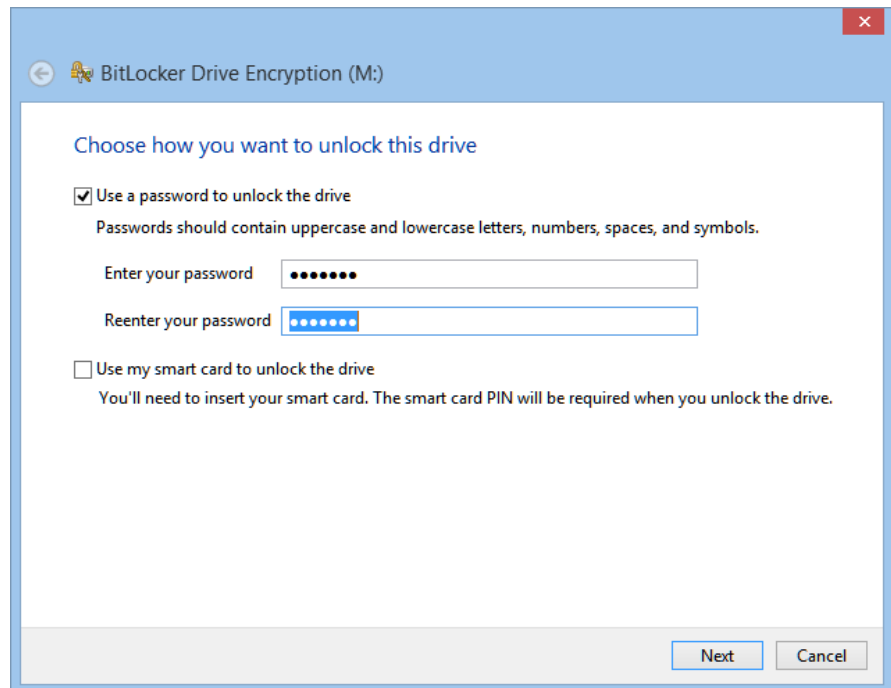
1. Sluit de USB-drive op de computer aan, zoek de afbeelding op in de Windows verkenner en klik daar op met de rechter muisknop. Er verschijnt een popup menu; kies daarin voor 'Turn on BitLocker'.



Het BitLocker venster verschijnt:

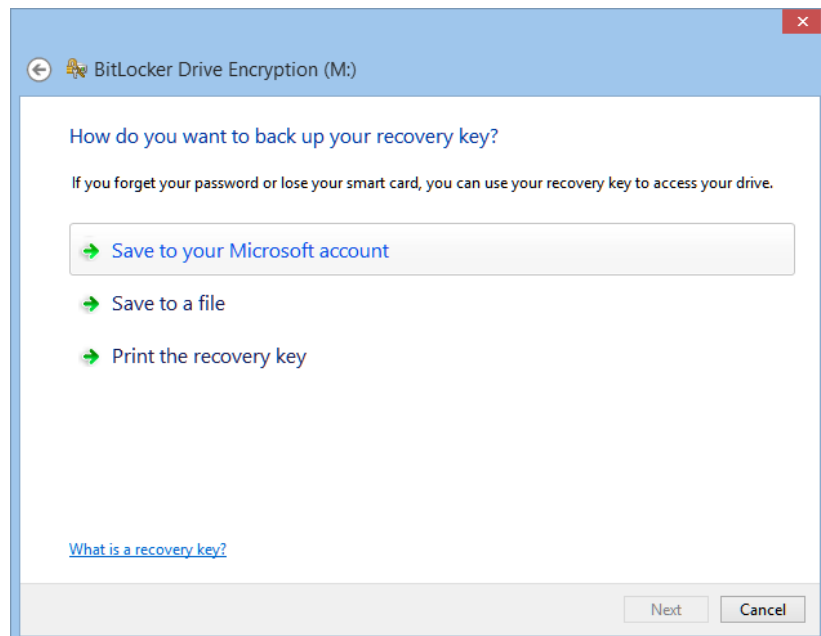


2. U kunt vervolgens aangeven wat de bedoeling is. In dit voorbeeld is dat 'password protection'.



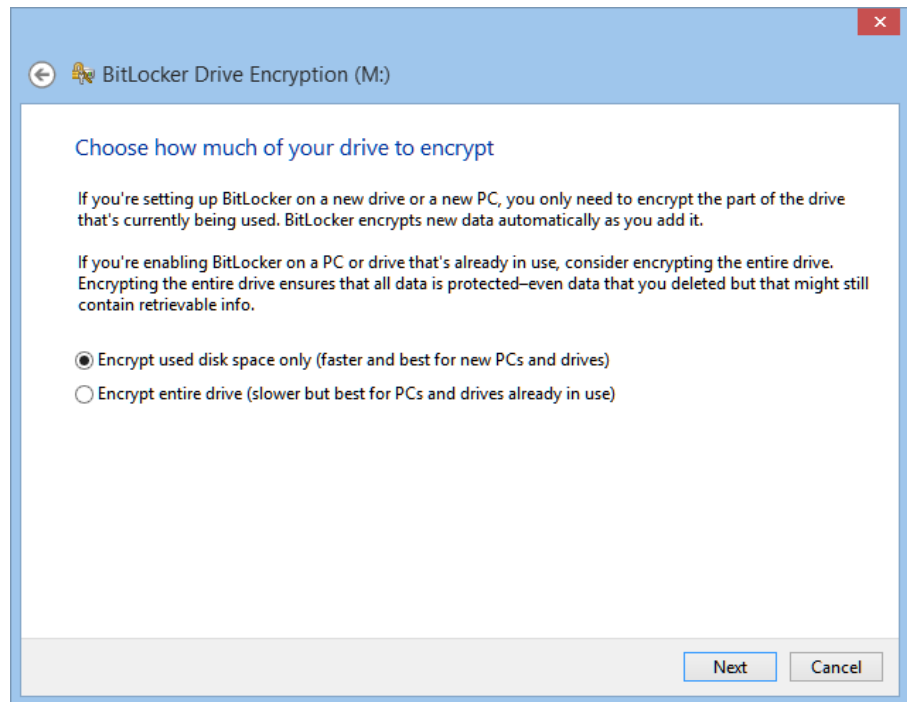
LET OP: Het wachtwoord moet een hoofdletter, een kleine letter en een cijfer bevatten.

3. Klik Next als u gereed bent. Dan verschijnt het volgende:

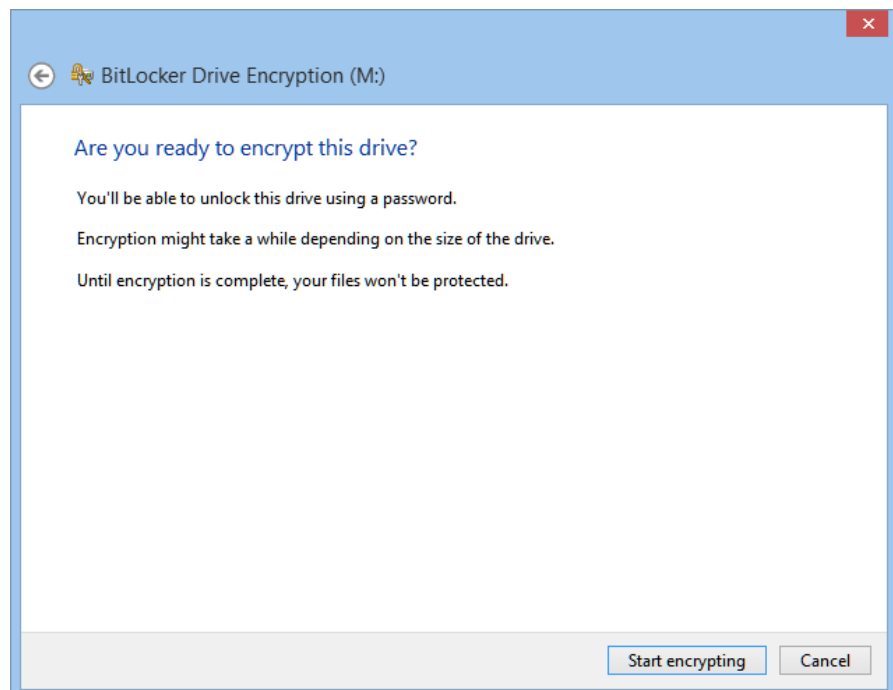


BitLocker vraagt u om een reservesleutel te bewaren, die u kunt gebruiken als u het wachtwoord zou vergeten. Bewaar de reservesleutel in uw Microsoft account, sla het op in een bestand

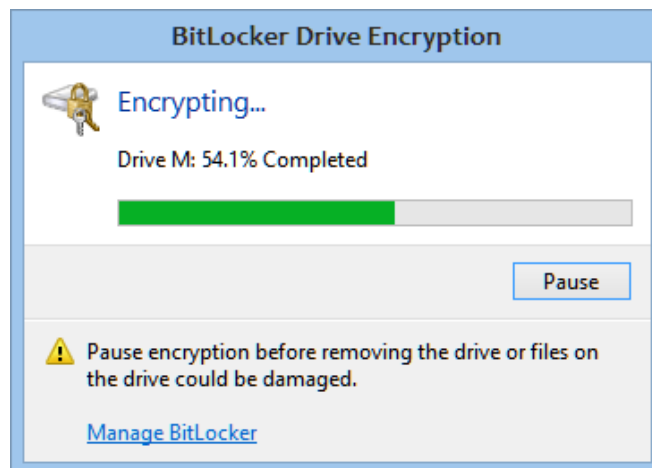
(niet op de USB drive!) of druk het af. Daarna bent u gereed voor encryptie:



In het geval van een externe USB-drive raden we aan deze in zijn geheel te coderen via de onderste optie: *Encrypt entire drive*.

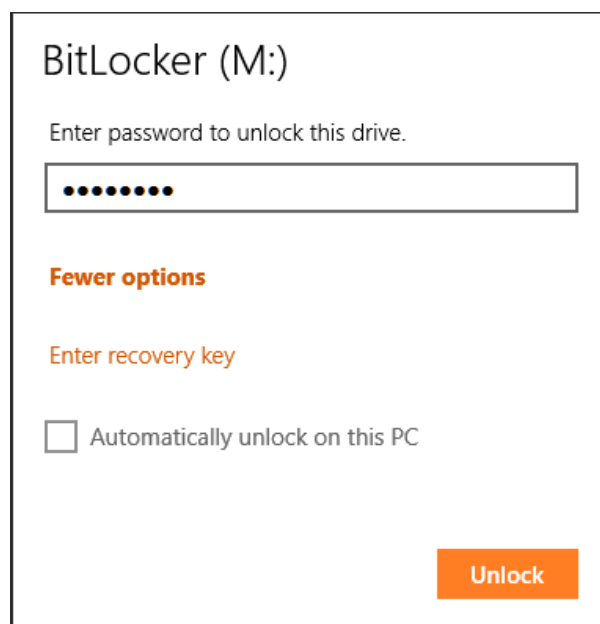


Bitlocker geeft een korte samenvatting, waarna u de encryptie kunt starten (of alsnog afbreken).

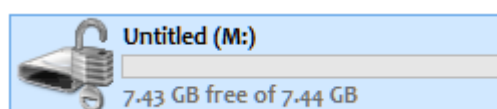


De snelheid van coderen hangt af van de omvang van de USB-drive. Een 8GB drive duurt ongeveer twee minuten om te coderen.

Als u nu de USB-drive verwijderd en weer opnieuw aansluit, zal bitlocker uw wachtwoord vragen (of kies voor de reservesleutel *Enter recovery key*, als u het wachtwoord vergat). Kruis eventueel *Automatically unlock on this PC* aan om te zorgen dat u op deze computer voor deze USB-drive niet meer het wachtwoord hoeft in te voeren.



Als de drive beschikbaar is, ziet dat er als volgt uit:



Om de versleuteling van de USB-drive op te heffen, klikt u met de rechter muisknop op de drive afbeelding en kiest u voor *Manage Bitlocker*. Daarmee opent u een venster waarin u onder meer kunt kiezen voor *Remove password from this drive*.

Multi platform encryptie software

Als de meegeleverde encryptie software voor u niet goed werkt of u heeft encryptie voor meerder besturingssystemen nodig, dan kunt u een van deze tools overwegen:

- <https://www.veracrypt.fr/en/Home.html>
Deze gratis open source encryptie tool vervangt het eerder populaire TrueCrypt en is beschikbaar voor Windows, macOS en Linux.
LET OP: Op een standaard Windows werkplek kunt u Veracrypt laten installeren via het formulier '[Aanvraag software](#)'.
- <https://www.axcrypt.net/>
Deze encryptie tool staat bekend om de intuïtieve gebruikersinterface en beschikbaarheid voor Windows, macOS, iOS en Android.
- <https://www.boxcryptor.com/en/boxcryptor-portable-download>
Een commercieel encryptie tool met een gratis versie voor lokale, portable installation (Windows, macOS, Linux) op één of twee USB-drives.

Zelf kunt u VeraCrypt, Axcrypt of BoxCryptor installeren op een PC waarop u zelf beheerder bent. (Dit betekent dat u deze programma's niet kunt installeren op een standaard Mac of Linux werkplek.)

Deze Quick reference is een aangepaste en vertaalde tekst van:

- een on line handleiding van Syracuse University:

<https://answers.syr.edu/x/HIOoAQ>.