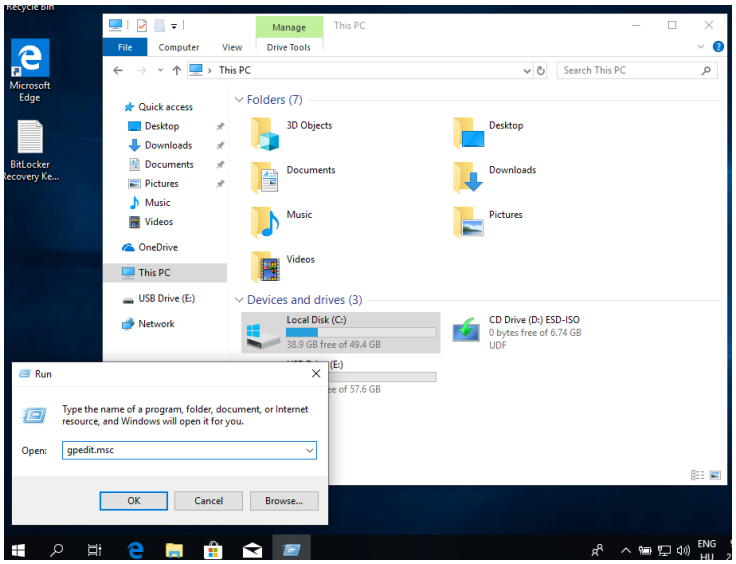
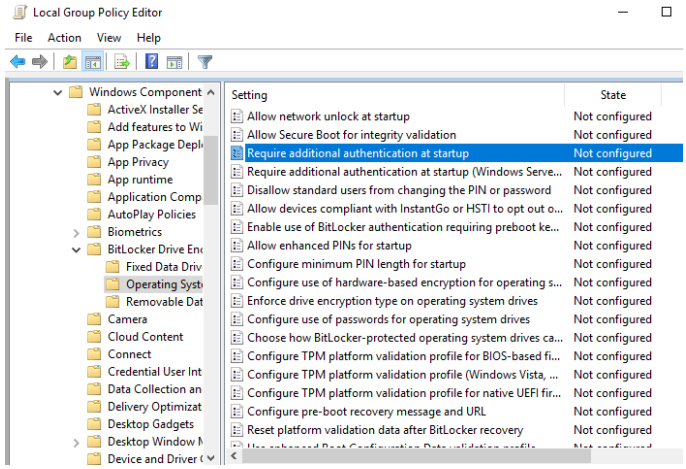
Adatok titkosítása

Rendszerlemez titkosítása BitLocker segítségével

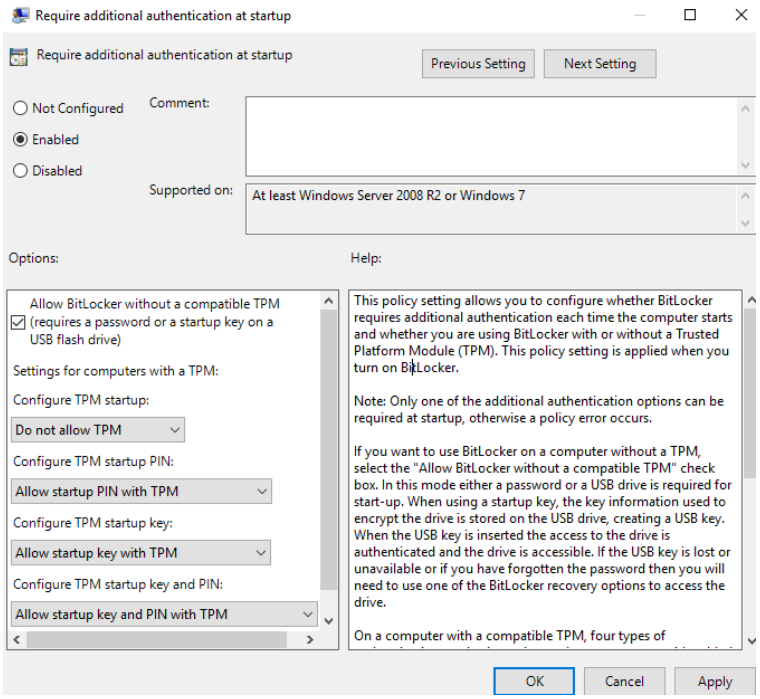
1. Telepítse fel a Windows 10 pro verzióját. A telepítés közben törölje a meglévő partíciókat, majd az üres diszket válassza ki a telepítésre.
2. A titkosítás során nem használunk TPM-et, ezért annak kötelező használatát ki kell kapcsolni a következő módon:
   a. A telepítés után belépve indítsa el a Group Policy Editort a gpedit.msc segítségével.



   b. Az editorban keresse meg a „Computer Configuration \ Administrative Templates \ Windows Components \ Bit Locker Drive Encryption \ Operating System Drives” pontot.

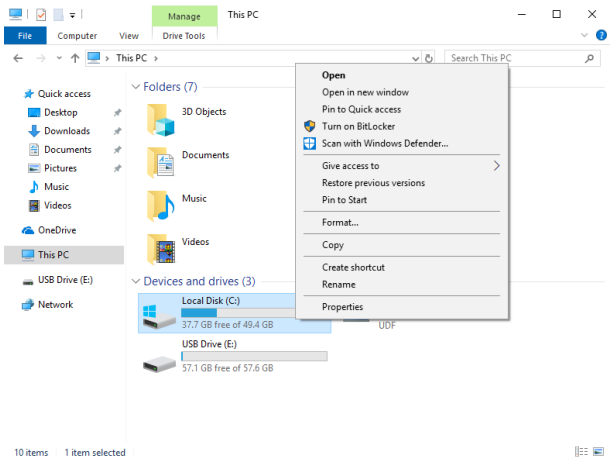


   c. Állítsa „Enabled”-re a „Require additional authentication at startup”-ot.
   Kapcsolja be az „Allow BitLocker without a compatible TPM”-et.
   A „Configure TPM startup:” pontban válassza ki a „Do not allow TPM”-et!



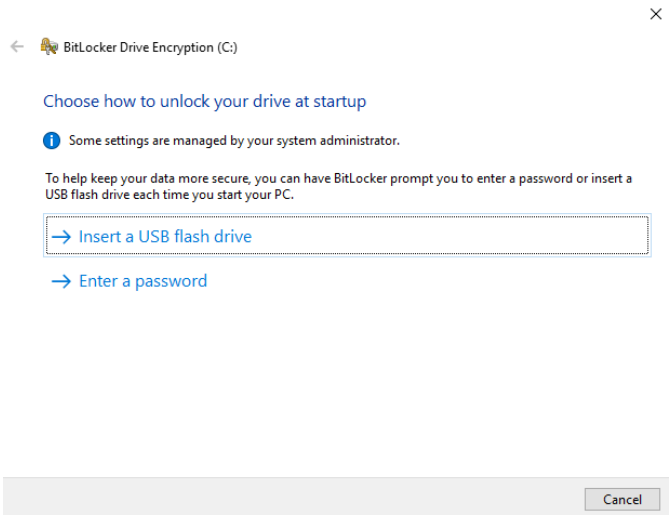
d. Tanulmányozza át a lehetséges beállításokat.

3. BitLocker segítségével titkosítsa le a rendszerlemezt:
   a. Jobb gomb a rendszerköteten, majd „Turn on BitLocker”.



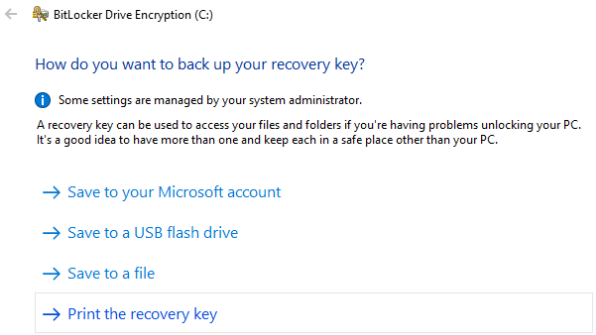
   b. Indítsa el a BitLocker-t.

   c. Válassza ki a kívánt indításkori hitelesítési módot!



d. „USB flash drive” esetén csatlakoztassa a pendriveot, és válassza ki!

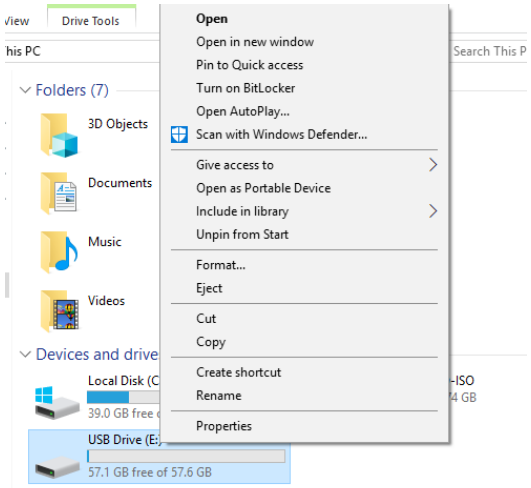
e. Nyomtassa ki egy PDF állományba a visszaállítási kulcsot! (Próbálja meg pendrivera is lementeni!)



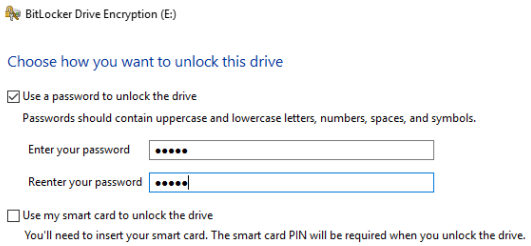
f. Értelemszerűen haladjon tovább.
g. Ha végzett, indítsa újra számítógépét, figyelje meg a rendszerindítás folyamatát, belépés után tanulmányozza a pendrive tartalmát.
h. Kapcsolja ki a rendszerlemez titkosítását!

Pendrive titkosítása BitLocker To Go segítségével

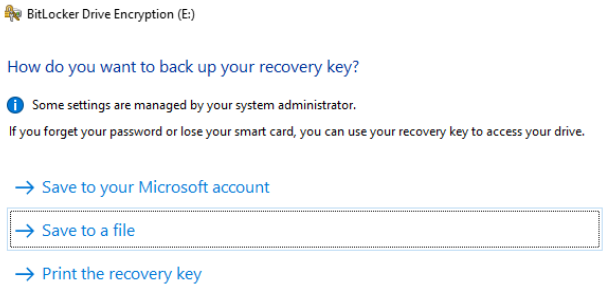
1. Egy üres pendrivera másoljon fel néhány tetszőlegesen kiválasztott állományt.
2. Válassza ki a pendriveot, majd jobb klikk és „Turn on BitLocker”!



3. A BitLocker To Go segítségével titkosítsa le a pendrive tartalmát (jelszó használatával)!



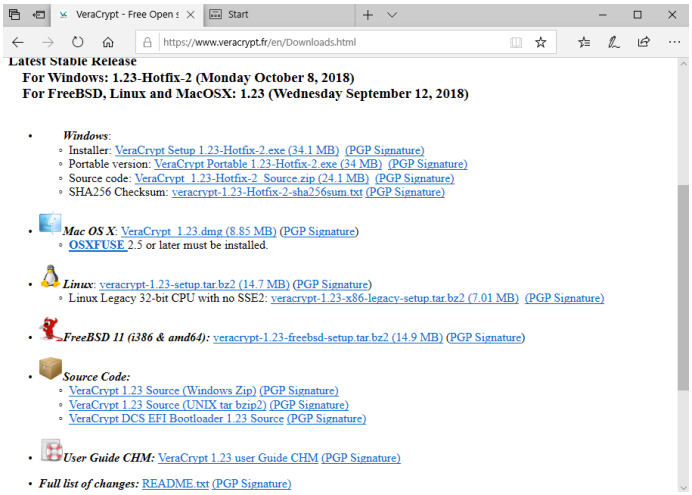
4. A helyreállítási kulcsot mentse le az asztalra!



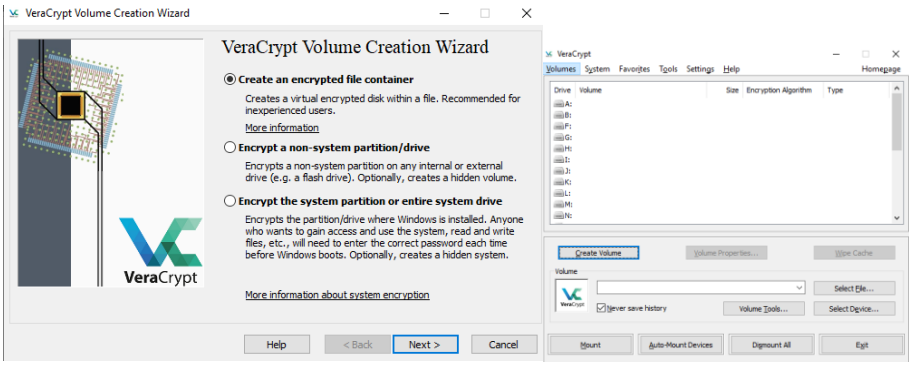
5. Ha elkészült a titkosítás, távolítsa el a pendriveot.
6. Csatlakoztassa újra a pendriveot, eközben figyelje meg a rendszer viselkedését.
7. Nézze meg, hogy a pendriveon megtalálhatóak-e a felmásolt állományok.
8. Próbálja ki szomszédjával is az ő számítógépén a pendrive működését.
9. Lépjen ki „Command prompt”-ba.
10. A `manage-bde -status` parancs segítségével kérdezze le a titkosított diszkek állapotát, és a titkosítás módját.
11. Sikerült a lekérdezés? Ha nem, oldja meg a problémát.
12. Szüntesse meg a pendrive titkosítását!

Titkosított konténer létrehozása VeraCrypt segítségével

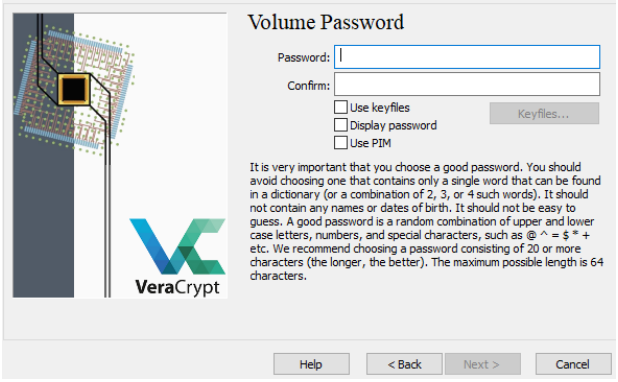
1. Töltse le a VeraCrpyt legfrissebb verzióját a https://www.veracrypt.fr oldalról.



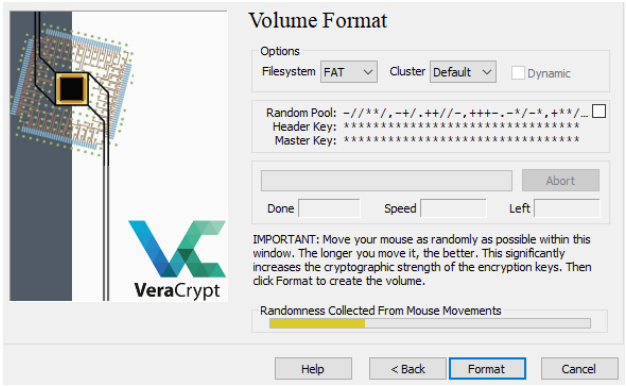
2. Telepítse a letöltött programot.
3. Indítsa el a feltelepített programot Administratorként.
4. Klikklejen a „Create Volume” gombra, majd tanulmányozza a felkínált lehetőségeket.



5. Válassza a „Create an encrypted file container” menüpontot, majd „Next”.
6. Tanulmányozza a felkínált lehetőségeket.
7. Válassza a „Standard VeraCrypt volume” menüpontot, majd „Next”.
8. Válasszon tetszőleges nevet a container részére, és a pendriveon helyezze el.
9. Tanulmányozza a felkínált titkosítási algoritmusokat (leírásukkal együtt).
10. Tanulmányozza a felkínált hash algoritmusokat.
11. Válassza ki az „AES” titkosítást, majd „Next”.
12. Méretnek 1GB-t állítson be, majd „Next”.
13. Válasszon jelszót!



14. Az egér mozgatásával segítse a véletlenszámgenerálás folyamatát, majd „Format”!



15. Figyelje meg a titkosítás sebességét.
16. Tallózza ki a létrehozott Containert tartalmazó állományt, majd a „Mount” gomb segítségével csatolja fel azt tetszőleges meghajtónak.
17. A „Volume Properties…” gomb segítségével tanulmányozza a meghajtó titkosítását.
18. „Dismount All” segítségével csatoljon le minden titkosított Containert.