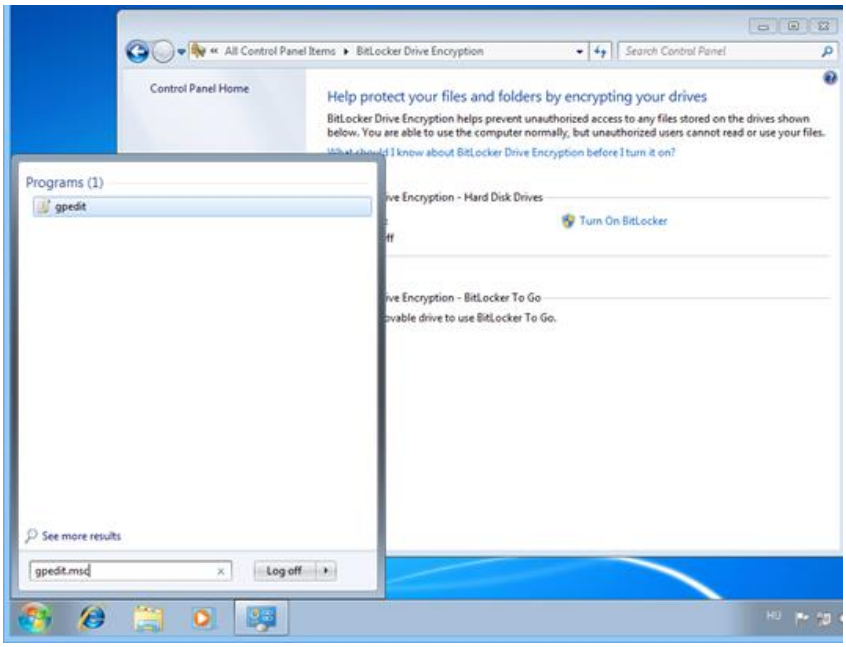
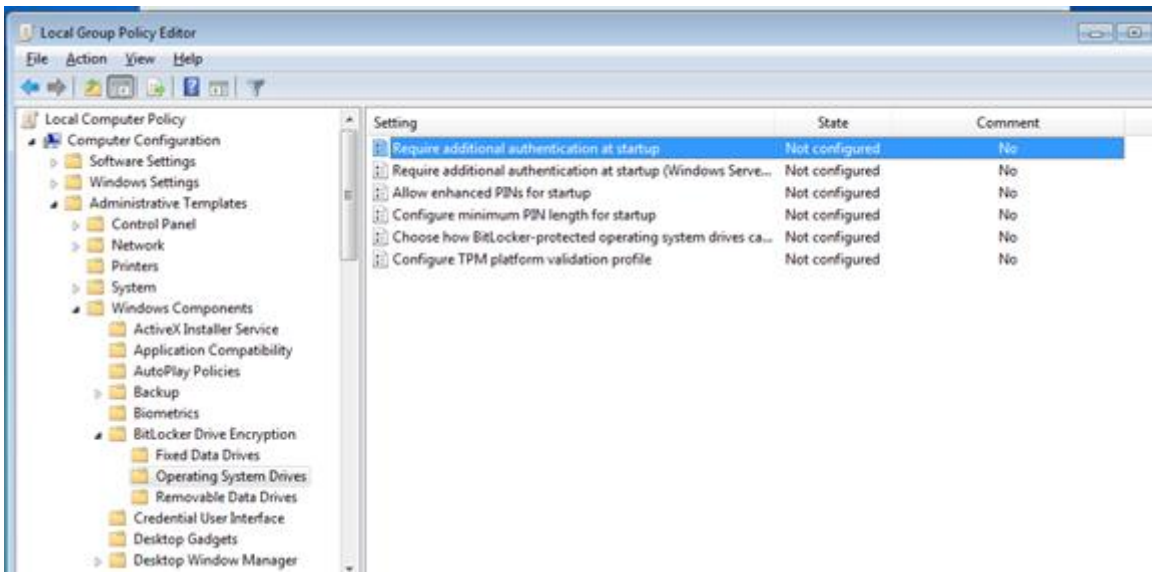
Adatok titkosítása

Rendszerlemez titkosítása BitLocker segítségével

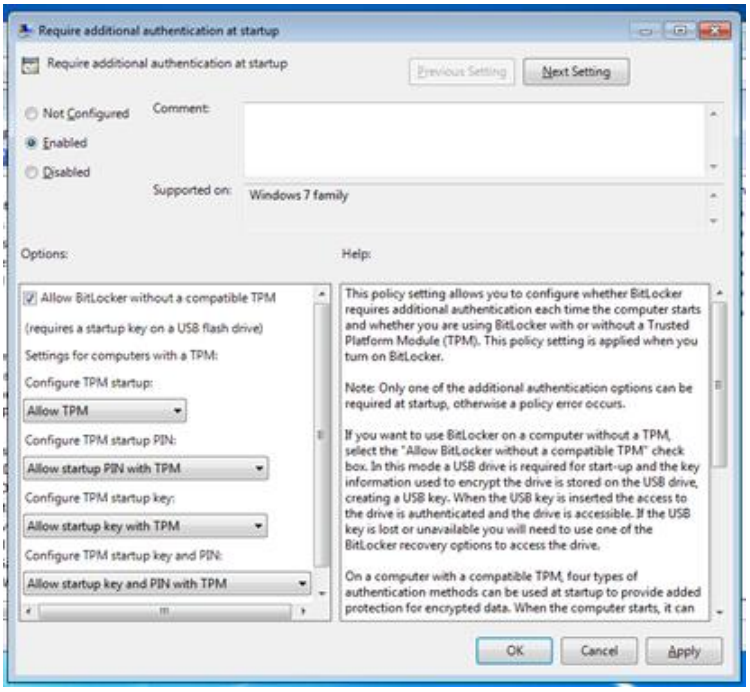
1. Telepítse fel a Windows 7 Enterprise verzióját. A telepítés közben törölje a meglévő partíciókat, majd az üres diszket válassza ki a telepítésre.
2. A titkosítás során nem használunk TPM-et, ezért annak kötelező használatát ki kell kapcsolni a következő módon:
   a. A telepítés után belépve indítsa el a Group Policy Editort a gpedit.msc begépelésével.



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

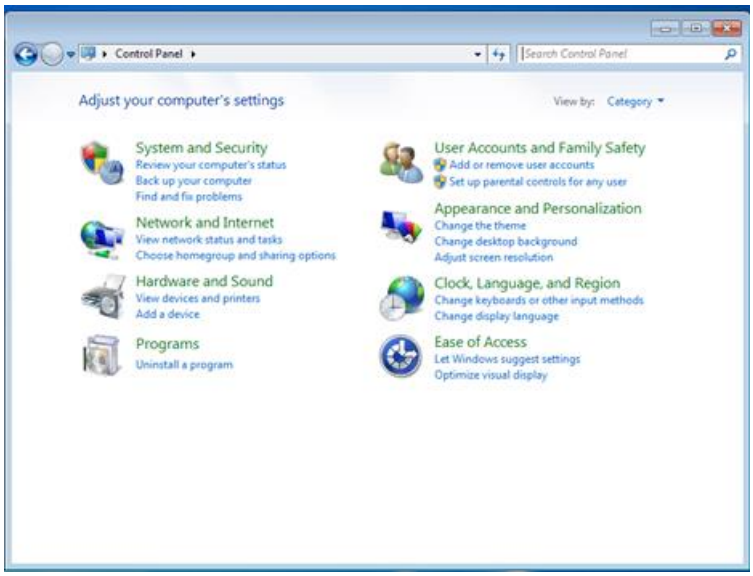


c. Állítsa „Enabled”-re a „Require additional authentication at startup”-ot.

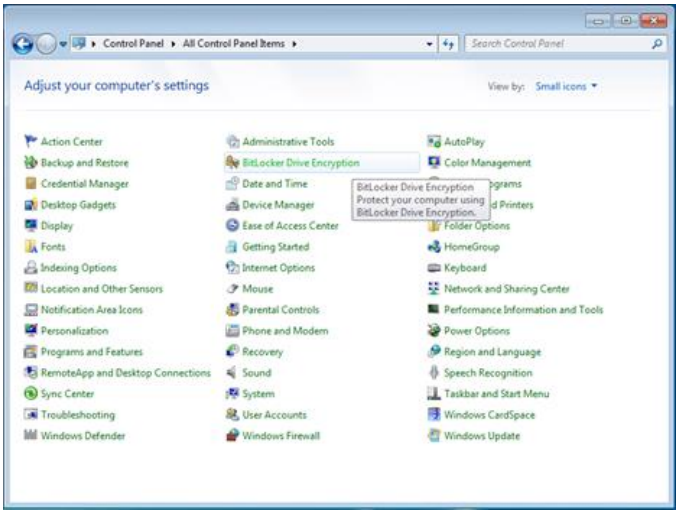


d. Tanulmányozza át a lehetséges beállításokat.

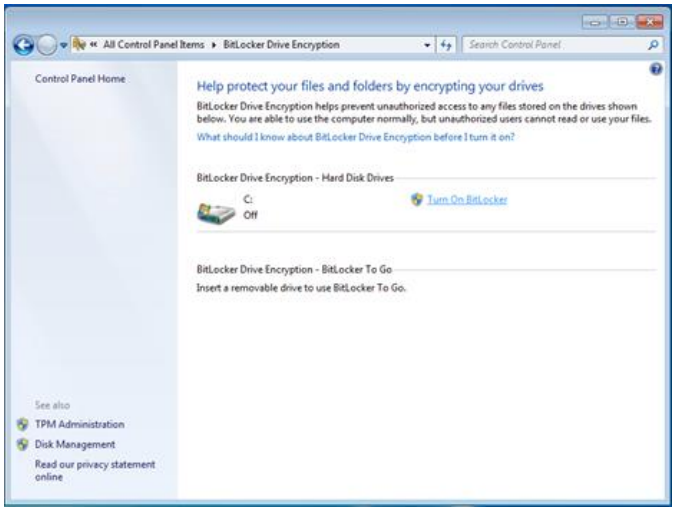
3. BitLocker segítségével titkosítsa le a rendszerlemezt:
   a. Indítsa el a „Control Panel”-t.



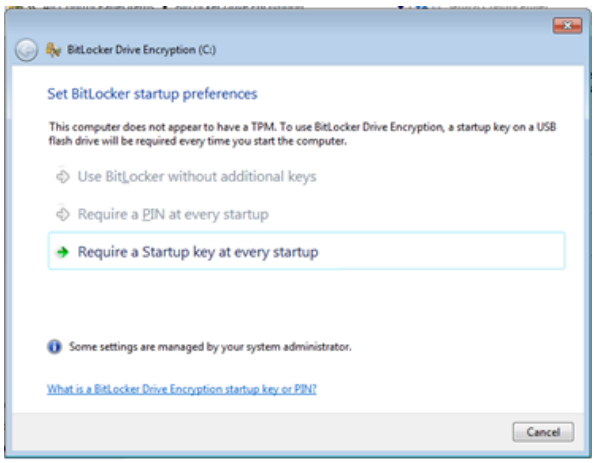
   b. Indítsa el a BitLocker-t.



c. Kapcsolja be a BitLocker-t.



d. Válassza a „Require a Startup key at startup” pontot. E pont kiválasztása esetén minden bootolást megelőzően USB kulcsot kér a rendszer, melyen a diszk titkosításához használt kulcs található.



e. Értelemszerűen haladjon tovább.
f. Ha végzett, indítsa újra számítógépét, figyelje meg a rendszerindítás folyamatát, belépés után tanulmányozza a pendrive tartalmát.

Pendrive titkosítása BitLocker To Go segítségével

1. Egy üres pendrivera másoljon fel néhány tetszőlegesen kiválasztott állományt.
2. A Control panelen válassza ki a BitLocker-t.
3. A BitLocker To Go segítségével titkosítsa le a pendrive tartalmát.
4. Ha elkészült a titkosítás, távolítsa el a pendriveot.
5. Csatlakoztassa újra a pendriveot, eközben figyelje meg a rendszer viselkedését.
6. Nézze meg, hogy a pendriveon megtalálhatóak-e a felmásolt állományok.
7. Próbálja ki szomszédjával is az ő számítógépén a pendrive működését.
8. Lépjen ki „Command prompt”-ba.
9. A `manage-bde -status` parancs segítségével kérdezze le a titkosított diszkek állapotát, és a titkosítás módját.
10. Sikerült a lekérdezés? Oldja meg a problémát.

Titkosított konténer létrehozása TrueCrypt segítségével

1. Töltse le a TrueCrpyt 7.1a verzióját a https://www.grc.com/misc/truecrypt/truecrypt.htm 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 TrueCrypt volume” menüpontot, majd „Next”.
8. Válasszon tetszőleges nevet a container részére, és a C:\ könyvtárban helyezze el.
9. Tanulmányozza a felkínált titkosítási algoritmusokat (leírásukkal együtt).
10. Tanulmányozza a felkínált hash algoritmusokat.
11. Válassza ki az „AES-Twofish-Serpent” titkosítást, majd „Next”.
12. Méretnek 1GB-t állítson be, majd „Next”.
13. Tanulmányozza, a megjelenő leírást, majd válasszon tetszőleges jelszót, majd „Next”.
14. Figyelje meg a titkosítás sebességét.
15. Tallózza ki a létrehozott Containert tartalmazó állományt, majd a „Mount” gomb segítségével csatolja fel azt tetszőleges meghajtónak.
16. A „Volume Properties…” gomb segítségével tanulmányozza a meghajtó titkosítását.
17. „Dismount All” segítségével csatoljon le minden titkosított Containert.