Vírusirtó kétszeres védelemmel

G Data lakossági termékek

Felhasználói útmutató

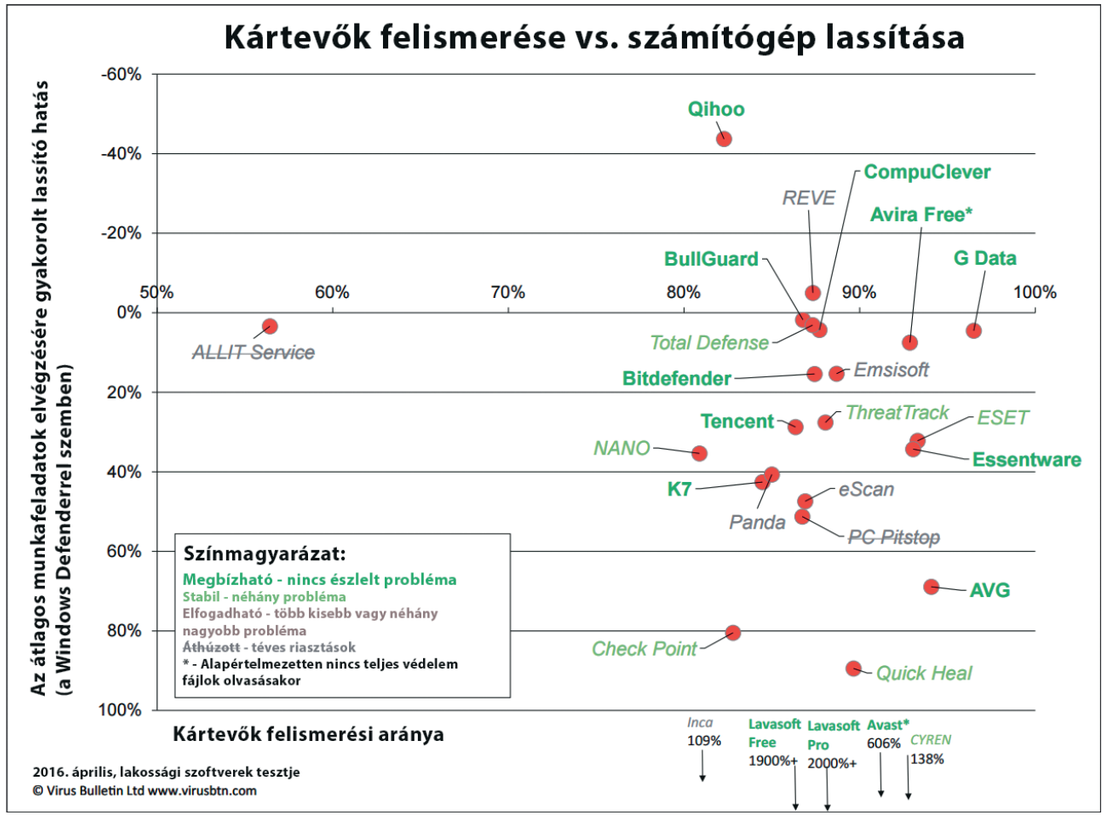
G Data. A biztonság németül.

Tisztelt Vásárlónk!

Köszönjük, hogy a G Data termékére bízta számítógépének védelmét az internetes kártevők ellen. Döntését nem fogja megbánni, mivel a G Data dupla keresőmotoros vírusvédelme a lehető legjobb vírusfelismerési arányt biztosítja.

A dupla keresőmotoros vírusvédelem jobb vírusfelismerési arányokat és gyorsabb reakcióidőt biztosít a G Data szoftverei számára, de nem jelent megnövekedett erőforrásigényt. A két független keresőmotor működése úgy van optimalizálva, hogy az első motor minden állományt átvizsgáljon, de a második motor csupán az állományok kritikus körülbelül 5 százalékát vizsgálja át. Éppen ezért a két keresőmotor használata növeli a biztonságot, de nem fogja leterhelni a számítógépet.

Kézikönyvünk segítséget nyújt a megvásárolt verzió telepítéséhez és beállításához.



Tartalomjegyzék

Bevezető 1
Tartalomjegyzék 1
Alapvető beállítások 2
Telepítés 2
Telepítés és használat több számítógépen 7
Gépcsere 7
Használatba vétel 7
Jogosultságok kezelése 9
Vírusriasztások kezelése 9
Részletes beállítások 10
Általános beállítások 11
Vírusvédelem beállításai 11
Az állandó vírusvédelem beállításai 11
A kézi indítású víruskeresés beállításai 12
Frissítések és licenc beállítása 12
A webes védelem beállításai 13
E-mail forgalom védelme 14
Automatikus vírusellenőrzés 15
Levélszemétszűrő beállításai 16
Tűzfal beállításai 18
Tűzfalszabályok kezelése 20
Indítólemez létrehozása 23
Szülői felügyelet beállításai 24
Az internetelérés és a számítógép-használat korlátozása 26
Adatmentés és archiválás 27
Fájlok visszaállítása 30
Lemezképek mentése 30
Adattörlés beállításai 30
Jelszókezelő 31
Biztonsági tuning 33
Titkosítás beállítása 36
Mobil fájlszéfek létrehozása 37
Autostart Manager 39
Eszközkontroll 40
Terméktámogatás 41

G Data AntiVirus
G Data InternetSecurity
G Data TotalProtection

Alapvető beállítások

Telepítés

A szoftver telepítése előtt érdemes a legfrissebb verziót letöltenünk a G Data magyar weboldaláról (http://virusirto.hu). A letöltés során ügyeljünk arra, hogy a megvásárolt licencnek megfelelő szoftvert töltsük le, mely lehet a G Data AntiVirus, a G Data InternetSecurity vagy a G Data TotalProtection. Amennyiben nincs módunk letölteni a legfrissebb verziót, a szoftvert lemezről vagy USB kulcsról is telepíthetjük.

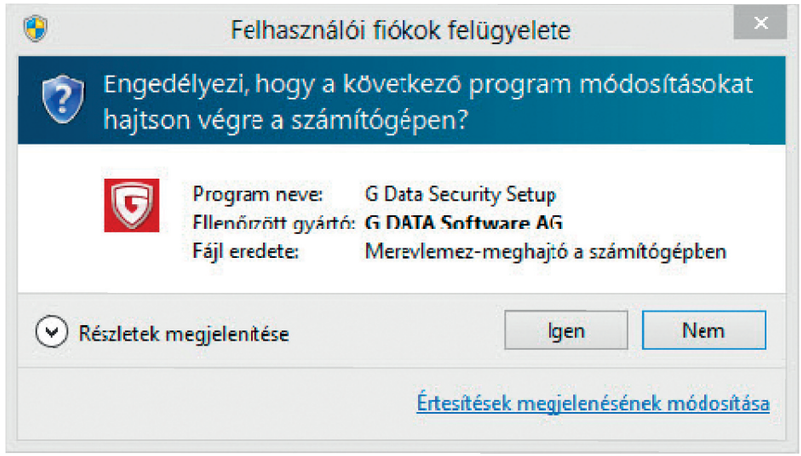
Ügyeljünk arra, hogy a számítógépeken egyszerre csak egy vírusirtó futhat. Ezért a telepítés előtt távolítsuk el a korábbi vírusirtót, amennyiben az van a gépen.

Tipp 1: A G Data védelmi szoftverei mellett nem szükséges más állandóan a memóriában lévő, automatikusan betöltődő védelmi program használata, a G Data programjai teljes körű védelmet nyújtanak a kártevők minden fajtája ellen, beleértve a kémprogramokat is. Más kiegészítő védelem használata lassíthatja a számítógépet.

Tipp 2: Néhány vírusirtó szoftvert a Windows nem tud megfelelően eltávolítani. Ezért javasoljuk, hogy töltse le a korábbi vírusirtó szoftverének gyártója által biztosított eltávolító segédprogramot (G Data esetében ez a G Data AV-Cleaner), és ezt futtassa le a számítógépen a G Data telepítése előtt.

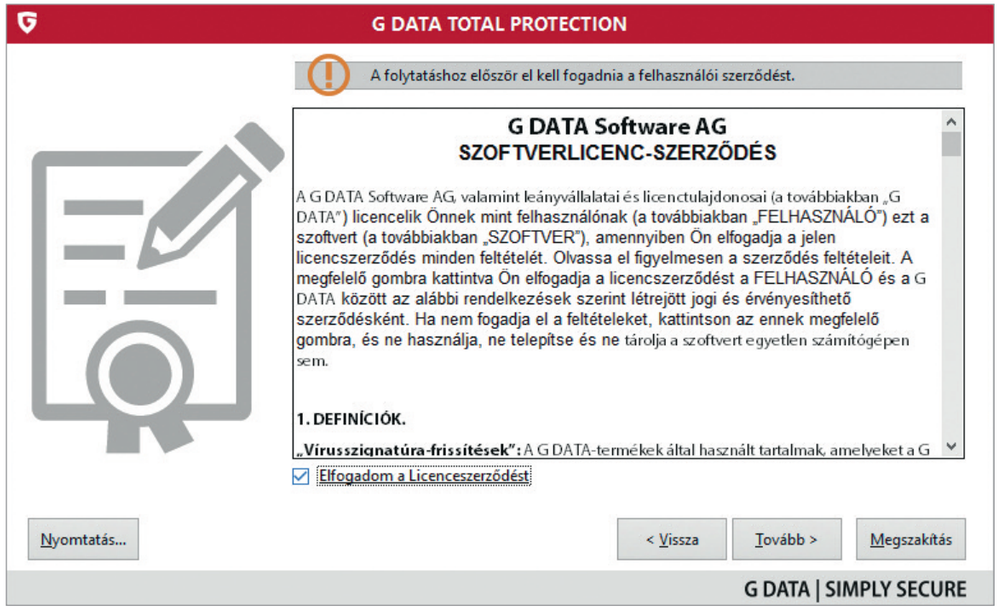
Az egyes funkciókat a G Data TotalProtection kezelőfelületén keresztül mutatjuk be, mivel ez a szoftverünk tartalmazza a legtöbb kényelmi funkciót. Éppen ezért előfordulhat, hogy bizonyos szolgáltatások nem érhetőek el az Ön által választott G Data AntiVirus vagy G Data InternetSecurity programban, de természetesen ezek a szoftverek ugyanazt a biztos védelmet nyújtják a kártevők ellen, mint a G Data TotalProtection.

A telepítést a telepítőcsomagra történő dupla kattintással indíthatjuk el. Amennyiben a Windows rendszeren be van kapcsolva a felhasználói fiókok felügyelete, a telepítés elindítását engedélyeznünk kell a felugró párbeszédablakon.



A következő párbeszédablakon a tovább gombra kattintva indítsuk el a telepítést.

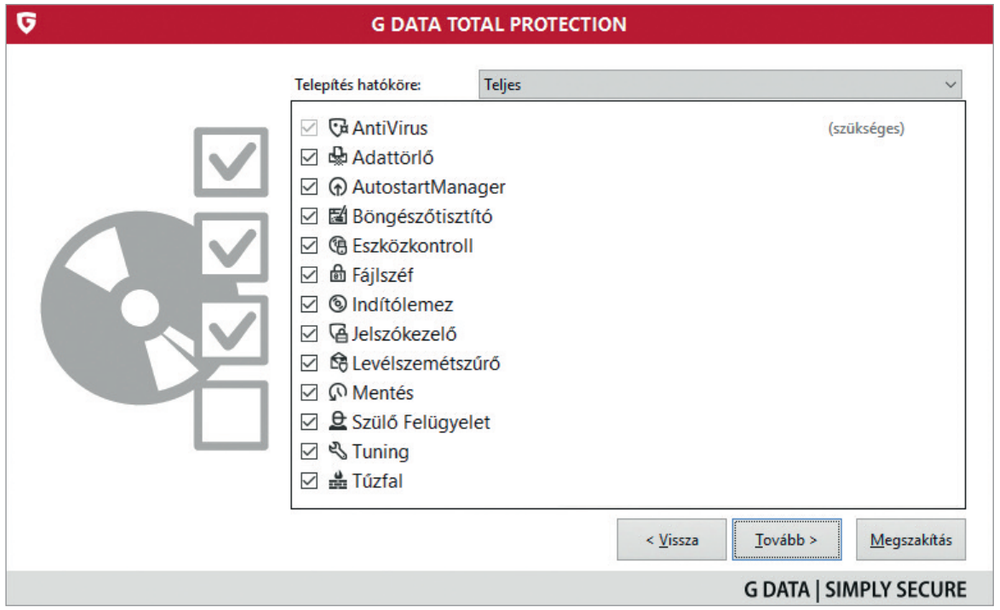
A telepítés megkezdése előtt el kell fogadnunk a licencszerződést. Kattintsunk a tovább gombra.



Ha az egyéni telepítést választottuk, akkor a következő ablakban meg kell adnunk azt a mappát, ahova a programot telepíteni szeretnénk.

Erre a legtöbb esetben nincs szükség, de ha a C meghajtón nincs elég tárhelyünk, ezt kell választani. Kattintsunk a tovább gombra.

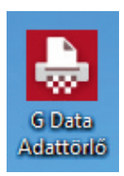
A következő ablakban válasszuk ki, hogy milyen programösszetevőket szeretnénk telepíteni. (Az alábbi kép a G Data TotalProtection összetevőit ábrázolja, más szoftverekben nem minden kényelmi funkció érhető el.)



A Szülői Felügyelet segítségével korlátozhatjuk, hogy a gépen a nem rendszergazdai jogosultságokkal rendelkező felhasználói fiókok tulajdonosai milyen weboldalakat tekinthetnek meg, mennyit és mikor használhatják a számítógépet, illetve az internetet.

A G Data Adattörlő a lomtárat helyettesíti. Segítségével véglegesen és helyreállíthatatlan módon törölhetjük azokat a fájlokat, melyekre már nincs szükségünk. Ha az egérrel az Adattörlő ikonjára húzunk egy fájlt vagy mappát, az nem a lomtárba kerül, hanem véglegesen törlődik.

Amennyiben szeretnénk ezeket a funkciókat telepíteni, a fenti párbeszédablakon pipáljuk be őket. Ezután kattintsunk a tovább gombra.



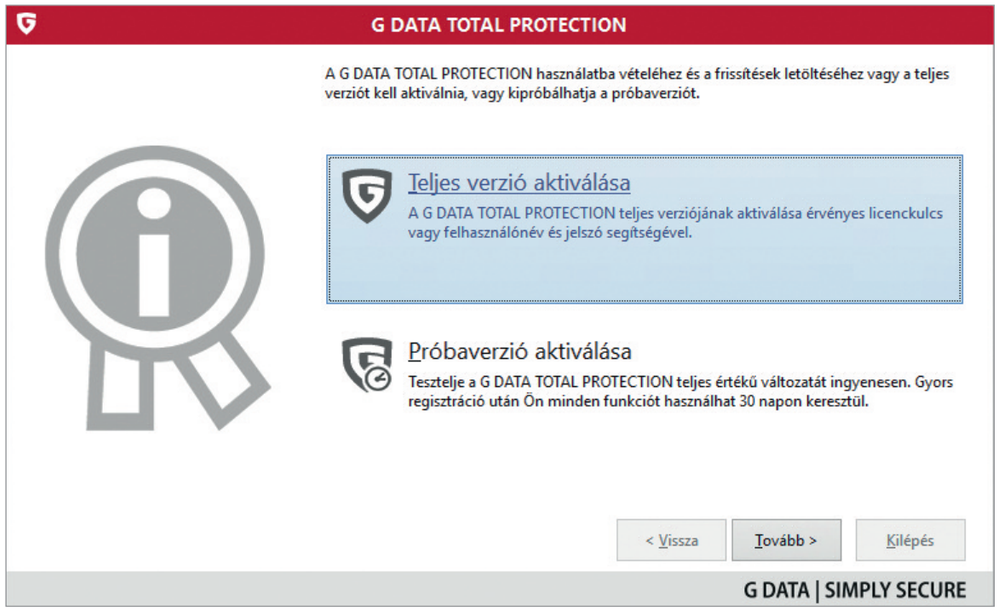
A következő párbeszédablakon jóváhagyjuk a telepítést.

A szoftver ezután telepíti magát. Várjunk egy kicsit, a folyamat eltarthat néhány percig.

A telepítést a Megszakítás gombra való kattintással állíthatjuk le, azonban ebben az esetben a szoftver nem fog települni a számítógépünkre.

A következő párbeszédablak segítségével kiválaszthatjuk, hogy a szoftver kereskedelmi, teljes verzióját szeretnénk telepíteni, vagy pedig a próbaverziót telepítjük.

Amennyiben rendelkezünk megvásárolt licenckóddal, válasszuk a teljes verziós telepítést. Amennyiben még nem rendelkezünk megvásárolt licenckóddal, és ki szeretnék próbálni a szoftvert, válasszuk a telepítést próba üzemmódban.



Amennyiben a teljes verziós telepítést választottuk, a következő párbeszédablak segítségével kiválaszthatjuk, hogy új licenckulcsot vagy már meglévő hozzáférési adatokat szeretnénk megadni.

Amennyiben a vásárláskor kapott licenckulcsot még nem aktiváltuk, akkor ennek segítségével kell telepítenünk a szoftvert. Ezért válasszuk az új regisztrációs adatok megadását. Amennyiben már felhasználtuk a licenckulcsunkat, az e-mail címünkre megkapott hozzáférési adat segítségével telepíthetjük a szoftvert.
Ebben az esetben az alábbi ablakban adjuk meg a felhasználónevet és a jelszót, amit e-mailben megkaptunk a regisztráció során.

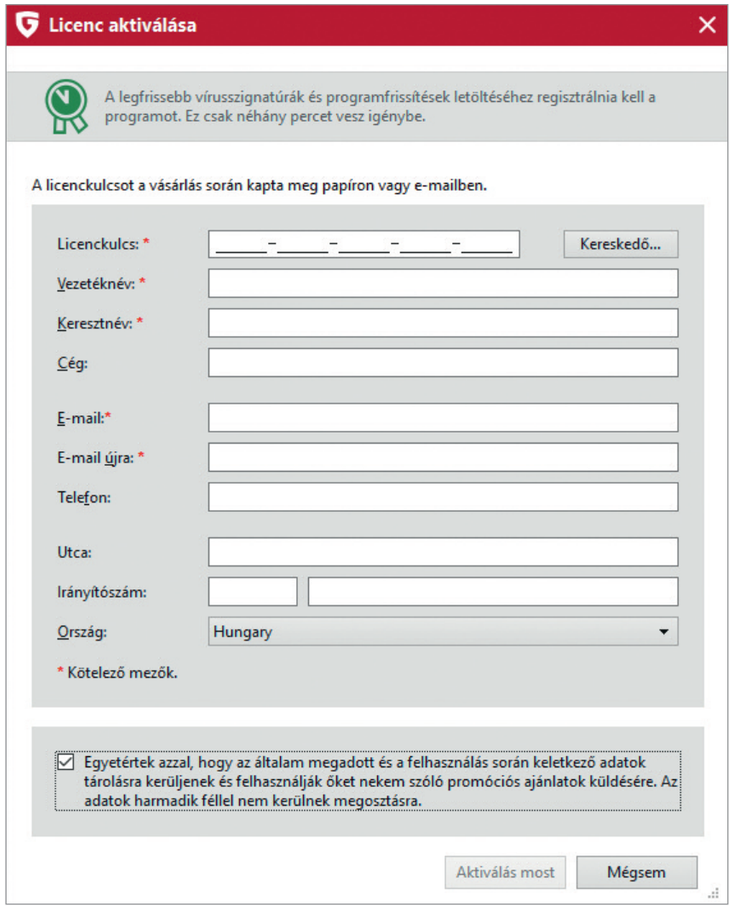
**A vásárláskor kapott licenckulcs csak egyszer használatos, akkor is, ha a szoftvert több számítógépre vásároltuk meg. Ilyen esetben a licenc-kulcsot a telepítés során az első gépen lehet megadni. Ezt követően a regisztrációs űrlapon megadott e-mail címünkre egy felhasználónevet és egy jelszót kapunk a G Datától. Ez a hozzáférési adatunk.
A többi számítógépre már ennek segítségével kell telepítenünk a szoftvert, és amennyiben újratelepítjük a gépünket, szintén ezt a hozzáférési adatot kell használnunk.**

Úgyszintén a hozzáférési adatra lesz szükségünk akkor is, ha a megvásárolt szoftver időközben megjelent új verzióját szeretnénk telepíteni a számítógépre. Éppen ezért a hozzáférési adatot érdemes feljegyeznünk.

Tipp! A G Data összes felhasználója jogosult a megvásárolt szoftver legfrissebb verziójának használatára. Éppen ezért, ha a használt szoftverből új verzió jelenik meg, arra mindig érdemes áttérni. Az évszámokhoz kötött fő verziók esetében ez az új verzió letöltését és a védelem újratelepítését jelenti. A vírusdefiníciós adatbázis frissítéséhez és a kisebb programfrissítésekhez nincs szükség a szoftver újratelepítésére.

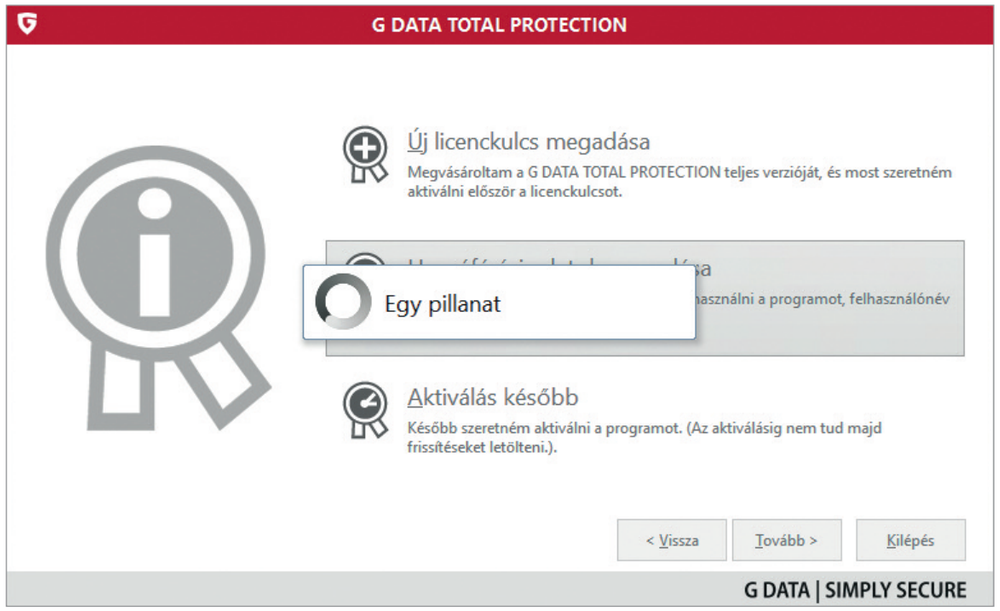
Amennyiben a telepítés során az utólagos aktiválás lehetőséget választottuk, a szoftver addig, amíg nem regisztráltuk, nem tölti le a legfrissebb vírusdefiníciós adatbázisokat, ezért nem nyújt teljes védelmet a legfrissebb kártevők ellen.

Amennyiben a licenckulcsunkat először használjuk, a következő lépésben aktiválnunk kell a szoftvert.



Az űrlapon adjuk meg a licenckulcsot, amit vásárláskor kaptunk. Töltsük ki a Vezetéknév és a Keresztnév mezőket, majd az elgépelések elkerülése érdekében adjuk meg kétszer az e-mail címünket.

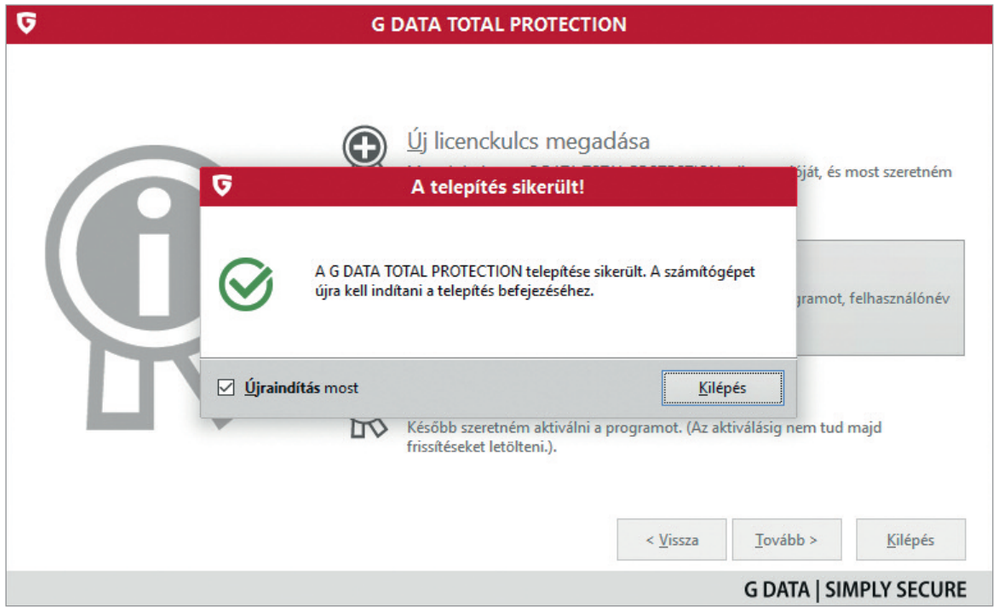
Amennyiben a licenckulcsunkat már felhasználtuk, akkor a regisztráció során megadott hozzáférés adatokat kell megadnunk.



Tipp! Amennyiben elvesztettük hozzáférési adatunkat, kattintsunk a bal alsó sarokban lévő gombra, mely megnyit egy böngészőablakot. A böngészőben megnyílt weboldalon megadhatjuk eredeti licenckulcsunkat, ami után a hozzáférési adatokat a G Data rendszere újra elküldi a regisztráció során megadott e-mail címre.

A funkció használatához és a szoftver regisztrációjához működő internetkapcsolat szükséges.

Gratulálunk! A telepítés sikeresen befejeződött. A szoftver használatba vételéhez még szükség van a számítógép újraindítására. Amennyiben a lenti párbeszédablakon található pipát nem vesszük ki, és a Kilépés gombra kattintunk, a számítógép automatikusan újraindul.
Ezután nincs több dolgunk. A szoftver automatikusan frissíteni fogja magát az interneten keresztül, és naprakész védelmet biztosít számítógépünk számára.



A kézikönyv tovább fejezetei az egyéni beállításokat és a védelmi funkciók működését mutatják be.

Telepítés és használat több számítógépen

Amennyiben a licencet több számítógépre vásárolta meg, a licenckulcsot csak a legelső számítógépen történő telepítéskor, egyetlen alkalommal kell használnia. Ezután minden további számítógépre az első telepítés során e-mailben megkapott hozzáférési adattal kell telepíteni a szoftvert.

Gépcsere

A G Data termékeit nem lehet több számítógépen egyszerre használni, mint amelyre a licenc szól, de lehet több számítógépen telepíteni. Amennyiben például a licencet két számítógépre vásárolta meg, és a terméket egy harmadik gépre szeretné telepíteni, a szoftver az aktiválás során rákérdez arra, hogy szeretné-e a licencet áthozni erre a gépre. Amennyiben igennel válaszol, a licenc átkerül az új gépre, és a G Data az új gépen fogja ellátni a frissített védelmet.

A licenc a fenti esetekben törlődik arról a gépről, mely a legrégebben csatlakozott a G Data frissítési szerveréhez.

Ha tehát Önnek két számítógépe van, és a G Data termékét mindkét gépen használja, de most az egyik számítógépét szeretné lecserélni, akkor a következőket kell tennie:

Arról a gépről, amelyiken már nem szeretné használni a G Data védelmét, törölje le a szoftvert. Kapcsolja be a második gépet, melyen továbbra is szeretné használni a szoftvert, és hajtson végre egy frissítést. Ezután a szoftvert telepítse a harmadik gépre. A telepítés során válaszoljon igennel arra a kérdésre, hogy a licencet szeretné-e áthozni az új gépre.

Amennyiben a második gépet nem kapcsolta be, és azon nem hajtott végre frissítést, nem kell aggódnia. Ebben az esetben megtörténhet, hogy a szoftver az első bekapcsoláskor ezen a gépen is rá fog kérdezni, hogy szeretné-e a licencet áthozni erre a gépre. Válaszoljon igennel, és használja tovább a szoftvert. Most már mindkét gépén naprakész és folyamatosan frissül a védelem.

Használatba vétel

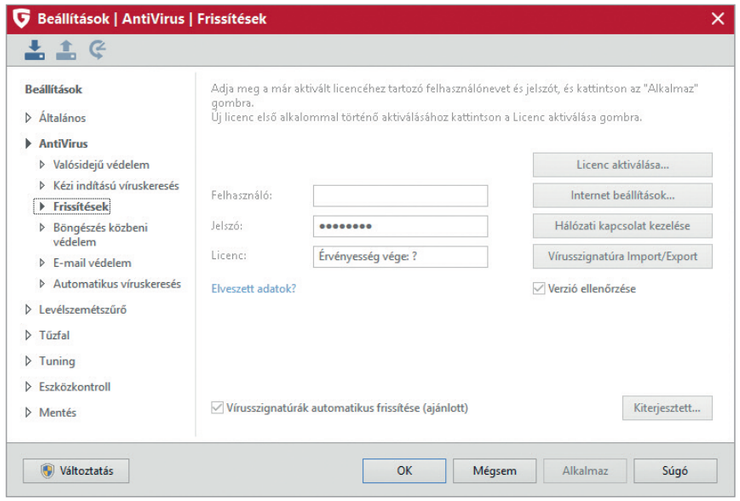
A szoftver első elindulása után A vírusszignatúrák elavultak felirat mellett egy piros háromszögben lévő felkiáltójelet láthatunk, mely jelzi, hogy a védelem nem teljes.

Ez normális, hiszen amennyiben a telepítés után azonnal megnyitottuk, a szoftvernek még nem volt lehetősége letöltenie a legfrissebb vírusdefiníciós fájlokat.

Amennyiben ez a probléma, a frissítést a felirat melletti körbeforgó nyilakra kattintva mi magunk is kezdeményezhetjük.

Ha a javítás gomb megnyomása után az alábbi ablakban nincs kitöltve a felhasználónév és a jelszó, az azt jelenti, hogy a telepítés során nem adtuk meg ezeket, és aktiválás nélkül telepítettük a szoftvert.

Ebben az esetben kattintsunk a Licenc aktiválása gombra, mely után kiválaszthatjuk, hogy új licenckulcsot adunk meg vagy már meglévő hozzáféréssel használjuk a szoftvert. Ha a gombok nem aktívak, akkor nem rendszergazda jogosultsággal vagyunk bejelentkezve a számítógépre. Ebben az esetben a bal alsó sarokban kattintson a Változtatás gombra, és adja meg a rendszergazda jelszavát.



Amennyiben sikeresen aktiváltuk a szoftvert, a G Data letölti a vírusdefiníciós frissítéseket mindkét motorhoz. A letöltés a hálózat terheltségétől függően eltarthat néhány percig az első alkalommal. A sikeres frissítést zöld pipák jelzik.

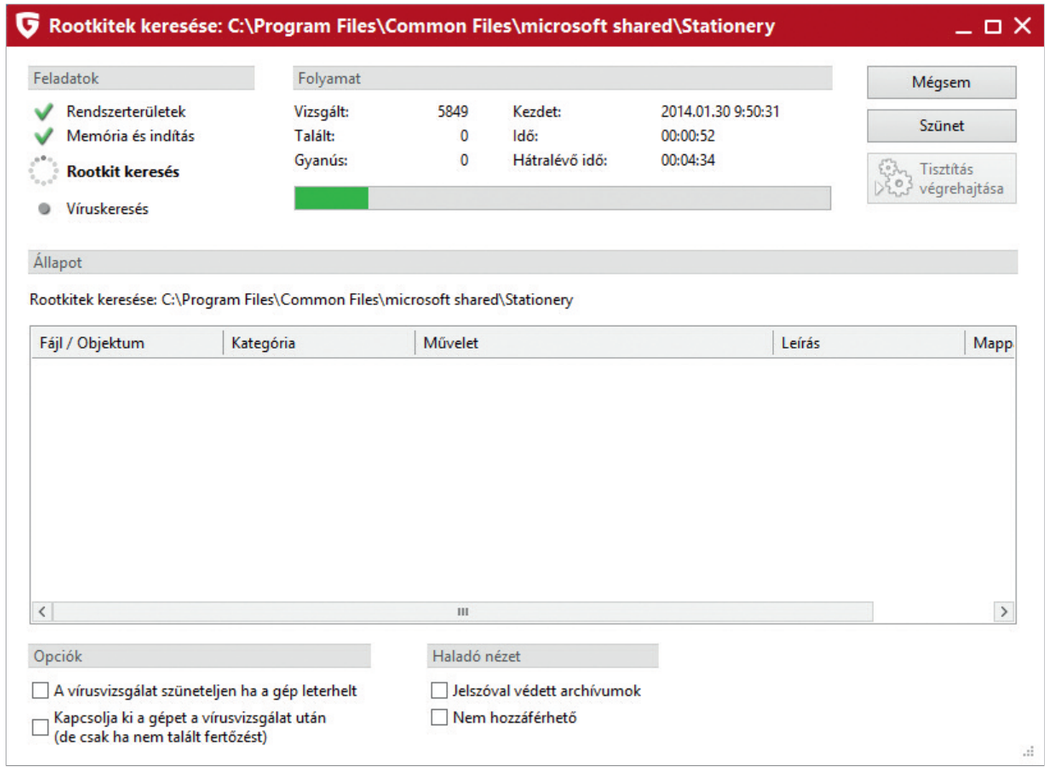
A Biztonsági Központ felirat alatt zöld háromszögben megjelenő pipa jelzi, hogy nincs több biztonsági probléma, és a védelem naprakész.

A víruskeresés indításához kattintsunk a következő fülre, majd a Számítógép ellenőrzése (minden helyi lemez) feliratra.

A feliratra kattintás automatikusan elindítja a víruskeresést, amit a megnyíló párbeszédablakon nyomon követhetünk.

Az ujjlenyomat-képzési technológiának köszönhetően a G Data termékei a megismételt víruskeresések során jóval gyorsabban fognak végezni a merevlemezek átvizsgálásával, mint az első alkalommal.

Az ujjlenyomatképzés ugyanis eltárolja a már átvizsgált fájlok azonosítóit, és a következő vírusvizsgálatkor felhasználja azokat. Egy tipikus számítógépen az első vírusvizsgálat körülbelül két órát vesz igénybe, de az ezt követő vírusvizsgálathoz szükséges idő az ujjlenyomat-képzési technológiának köszönhetően körülbelül háromnegyed órára, majd akár néhány percre csökken.



Tipp! Amennyiben szeretnénk, hogy a számítógép kikapcsoljon, miután végzett a vizsgálattal, tegyen pipát a gép kikapcsolása mellé. A gép csak akkor kapcsol ki, ha nem talált fertőzést, ellenkező esetben bekapcsolva marad.

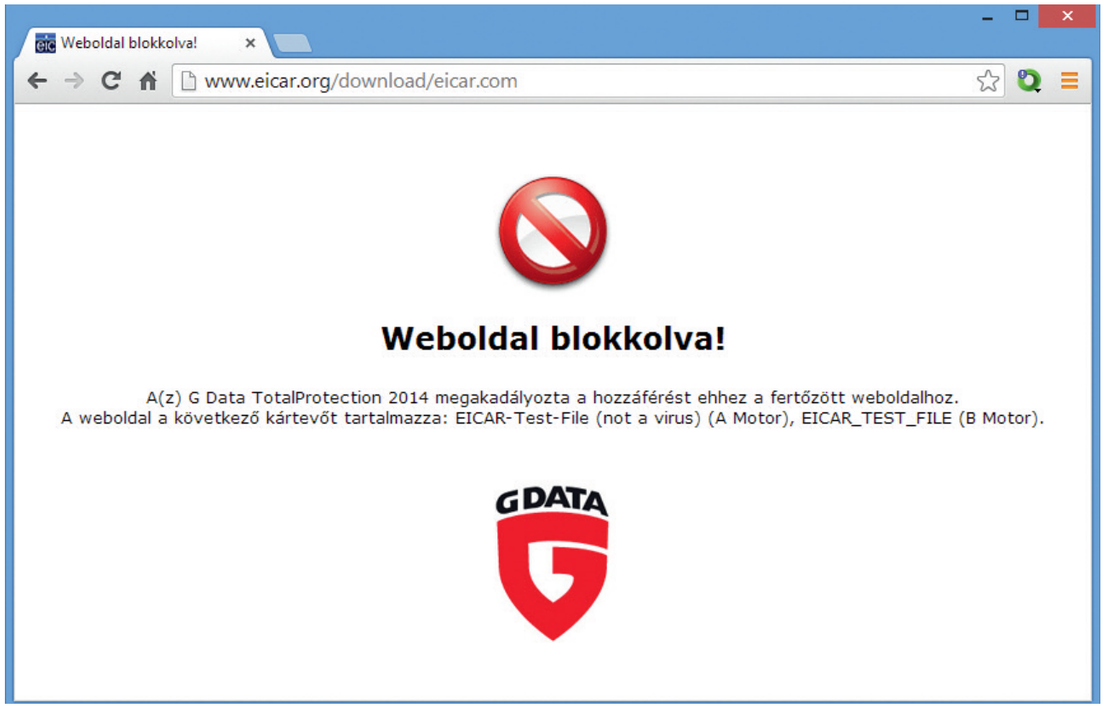
A haladó nézet alatt beállíthatjuk, hogy a szoftver riportolja-e a jelszóval védett tömörített állományokat és azokat a fájlokat, melyekhez nem tudott hozzáférni.

Jogosultságok kezelése

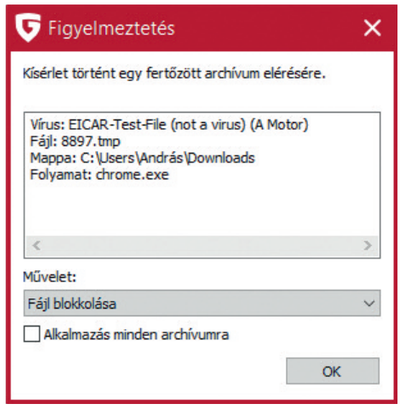
A G Data védelmi szoftvereinek beállításai a Windows fiókok jogosultságaihoz kötődnek. A rendszergazdai jogosultságokkal rendelkező felhasználók módosíthatják a G Data szoftverek beállításait, míg a rendszergazdai jogosultságokkal nem rendelkező felhasználók nem módosíthatják a szoftver alapvető beállításait.

Vírusriasztások kezelése

A G Data védelmi szoftverei böngészés közben is védelmet nyújtanak. Amennyiben egy weboldal fertőzést tartalmaz, a G Data blokkolja a hozzáférést, és az alábbi üzenetet jeleníti meg.

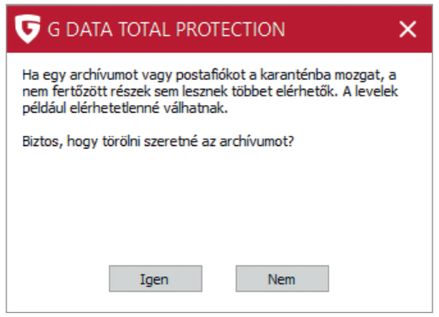


Amennyiben a G Data védelmi rendszere a számítógépen észlel egy kártevőt, az alapbeállítások szerint egy felugró riasztási ablakot jelenít meg, melynek segítségével meghatározhatjuk, hogy milyen akciót szeretnénk végrehajtani a fertőzött fájllal.



Az alapértelmezett beállítás a megtisztítás, és amennyiben ez nem lehetséges, a karanténba helyezés Ebben az esetben a G Data megpróbálja megtisztítani a fertőzött fájlt, és ha ez valamilyen okból nem lehetséges, karanténba helyezi. Tömörített fájlok esetén az alapértelmezett beállítás a fájlhoz való hozzáférés blokkolása.

Amennyiben a fájl maga egy kártevő, a tisztítás a fájl törlését jelenti. Amennyiben a fertőzött fájl eredetileg egy tiszta, más információkat tartalmazó állomány (például szöveges dokumentum, mely megfertőződött), a G Data megpróbálja a fájl eredeti tartalmát visszaállítani.



Amennyiben egy tömörített fájlt vagy e-mail archívumot (.pst fájl) törlünk, akkor nem csupán a fertőzött részek, hanem a tiszta részek is törlésre kerülnek. Ez azt is jelentheti, hogy a levelezésünket nem fogjuk többet elérni. Éppen ezért tömörített fájlok és e-mail postafiókok esetén javasoljuk, hogy a törlés előtt gondolja végig, biztosan nincs-e szüksége a fájl tartalmára.

Amennyiben inkább karanténba helyeznénk a fájlt, válasszuk a karanténba mozgatás lehetőséget. Ebben az esetben a fájl karanténba kerül a számítógépen, de nem törlődik.

Részletes beállítások

A szoftver részletes beállításai a jobb felső sarokban található kék színű fogaskerék ikonra kattintva nyithatóak meg.

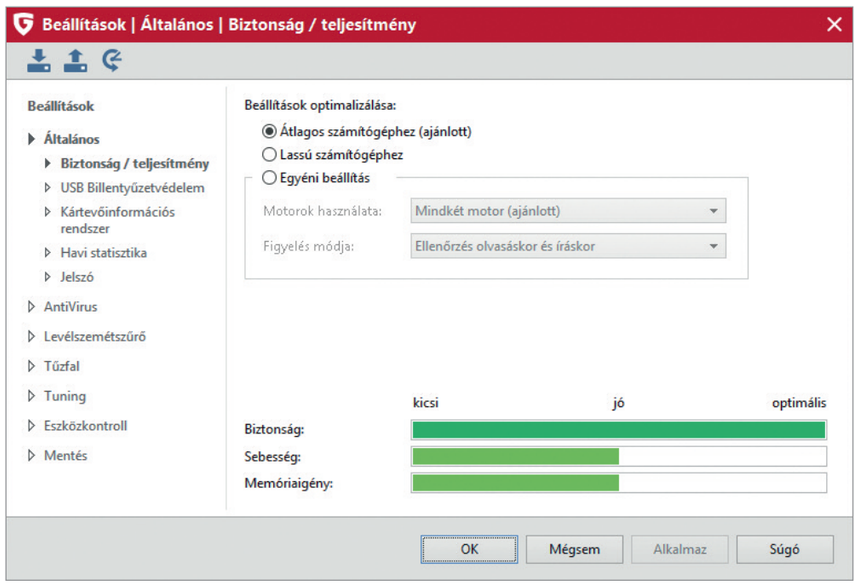
A megnyíló párbeszédablakban a bal oldali menüből választhatjuk ki, hogy milyen modul beállításait szeretnénk megváltoztatni.

Általános beállítások

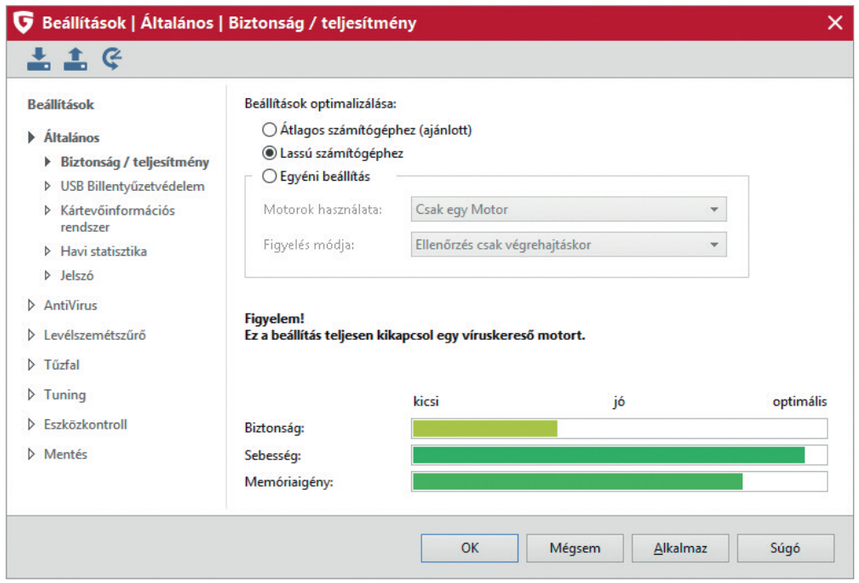
Az általános beállítások megváltoztatásával egyszerűen igazíthatjuk a szoftver beállításait a számítógép teljesítményéhez.

A javasolt alapértelmezett beállítások valók egy átlagos számítógép számára. Ebben az esetben a G Data védelmi programja mindkét víruskereső motort használja, és az állományokat mind íráskor, mind olvasáskor ellenőrzi.

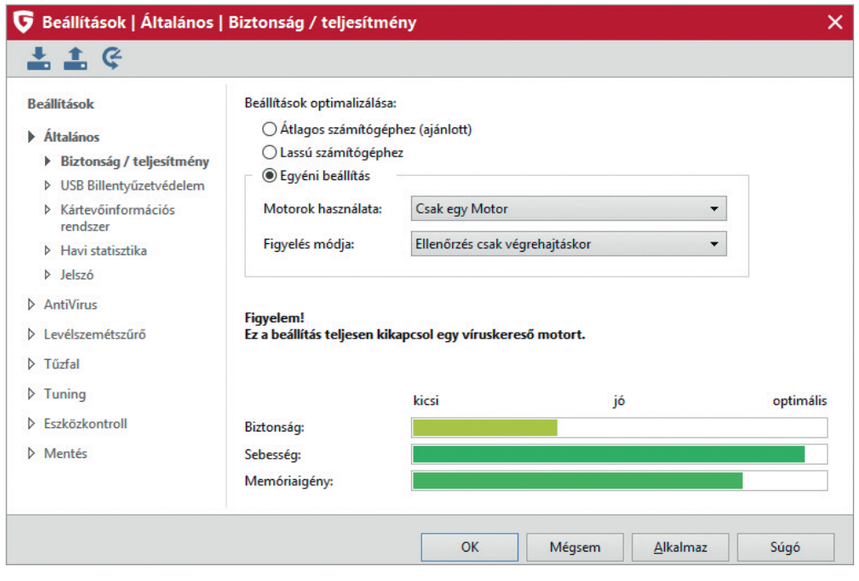
Ez a beállítás biztosítja a legmagasabb védelmi szintet.



Amennyiben számítógépünk az átlagosnál öregebb vagy lassabb, válasszuk ki a lassú gépekhez való beállítást. Ez a beállítás kikapcsolja a második keresőmotort, és az állományokat csak végrehajtáskor ellenőrzi.
Ez csökkenti a védelem szintjét, de növelheti a számítógép teljesítményét.



Az egyéni beállítások kiválasztásával testre szabhatjuk a beállításokat. Lehetőségünk van a keresőmotor kiválasztására, és azt is beállíthatjuk, hogy a motor mikor ellenőrizze az állományokat. Amennyiben nem érthető, hogy melyik beállítás mit jelent, azt javasoljuk, hogy ne változtassa meg az alapbeállításokat.



Vírusvédelem beállításai

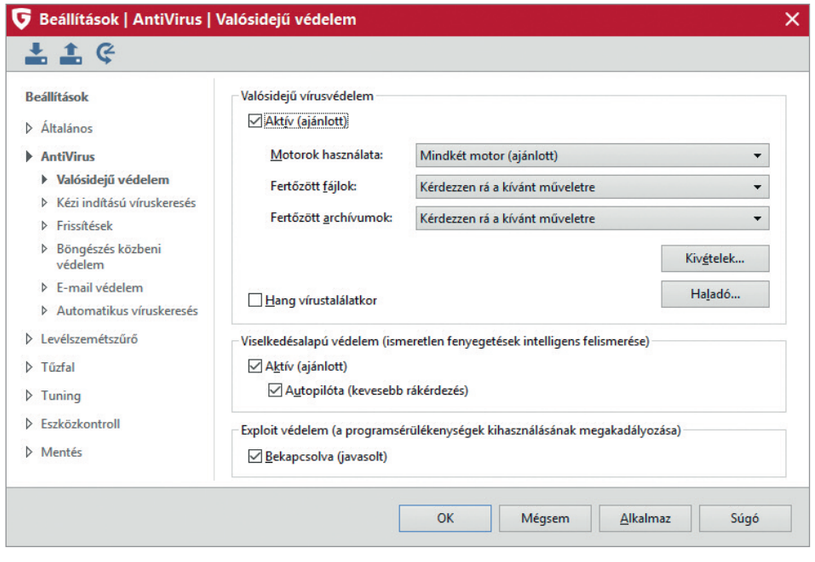
A bal oldali menüből válasszuk ki az AntiVirus beállításait.

Az állandó vírusvédelem beállításai

A párbeszédablakon be- és kikapcsolhatjuk a vírusvédelmet, szabályozhatjuk, hogy a szoftver melyik vírusirtó motorokat vagy mindkét motort használja.

Beállíthatjuk azt, hogy a szoftver hogyan reagáljon a fertőzött fájlokra és a fertőzött tömörített állományokra. Az alapbeállítás mindkét esetben az, hogy a G Data kérdezzen rá, hogy mit szeretnénk tenni a fertőzött állományokkal.

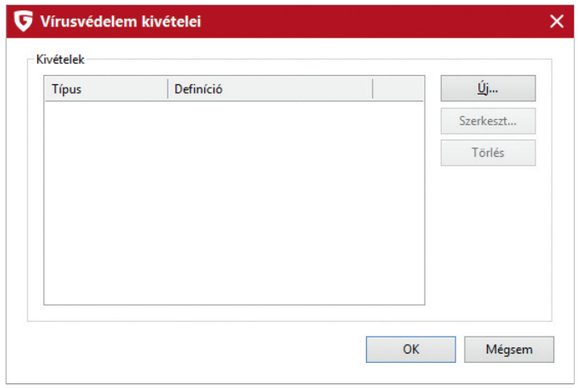
A lehetséges választások közül a hozzáférés blokkolása és a karanténba helyezés megőrzi a fájlt. A fájl megtisztítása viszont sok esetben csak úgy lehetséges, hogy maga a fájl is használhatatlanná válik. Ez történik minden olyan esetben, amikor a fájl egy kártevő, nem pedig egy eredetileg tiszta fájl, ami csak hordozza a kártevőt.



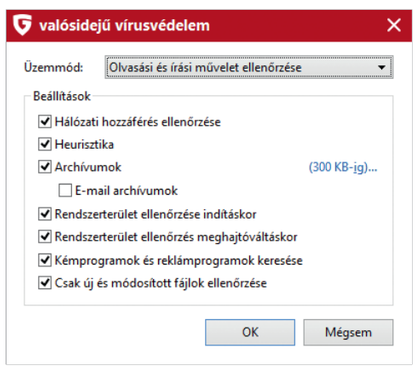
Az alapbeállítás szerint a G Data védelmi szoftver minden esetben rá fog kérdezni a kívánt műveletre. Amennyiben ezt meg szeretnénk változtatni, javasoljuk a karanténba való mozgatást, ami megőrzi a fájlt.

A Viselkedésalapú védelem egy plusz védelmi funkcionalitás, mely a hagyományos vírusvédelmen és a kiterjesztett heurisztikán túl plusz védelmet nyújt. A viselkedés megfigyelésének bekapcsolása riasztást fog adni minden olyan program esetében, mely védelmi szempontból gyanús műveletet hajt végre. Ilyen lehet például egy frissen megvásárolt nyomtató meghajtóprogramja, amely a telepítés után az internetről le szeretné tölteni saját frissítéseit. Ezt a tevékenységet a G Data védelmi szoftvere gyanúsnak érzékelheti. Ebben az esetben a viselkedésalapú védelem rá fog kérdezni, hogy szeretnénk-e engedélyezni a gyanús szoftver futását.

Ha szeretnénk, kapcsoljuk be a viselkedésalapú védelmet, de legyünk rá felkészülve, hogy néhány program esetében döntést kell majd hoznunk, hogy engedélyezzük-e a futását.
Az Exploit védelem a harmadik fél által gyártott szoftverek (Microsoft Word, Adobe Reader, stb.) sérülékenységei ellen véd a memóriafolyamatok felügyeletével. A funkciót ajánlott bekapcsolva tartani.



A kivételek hozzáadása segítségével fájlokat, mappákat vagy teljes meghajtókat vonhatunk ki a vírusellenőrzés alól. A vírusellenőrzés alól kivont útvonalakat a G Data védelmi szoftvere nem fogja átvizsgálni.

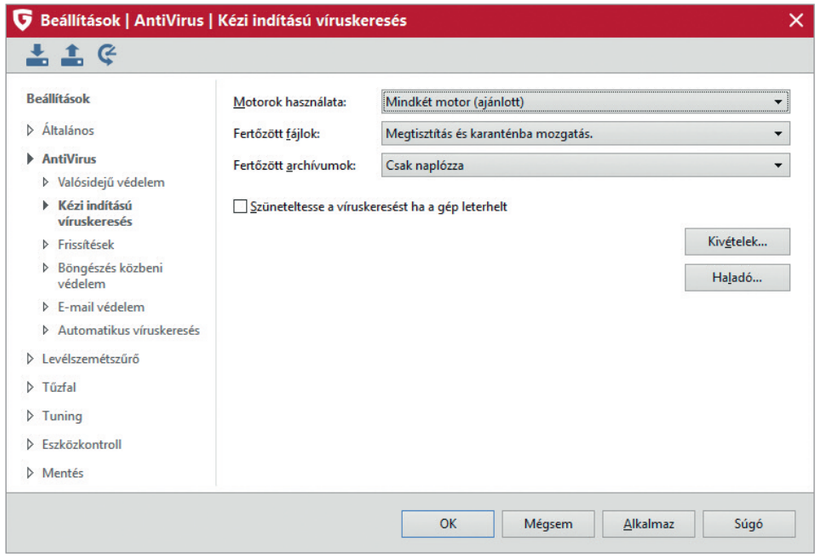


A haladó beállítások segítségével testre szabhatjuk a vírusirtó motor működését. Az alapbeállítások megváltoztatása kizárólag azok számára javasolt, akik tudják, hogy az egyes beállítások mit jelentenek, mivel bármilyen változtatás jelentős hatással van a vírusvédelem működésére.

A kézi indítású víruskeresés beállításai

A bal oldali menüből válasszuk ki a kézi indítású víruskeresést. A beállítások segítségével az előzőekhez hasonlóan megadhatjuk, hogy a szoftver mindkét motort használja-e (az alapbeállítások szerint igen), valamint, hogy mit tegyen az észlelt fertőzött állományokkal. A fertőzött archív (tömörített) állományokra való alapértelmezett reakció a naplózás, mivel ezek az állományok a fertőzés mellett jó fájlokat is tartalmazhatnak.

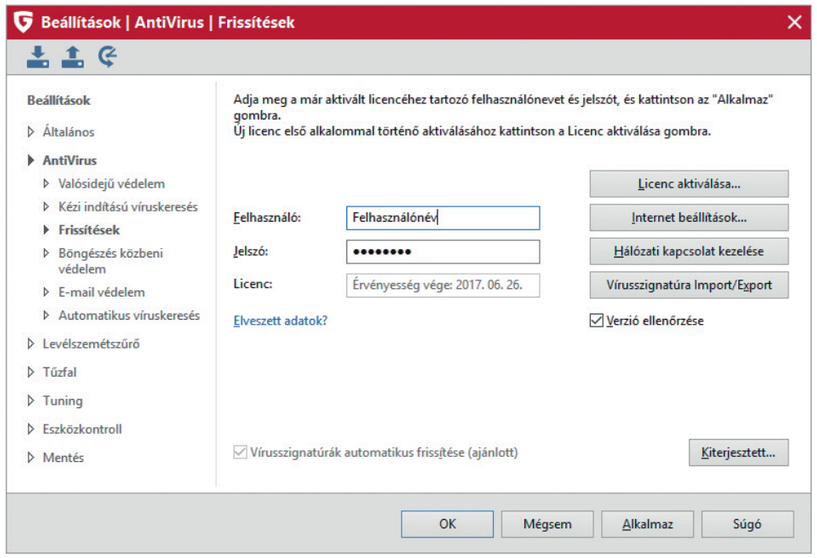
A kivételek hozzáadása és a haladó beállítások funkcionalitása ugyanúgy működik, mint az állandó vírusvédelem beállításai esetén.



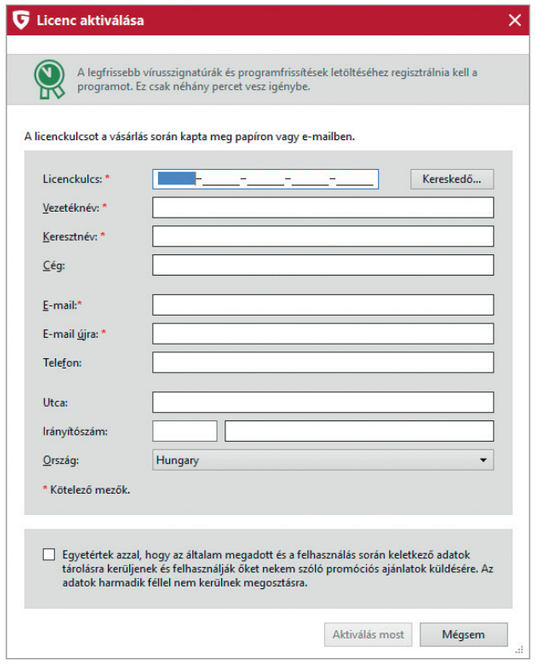
Frissítések és licenc beállítása

A bal oldali menüből válasszuk a frissítések menüpontot.
A párbeszédablakon láthatjuk felhasználónevünket és jelszavunkat.
Ha ezek a mezők nincsenek kitöltve, akkor a szoftvert még nem aktiváltuk.

Az elvesztett adatok feliratra kattintva lehetőségünk van a hozzáférési adataink újbóli lekérésére.



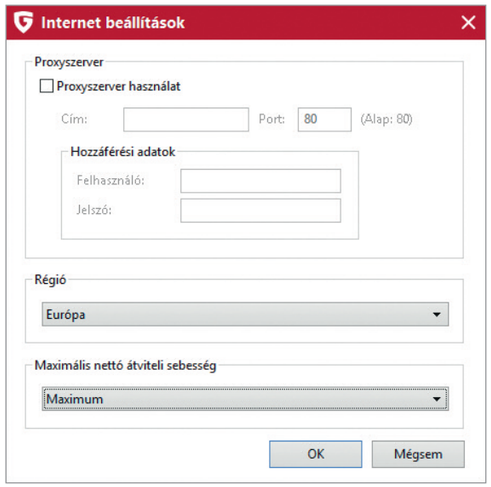
A szoftver alapbeállítása szerint óránként tölti le a frissítéseket és ezeket feljegyzi (loggolja). A beállításokat testre szabhatjuk, ha ezt szeretnénk megváltoztatni.



A licencaktiválás gomb az alábbi párbeszédablakot jeleníti meg.

A párbeszédablak segítségével új licenckulcsot adhatunk meg a szoftver számára, melyet e-mail címünkhöz tartozóan regisztrálhatunk. A szoftvert ezután a megkapott felhasználónév és jelszó segítségével használhatjuk.

Az internetbeállítások gomb megnyomása segítségével beállíthatjuk azt, hogy a gépünk hogyan kapcsolódik az internethez. Erre a beállításra akkor van szükség, ha gépünk úgynevezett proxy szerveren kapcsolódik az internethez, és ehhez külön felhasználónévre és jelszóra van szükség.

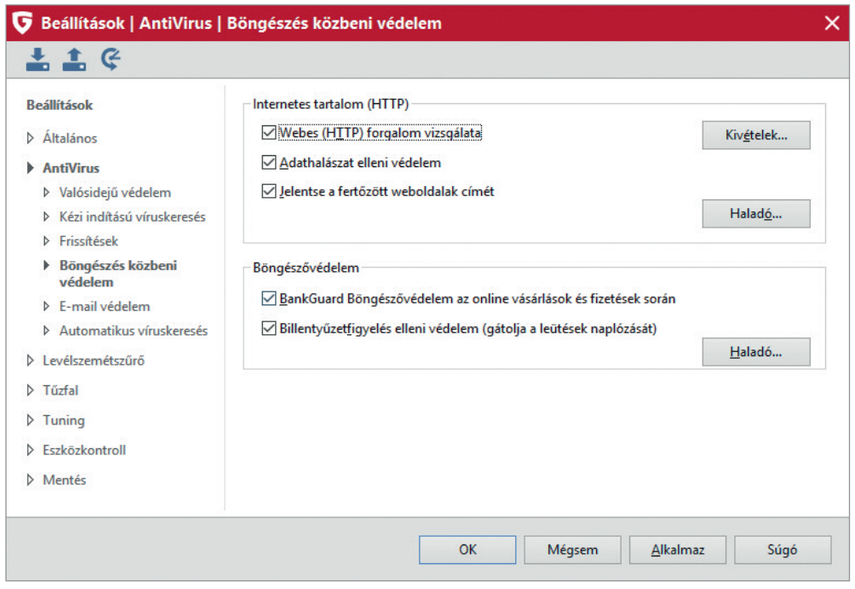


Ezen a párbeszédablakon adhatjuk meg azt is, hogy melyik régióban használjuk a szoftvert. Ez a beállítás határozza meg, hogy a G Data melyik frissítőszerverről tölti le a frissítéseket.

A böngészés közbeni védelem védelem beállításai

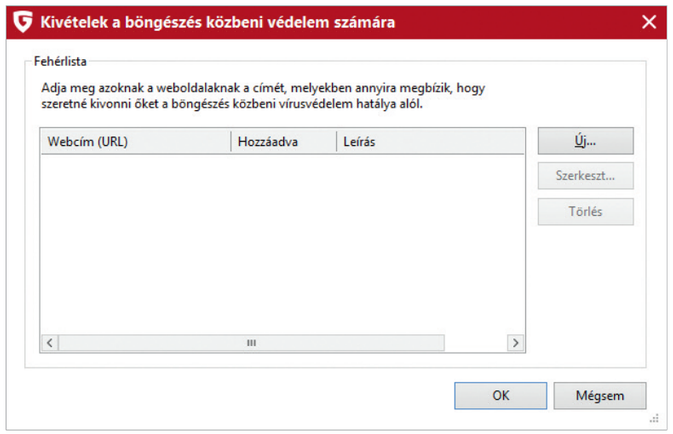
A böngészés közbeni védelem védelem beállításainak megváltoztatásához a bal oldali menüből válasszuk ki azt.

A http forgalom átvizsgálása a böngészés közbeni védelmet jelenti. Ezt nem érdemes kikapcsolni. Az adathalászat elleni védelem szintén fontos része a védelemnek, melyet nem érdemes kikapcsolni.

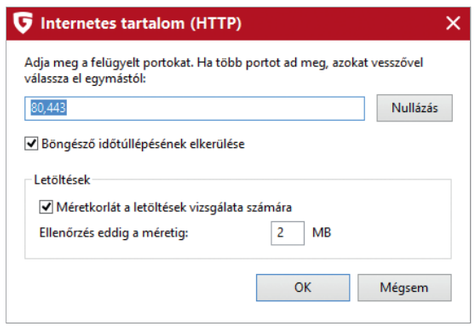


A fertőzött url címe segíti a felhő alapú védelem naprakészen tartását.

A BankGuard Böngészővédelem egyedülálló technológia a G Data szoftvereiben. A saját fejlesztésű BankGuard megakadályozza, hogy a jelszótolvaj kémprogramok a böngészőkből kinyerjék a különböző hitelkártya-adatokat, jelszavakat és felhasználóneveket. A BankGuard technológiát érdemes bekapcsolva tartani. A billentyűzetfigyelés elleni védelem a kémprogramok ellen nyújt védelmet.



A kivételek hozzáadásával megadhatjuk, hogy az általunk meghatározott weboldalakat a szoftver ne vizsgálja át. Erre bizonyos vállalati weboldalak esetében lehet szükség, amennyiben cégünk weboldala valamilyen speciális kapcsolatot kíván teremteni számítógépünkkel.



A haladó beállításokban megadhatjuk az internetezéshez használt portot és azt, hogy a szoftver milyen méretig vizsgálja át letöltés közben a fájlokat. Az alapbeállításokat nem érdemes megváltoztatni, kivéve, ha erre valamilyen speciális konfiguráció miatt szükség van.

E-mail védelem

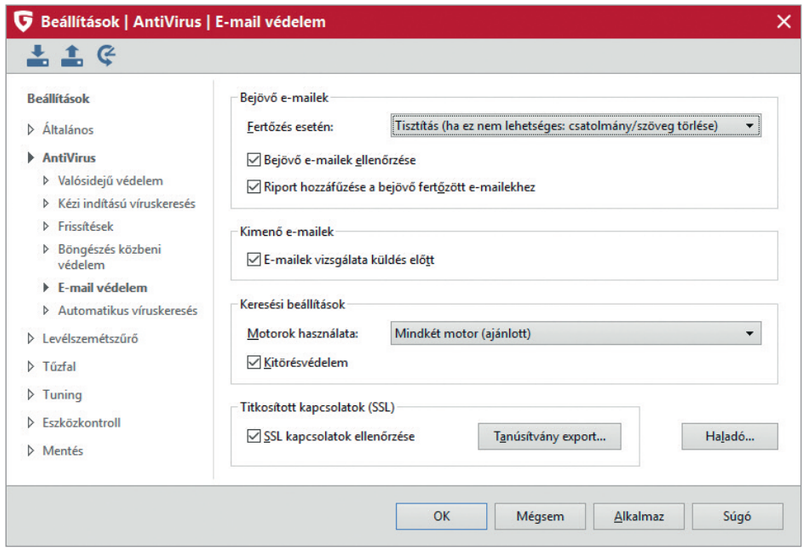
Az e-mail forgalom védelmének beállításaihoz a bal oldali menüből válasszuk ki az e-mail védelem menüpontot.

Alapértelmezés szerint a szoftver a fertőzött csatolmányokat megpróbálja megtisztítani, és ha ez nem lehetséges, törli a csatolmányt. Amennyiben ezt nem szeretnénk, a beállítást átállíthatjuk úgy, hogy a G Data csak figyelmeztetést helyezzen el a fertőzött e-mailben. Ez azonban csökkenteni fogja a biztonságot.

A szoftver alapbeállítás szerint ellenőrzi a fogadott e-maileket és a fertőzött levelekhez figyelmeztetést csatol.

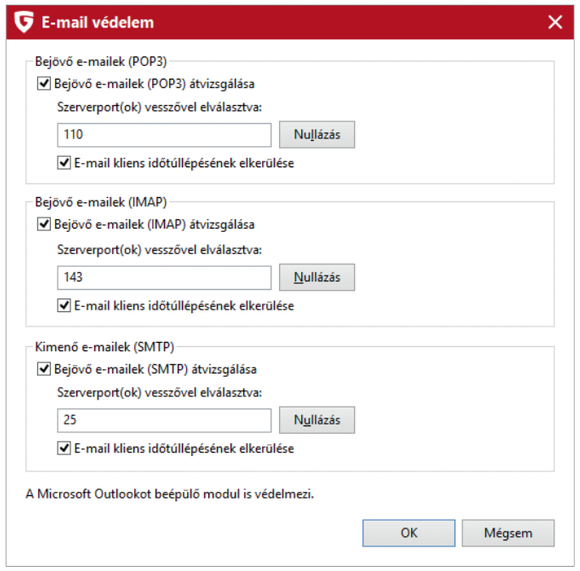
A keresési beállításoknál megadhatjuk, hogy a G Data melyik motorokat használja. A szoftver alapbeállítás szerint mindkét víruskereső motort használja.

A kitörésvédelem egy felhő alapú védelem, melynek segítségével a G Data azonnal védelmet tud nyújtani az úgynevezett nulladik napi fenyegetések ellen.



A haladó beállításokban megadhatjuk, hogy milyen portokat használunk a levelezésre. Ezt csak akkor kell átállítani, ha valamilyen speciális konfiguráció miatt erre szükség van.

Mivel a G Data külön integrált plugin segítségével védi a Microsoft Outlook levelezőprogramot, amennyiben teljesítménylassulást tapasztalunk az Outlook esetében, és nem használunk más szoftvert a levelezésre, a portok átvizsgálását kikapcsolhatjuk. Az alapértelmezett beállításokat egyébként nem érdemes megváltoztatni.



Automatikus vírusellenőrzés

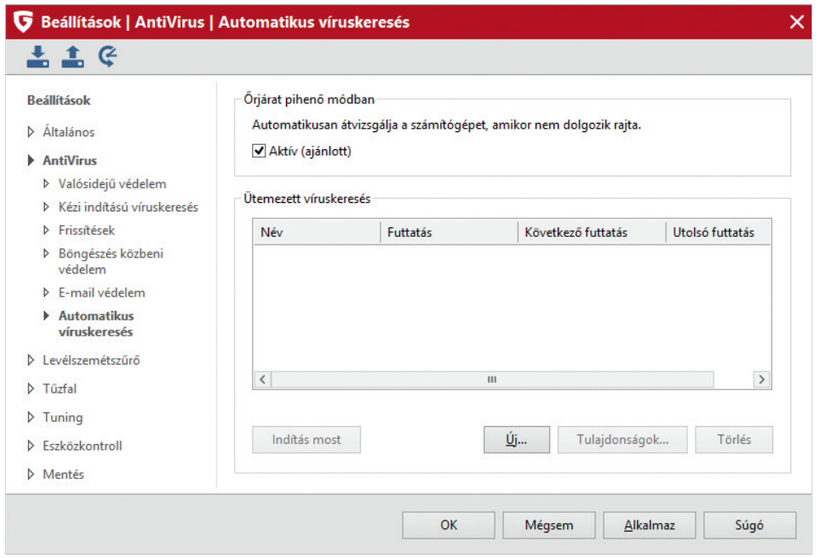
Az automatikus vírusellenőrzések beállításához a bal oldali menüben válasszuk ki a megfelelő menüpontot.

Az őrjárat technológia a G Data szoftverek integrált részét képezi. Használatával a G Data olyankor vizsgálja át a számítógépet, amikor azon nem végzünk más tevékenységet.

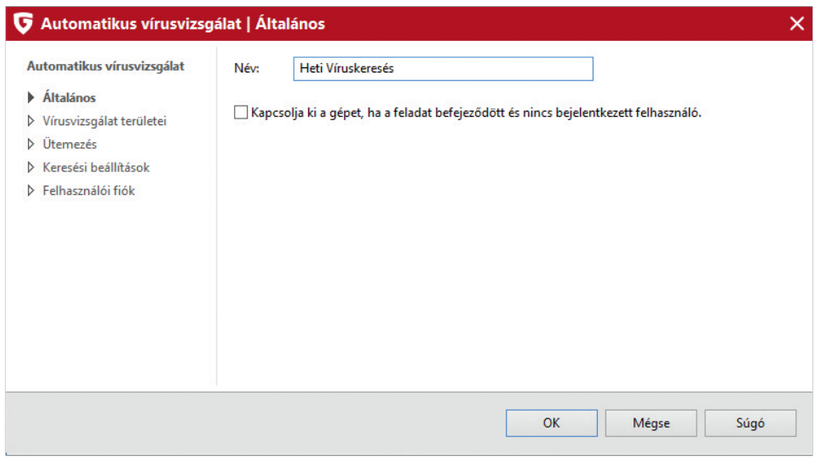
Az őrjárat ilyenkor egy képernyővédőt jelenít meg a monitoron, ami jelzi, hogy a szoftver vírusellenőrzést végez a számítógépen. Az őrjárat ezt hetente egyszer teszi meg, és ha végez a vírusellenőrzéssel, csak a következő héten vizsgálja újra a gépet.

Az őrjárat plusz védelmet jelent a gépünk számára, ezért nem érdemes kikapcsolnunk. Kikapcsolhatjuk azonban az őrjáratot, ha azt tapasztaljuk, hogy zavarja más szoftverek használatát. Az őrjárat kikapcsolása NEM csökkenti a számítógép megszokott vírusvédelmét, mivel az őrjárat egy kiegészítő automatikus víruskeresés.

Az ütemezett víruskeresések segítségével víruskeresési feladatokat hozhatunk létre a gépen, melyek automatikusan lefutnak.



Az új ütemezett víruskeresési feladat hozzáadása során meghatározhatjuk, hogy az adott feladat mikor fusson le, és hogy a víruskeresés milyen mappákat, meghajtókat nézzen át. A felhasználói fiók megadásával hozzáférést biztosíthatunk a szoftver számára a jelszóval védett hálózati mappákhoz és meghajtókhoz.



Levélszemétszűrő beállításai

A G Data védelmi szoftverei összetett, fejlett levélszemétszűrő modult tartalmaznak a kéretlen reklámlevelek kiszűrésére. Az alapbeállítások a legtöbb esetben megfelelőek, de lehetőség van ezeket teljesen testre szabni.

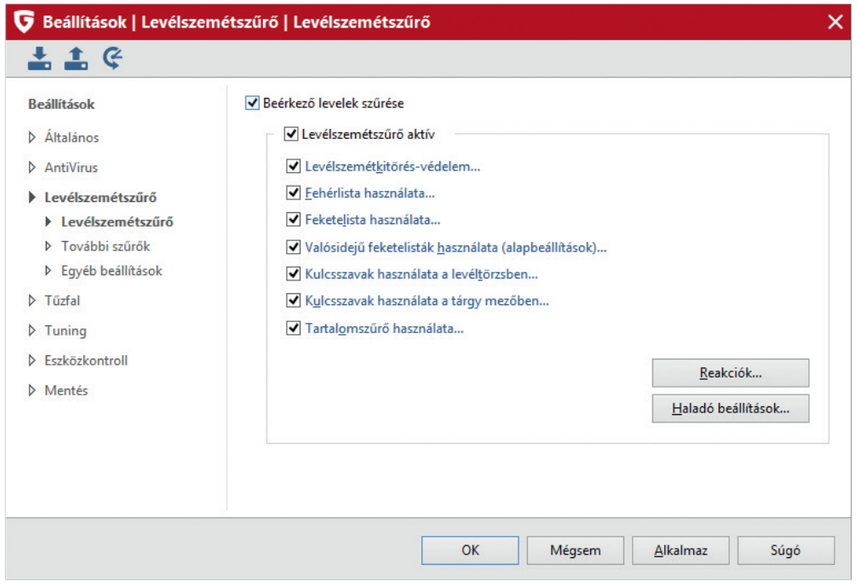
A párbeszédablak jobb oldali részén található linkekre kattintva megnyílnak az egyes modulok részletes beállítási lehetőségei. Az alapbeállítások átállítása csak a hozzáértő felhasználók részére javasolt.

A levélszemétkitörés-védelem a Commtouch szolgáltatásán alapuló technológia, mely biztosítja, hogy a G Data szoftverei már a legelső pillanattól kezdve védelmet nyújtsanak a legújabb levélszeméthullámok ellen.

A fehérlista segítségével meghatározhatjuk azoknak a feladóknak vagy domaineknek körét, ahonnan minden levelet el szeretnénk fogadni. (Megbízható küldők listája.) A feliratra kattintás után megnyíló párbeszédablak segítségével feladókat (nev@domain.hu) vagy domaineket (domain.hu) adhatunk hozzá a fehérlistához.

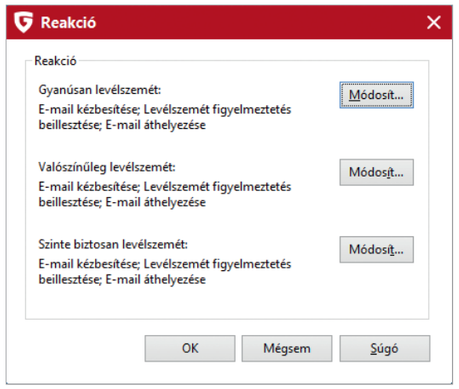
A feketelista ugyanígy működik, de ehhez a listához azokat a feladókat adhatjuk hozzá, akiktől nem kívánunk e-maileket elfogadni.

A valós idejű feketelisták külső szolgáltatók által karbantartott listák, melyek tartalmazzák az elterjedt reklámlevelek és reklámlevélküldők adatait.
Az alapbeállításokat csak indokolt esetben változtassuk meg.

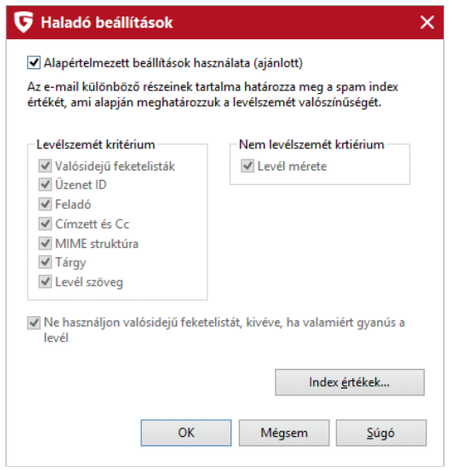


A levélszemétszűrő működésének finomításához kulcsszavakat határozhatunk meg, melyeket a levélszemétszűrő a levél törzsében vagy a levél tárgyában fog keresni. A feliratra, majd az új gombra kattintva kulcsszavakat – például: „akciós ajánlat”, „szenzációs ajánlat” – adhatunk hozzá a listákhoz.

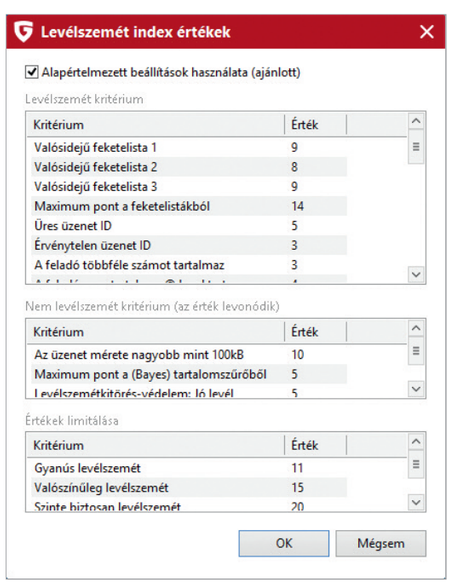
A tartalomszűrő egy öntanuló modul, mely Bayes-elmélet alapján elemzi a levelek tartalmát, és megtanulja, hogy a valódi e-mailekben és a kéretlen reklámlevelekben milyen szavak fordulnak elő a leggyakrabban. Ez a modul segít abban, hogy a levélszemétszűrő működése egyre jobbá és jobbá váljon.



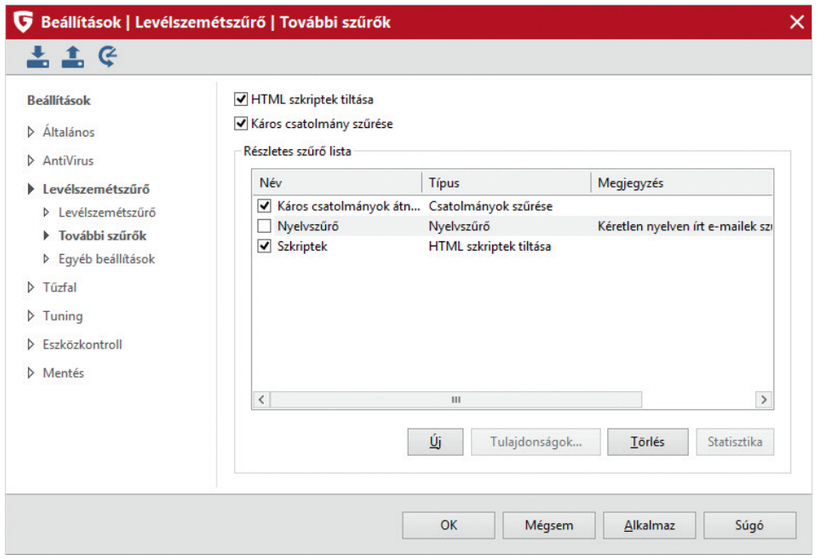
A párbeszédablak reakció gombja megnyomásával beállíthatjuk, hogy a spamszűrő hogyan reagáljon a gyanús reklámlevelekre, valamint a valószínű és a szinte biztosan reklámlevelekre. A Módosít gomb megnyomásával beállíthatjuk, hogy a G Data védelmi szoftvere milyen megjegyzést fűzzön a reklámlevelekre, és azt is, hogy melyik mappába tegye át azokat.



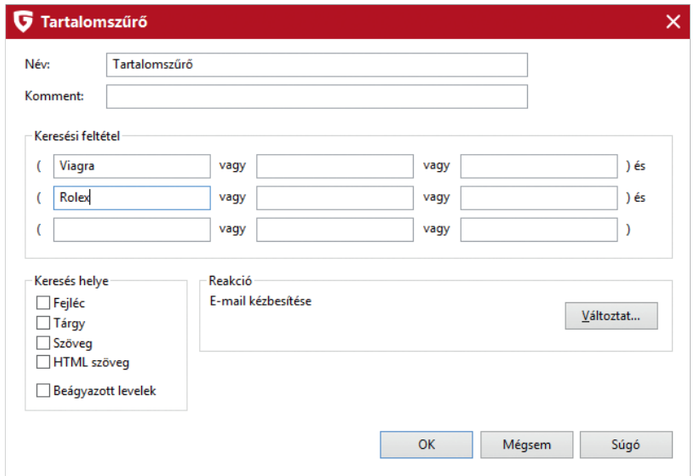
A haladó beállítások gomb megnyomásával beállíthatjuk, hogy a levélszemétszűrő az átvizsgált levelek milyen jellemzőit vegye figyelembe. Az alapbeállítások megváltoztatása csak hozzáértő felhasználók számára javasolt.



A levélszemét index értékek megváltoztatásával finomra hangolhatjuk, hogy a levélszemétszűrő milyen súlyt rendeljen az egyes jellemzőkhöz, amikor levélszemétnek nyilvánít egy e-mailt. Az alapbeállítások megváltoztatása csak hozzáértő felhasználók számára javasolt.



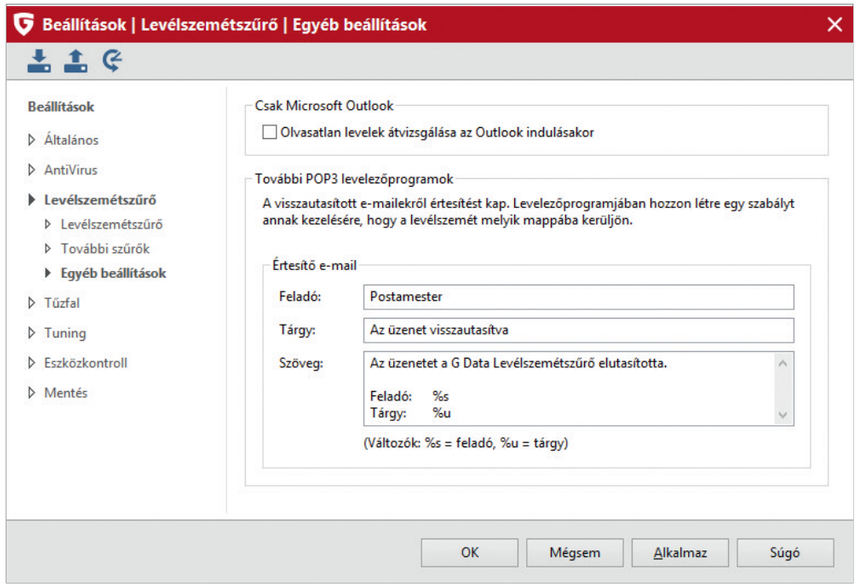
A bal oldali menüben a további szűrők gombra kattintva újabb szűrőket adhatunk a levélszemétszűrőhöz.



Az új gombra kattintva ÉS és VAGY kapcsolatok segítségével több kulcsszóból vagy kulcskifejezésből álló szűrőket adhatunk a modul működéséhez.

A bal oldali menüben a további beállítások gombra kattintva szabályozhatjuk, hogy a levélszemétszűrő átvizsgálja-e az olvasatlan leveleket a Microsoft Outlook elindulásakor. Ezt a beállítást NE használjuk, ha sok az olvasatlan levelünk az Outlookban, mivel ebben az esetben a G Data az olvasatlan leveleket újra és újra át fogja nézni.

Más levelezőszoftverek esetében itt állíthatjuk be, hogy a G Data milyen üzenetet jelenítsen meg, ha levélszemetet talál.



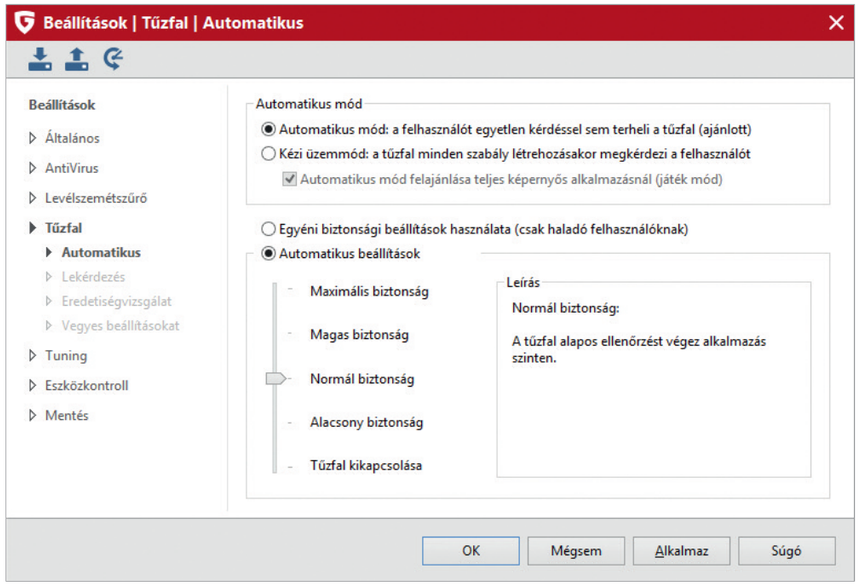
Tűzfal beállításai

A G Data termékek tűzfala alapértelmezett beállításai szerint automatikus üzemmódra van állítva. Ebben az üzemmódban a G Data tűzfal maga hoz döntéseket arról, hogy melyik szoftvereket engedi kommunikálni az internettel. Ez a működési mód a tűzfal csendes, automatikus működését jelenti. A tűzfal ilyenkor teszi a dolgát, de nem zavarja kérdésekkel a felhasználót.

A legtöbb felhasználó számára az automatikus mód a megfelelő, ugyanakkor előfordulhat, hogy ebben a működési módban olyan szoftvereket is blokkol, melyeknek meg szeretnénk engedni, hogy kommunikáljanak az internettel. Ilyen lehet a népszerű Total Commander szoftver FTP kapcsolódási kísérlete, vagy akár a játékkonzol és a PC összekapcsolása. Ezeket a kommunikációkat automatikus üzemmódban a tűzfal megakadályozhatja.

Éppen ezért olyankor, amikor nem hétköznapi funkció vagy szoftver internetes kapcsolódását szeretnénk engedélyezni, a tűzfalat érdemes manuális módba kapcsolni.

Ha egy adott szoftver esetében automatikus módban használt tűzfal mellett próbáljuk meg engedélyezni az internetes kapcsolódást, a tűzfal egy szabályt készít a kapcsolódásról. Ezután – hiába kapcsoljuk manuális módba – a tűzfal már nem fog rákérdezni arra, hogy engedélyezni szeretnénk-e a kapcsolódást. Éppen ezért, ha azt észleljük, hogy egy adott szoftver esetében nem tudjuk létrehozni az internetes kapcsolódást, nyissuk meg a tűzfal kezelőfelületét és ellenőrizzük, hogy létezik-e már az adott szoftverre vonatkozó tiltó szabály. Azt, hogy a tűzfal akadályozza-e meg a szoftver internetes kapcsolódását, tesztelhetjük a tűzfal ideiglenes, néhány perces kikapcsolásával is.



Amennyiben a tűzfalat manuális módba állítjuk, az alábbi párbeszédablak jelenik meg, amikor egy olyan szoftver szeretne internetes kapcsolódást teremteni, melyre nézve még nem hoztunk szabályt. A párbeszédablakon látjuk, hogy melyik alkalmazás próbál meg kapcsolódni, és azt is, hogy ezt melyik alkalmazás indította el. Láthatjuk a portot, a kapcsolat típusát és azt az IP címet, melyhez a szoftver kapcsolódni próbál.

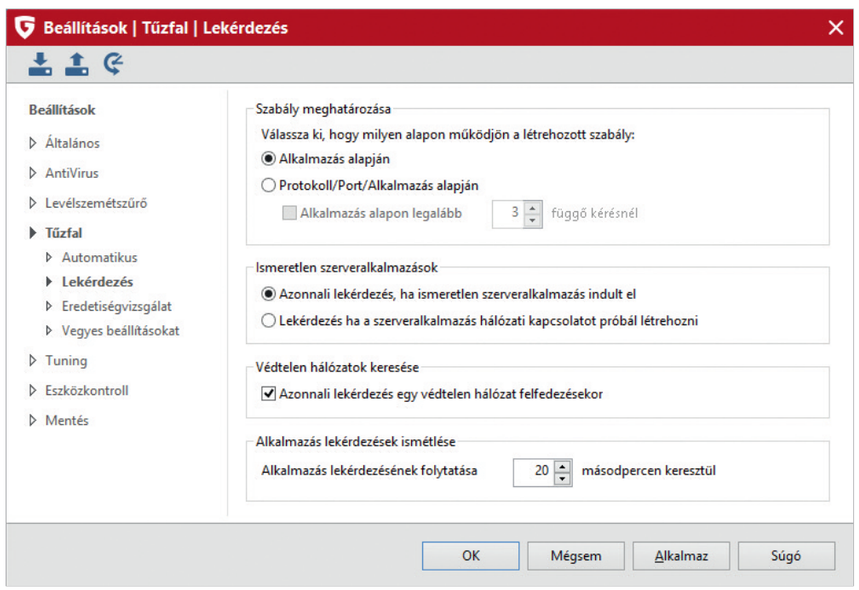
A fenti információk alapján döntést kell hoznunk arról, hogy az adott szoftver kapcsolódását megengedjük-e. Dönthetünk úgy, hogy az adott szoftver kapcsolódását mindig megengedjük. Ebben az esetben engedélyező tűzfalszabály jön létre. Dönthetünk úgy, hogy az adott szoftver kapcsolódását mindig tiltjuk. Ebben az esetben tiltó tűzfalszabály jön létre.

Emellett dönthetünk úgy is, hogy ideiglenes engedélyező vagy tiltó tűzfalszabályt hozunk létre. Ebben az esetben a szoftver ismételt futtatásakor a tűzfal újra rá fog kérdezni, hogy engedélyezni vagy tiltani szeretnénk a kapcsolódást.

A tűzfal alapértelmezetten normál biztonsági szintre van állítva, melyet két lépcsőben szigoríthatunk vagy enyhébbre állíthatunk. Az alapbeállítás a legtöbb felhasználó számára megfelelő, átállítását csak haladó felhasználók számára javasoljuk.

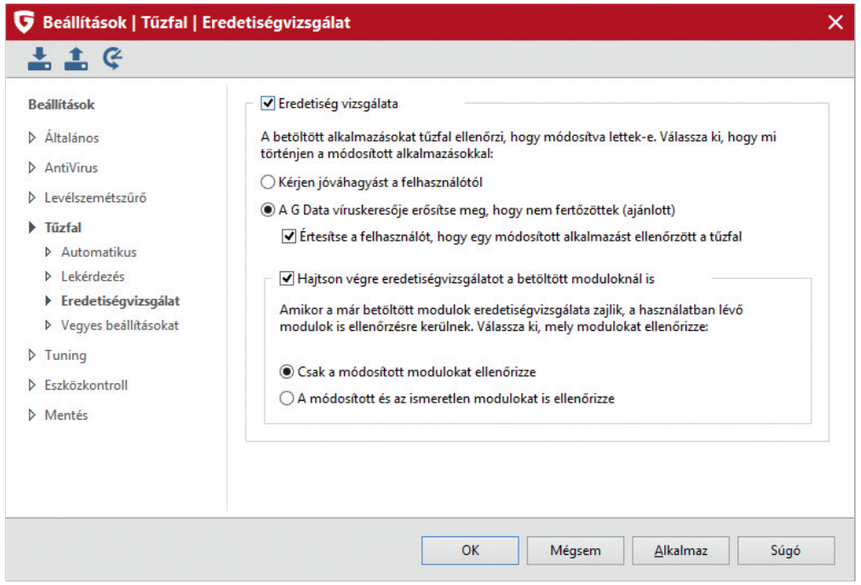
Amennyiben a működést egyéni biztonsági beállításokra állítjuk, a bal oldali menüben újabb menüpontok válnak elérhetővé.

A lekérdezési mód menüpontban beállíthatjuk, hogy a tűzfal hogyan – alkalmazások vagy portok szerint – hozza létre a szabályokat, és rákérdezzen-e a kívánt beállításokra, ha egy ismeretlen szerveroldali alkalmazás próbál csatlakozni a géphez vagy ha egy nem biztonságos hálózathoz csatlakozunk.



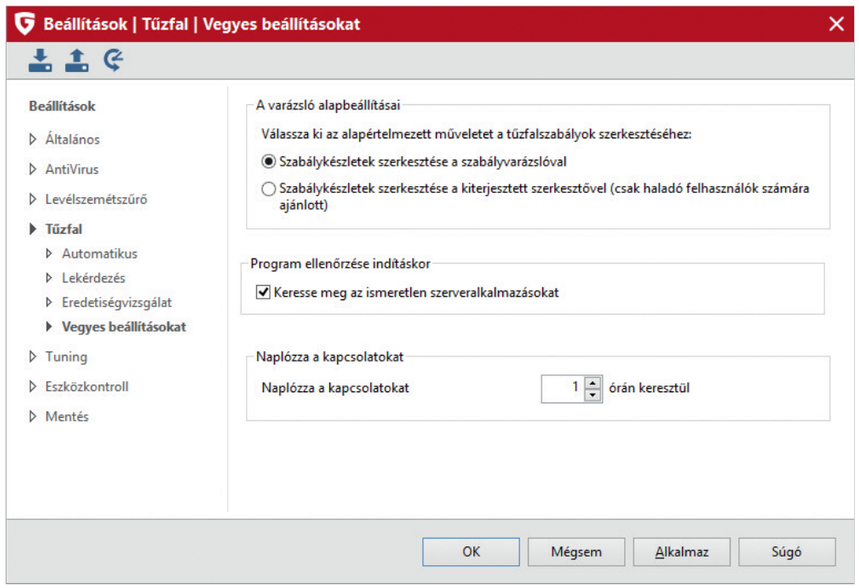
Az eredetvizsgálat segítségével a tűzfal azoknak a szoftvereknek a kapcsolódásait is ellenőrzi, melyeket korábban már engedélyeztünk, amennyiben az adott szoftver valamilyen módosításra került.

Az alapértelmezett beállítások szerint ilyenkor a tűzfal nem kér újbóli jóváhagyást a felhasználótól, hanem a G Data AntiVirus motorok segítségével vizsgálja át a szoftvert, hogy megállapítsa, valamilyen kártevő okozta-e a szoftver módosítását. A tűzfal az eredetvizsgálatot a már betöltött modulok esetében is elvégzi, de csak a módosított modulokra nézve. A beállítást még szigorúbbra vehetjük, ha bekapcsoljuk a módosított és az ismeretlen modulok átvizsgálását is.



A további beállítások kiválasztásával beállíthatjuk, hogy a szabályok szerkesztését a varázsló vagy pedig a szabályszerkesztő segítségével szeretnénk elvégezni.

Azt is megadhatjuk, hogy a tűzfal indításkor ellenőrizze-e az ismeretlen szerveroldali alkalmazásokat és hogy mennyi időre őrizze meg az egyes kapcsolatok naplófájljait.



Tűzfalszabályok kezelése

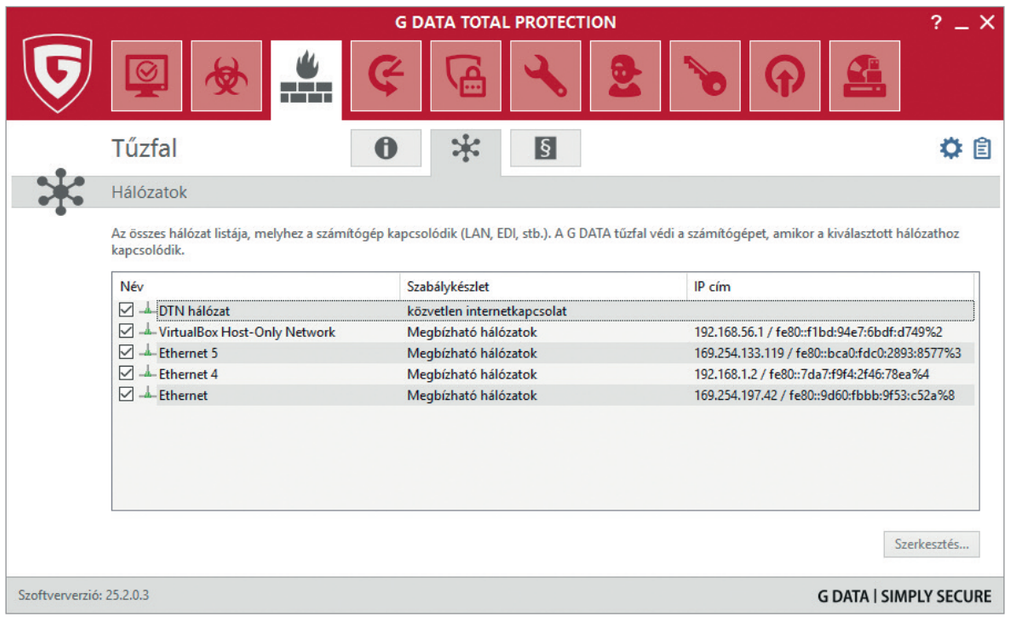
A tűzfalszabályok kezeléséhez meg kell nyitnunk a tűzfalbeállítások párbeszédablakát. Ehhez kattintsunk a tűzfal fülre a G Data szoftverének fő kezelőablakán.

A megnyíló párbeszédablakon láthatjuk a tűzfal állapotát. A zöld körben elhelyezett pipák és a piros háromszögben megjelenő felkiáltójelek mellett lévő feliratok linkként működnek. Ha rájuk kattintunk, megnyílnak a hozzájuk tartozó beállítások.

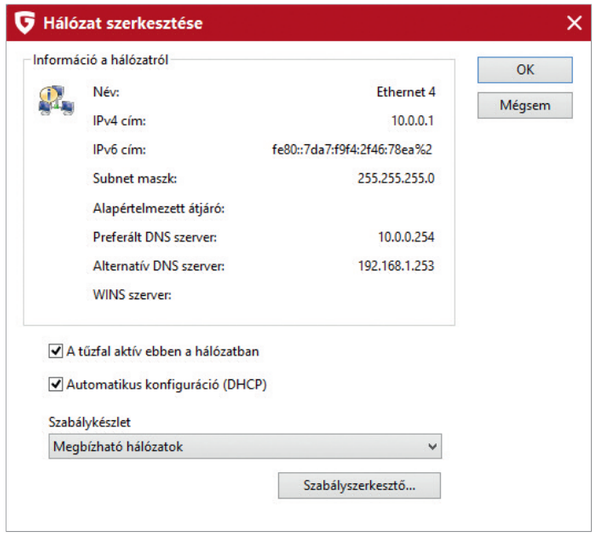
Ha a biztonság feliratra kattintunk, a már ismert párbeszédablak nyílik meg, melyen a tűzfal működésének szigorúságát állíthatjuk be.

Az üzemmód felirat ugyanezt a párbeszédablakot nyitja meg, és lehetőséget biztosít az automatikus és a manuális mód közötti választásra.

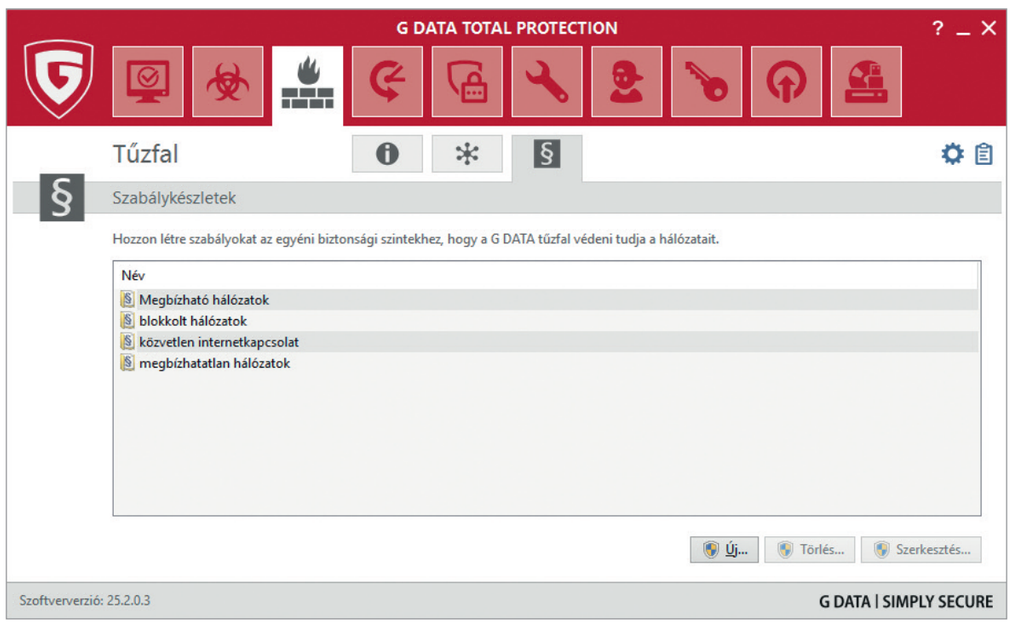
A hálózatok a számítógép által ismert hálózatok listáját nyitja meg. Ugyanezt a párbeszédablakot elérhetjük a bal oldali menüből is a hálózatok menüpontra kattintva.

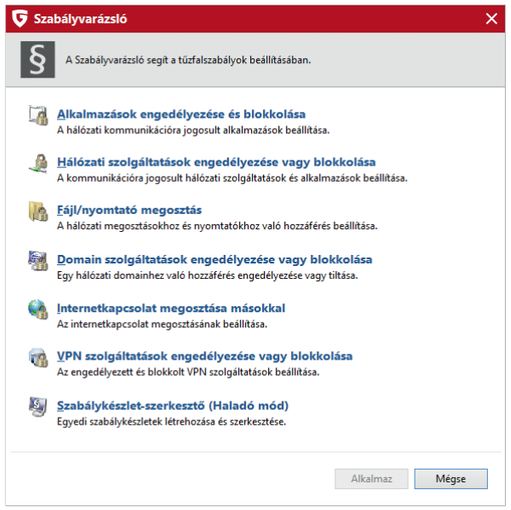


Amennyiben az egyes hálózatokat dupla kattintással megnyitjuk, lehetőségünk van a hálózathoz kapcsolódó szabályrendszerek szerkesztésére és a hálózat biztonságosnak vagy megbízhatatlannak való megjelölésére. Az egyes beállításokhoz szigorúbb vagy enyhébb tűzfalszabályok tartozhatnak, melyeket magunk is szerkeszthetünk. A szabályok szerkesztése azonban haladó felhasználók számára javasolt.



A menüben a szabálykészletek menüpontra kattintva megnyílnak az egyes csoportok.





Ha egy szabályrendszer nevére kattintunk, megnyílik a szabályvarázsló, melynek segítségével új szabályokat adhatunk a szabályrendszerhez.
Ha például kiválasztjuk a megbízható hálózatok szabályrendszerét, a szabályvarázsló segítségével kiválaszthatjuk, hogy milyen szabályt szeretnénk hozzáadni a szabályrendszerhez.

A lehetőségek sorban:

1. Átengedhetünk vagy blokkolhatunk egy megadott alkalmazást.

2. Átengedhetünk vagy blokkolhatunk hálózati szolgáltatásokat.

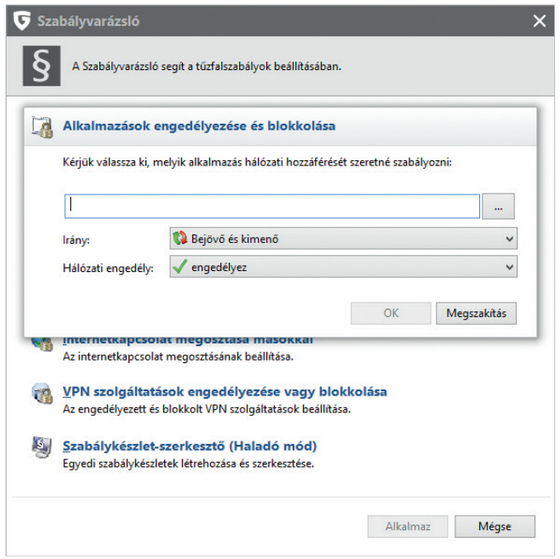
3. Megengedhetjük vagy tilthatjuk az adott hálózatra vonatkozóan a fájl- és a nyomtatómegosztást.

4. Engedélyezhetjük vagy tilthatjuk a domainszolgáltatásokat.

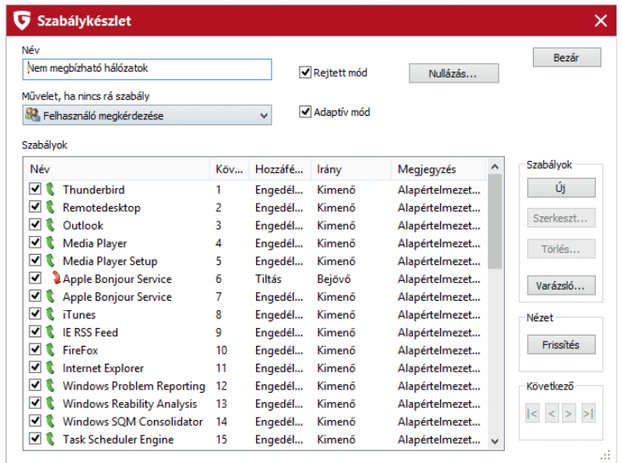
5. Megengedhetjük az internetnetkapcsolat megosztását.

6. Megengedhetjük vagy tilthatjuk a VPN kapcsolatok létrehozását.

7. És végül kiterjesztett szerkesztőmódba válthatunk.



A szabályvarázsló segítségével egyszerűen hozhatunk létre új szabályokat.

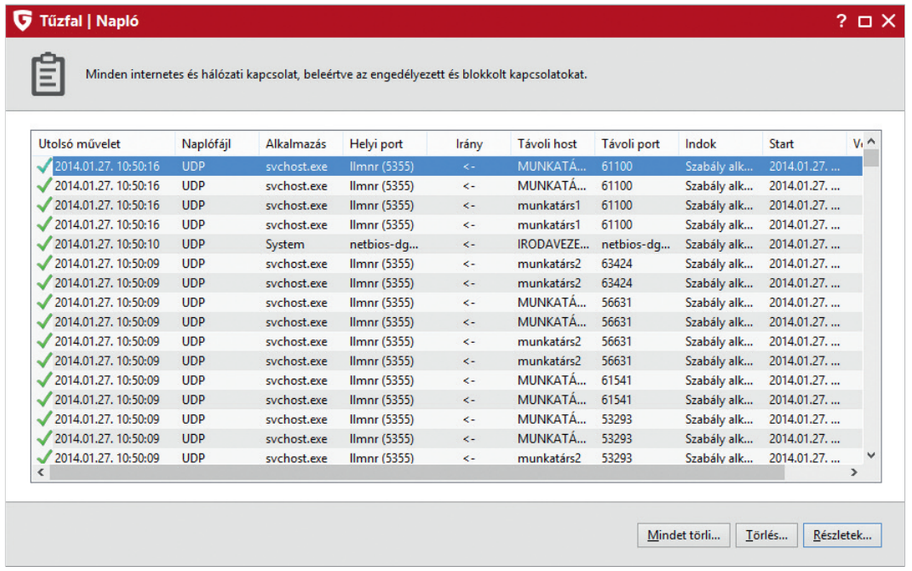


A haladó szerkesztőmód megnyitása után megadhatjuk, hogy milyen protokollra, milyen portra nézve szeretnénk szabályt létrehozni, azt, hogy a kimenő, a bejövő vagy mindkét irányú kapcsolatot engedélyezzük (vagy tiltjuk), és azt is, hogy a szabályt kizárólag egy adott alkalmazás számára hozzuk-e létre.

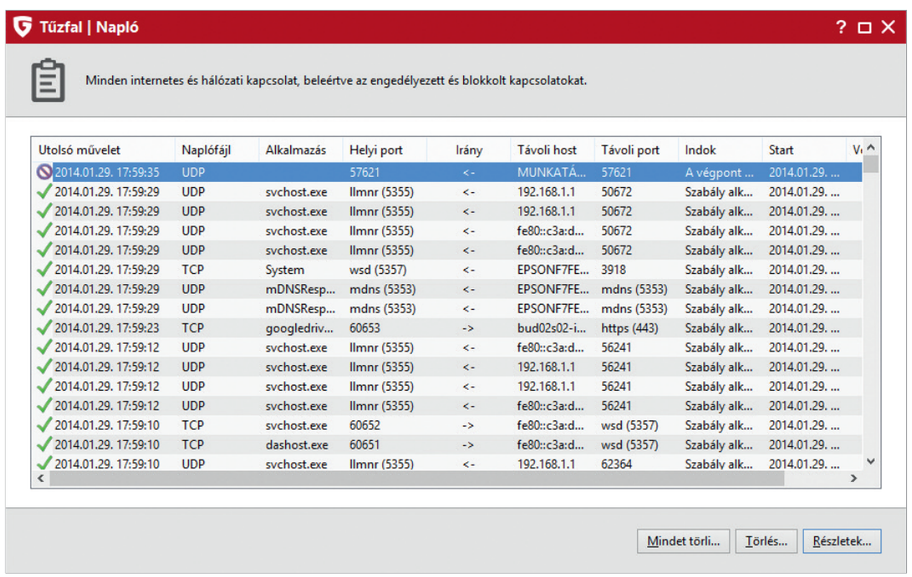
A kiterjesztett szabályszerkesztő segítségével időkeretet és IP tartományt is megadhatunk, melyekre nézve érvényesítjük a szabályt.

A bal oldali menüben a napló (log) menüpontot kiválasztva láthatjuk, hogy a tűzfal milyen szabályokat hozott létre.

Amennyiben az egyes szabályokra kattintunk a jobb egérgombbal, lehetőségünk van megnyitni és szerkeszteni az adott szabályt.



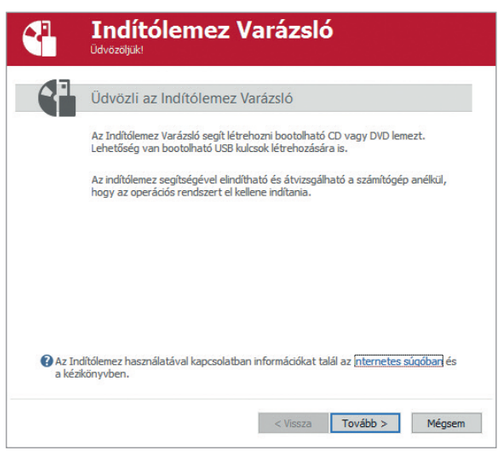
Tipp! Amennyiben egy általunk használni kívánt alkalmazást blokkol a tűzfal, keressük meg az adott szabályt a naplóban és engedélyezzük a kommunikációt. A szűrő segítségével lehetőségünk van arra, hogy szűrjük a szabályok listáját. A szűrőt egy naplóbejegyzésre kattintva a jobb egérgombbal hívhatjuk elő.



Indítólemez létrehozása

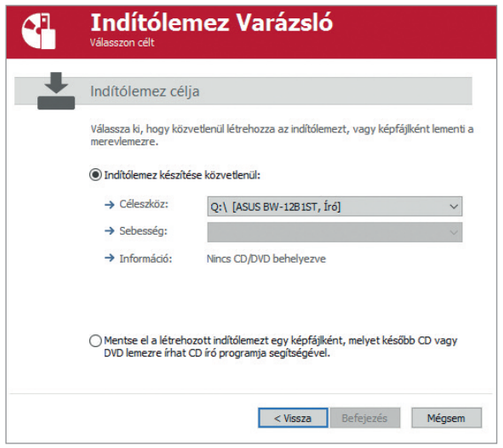
Az indítólemez fontos funkciókkal rendelkezik. Ha a gépünk megfertőződik, az indítólemez segítségével állíthatjuk helyre. Az indítólemezt arra is használhatjuk, hogy olyan gépet tisztítsunk meg, melyen nem fut a G Data védelmi szoftvere.

Az indítólemez készítését a szoftver fő kezelőablakának vírusvédelem fülén, a jobb alsó sarokban érjük el.



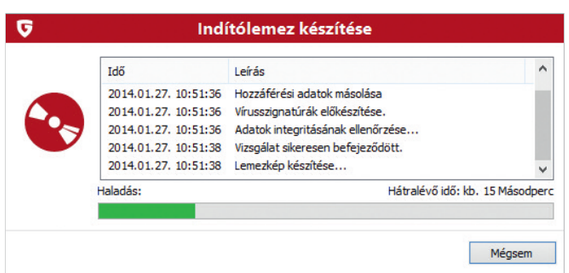
Kattintsunk az indítólemez készítése gombra, és megjelenik az alábbi párbeszédablak.

A varázsló lépésenként végig fog vezetni minket az indítólemez létrehozásán. Elsőként a vírusdefiníciós adatbázist frissíti, annak érdekében, hogy az indítólemezre a legfrissebb adatbázis kerüljön.



Ezután kiválaszthatjuk, hogy CD-lemezt írunk, vagy egy fájlban, a merevlemezre készítjük el a lemezképet, melyet a későbbiek során írunk CD-re. Amennyiben a gépben nincs CD-író, csak ez az utóbbi lehetőség áll rendelkezésünkre.

A befejezés gombra kattintás után a varázsló összegyűjti az adatokat a lemezre íráshoz, majd megírja a lemezt. A folyamat sikeres befejezése után a bezárás gombra kattintva léphetünk ki a varázslóból.



Szülői felügyelet beállításai

A szülői felügyeletet a G Data szoftverek fő kezelőablakán a szülői felügyelet, majd a szülői felügyelet megnyitása gombokkal nyithatjuk meg.

A szülői felügyelet használatához szükséges, hogy a számítógépen egy rendszergazdai jogosultságokkal rendelkező szülői fiókot és egy vagy több rendszergazdai jogosultságokkal nem rendelkező fiókot hozzunk létre a gyerekek számára. A rendszergazdák módosíthatják a szülői felügyelet beállításait.

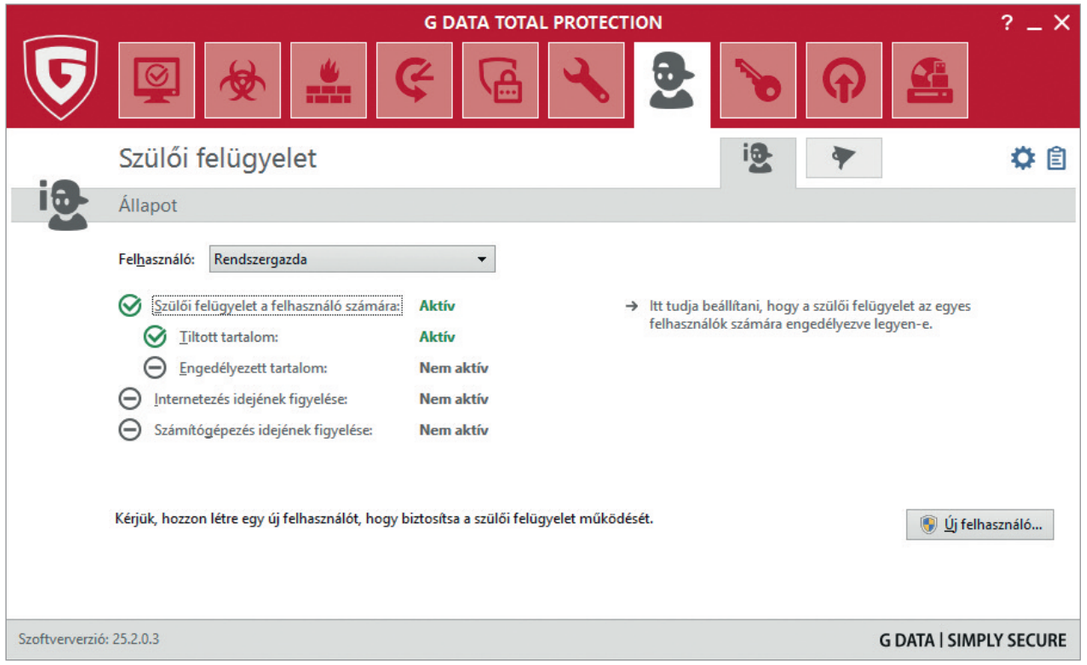
A szülői felügyelet párbeszédablakán kiválaszthatjuk, hogy melyik felhasználó beállításait szeretnénk módosítani. Az egyes beállítások mellett zöld körben lévő pipák vagy barna körben lévő mínusz jelek jelzik, hogy az adott beállítás aktív-e.

Amennyiben szeretnénk aktiválni a szülői felügyeletet, kattintsunk az első feliratra. A megjelenő zöld körben lévő pipa jelzi, hogy aktiváltuk a szülői felügyeletet.

A szülői felügyelet két módon működhet a számítógépen. Az első, hogy bizonyos tartalmakat kategóriák és kulcsszavak szerint tiltunk.
A második, hogy kizárólag bizonyos weboldalak megtekintését engedélyezzük a számítógépen.

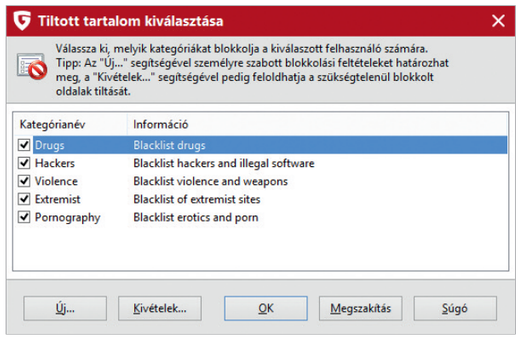
A két mód közül egyszerre mindig csak az egyiket aktiválhatjuk, azaz a szoftver vagy kategóriák és kulcsszavak alapján tiltja a weboldalakat, vagy kizárólag azon weboldalak felkeresését engedélyezi, melyeket felvettünk a fehérlistára.

Az alábbi ablakot láthatjuk, amikor a szoftver kategóriák és kulcsszavak alapján szűri a weboldalakat.



És az alábbi ablakot láthatjuk, amikor a szoftver csak azoknak a weboldalaknak a felkeresését engedélyezi, melyeket felvettünk a fehérlistára.

Amennyiben kategóriák alapján szeretnénk szűrni a weboldalakat, győződjünk meg arról, hogy a tiltott oldalak szűrése van bekapcsolva.

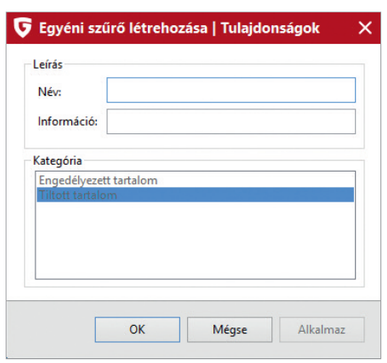


Kattintsunk duplán a tiltott tartalmak feliratra, és az alábbi párbeszédablak jelenik meg.

Az előre definiált kategóriákkal a drogokkal (drugs), kapcsolatos, a hackerekkel (hackers), az erőszakkal (violence), az extrém tartalmakkal (extremist) kapcsolatos és a pornográf (pornography) weboldalakat szűrhetjük.

Új – a nem kívánt magyar szavakat tartalmazó lista készítéséhez – kattintsunk az új gombra. A megjelenő párbeszédablakban adjunk nevet a listánknak, majd kattintsunk az OK gombra.

A megjelenő párbeszédablakon kulcsszavakat adhatunk a listánkhoz, és az egyes kulcsszavakhoz kapcsolódóan beállíthatjuk, hogy a G Data védelmi szoftvere hol keresse az adott kulcsszót a weboldal tartalmában. Az alapbeállítás szerint a G Data keresni fogja a kulcsszavakat a webcímben (url), a fejlécben, a weboldal metainformációiban és a weboldal teljes szövegében.



Adjunk tetszés szerinti kulcsszót a listához, majd kattintsunk az alkalmaz gombra.

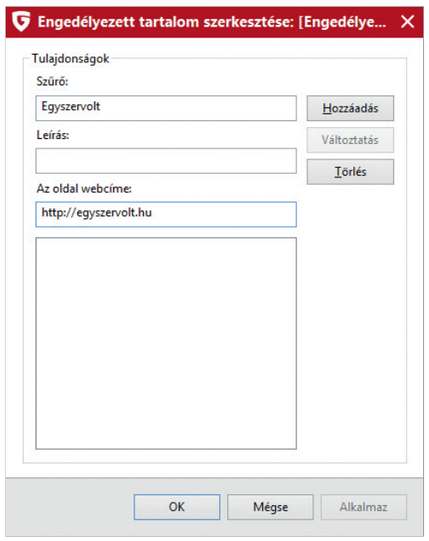
A tiltott tartalmak beállítása a szülői felügyelet használatának enyhébb módja, mivel a G Data védelmi rendszere csak azokat a weboldalakat fogja tiltani, melyek szerepelnek a tiltólistán vagy amelyek tartalmában tiltott kulcsszó szerepel.
Ez a működésmód korlátozza a tartalmak megjelenítését a nagyobb gyerekek számára, de soha nem tudja 100 százalékosan kiszűrni az összes felnőtt-tartalmat, mivel nem tud kulcsszavakat keresni például videófájlokban.

Az engedélyezett tartalmak listájának használata a szülői felügyelet használatának szigorúbb módja, melyet a kisebb gyermekek felhasználói fiókjainak védelmére ajánlunk.

Amennyiben ezt az üzemmódot szeretnénk aktiválni, a szülői felügyelet fő kezelőablakán kattintsunk kétszer az engedélyezett tartalmak feliratra.
A megnyíló ablakon válasszuk ki azokat a kategóriákat, melyeket engedélyezni szeretnénk. A gyermekeknek (kids) és a tinédzsereknek (teens) szóló tartalmakat külön címkék jelzik.

Az egyes kategóriák – a tiltólistákhoz hasonlóan – több ezer weboldalt tartalmaznak, melyeket a tartalomszűréssel foglalkozó nemzetközi Commtouch tart karban.

A magyar weboldalakat tartalmazó egyéni kategóriát az új gombra kattintva hozhatunk létre. A megjelenő párbeszédablakon először adjunk egy nevet a listánknak, majd kattintsunk az OK gombra.

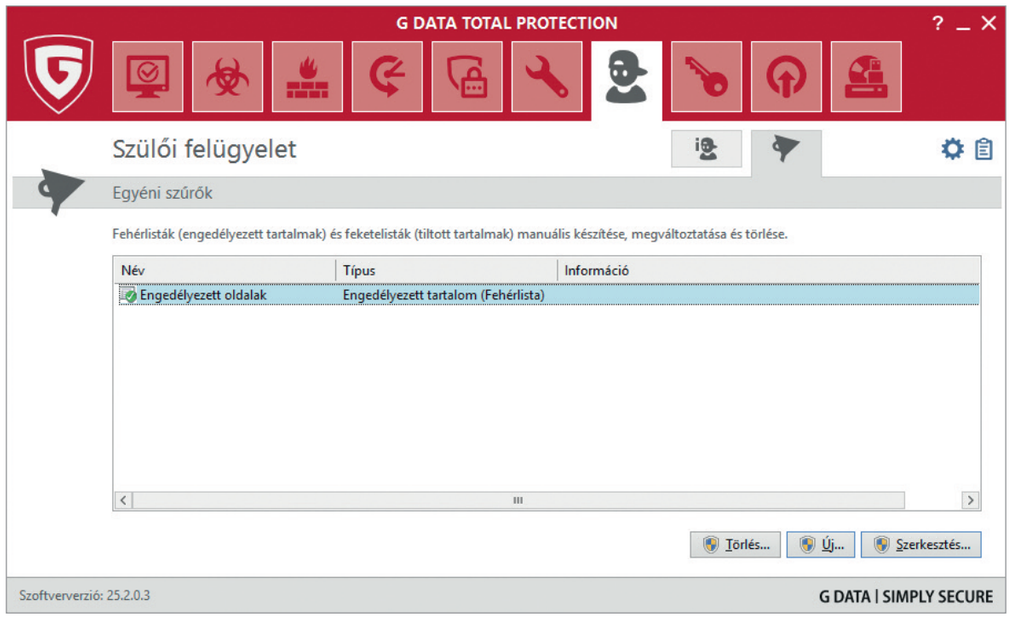


Ekkor egy párbeszédablak jelenik meg, melynek segítségével webcímeket adhatunk a listánkhoz. Amennyiben azt szeretnénk például, hogy kisgyermekünk csak néhány gyerekoldalt tudjon felkeresni, adjunk ehhez a listához ilyen weboldalakat (például: http://egyszervolt.hu, http://mese.tv).

Ezután kattintsunk az OK gombra. Ha semmilyen más kategóriát nem engedélyeztünk, a gyermekünk ezután csak az általunk meghatározott korlátozott számú meseoldalt tudja felkeresni az interneten.

Az általunk létrehozott szabályokat a bal oldali menüben a személyes szűrők menüpont kiválasztása után tudjuk szerkeszteni. A jobb oldali ablakban láthatjuk a fehérlistát és a feketelistát, melyek az engedélyezett és a tiltott weboldalakat tartalmazzák.

Ne felejtsük el, hogy a szoftvert vagy fehérlistákkal, vagy feketelistákkal tudjuk használni, az engedélyezett vagy a tiltott tartalmak listájának engedélyezésével, de egyszerre nem tudunk fehérlistákat és feketelistákat használni.



Kisebb, 8 év alatti gyermekek szülői felügyeletének beállítása során azt javasoljuk, hogy mi magunk határozzuk meg, hogy milyen weboldalakat látogathatnak, ezért használjuk az engedélyezett tartalmak üzemmódot. Nagyobb, 8 év feletti gyermekek szülői felügyeletének beállítását elvégezhetjük a tiltott tartalmak használatával, így ők már a webes tartalmak szélesebb körét fogják elérni.

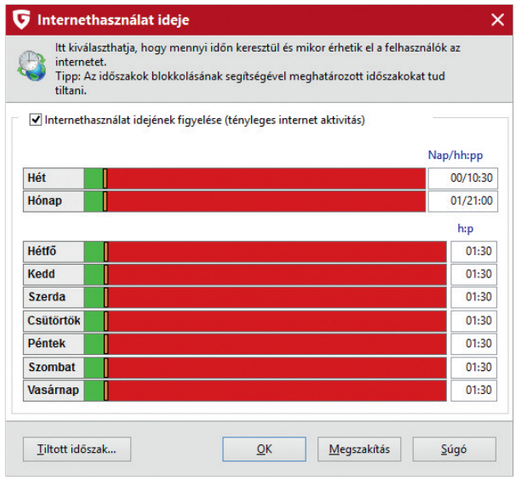
Amennyiben a családban több gyermek van, akik egy számítógépet használnak, azt javasoljuk, hogy a kisebb és a nagyobb gyermekek számára készítsünk külön felhasználói fiókot a Windowsban, így ezekre a fiókokra nézve különbözőképpen állíthatjuk be a szülői felügyeletet.

Az internetelérés és a számítógép-használat korlátozása

A szülői felügyelet fő kezelőablakán megtaláljuk a lehetőségét az internethasználat és a számítógép-használat korlátozásának és felügyeletének.

Mindkét beállítás hasonlóan működik. Kattintsunk a használni kívánt funkció nevére a megnyitáshoz.

Ha az internethasználat felügyeletére kattintunk, az alábbi párbeszédablak jelenik meg:

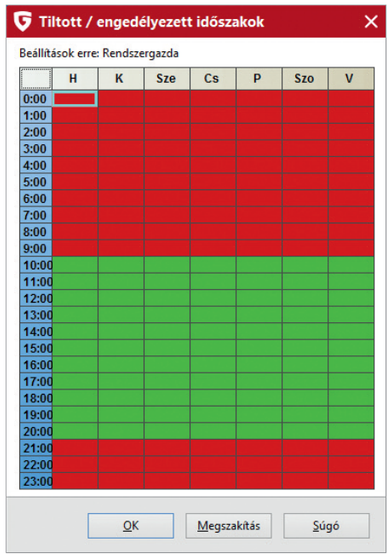


A csúszkák mozgatásával vagy a jobb oldalon található számok átírásával beállíthatjuk, hogy a gyermek mennyi ideig használhatja az internetet egy héten, egy hónapban vagy a hét különböző napjain.

A szoftver mindig a legalacsonyabb értéket fogja figyelembe venni. Így például ha engedélyezünk egy hónapra 3 napnyi használatot (ami 72 órát jelent), egy hétre pedig 10 órát, szerdára pedig 2 órát, akkor a gyermek szerdánként csak két órát fog tudni internetezni a számítógépen.

Ugyanez igaz a számítógép használatára. Amennyiben ezt a beállítást aktiváljuk, akkor a gyermek nem csak az internetet nem használhatja, de a G Data kilépteti őt a felhasználói fiókjából, így a számítógépet sem fogja tudni használni.

Mindkét korlátozást köthetjük időpontokhoz is, ha a fenti párbeszédablak alján található blokkolt időtartamok gombra kattintunk.



A megjelenő párbeszédablakon alapértelmezés szerint minden időpont engedélyezett (minden zöld). A módosításhoz az egérrel jelöljük ki a blokkolni kívánt időtartamot, majd a felugró ablakon kattintsunk az időtartam blokkolására. Ezzel a módszerrel beállíthatjuk, hogy a gyermek csak nappal vagy csak adott órákban használhassa az internetet vagy a számítógépet.

Fontos, hogy az alapértelmezett beállítások szerint a web monitor modulban csak a http protokoll (80-as port) szűrése van bekapcsolva, míg bizonyos weboldalak a titkosított https protokollt és az ehhez tartozó 443-as portot használják az interneteléréshez. A szülői felügyelet modulban az internethasználat korlátozása éppen ezért alapértelmezésben csak a titkosítatlan, http protokollon elért weboldalakat szűri.

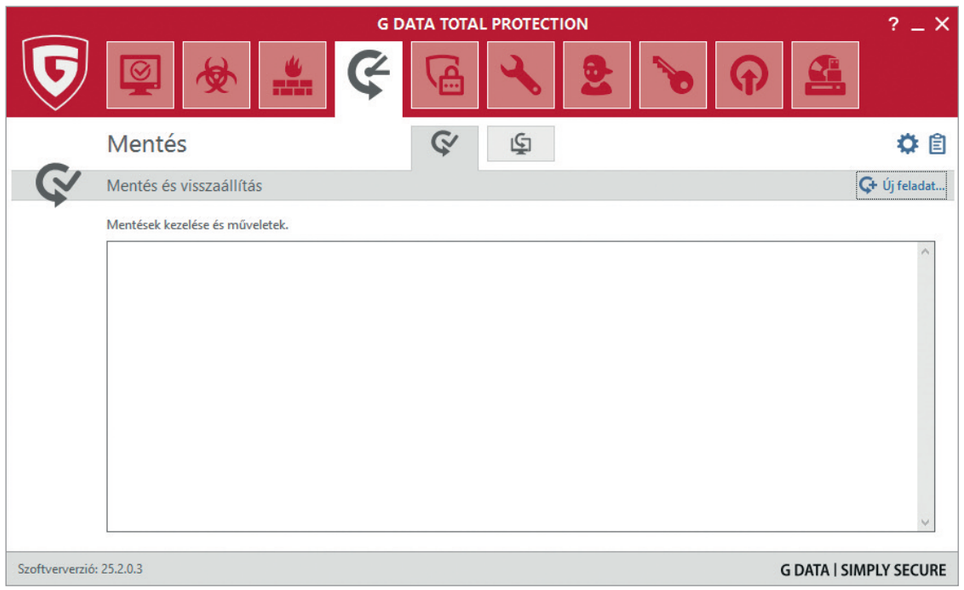
Adatmentés és archiválás

A G Data TotalProtection része egy adatmentés és archiválás modul. Megnyitásához a szoftver fő kezelőablakán kattintsunk az adatmentés, majd az adatmentés megnyitása gombra.

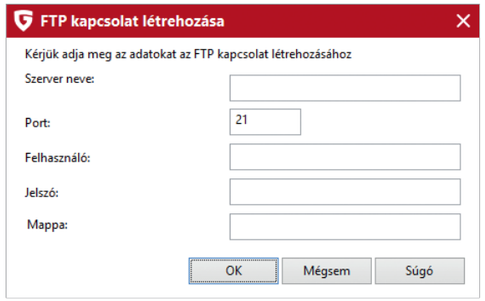
A megnyíló mentés modulban kiválaszthatjuk, hogy egy teljes lemezt vagy mappákat és fájlokat kívánunk archiválni.

Amennyiben a fájlok archiválását választjuk, meghatározhatjuk, hogy milyen típusú fájlokat – például képeket, zenei fájlokat, dokumentumokat – archiválunk. A keresési mappák meghatározásával kibővíthetjük, hogy a szoftver hol keresse a meghatározott fájlokat, a mentési mappák hozzáadásával pedig kijelölhetünk mappákat és fájlokat, melyek archiválására fognak kerülni.

Tipp! A G Data szoftvere nem másolja a fájlokat és a mappákat, hanem egyetlen tömörített, speciális típusú fájlba menti az adatokat, melyből csak a szoftver segítségével állíthatjuk vissza a mentett adatokat. Az adatok visszaállítása során lehetőségünk van a teljes mentés visszaállítására, vagy arra, hogy csak kiválasztott fájlokat és mappákat állítsuk vissza.

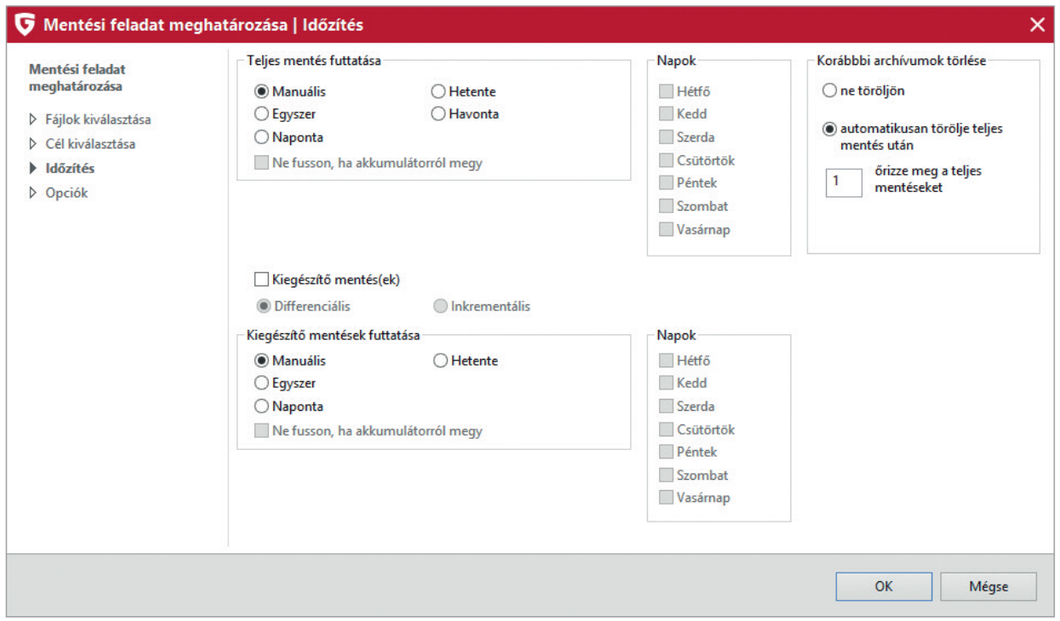


A cél kiválasztásával adhatjuk meg, hogy hova történjen a mentés. Fájljainkat menthetjük helyi meghajtókra és távoli FTP szerverre is. Ez utóbbihoz jelöljük be az FTP szerverre másolás pipát, és a megjelenő ablakban adjuk meg az FTP szerver elérhetőségét. A G Data TotalProtection szoftver mellé a G Data 2GB ingyenes tárhelyet biztosít. Ennek használatához a regisztráció során e-mailben megkapott FTP címet, valamint hozzáférési adatunkat kell megadnunk az alábbi ablakban.



A 1:1 másolatok nem készíthetőek el FTP szerverekre. A 1:1 másolatok egy az egyben képezik le a forrásmappát a célmappába. Ez a beállítás törli a célmappában lévő eredeti fájlokat.

A fő ablakon az ütemezés megnyitásával beállíthatjuk, hogy a mentés meghatározott időpontokban és szabályok szerint újra és újra megtörténjen.



A teljes adatmentés esetében meghatározhatjuk, hogy naponta, hetente vagy havonta történjen meg az adatmentés, és megadhatjuk, hogy ne fusson le olyankor, amikor a notebook akkumulátorról működik.

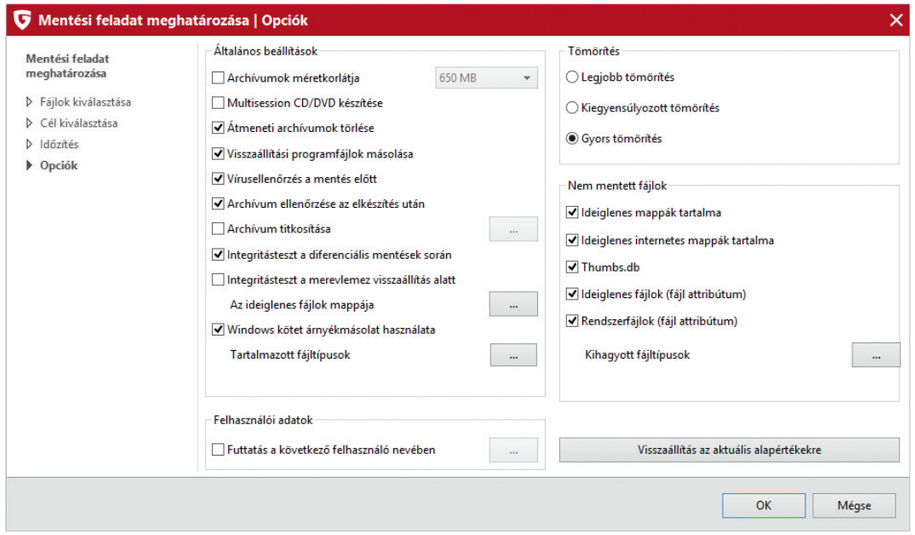
A korábbi archívumok törlése mezőben meghatározhatjuk, hogy a korábbi mentések ne kerüljenek törlésre, vagy azt, hogy a korábbi mentések automatikusan törlődjenek sikeres mentés után. Itt adhatjuk meg azt is, hogy a rendszer hány mentést őrizzen meg.

A részleges mentések esetében választhatunk a különbözeti mentés (differenciális) és a kiegészítő mentések (inkrementális) között. A két technológia közötti különbség, hogy a differenciális mentés esetében a szoftver az eredeti mentéshez képest mindig újra és újra elmenti a különbséget. Az inkrementális mentések esetében a szoftver viszont mindig csak az újabb és újabb különbséget menti el a legelső mentéshez képest.

Az inkrementális mentések ezért kisebbek, és gyakrabban lehet futtatni őket, mint a teljes mentéseket vagy a differenciális mentéseket. Így amennyiben egy teljes mentést ütemezünk minden hétre, ezt kiegészíthetjük napi inkrementális mentésekkel.

A mentési feladatok konfigurálását az adatmentés modul fő ablakának beállítások gombjára kattintva nyithatjuk meg (a gomb a fő ablak jobb felső sarkában található). Az alapbeállítások megváltoztatása csak haladó felhasználók részére javasolt.

Ha ide kattintunk, az alábbi ablak nyílik meg:



A beállítások segítségével meghatározhatjuk, hogy a G Data hogyan végezze el a fájlok archiválását.

Bal oldali mezők:

- Beállíthatjuk az egyes archív fájlok méretét attól függően, hogy azokat CD-re vagy DVD-re szeretnénk írni.
- Több menetben írható (multisession) CD- és DVD-lemezeket készíthetünk.
- Törölhetjük az ideiglenes archív fájlokat.
- Másolhatjuk és visszaállíthatjuk a programfájlokat.
- Vírusellenőrzést futtathatunk az archiválásra kerülő fájlokon.
- Az elkészült archív fájlokat ellenőrizhetjük.
- Titkosíthatjuk az archív fájlokat.
- Ellenőriztethetjük az inkrementális mentések integritását.
- Ellenőriztethetjük a merevlemez integritását visszaállítás alatt.
- Ellenőrizhetjük, hogy a forrás és a céllemez ugyanazon a merevlemezen van-e.
- Beállíthatjuk, hogy a gép minden felhasználójának személyes fájljait archiválja a program.

A gomb segítségével megadhatjuk az ideiglenes fájlok mappáját, melyet a szoftver használni fog, mialatt dolgozik.

A felhasználói adatoknál megadhatjuk, hogy melyik felhasználó nevében futtatjuk a feladatot.

Jobb oldali mezők:

- A tömörítési beállításokkal megadhatjuk, hogy a szoftver minél kisebb archív fájlokat készítsen (legjobb tömörítés), vagy inkább gyorsan igyekezzen végezni a feladattal (gyors tömörítés). Középútként választhatjuk a kiegyensúlyozott tömörítést.
- A kizárt fájlok megadásával eldönthetjük, hogy milyen fájlok ne kerüljenek archiválásra. A következő típusokat zárhatjuk ki:
  - Ideiglenes könyvtárak fájljai.
  - Böngészők ideiglenes könyvtárainak fájljai.
  - Thumbs.db fájlok.
  - Ideiglenes fájlok a fájlattribútumok szerint.
  - Rendszerfájlok a fájlattribútumok szerint.

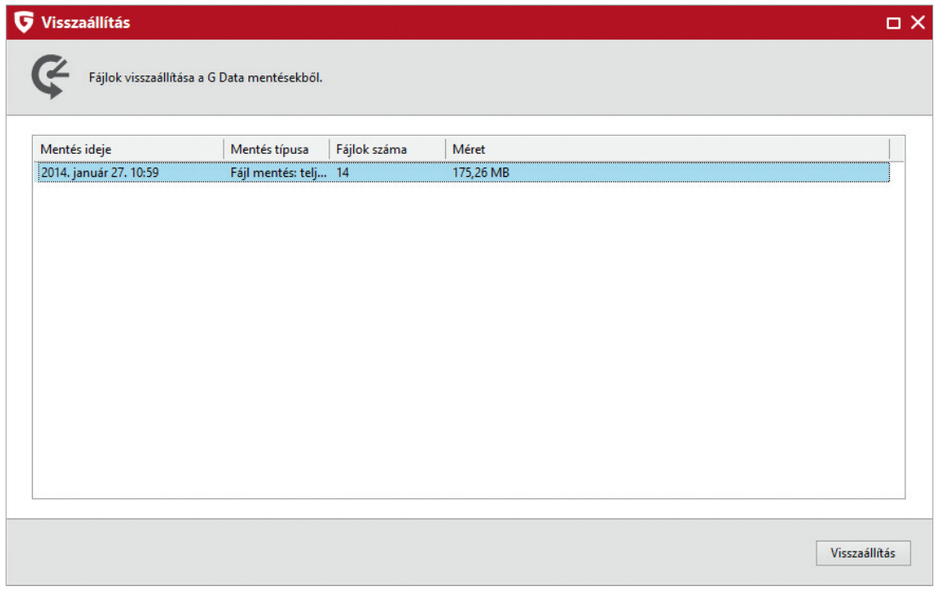
A fájltípusok kizárása gombbal plusz fájltípusokat adhatunk a kizárt fájlok listájához.

Az alapbeállítások visszaállítása gombbal visszaállíthatjuk a szoftver eredeti beállításait.

A Windows volume shadow copy technológia lehetővé teszi a fájlok másolását akkor is, ha azok zárolva vannak.

Fájlok visszaállítása

A mentések visszaállításához kattintsunk a bal oldali menüben a restore menü-pontra, majd dupla kattintással vagy a jobb alsó sarokban található visszaállítás gombbal válasszuk ki, hogy melyik mentést szeretnénk visszaállítani.



A megjelenő ablakban kiválaszthatjuk, hogy a teljes lemezt vagy partíciót szeretnénk visszaállítani, vagy csak a kiválasztott partíciókat és fájlokat.

A bal oldali menüből a feladatok (actions) gombot választva láthatjuk, hogy milyen munkákat végezhetünk el a szoftver segítségével.

- Kezelhetjük az online archívumokat.
- CD-re vagy DVD-re írhatjuk a korábbi mentéseket.
- Importálhatunk archív fájlokat, melyek más gépen készültek.
- Klónozhatjuk a merevlemezt.
- Indítólemezt készíthetünk.

A merevlemez klónozása egy-az-egyben másolatot készít a merevlemez tartalmáról egy másik külső vagy belső merevlemezre.

Ha a bal oldali menüből a naplót választjuk, megtekinthetjük a korábbi mentések naplófájljait.

Lemezképek mentése

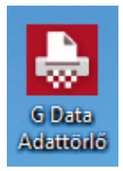
A lemezképek mentésének segítségével a teljes rendszert kimenthetjük külső meghajtóra. Ebben az esetben a merevlemez tartalma klónozódik a külső meghajtóra, és rendszerösszeomlás esetén ezt a lemezképet használhatjuk arra, hogy visszaállítsuk a rendszert.

Lemezkép készítéséhez az adatmentés fő ablakában az alapértelmezett fájlok mentése helyett válasszuk a lemezkép mentése opciót.

A forrás (source) az a meghajtó, melyet menteni szeretnénk, a cél pedig az a hely, ahova menteni szeretnénk. A start gombra való kattintásra a mentés elindul.

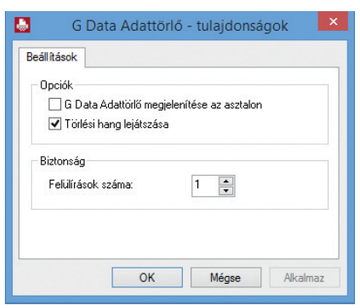
Rendszerösszeomlás esetén a G Data BootCD, azaz a G Data indítólemez segítségével állíthatjuk vissza az adatainkat. Indítsuk el a számítógépet az indítólemez segítségével, és a párbeszédablakban válasszuk ki a rendszer-visszaállítás lehetőséget. A lemezkép kiválasztása után a G Data TotalProtection visszaállítja a rendszert.

Adattörlés beállításai



Amennyiben a szoftver telepítése során telepítettük a G Data Adattörlőt, az asztalon elérhető a funkció ikonja.

Ha erre az ikonra kattintunk a jobb egérgombbal, előhívhatóak az adattörlő tulajdonságai.



A beállítások segítségével eldönthetjük, hogy szeretnénk-e megjeleníteni az asztalon az adattörlő ikonját, és az egyes adattörléseknél szeretnék-e lejátszani az alapértelmezett hangot.

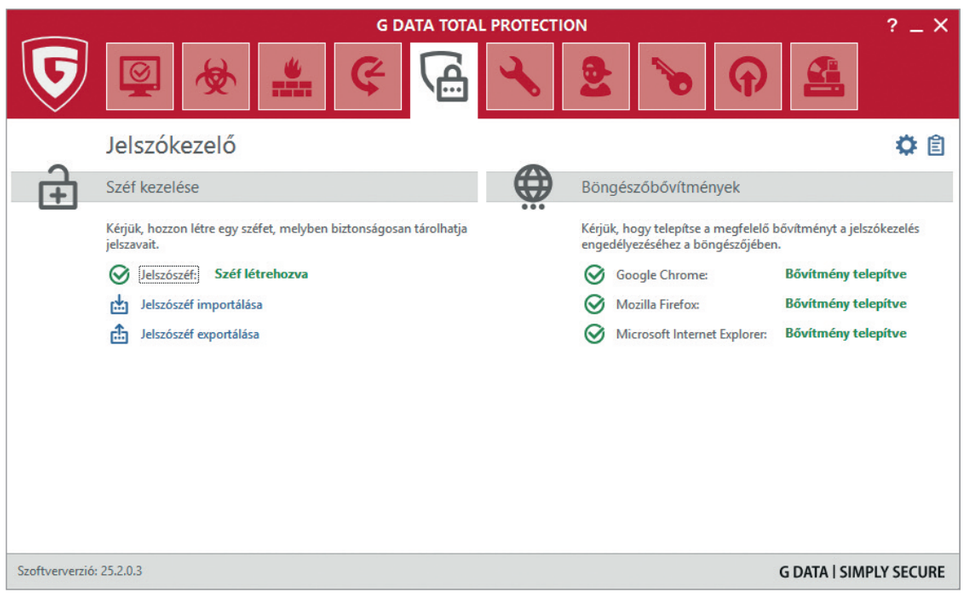
A biztonsági beállítások segítségével meghatározhatjuk, hogy a G Data Adattörlő hány alkalommal írja felül a törölt fájlok korábbi helyét.

Az alapértelmezett beállítás 1, ami a legtöbb esetben elegendő. A G Data Adattörlő nem a lomtárba helyezi a fájlokat, hanem véglegesen törli azokat, és a helyüket felülírja. Így az adatok nem állíthatóak vissza.

Az adattörlőt olyankor érdemes használnunk, amikor egy bizalmas dokumentumot végleg törölni szeretnénk a merevlemezről. Az adattörlés valamivel több időt vesz igénybe, mint a hagyományos törlés, mivel az eredeti adatok helyét a szoftver felülírja.

Jelszókezelő

A G Data Jelszókezelő amellett, hogy a különböző belépési adatokat megjegyzi, a biztonság növelésében is segítséget nyújt, mivel automatikusan képes megfelelően erős kombinációkat létrehozni az egyes weboldalakhoz. Az elmentett belépési adatok titkosítva tárolódnak a számítógép merevlemezén, ahonnan exportálás segítségével másik gépre is átvihetők. Az erős jelszavak, a titkosított tárolás és az automatikus működés így megnöveli az internetezés biztonságát és kényelmesebbé teszi a belépési adatok kezelését.

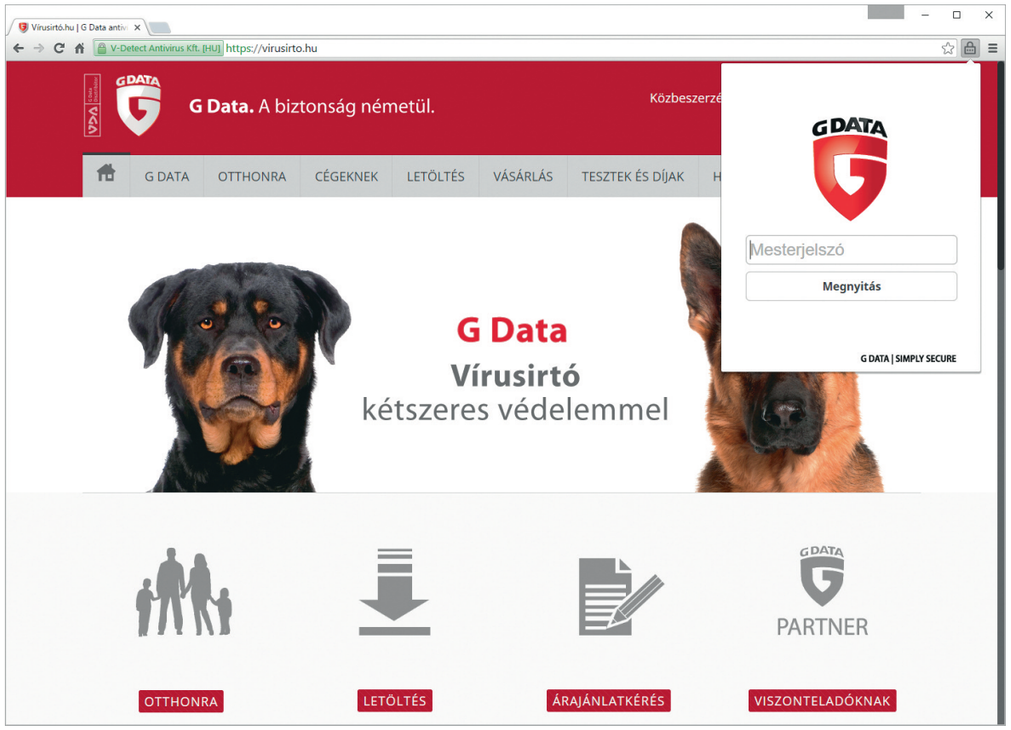


A Jelszókezelő használatba vételéhez először egy jelszószéfet kell létrehozni. Ez egy titkosított módon tárolt fájl, melybe a G Data az összes jelszavunkat menteni fogja. A jelszószéfet egy úgynevezett mesterjelszó védi. Így a felhasználónak egyedül a G Data mesterjelszavát kell megjegyeznie, a többi jelszavát a G Data Jelszókezelőben tárolhatja.

Fontos, hogy mesterjelszónak összetett kombinációt állítsunk be, mely tartalmaz kis- és nagybetűket, számokat és speciális írásjeleket is.

Minden gépen egyetlen egy jelszószéf lehet létrehozva.
Amennyiben új jelszószéfet hoz létre, a korábban beállított jelszószéf – minden tárolt jelszóval együtt – felülírásra kerül.

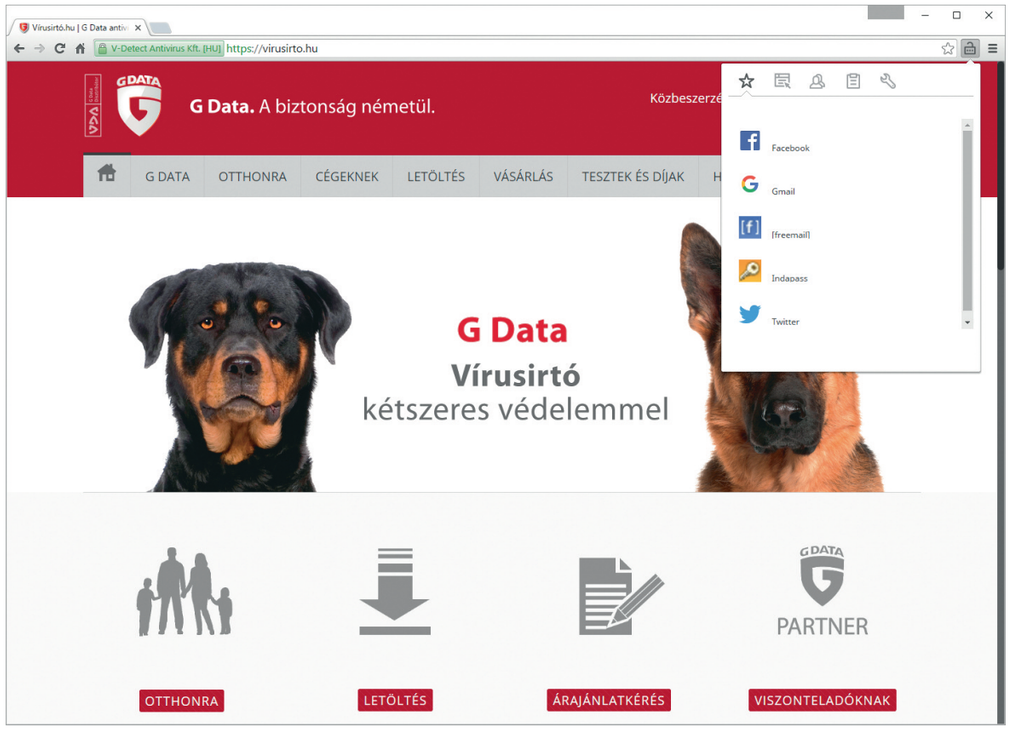
A jelszószéf létrehozása után a G Data Jelszókezelőt telepíthetjük a böngészőkbe. A modul jelenleg a Google Chrome, az Internet Explorer és a Mozilla Firefox különböző verzióit támogatja. A telepítés után a címsor mellett egy lakat ikon jelzi a jelenlétét, amelyre ha rákattintunk, akkor felajánlja az aktuális weboldalhoz korábban elmentett adatok beírását.



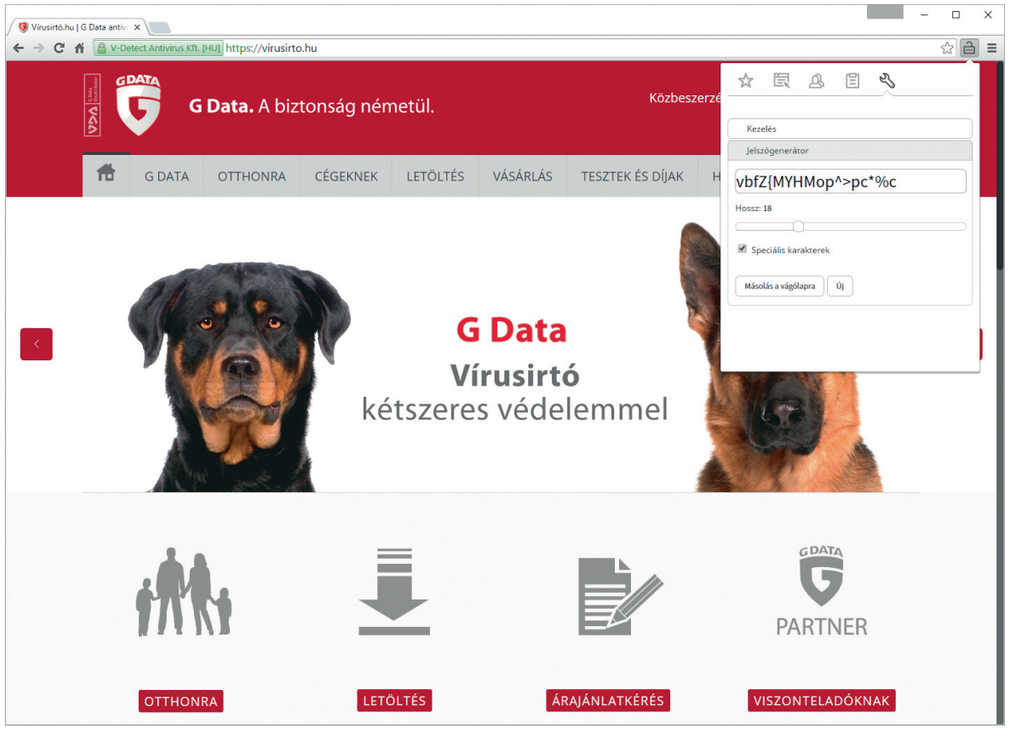
A Jelszókezelő használatba vételéhez a böngészőben először be kell lépnie a Jelszókezelő modulba a mesterjelszó megadásával.

A G Data Jelszókezelő ezután minden weboldalhoz automatikusan felajánlja a jelszavak elmentését.

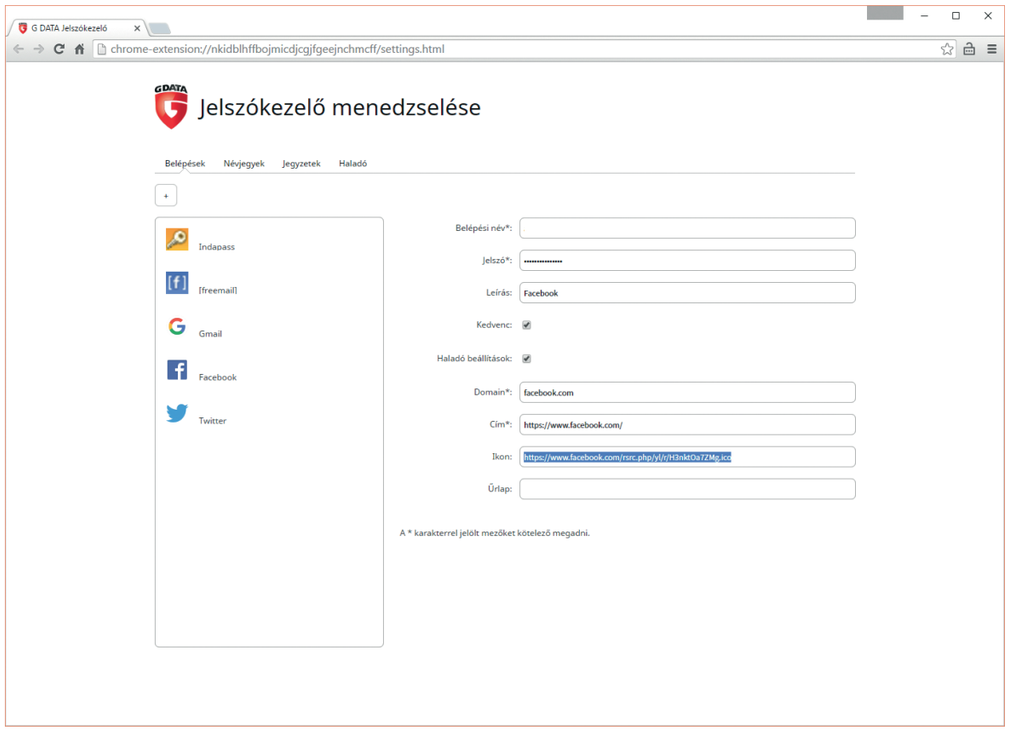
A Jelszókezelőben a kedvencként elmentett oldalakra kattintva az adott weboldalt automatikusan megnyitja a böngésző, és a G Data Jelszókezelő beírja az elmentett belépési adatokat.



A Jelszókezelő automatikusan képes erős jelszavakat generálni az egyes weboldalakhoz.



Az elmentett adatokat szerkeszteni tudjuk, ha megnyitjuk a Jelszókezelő beállításait.



Biztonsági tuning

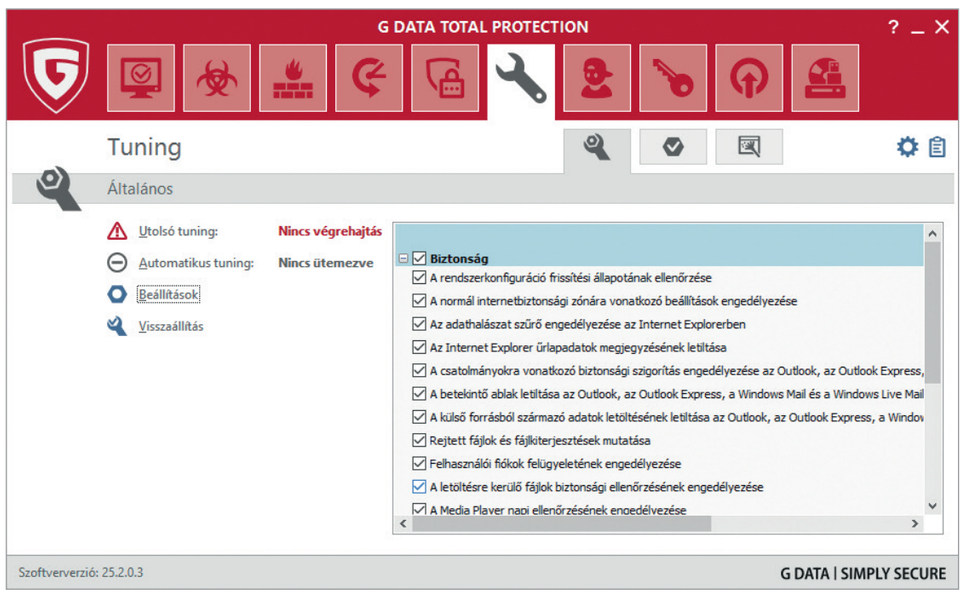
A G Data TotalProtection szoftver részét képezi a biztonsági tuning, mely a számítógép biztonsági beállításainak finomhangolására szolgál.

Fontos tudnunk, hogy a biztonsági tuningolás a számítógép beállításainak nem kívánt átállításával járhat, amennyiben olyan szigorúbb beállításokat eszközöl, melyek csökkentik a számítógép használatának kényelmét. Ilyen lehet például a Microsoft Outlook program esetén a beérkező levelekbe beágyazott képek letiltása.

A biztonsági tuning olyan beállításokat is visszaállíthat, melyeket magunk hoztunk létre, és ezzel befolyásolhatja a számítógép működését. Éppen ezért a biztonsági tuning futtatása csak gyakorlott felhasználók számára javasolt.

A tuning alapbeállításait a G Data fő kezelőablakának jobb felső sarkában lévő beállítások gombra kattintva nyithatjuk meg, vagy a tuning gomb mellett lévő lefelé mutató nyíl, majd a beállítások gomb megnyomásával hívhatjuk elő.

A fenti gombokra kattintva az alábbi párbeszédablakot kell látnunk:



Az alapbeállítások között megadhatjuk, hogy a G Data törölje a korábbi tuningokból megőrzött adatokat az alábbiak szerint:

- Visszaállítási adatok törlése 14 nap után.
- Megőrzött adatok törlése 14 nap után.
- Asztali parancsikonok törlése 180 nap után.

Ezenkívül beállíthatjuk, hogy a szoftver:

- Keressen Office frissítéseket a Windows frissítések mellett.
- Ne (!) készítsen részletes naplót a törölt elemekről.
- Véglegesen törölje az ideiglenes fájlokat.
- Ne (!) indítsa újra automatikusan a számítógépet.
- Hozzon létre egyéni visszaállítási pontokat.
- Hagyja figyelmen kívül a meghajtó típusát, amikor töredezettségmentesítést végez.

Az alapbeállítások módosítása ebben az esetben is csak haladó felhasználók számára javasolt.

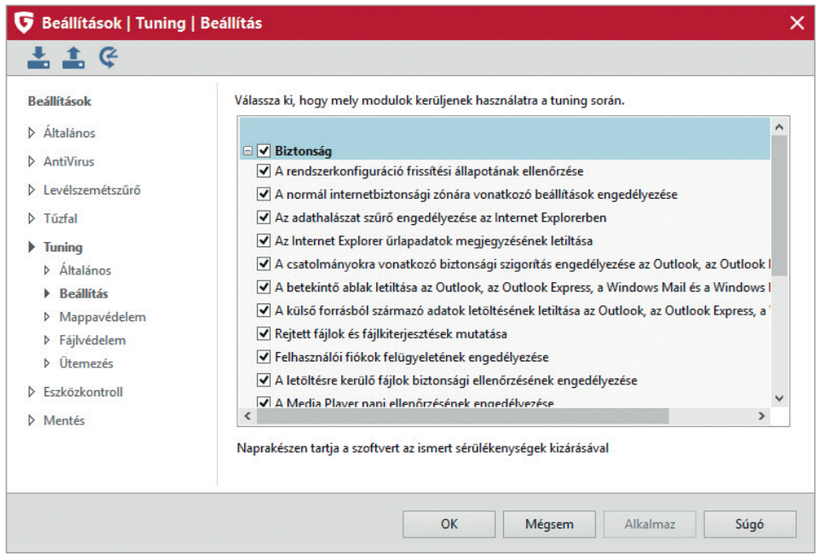
A bal oldali menüben a konfiguráció menüpontot választva láthatjuk és beállíthatjuk, hogy milyen akciókat hajt végre a tuning.

Ahogy említettük, a tuning végrehajtása csak haladó felhasználók számára javasolt, mivel a tuning megváltoztat vagy visszaváltoztat olyan biztonsági beállításokat, melyek a számítógép használatát befolyásolhatják.

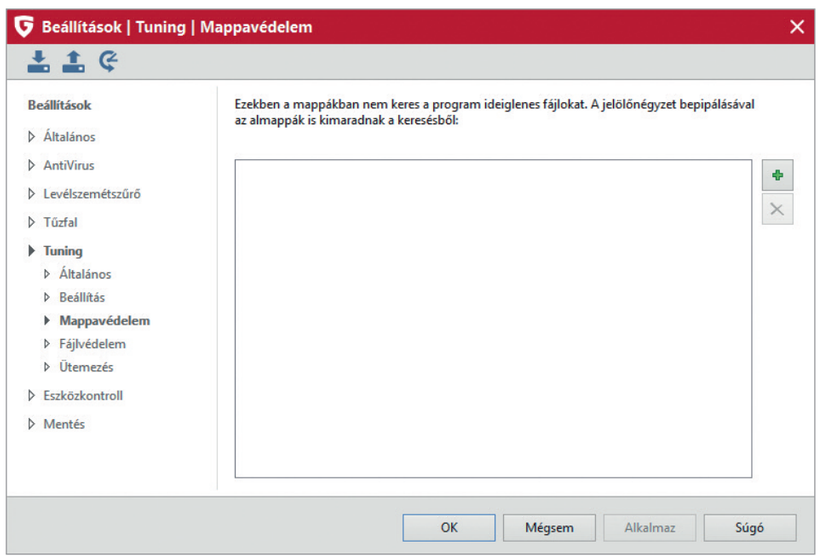
Az alapbeállítások szerint a tuning például:

- Törli a böngészők eltárolt jelszavait, így nem tudunk majd automatikusan bejelentkezni az általunk látogatott weboldalakra.
- Eltünteti a rejtett mappák és a fájlkiterjesztések láthatóságát.
- Kikapcsolja az Outlook Express és a Windows Mail betekintő ablakát.
- Kikapcsolja a külső adatok (például képek) letöltését a levelezőprogramokban.

Ezekkel a beállításokkal a tuning növeli a számítógép biztonságát, de sok felhasználó számára kényelmetlenebbé teszi annak használatát. Ne lepődjünk meg, ha a tuning lefuttatása után nem jelennek meg a képek a levelezőprogramokban vagy ha nem tudunk automatikusan bejelentkezni a kedvenc weboldalainkra és közösségi portáljainkra!



Amennyiben szeretnénk, hogy a tuning során egyes mappákban megőrződjenek az ideiglenes fájlok (.tmp), a bal oldali menüben válasszuk ki a védett mappák menüpontot, és adjuk ezeket a mappákat hozzá a védett mappák listájához.



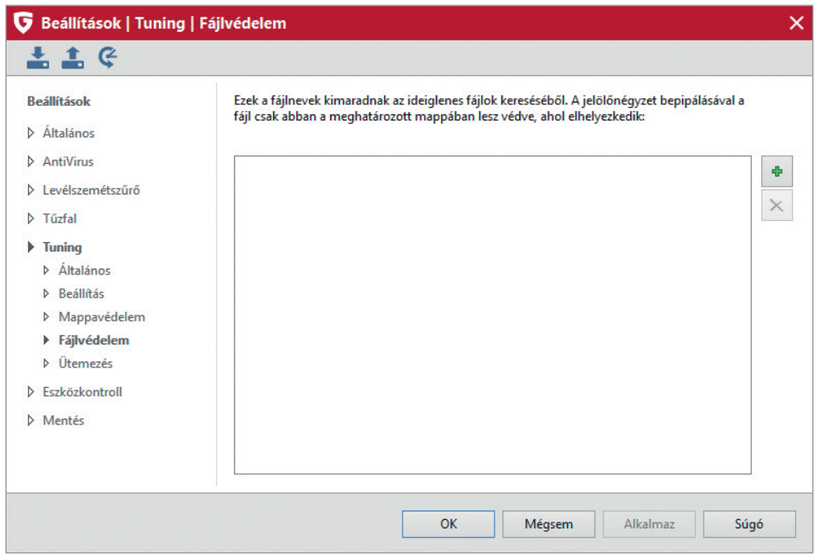
Ha a bal oldali menüben a védett fájlok menüpontra kattintunk, megadhatjuk a védett fájlok listáját, melyeket a szoftver érintetlenül hagy a tuning során.

Amennyiben pipát teszünk az egyes fájlok neve melletti jelölőnégyzetbe, a szoftver csak akkor hagyja érintetlenül az adott fájlokat, ha azok a pontosan a megadott mappában helyezkednek el.

A fájlnevek megadása során jokerként használhatjuk a * és a ? karaktereket. A * karakter több karaktert helyettesít, a ? pedig egyetlen karaktert helyettesít.

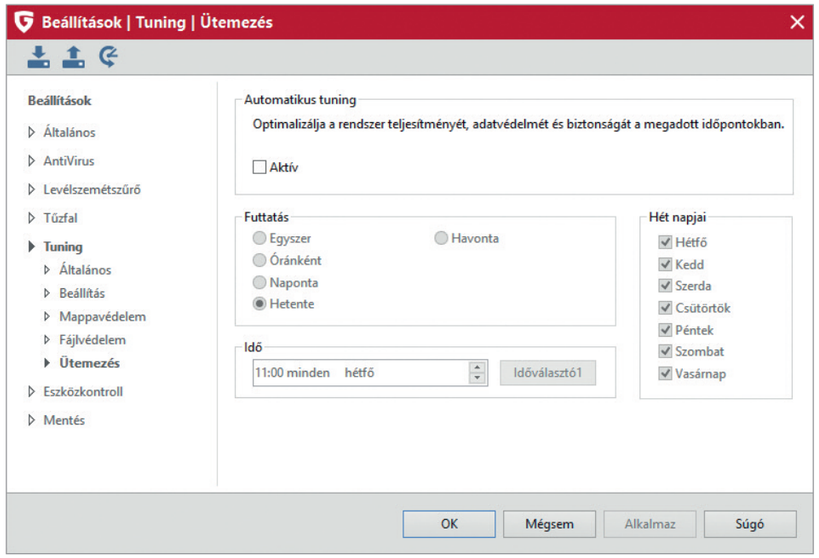
A *.doc, *.docx fájlnevek segítségével például védetté tehetjük a dokumentumfájlokat, míg a szerződés?.doc fájlnév csak a szerződés1.doc, a szerződés2.doc, a szerződés3.doc (és így tovább) fogja védeni, de nem fogja védeni a szerződés11.doc fájlt.

Amennyiben az összes olyan fájlt védeni kívánjuk, melynek a nevében szerepel a szerződés szó, ezt a *szerződés*.* parancs felvételével tehetjük meg. Ez védeni fogja az adásvételi_szerződés.doc és az ingatlan_szerződés.pdf fájlokat is.



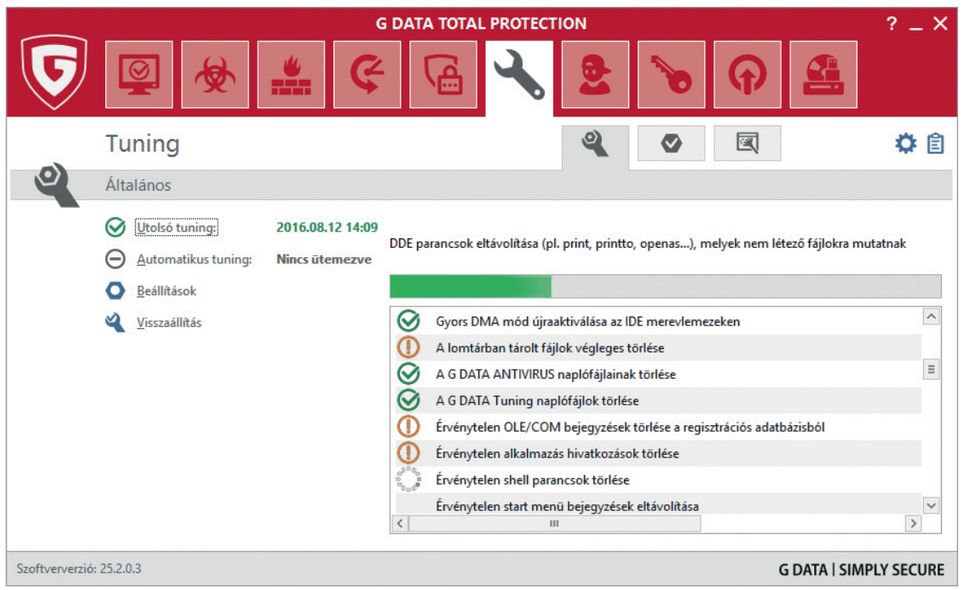
A tuning ütemezéséhez a bal oldali menüben válasszuk az ütemezés menüpontot.

A megjelenő párbeszédablakon az engedélyezett jelölőnégyzet bepipálásával engedélyezhetjük az ütemezést. Ezután a párbeszédablak segítségével beállíthatjuk, hogy a tuning mikor fusson le automatikusan.

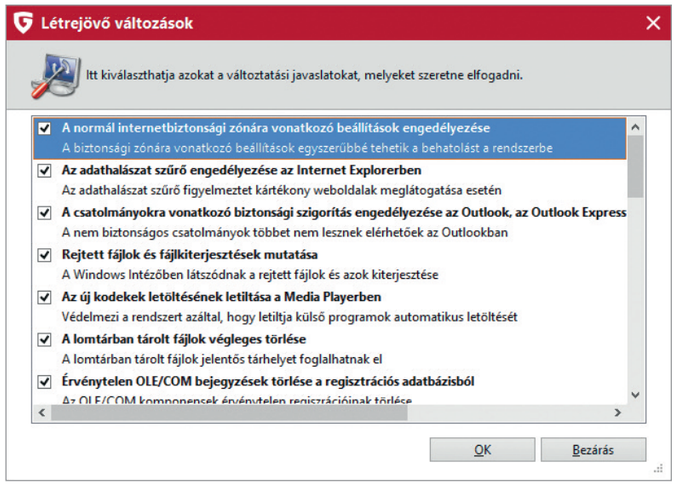


A tuningot a G Data TotalProtection fő párbeszédablakának segítségével indíthatjuk el. Kattintsunk az utolsó tuning, majd a tuning futtatása most feliratra.

Ekkor elindul a tuning, és az alábbi státuszablakot látjuk:



Ekkor a szoftver összegyűjti a javasolt változtatásokat, majd engedélyt kér az egyes változtatásokra.

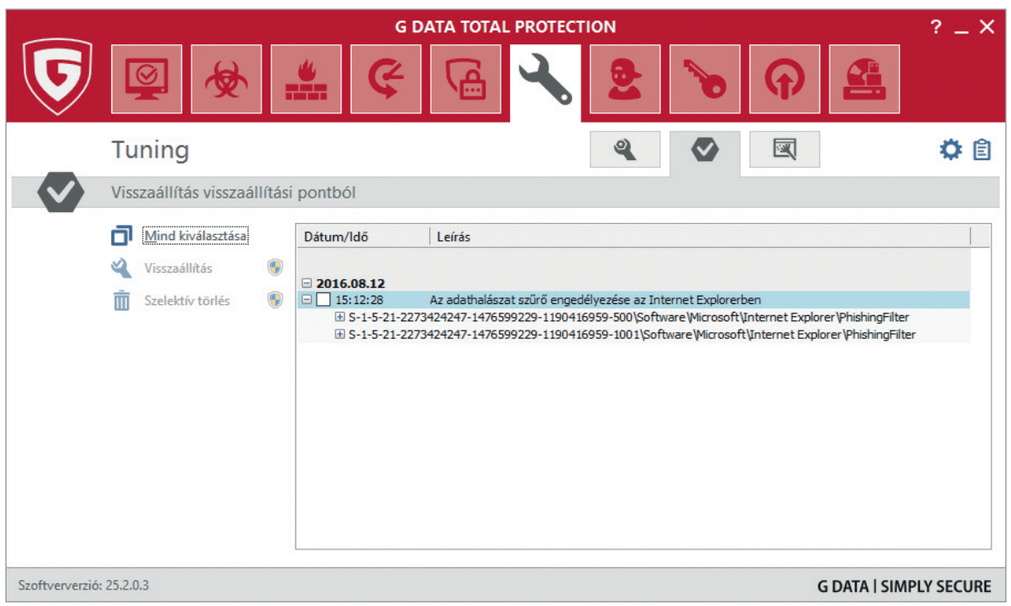


A megjelenő listából válasszuk ki, hogy melyik változtatásokat szeretnénk jóváhagyni, majd kattintsunk az OK gombra ahhoz, hogy megtörténjenek a változtatások.

Amennyiben nem vagyunk elégedettek a változtatásokkal, a fő párbeszédablakon kattintsunk a tuning alatti hatszögben található pipára.

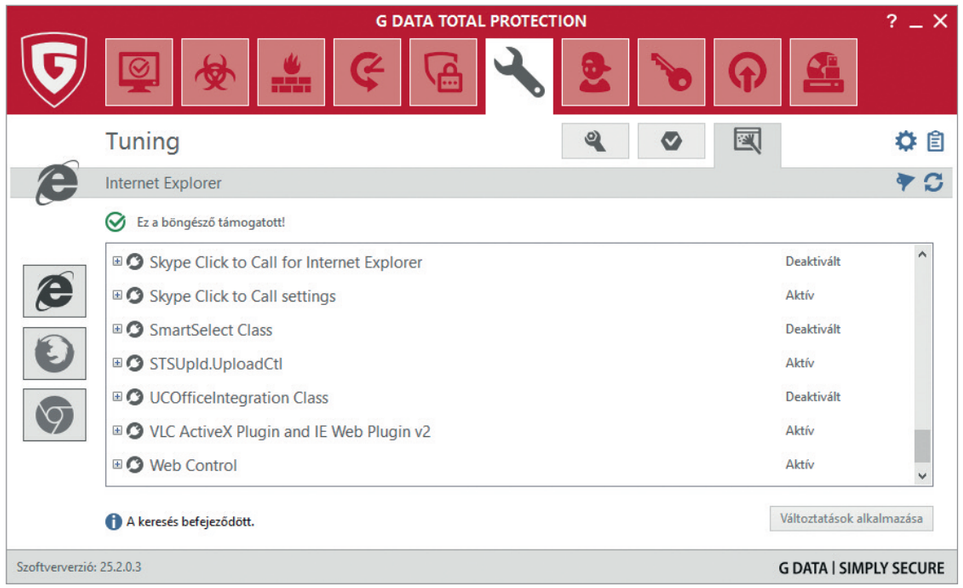
A megjelenő listában láthatjuk a megőrzött visszaállítási pontokat és az ezekhez tartozó változtatások listáját. Ha szeretnénk visszaállítani valamelyik változtatást, tegyünk pipát a mellette lévő jelölőnégyzetbe, majd kattintsunk a visszaállítás gombra.

Minden változtatás kijelöléséhez kattintsunk az összes kijelölése gombra, a megőrzött változtatások törlését pedig a kiválasztottak törlése gombra kattintva tehetjük meg.



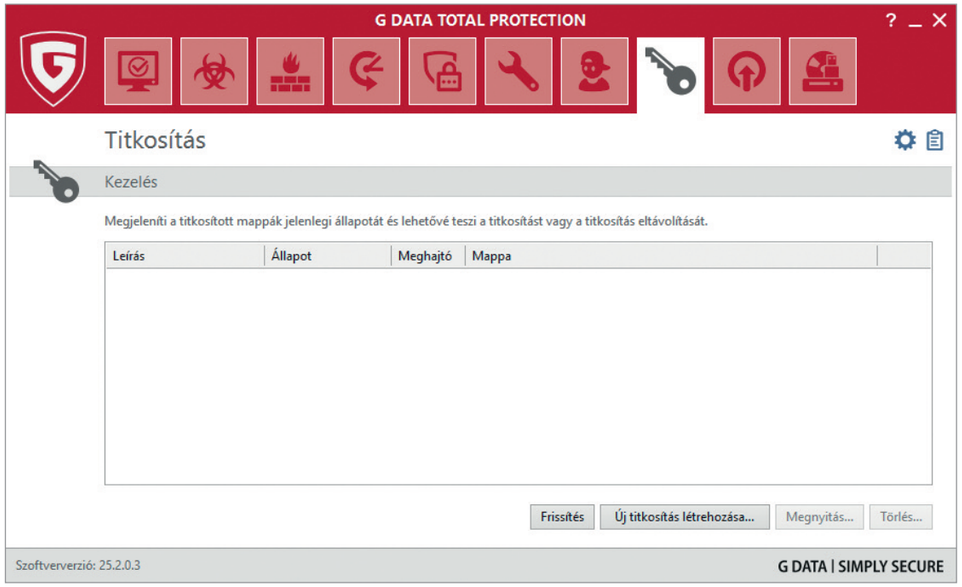
A G Data böngészőtisztító modul megmutatja, hogy az egyes böngészőkbe milyen bővítmények települtek.

A modul segítségével letilthatja a nem kívánt vagy gyanús böngészőket, így megakadályozhatja azok indulását.



Titkosítás beállítása

A G Data TotalProtection részét képező fájlszéfben titkosítva tárolhatjuk a bizalmas dokumentumainkat.

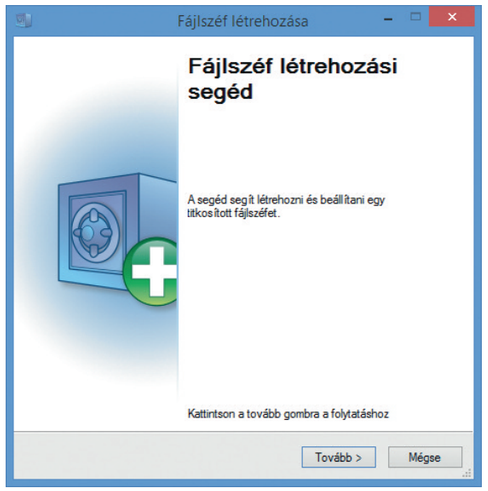


A fájlszéf segítségével titkosított virtuális meghajtót hozhatunk létre a merevlemezünkön, vagy titkosított USB kulcsot hozhatunk létre (mobil fájlszéf). Ezeket a meghajtókat jelszóval védhetjük, így azok tartalmához csak mi férhetünk hozzá a G Data fájlszéf alkalmazás segítségével.

Amennyiben mobil fájlszéfet hozunk létre egy USB kulcson vagy memóriakártyán, az alkalmazás futtatásához nem szükséges, hogy a G Data TotalProtection telepítve legyen a számítógépen. Így a mobil fájlszéfet bármilyen számítógépen tudjuk használni.

Fontos, hogy a fájlszéfekben tárolt információk – szerződések, fotók és más dokumentumok – biztonsága a választott jelszó erősségének függvénye. Amennyiben a jelszó gyenge, a fájlszéf nem tudja kellően megvédelmezni a tárolt adatokat. Ezért válasszunk olyan jelszavakat, melyek legalább 12 karakterből állnak, és tartalmaznak kis- és nagybetűket, számokat, valamint speciális írásjeleket (vessző, pont, pontosvessző, felkiáltójel stb.).

Fájlszéf létrehozásához kattintsunk a G Data TotalProtection fő kezelőablakán a fájlszéf (file safe) felirat melletti lefelé mutató háromszögre, majd a fájlszéf létrehozása feliratra.

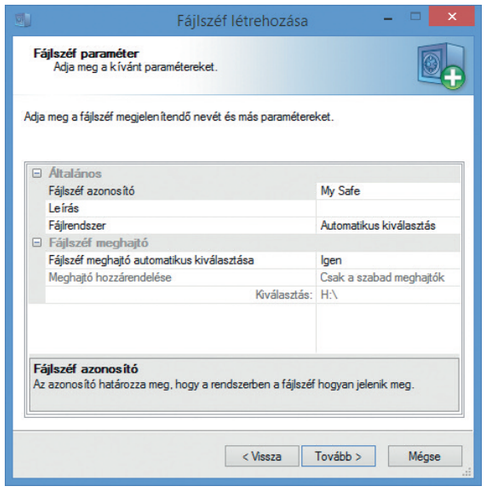


A megnyíló fájlszéfvarázsló végigvezet minket a fájlszéf létrehozásának lépésein.

Az első párbeszédablakon a létrehozandó fájlszéf helyét és nagyságát választhatjuk ki. A fájlszéfet helyezhetjük a merevlemezre vagy mobil adathordozóra (USB kulcs, memóriakártya), de ez utóbbi nem lesz azonos a mobil fájlszéffel, és csak olyan számítógépeken játszható le, melyekre telepítve van a G Data TotalProtection szoftver.

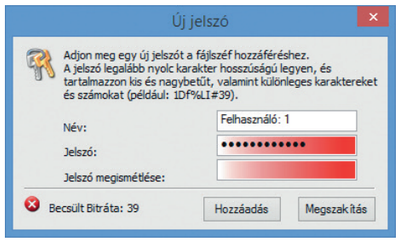
A párbeszédablakon válasszuk tehát ki a fájlszéf helyét, majd a csúszka segítségével vagy a csúszka bal oldalán elhelyezkedő lefelé mutató háromszögre való kattintással állítsuk be a kívánt fájlszéf nagyságát.

Fontos, hogy a fájlszéf nem merevlemezt vagy partíciót hoz létre, hanem egy fájlt készít a merevlemezen, melyet ezután a lemezképekhez (ISO fájlokhoz) hasonlóan virtuális meghajtóként tudunk használni. A létrehozott .ts4 kiterjesztésű fájl maga a fájlszéf, a szoftver ebbe a fájlba tömöríti bele titkosítva a megőrizni kívánt dokumentumokat. Ezért amennyiben a számítógép összeomlik vagy egy másik számítógépen szeretnénk megtekinteni a fájlszéf tartalmát, nincs más dolgunk, mint ezt a .ts4 kiterjesztésű fájlt megnyitni a G Data Top Secret alkalmazással, mely a fájlszéf része.



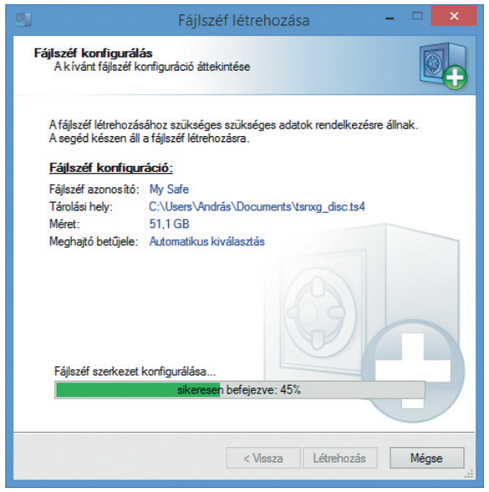
A következő lépésben nevet adhatunk a fájlszéfünknek. Ez alapértelmezésben a My Safe. Ha át szeretnénk írni, kattintsunk a My Safe feliratra és adjuk meg a használni kívánt nevet.

A párbeszédablak segítségével megadhatjuk még a széf fájlrendszerének típusát, és beállíthatjuk, hogy a szoftver automatikusan kiválassza-e a széfként használni kívánt meghajtó betűjelét.



A következő lépésben jelszót kell adnunk a fájlszéfünknek. A szoftver alul megjeleníti a választott jelszó bitrátáját, mely a jelszó erősségét jelzi, illetve megfelelőnek ítélt jelszó esetében pirosról zöldre változik a jelszó beírására szolgáló mező háttere.

A fájlszéf a hozzáadás (add) gombra való kattintás után elkészül. A fájlszéf kezeléséhez kattintsunk a G Data TotalProtection fő kezelőablakán lévő fájlszéf felirat melletti lefelé mutató háromszögre, majd a fájlszéfek kezelése feliratra.

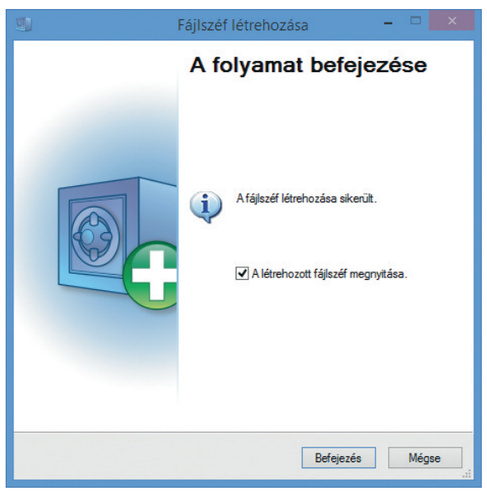


A megnyíló párbeszédablak segítségével kezelhetjük a meglévő fájlszéfeket. A megnyitás gomb segítségével megnyithatjuk a széfet, a törlés gomb segítségével pedig törölhetjük.

A frissítés gomb segítségével frissíthetjük a fájlszéfek állapotának kijelzését, az új fájlszéf létrehozása gombra kattintva pedig új fájlszéfet hozhatunk létre.

Mobil fájlszéfek létrehozása

Fontos, hogy mobil fájlszéfet csak a hagyományos fájlszéf másolataként tudunk létrehozni. Tehát amennyiben egy 2 GB-os USB kulcsunk van, és ezt szeretnénk fájlszéfként használni, először készítsünk egy 1,9 GB-os hagyományos fájlszéfet a merevlemezre. Ebbe helyezzük bele a bizalmas dokumentumokat, majd ezt a fájlszéfet tudjuk mobil fájlszéfként átmásolni az USB kulcsunkra vagy memóriakártyánkra.
Mobil fájlszéf létrehozásához a már megismert módon kattintsunk a fájlszéfek kezelésének megnyitására és jelöljük ki azt a fájlszéfet, melyet mobil adathordozóra szeretnénk tükrözni.



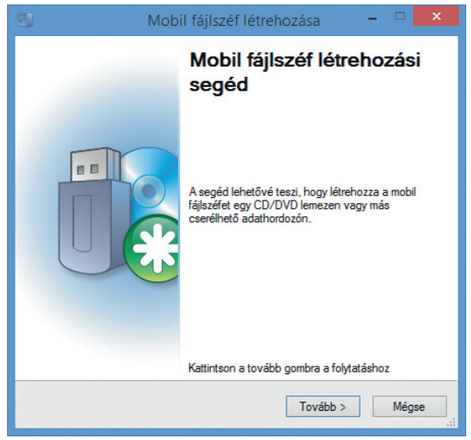
A fájlszéf mérete nem lehet nagyobb, mint amennyi helyünk a mobil adathordozón (USB kulcs, memóriakártya) rendelkezésre áll. A mobil adathordozón ezenkívül szükség van körülbelül 10 MB helyre a rendszeradatok tárolásához.

Ha az egérrel kijelöltük a fájlszéfet, melyet tükrözni kívánunk, az alsó gombok közül a második megváltozik, és segítségével mobil fájlszéfet hozhatunk létre.

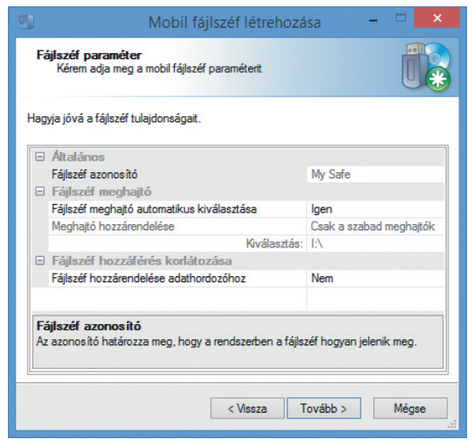
A mobil fájlszéfbe bele fognak kerülni azok a fájlok, melyeket az eredeti fájlszéfben tároltunk.

Kattintsunk a mobil fájlszéf létrehozása gombra, majd a megnyíló varázsló végigvezet minket a szükséges lépéseken.

Fontos, hogy miközben a fájlszéfet mobil fájlszéfként tükrözzük, az eredeti fájlszéfnek zárva kell lennie. Erre a program figyelmeztet bennünket, és a fájlszéfet bezárja.



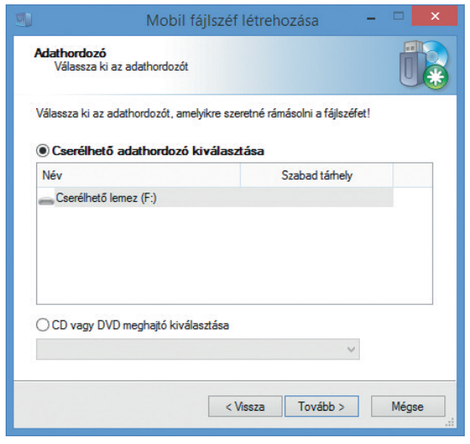
A mobil fájlszéf neve az eredeti fájlszéf nevével azonos lesz. A párbeszédablak segítségével beállíthatjuk, hogy a szoftver automatikusan rendeljen-e betűjelet a meghajtóhoz, és azt is, hogy a mobil fájlszéfet összekapcsolja-e a mobil adathordozóval.



Amennyiben a mobil fájlszéfet összekötjük a mobil adathordozóval, a fájlszéfet nem lehet más adathordozóra (más USB kulcsra vagy memóriakártyára) másolni, kizárólag azon az adathordozón fog működni, melyen eredetileg létrehoztuk.

A következő lépésben ki kell választanunk a mobil adathordozót, melyen a mobil fájlszéfet létre szeretnénk hozni.

Amennyiben a számítógépben nincs USB kulcs vagy memóriakártya, akkor a szoftver ezt jelzi számunkra. (Nincs megfelelő adathordozó).



Jelöljük ki a használni kívánt mobil adathordozót, majd kattintsunk a tovább gombra, és a szoftver létrehozza a mobil fájlszéfet.

A mobil fájlszéfet hagyományos USB kulcsként tudjuk használni bármely számítógépen. Ehhez nincs szükség arra, hogy a számítógépre a G Data TotalProtection szoftver telepítve legyen.

Ügyeljünk azonban arra, hogy amikor a mobil fájlszéfbe adatokat helyezünk, akkor a mobil fájlszéfet a kezelésére szolgáló szoftver segítségével zárjuk be, és ne csak egyszerűen kihúzzuk a számítógépből. Amennyiben az adathordozót egyszerűen kihúzzuk a számítógépből ahelyett, hogy megfelelően bezárnánk, a rámásolt adatok megsérülhetnek.

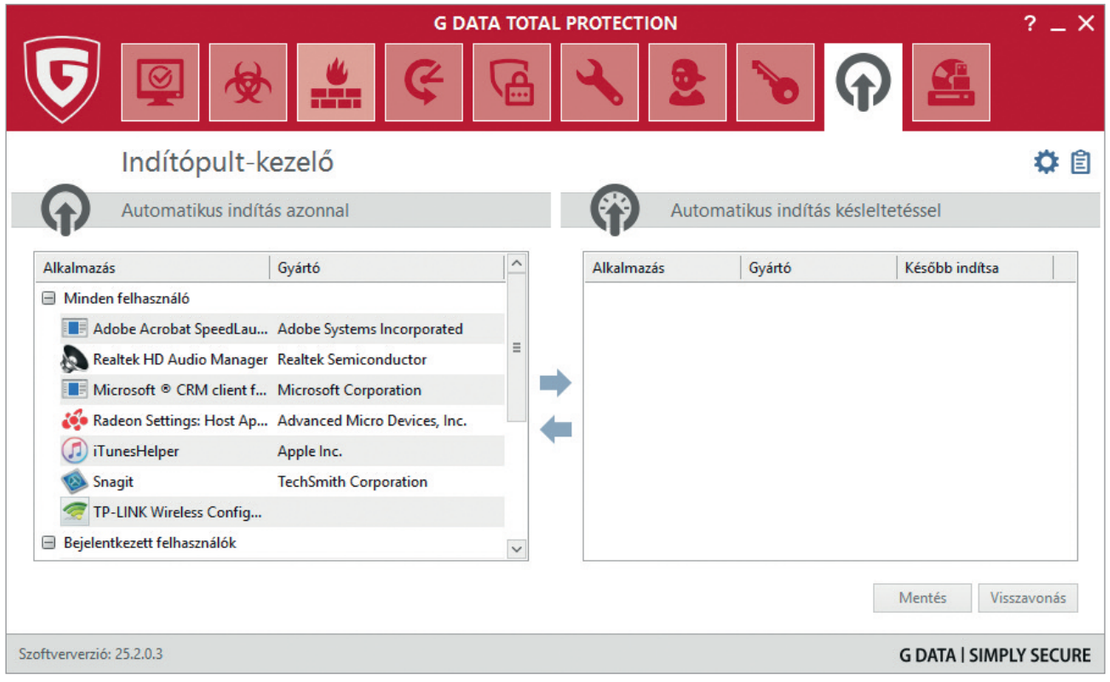
Amennyiben a számítógépen az automatikus futtatás funkció engedélyezve van, a mobil fájlszéf automatikusan megjelenik, ha azt a számítógépbe helyezzük. Amennyiben viszont az automatikus futtatás funkció nincs engedélyezve, a mobil fájlszéf behelyezése után a TSNxG_4 mappából a start.exe szoftverre való dupla kattintással el kell indítanunk a mobil fájlszéfet ahhoz, hogy használni tudjuk.

A jelszó megadása után a mobil fájlszéf virtuális meghajtóként látszik a számítógépen, és ugyanúgy használhatjuk, mint egy helyi merevlemezt.

Indítópult-kezelő

Az Indítópult-kezelő gyorsabbá teszi a számítógép indulását azáltal, hogy beállíthatjuk, hogy bizonyos alkalmazások ne, vagy ne rögtön kerüljenek betöltésre. Amikor a számítógép bootol (elindul), általában sok alkalmazás töltődik be, ami az indulást lassítja.

Az Indítópult-kezelő ablakának bal oldalán jelöljük ki azokat az alkalmazásokat, melyeket nem kívánunk azonnal elindítani, és a jobbra mutató nyíl segítségével helyezzük át őket a jobb oldalra.



Miután egy alkalmazás átkerült a jobb oldalra, alapértelmezésben két perccel a rendszer indítása után fog csak elindulni. Ha ezt az értéket szeretnénk megváltoztatni, akkor kattinsunk az idő kijelzésére, és válasszunk más értéket. Ha az alkalmazást szeretnénk letiltatni, válasszuk a ne indítsa el opciót.

Az indításkezelő segítségével még a régebbi gépek indítása is dinamikusabbá tehető.

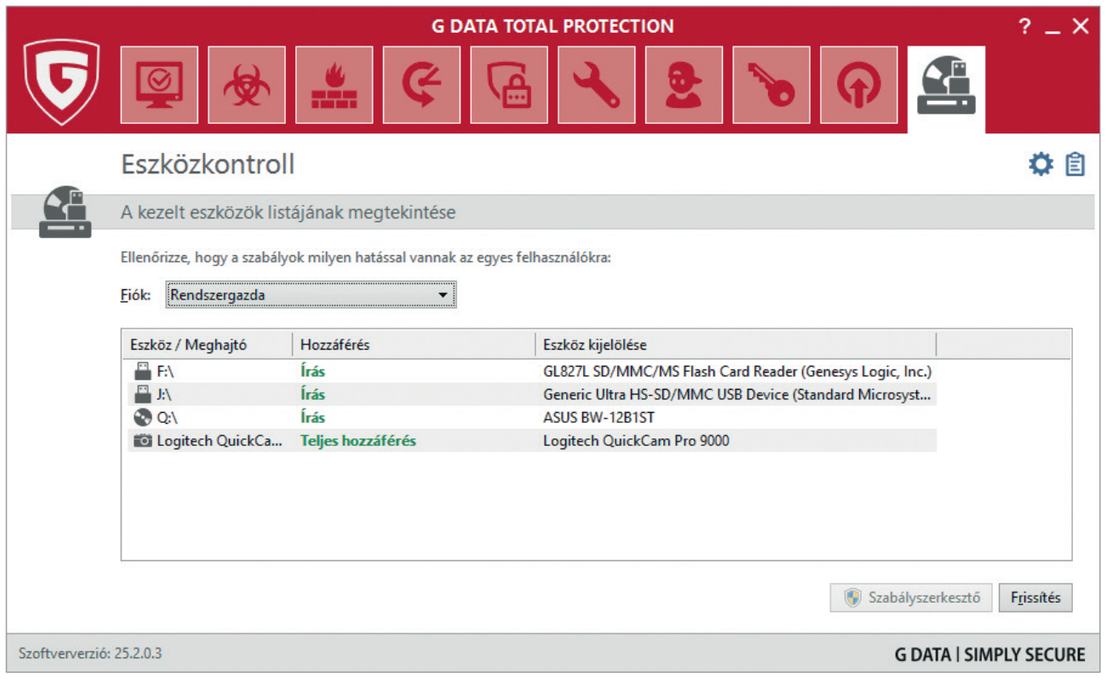
Eszközkontroll

Az eszközkontroll lehetővé teszi, hogy szabályozzuk, milyen adathordozók érhetőek el a számítógép felhasználói számára.

A felhasználói fiókok alatt látjuk a rendszerhez csatlakoztatott adathordozókat, és ezeknek a nevére kattintva módosíthatjuk elérhetőségüket.

A felhasználói fiókok legördülő listája lehetővé teszi, hogy megtekintsük, az egyes változtatások milyen hatással vannak az adott felhasználó jogosultságaira.

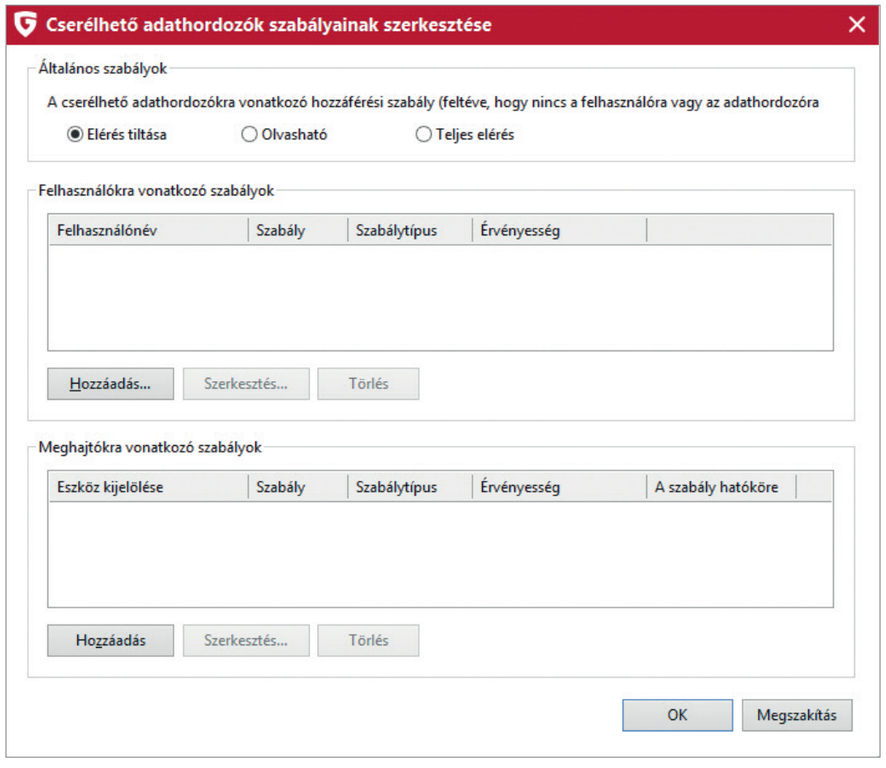
A jogosultságok érvényesítéséhez és kijelzéséhez kattintsunk a jobb alsó sarokban található frissítés gombra.



A szigorításnak akkor van értelme, ha nem csak mi használjuk a számítógépet, és nem szeretnénk, hogy arra egy USB kulcsról kártevő kerüljön, vagy szeretnénk elkerülni, hogy bizalmas dokumentumainkat valaki CD-re írja.

Szabályokat hozhatunk létre mind a felhasználókra (ebben az esetben a szabály az adathordozótól függetlenül mindig érvényes lesz a felhasználóra), vagy az adathordozókra.

A szabályokhoz érvényességi időt is rendelhetünk, így meghatározhatjuk, hogy mennyi ideig legyenek érvényesek.



Terméktámogatás

A G Data szoftvereinek kizárólagos magyarországi disztribútora
a V-Detect Antivírus Kft. A G Data szoftvereihez való terméktámogatás ingyenes,
és a http://virusirto.hu/segitseg oldalon keresztül érhető el.

V-DETECT ANTIVÍRUS KFT.
www.v-detect.hu