AVG Internet Security 2012

Felhasználói kézikönyv

Dokumentumverzió 2012.01 (1.9.2011)

Tartalom

1. Bevezetés

A felhasználói kézikönyv átfogó dokumentációt kínál az **AVG Internet Security 2012** termékhez.

Az AVG Internet Security 2012 többszintű védelmet biztosít online tevékenységeihez, ami azt jelenti, hogy nem kell személyazonosság-lopás, vírusok vagy veszélyes oldalak megnyitása miatt aggódnia. Az AVG Protective Cloud Technology és az AVG Community Protection Network is a termék részét képezik, ami azt jelenti, hogy összegyűjtjük a legutóbbi fenyegetésekkel kapcsolatos adatokat, és megosztjuk a közösséggel a lehető legjobb védelem biztosítása érdekében:

- Biztonságos online vásárlás és banki ügyintézés az AVG tűzfal, levélszemétszűrő és Identity Protection segítségével
- A közösségi oldalak biztonságos használata az AVG Social Networking Protection segítségével
- Magabiztos böngészés és keresés a LinkScanner valós idejű védelmével

2. AVG telepítési követelmények

2.1. Támogatott operációs rendszerek

Az AVG Internet Security 2012 a következő operációs rendszerű munkaállomások védelmére szolgál:

- Windows XP Home SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 és x64, minden kiadás)
- Windows 7 (x 86 és x64, minden kiadás)

(és esetlegesen újabb szervizcsomagok bizonyos operációs rendszerekhez)

***Megjegyzés**: Az ID Protection összetevő nem támogatott Windows XP x64 rendszerek alatt. Erre az operációs rendszerre kizárólag az AVG Internet Security 2012 terméket telepítheti, az IDP összetevő nélkül.*

2.2. Minimum és ajánlott hardverkövetelmények

Minimális hardverkövetelmények a **AVG Internet Security 2012** termékhez:

- Intel Pentium CPU 1,5 GHz
- 512 MB RAM memória
- 1000 MB szabad merevlemez-terület (telepítési célokra)

Ajánlott hardverkövetelmények a **AVG Internet Security 2012** termékhez:

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM memória
- 1550 MB szabad merevlemez-terület (telepítési célokra)

3. AVG telepítési folyamat

Honnan szerezhető be a telepítési fájl?

Az **AVG Internet Security 2012** telepítéséhez szüksége van a legújabb telepítőfájlra. Ha biztosan az **AVG Internet Security 2012** legfrissebb verzióját kívánja letölteni, azt javasoljuk, hogy használja az AVG webhelyét (http://www.avg.hu/). A ***Tudásbázis / Letöltés*** területen az AVG kiadásai szerint elrendezve megtalálja az összes telepítési fájlt.

Ha nem biztos benne, hogy melyik fájlra van szüksége a telepítéshez, használja a webhely alsó részén található ***Termék kiválasztása*** szolgáltatást. Három egyszerű kérdés megválaszolását követően a szolgáltatás meghatározza, hogy pontosan mely fájlokra van szüksége. A ***Tovább*** gombra kattintva az oldal átirányítja egy listához, amely minden olyan fájlt tartalmaz, amire szüksége lehet.

Miként zajlik a telepítés?

Miután letöltötte és mentette a telepítőfájlt a merevlemezre, indítsa el a telepítési folyamatot. A telepítés egyszerű, könnyen érthető párbeszédablakok sorozata. Minden párbeszédablak röviden leírja a telepítési folyamat adott lépésére vonatkozó tennivalókat. A következőkben az egyes párbeszédablakok részletes leírását találja:

3.1. Üdvözlőképernyő

A telepítési folyamat az ***Üdvözli az AVG telepítő*** párbeszédpanellel kezdődik:

Telepítési nyelv kiválasztása

Itt a párbeszédpanelen kiválaszthatja a telepítés nyelvét. A párbeszédpanel jobb oldali sarkában kattintson a kombinált listára a nyelvi menü legördítéséhez. Válassza ki a kívánt nyelvet, és a telepítés folytatódik a kiválasztott nyelven.

Figyelem: Az itt kiválasztott nyelv csak a telepítési folyamatra vonatkozik. Az AVG Internet Security 2012 alkalmazást a kiválasztott nyelven telepíti, az angol nyelvet pedig ezen felül mindig automatikusan telepíti a rendszer. Azonban több nyelvet is lehet telepíthet, és az AVG Internet Security 2012 terméket ezek bármelyikén használhatja. A program a későbbiekben, az Egyéni beállítások párbeszédpanelen lehetővé teszi, hogy megerősítse, mely alternatív nyelveket kívánja használni.

Licencszerződés

Ezenfelül az ***Üdvözli az AVG telepítő*** párbeszédpanel az AVG licencszerződés teljes szövegét is tartalmazza. Olvassa el figyelmesen. Nyomja meg az ***Elfogadom*** gombot, ha elolvasta, megértette és elfogadta a megállapodást. Ha nem ért egyet a megállapodással, akkor nyomja meg a ***Nem fogadom el*** gombot, ekkor a telepítési folyamat azonnal megszakad.

AVG Adatvédelmi nyilatkozat

A licencszerződés mellett ez a telepítési párbeszédpanel lehetőséget nyújt az AVG adatvédelmi nyilatkozat jobb megismerésére is. A párbeszédpanel bal oldali sarkában láthatja az ***AVG adatvédelmi nyilatkozat*** hivatkozást. Erre kattintva az AVG webhelyére (http://www.avg.hu/) kerül, ahol megtalálja az AVG Technologies adatvédelmi nyilatkozatát teljes terjedelmében.

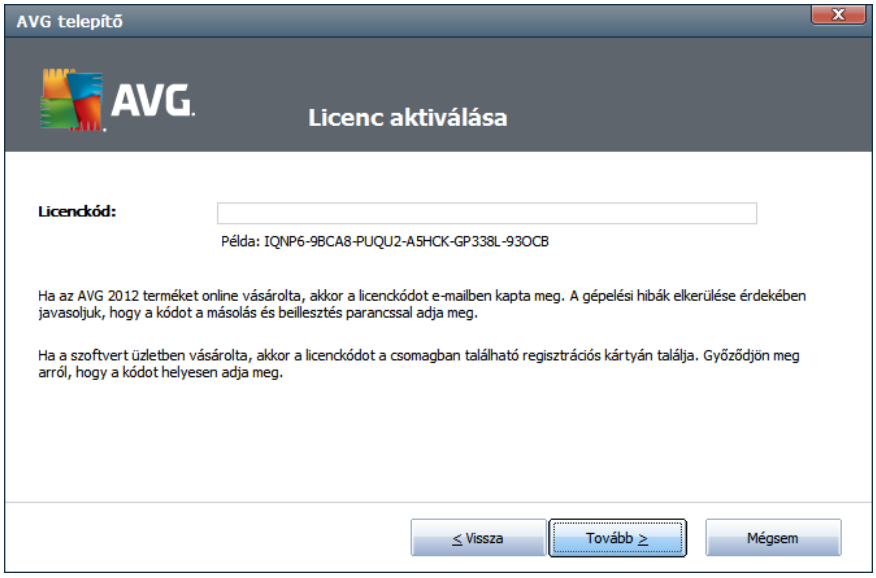
Vezérlőgombok

Az első telepítő párbeszédpanelen csak két vezérlőgomb található:

- ***Elfogadom*** – Erre kattintva megerősíti, hogy elolvasta, megértette és elfogadta a licenc feltételeit. A telepítés folytatódik és egy lépéssel tovább, a következő telepítési párbeszédpanelre ugrik.
- ***Elutasítom*** – Erre kattintva elutasítja a licencszerződést. A telepítési folyamat azonnal megszakad. **AVG Internet Security 2012**Az telepítése nem történik meg.

3.2. Licenc aktiválása

A ***Licenc aktiválása*** panelen írja be a licenckódot a megfelelő szövegmezőbe:



Hol találom a licenckódomat?

Az értékesítési számot saját **AVG Internet Security 2012** példányának dobozában, a CD csomagolásán találja. A licenckód az **AVG Internet Security 2012** megvásárlása után kapott megerősítő e-mailben lesz. A számot pontosan úgy kell megadnia, ahogyan az látható. Ha a licenckód elérhető digitális formában (*pl. emailben*), akkor javasoljuk, hogy használja a másolás és beillesztés funkciót a megadáshoz.

A másolás és beillesztés funkció használata

Ha a ***másolás és beillesztés*** funkciót használja az **AVG Internet Security 2012** licenckódjának megadásához, nem kell elgépeléstől tartania. Kövesse az alábbi lépéseket:

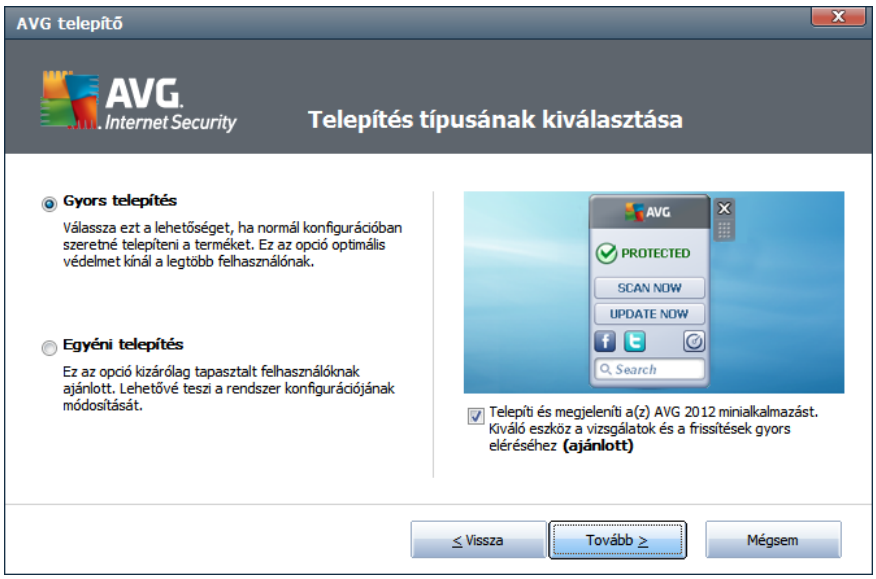
- Nyissa meg a licenckódot tartalmazó e-mailt.
- Kattintson a bal gombbal a licenckód elejére, majd a gombot nyomva tartva húzza a mutatót a szám végéig, és engedje fel a gombot. Ezzel kijelölte a számot.
- A ***Ctrl*** billentyűt nyomva tartva nyomja le a ***C*** billentyűt. Ezzel a vágólapra helyezte a számot.
- Kattintson arra a pontra, ahová be kívánja illeszteni a vágólapra helyezett számot.
- A ***Ctrl*** billentyűt nyomva tartva nyomja le a ***V*** billentyűt. Ezzel beilleszti a számot a kiválasztott helyre.

Vezérlőgombok

A legtöbb telepítési párbeszédpanelhez hasonlóan itt is három vezérlőgomb áll rendelkezésre:

- ***Vissza*** – Ide kattintva visszatérhet az előző telepítési párbeszédablakhoz.
- ***Tovább*** – Ide kattintva folytatja a telepítést, és a következő lépésre ugrik.
- ***Mégse*** – Ide kattintva azonnal megszakítja a telepítés folyamatát, és nem telepíti az **AVG Internet Security 2012** szoftvert.

3.3. Telepítés típusának kiválasztása



Telepítés típusai

A ***Telepítés típusának kiválasztása*** panel két lehetőséget kínál: ***Gyors telepítés*** és ***Egyéni telepítés***.

A legtöbb felhasználó számára a normál gyors telepítés használatát javasoljuk, amely teljesen automatikusan telepíti az **AVG Internet Security 2012** programot a gyártó által előre megadott beállításokkal. Ez a konfiguráció maximális biztonságot és a rendszererőforrások optimális használatát nyújtja. Ha a későbbiekben meg szeretné változtatni a konfigurációt, akkor ezt közvetlenül megteheti az **AVG Internet Security 2012** alkalmazáson belül. Ha a ***Gyors telepítés*** lehetőséget választotta, akkor nyomja meg a ***Tovább*** gombot a következő, Az AVG Biztonság eszköztár telepítése nevű panelre ugráshoz.

Az Egyéni telepítést csak azon tapasztalt felhasználóknak ajánljuk, akik mindenképp egyéni beállításokkal szeretnék telepíteni az **AVG Internet Security 2012** programot; például azért, hogy az megfeleljen bizonyos rendszerkövetelményeknek. Ha ezt a lehetőséget választotta, akkor nyomja meg a ***Tovább*** gombot az Egyéni beállítások panelre történő ugráshoz.

AVG minialkalmazás telepítése

A panel jobb oldali részén találhatja az AVG minialkalmazáshoz tartozó jelölőnégyzetet (*támogatott rendszerek: Windows Vista/Windows 7*). Ha telepíteni szeretné ezt a minialkalmazást, akkor jelölje be a megfelelő jelölőnégyzetet. Az AVG minialkalmazás a Windows oldalsávról érhető el, és azonnali hozzáférést biztosít az **AVG Internet Security 2012** legfontosabb szolgáltatásaihoz, pl. vizsgálat és frissítés.

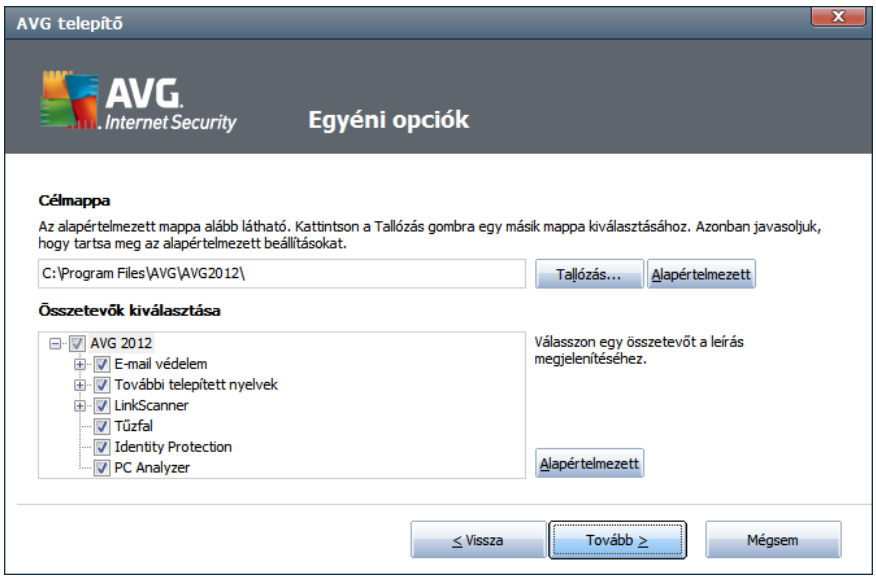
Vezérlőgombok

A legtöbb telepítési párbeszédpanelhez hasonlóan itt is három vezérlőgomb áll rendelkezésre:

- ***Vissza*** – Ide kattintva visszatérhet az előző telepítési párbeszédablakhoz.
- ***Tovább*** – Ide kattintva folytatja a telepítést, és a következő lépésre ugrik.
- ***Mégse*** – Ide kattintva azonnal megszakítja a telepítés folyamatát, és nem telepíti az **AVG Internet Security 2012** szoftvert.

3.4. Egyéni opciók

Az ***Egyéni opciók*** panel lehetővé teszi két paraméter beállítását a telepítéskor:



Célmappa

A ***Célmappa*** részen megadhatja az **AVG Internet Security 2012** telepítési helyét. Alapértelmezett állapotban az **AVG Internet Security 2012** a C: meghajtón található a Program Files mappába települ. Ha módosítani szeretné ezt a helyet, akkor használja a ***Böngészés*** gombot a meghajtó tartalmának megjelenítéséhez, majd válassza ki a kívánt mappát.

Összetevők kiválasztása

Az ***Összetevő kiválasztása*** rész az összes telepíthető **AVG Internet Security 2012** összetevőt mutatja. Ha az alapbeállítások nem felelnek meg Önnek, akkor eltávolíthat/hozzáadhat összetevőket.

Azonban csak olyan összetevőkből választhat, melyek használatára jogosult a megvásárolt AVG termékben!

Jelöljön ki egy elemet az ***Összetevő kiválasztása*** listán, ekkor az adott összetevő rövid leírása megjelenik a jobb oldalon. Az egyes összetevők részletes adataival kapcsolatban forduljon a dokumentáció Összetevők áttekintése fejezetéhez. A gyártó által megadott alapértékek visszaállításához használja az ***Alapértelmezett*** gombot.

Vezérlőgombok

A legtöbb telepítési párbeszédpanelhez hasonlóan itt is három vezérlőgomb áll rendelkezésre:

- ***Vissza*** – Ide kattintva visszatérhet az előző telepítési párbeszédablakhoz.
- ***Tovább*** – Ide kattintva folytatja a telepítést, és a következő lépésre ugrik.
- ***Mégse*** – Ide kattintva azonnal megszakítja a telepítés folyamatát, és nem telepíti az **AVG Internet Security 2012** szoftvert.

3.5. Az AVG Biztonság eszköztár telepítése

Az ***AVG Biztonság eszköztár telepítése*** panelen eldöntheti, hogy akarja-e telepíteni az AVG Biztonság eszköztárt. Ha nem módosítja az alapértelmezett beállításokat, akkor ez az összetevő

automatikusan települ a böngészőbe (*Microsoft Internet Explorer v. 6.0 vagy újabb, és Mozilla Firefox v. 3.0 vagy újabb* böngésző használata szükséges) és átfogó online védelmet nyújt az internet böngészése során.

Beállíthatja a(z) *AVG Secure Search (powered by Google)* keresőmotort alapértelmezett keresőnek. Ha igen, jelölje be a megfelelő jelölőnégyzetet.

3.6. Telepítési folyamat

A ***Telepítési folyamat*** panel a telepítési folyamat állapotát mutatja, és nem igényel semmilyen beavatkozást:

Miután a telepítési folyamat befejeződött, a program automatikusan továbblép a következő párbeszédpanelre.

Vezérlőgombok

Ezen a párbeszédpanelen csak egy vezérlőgomb érhető el, a ***Mégse***. Ezt gombot csak akkor használja, ha le kívánja állítani a futó telepítési folyamatot. Vegye figyelembe, hogy a folyamat leállítása esetén az **AVG Internet Security 2012** termék telepítése nem történik meg.

3.7. A telepítés sikerült

A telepítés sikerült párbeszédpanel megerősíti, hogy az **AVG Internet Security 2012** terméket a rendszer sikeresen telepítette és konfigurálta:

Termékfejlesztési program

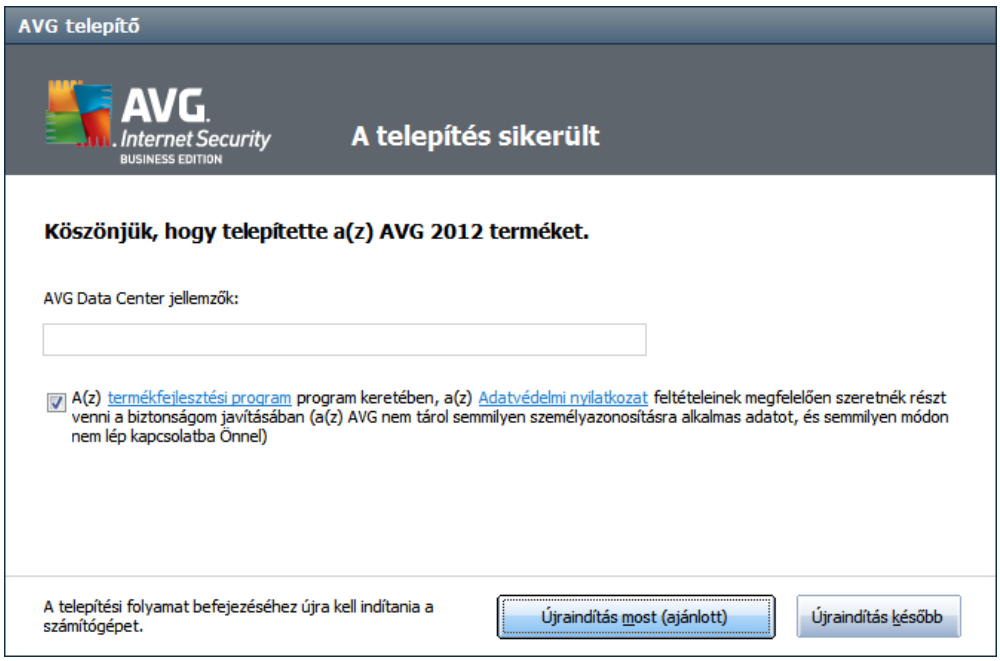
Ezen a párbeszédpanelen eldöntheti, hogy részt kíván-e venni a Termékfejlesztési programban (*erről részleteket a Haladó AVG beállítások / Termékfejlesztési program* című fejezetben talál), amely névtelen információkat gyűjt az észlelt fenyegetésekről az online biztonság növelése érdekében. Ha egyetért ezzel az állítással, hagyja bejelölve a ***Szeretnék részt venni az AVG 2012 webbiztonsági és termékfejlesztési programban ...*** lehetőséget *(ez alapértelmezett állapotban be van jelölve)*.

A számítógép újraindítása

A telepítési folyamat befejezéséhez indítsa újra a számítógépet: kattintson az ***Újraindítás most*** gombra, vagy ha el kívánja halasztani az újraindítást, kattintson az ***Újraindítás később*** gombra.

Üzleti licenc telepítése

Ha AVG üzleti licencet használ, és ha korábban telepítette a Távfelügyelet szolgáltatást *(további információ: Egyéni beállítások)*, akkor A telepítés sikerült panel a következő felülettel jelenik meg:



Adja meg az AVG DataCenter paramétereit, vagyis írja be az AVG DataCenter kapcsolódási karakterláncát kiszolgáló:port formájában. Ha ez az információ jelenleg nem érhető el, akkor hagyja a mezőt üresen, és később is beállíthatja azt a Haladó beállítások / Távfelügyelet panelen. Az AVG Távfelügyelettel kapcsolatos információkért tekintse meg az AVG Business Edition felhasználói kézikönyvet. Ezt az AVG webhelyéről (http://www.avg.hu/) töltheti le.

Tekintse meg az Összetevők áttekintése című fejezetet ebben a dokumentációban. A gyártó által megadott alapértékek visszaállításához használja az ***Alapértelmezett*** gombot.

Vezérlőgombok

A párbeszédpanelen az alábbi vezérlőgombok érhetők el:

- ***Újraindítás most (ajánlott)*** – Újraindítás szükséges az **AVG Internet Security 2012** telepítési folyamatának befejezéséhez. Javasolt a számítógép azonnal újraindítása. Csak az újraindítás után készül el teljesen az **AVG Internet Security 2012** telepítése, csak ezután tudhatja magát teljes biztonságban, megfelelő védelemmel.

- ***Újraindítás később*** – Ha bármi okból most nem tudja újraindítani a számítógépet, a műveletet későbbre halaszthatja. Azonban javasolt az azonnali újraindítás. Csak az újraindítás után tudja az **AVG Internet Security 2012** teljes mértékben védeni a számítógépet.

4. A telepítés utáni teendők

4.1. Termék regisztrálása

Miután befejezte az **AVG Internet Security 2012** telepítését, regisztrálja a terméket az AVG webhelyén (http://www.avg.hu/). A regisztráció után teljes hozzáférést kap saját AVG felhasználói fiókjához, az AVG Update hírlevélhez és számos egyéb, kizárólag regisztrált felhasználók számára elérhető szolgáltatáshoz.

Regisztrálni legkönnyebben közvetlenül az **AVG Internet Security 2012** felhasználói felületéről tud. A főmenüben válassza a Súgó/Regisztrálás most elemet. Ezután egyből az AVG webhely (http://www.avg.hu/) ***Regisztráció*** oldalára kerül. Kövesse az oldalon megjelenő utasításokat.

4.2. Hozzáférés a felhasználói felülethez

Az AVG fő párbeszédpanel többféle módon is elérhető:

- Kattintson kétszer az AVG ikonjára a tálcán
- kattintson duplán az AVG ikonra az Asztalon
- Kattintson kétszer az AVG minialkalmazás alsó részén található állapotsorra (*ha telepítve van, támogatott rendszerek: Windows Vista/ Windows 7*)
- a ***Start/Programok/AVG 2012/AVG felhasználói felület***

4.3. A teljes számítógép vizsgálata

Fennáll a veszély, hogy az**AVG Internet Security 2012** telepítése előtt vírus került a számítógépre. Ezért futtassa le a Teljes számítógép vizsgálata funkciót, hogy meggyőződhessen róla, hogy számítógépe vírusmentes.

A Teljes számítógép vizsgálata funkció futtatásával kapcsolatos információkért forduljon az AVG vizsgálat fejezethez.

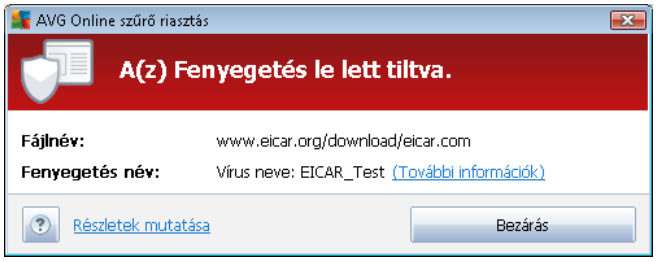
4.4. Eicar teszt

Az **AVG Internet Security 2012** sikeres telepítésének ellenőrzéséhez lefuttathatja az EICAR tesztet.

Az EICAR teszt a víruskeresési rendszer ellenőrzésének bevett és biztonságos módja. A teszt biztonságosan terjeszthető, mivel ez nem egy valódi vírus, tehát nem tartalmaz semmilyen veszélyes kódot. Csak a víruskereső működőképességének ellenőrzésére szolgál. A legtöbb vírusirtó vírusként azonosítja a tesztet (*bár a jelentésben valamilyen egyértelmű név szerepel, pl: „EICAR-AV-Test"*). Az EICAR vírust a www.eicar.com címen elérhető honlapról lehet letölteni az EICAR teszthez szükséges információkkal együtt.

Töltse le az ***eicar.com*** fájlt, és mentse a helyi lemezre. A tesztfájl letöltésének megerősítése után

az Online szűrő (*amely a LinkScanner összetevő része*) azonnal megjelenít egy figyelmeztető üzenetet. A figyelmeztető üzenet tanúskodik arról, hogy az AVG megfelelően lett telepítve a számítógépre.



A http://www.eicar.com webhelyről letöltheti az EICAR 'vírus' tömörített változatát (*pl. eicar_com.zip* néven). Az Online szűrő lehetővé teszi, hogy letöltse ezt a fájlt, illetve a helyi lemezre mentse, de ezután az Állandó védelem (*a Víruskereső összetevőn belül*) észleli a „vírust” a kicsomagolás során.

Ha az AVG nem azonosítja vírusként az EICAR tesztfájlt, akkor ismételten ellenőriznie kell a program beállításait.

4.5. AVG alapértelmezett konfiguráció

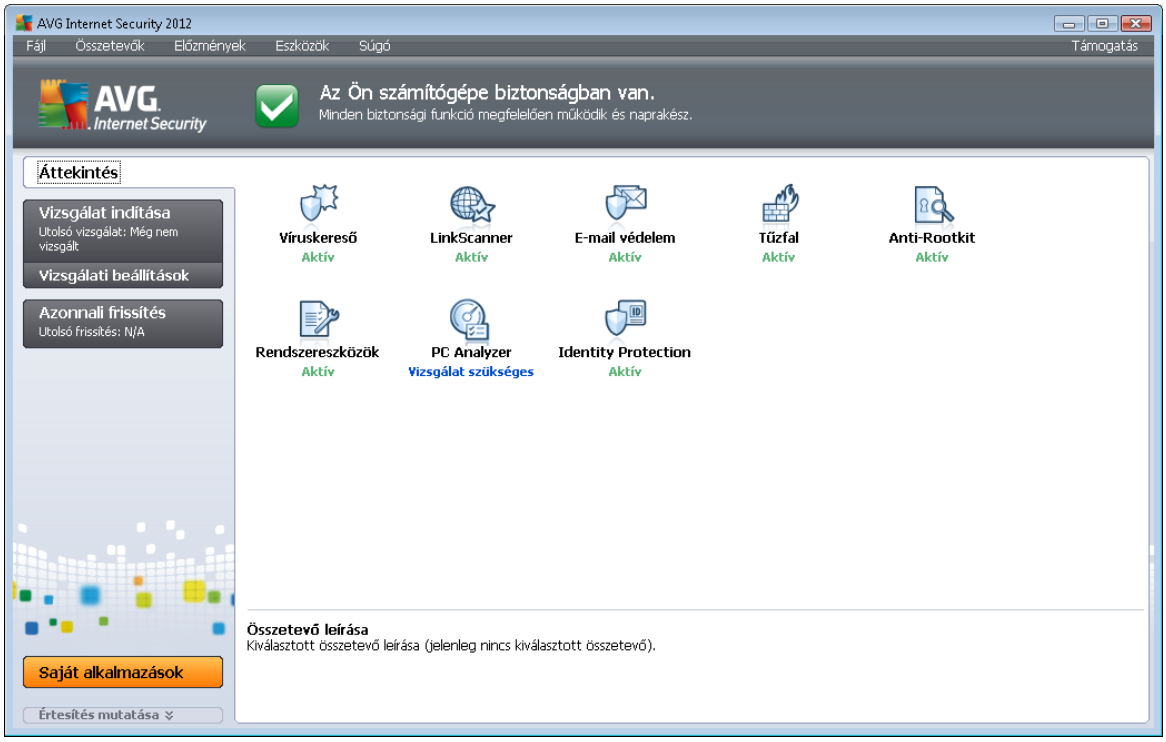
Az alapbeállításokat (*vagyis a program telepítés utáni viselkedését*) a **AVG Internet Security 2012** szoftvergyártó előre meghatározta az összes funkció és összetevő optimális teljesítményének érdekében.

Ne változtassa meg az AVG beállításokat, hacsak nem feltétlenül szükséges! Bármely változtatást tapasztalt felhasználónak kell végeznie.

Az AVG összetevők alapbeállításainak szerkesztése elérhető közvetlenül az adott összetevő felhasználói felületéről. Ha meg kell változtatnia az AVG beállításait, hogy jobban megfeleljen igényeinek, akkor menjen a Haladó AVG beállítások részbe: válassza a ***Eszközök/Haladó beállítások*** menüt, majd módosítsa az AVG opciókat az újonnan megnyílt Haladó AVG beállítások ablakban.

5. AVG felhasználói felület

Az AVG Internet Security 2012 megnyílik a főablakkal együtt:



A főablak több részből áll:

- ***A Rendszermenü*** *(az ablakban a felső sor)* a normál kiindulópont, ahonnan az összes **AVG Internet Security 2012** összetevőt, szolgáltatást és funkciót elérheti – részletek >>
- ***A Biztonsági állapot információk*** *(az ablak felső részén)* részletekkel szolgál az **AVG Internet Security 2012** program aktuális állapotával kapcsolatban – részletek >>
- ***A Gyorshivatkozások*** *(az ablak bal oldalán)* lehetővé teszik, hogy azonnal hozzáférjen a legfontosabb és leggyakrabban használt **AVG Internet Security 2012** feladatokhoz – részletek >>
- ***A Saját alkalmazások*** *(az ablak bal alsó részén)* egy áttekintést nyit meg az **AVG Internet Security 2012** további alkalmazásairól: LiveKive, Family Safety és PC Tuneup
- ***Az Összetevők áttekintése*** *(az ablak középső részén)* áttekintést nyújt az **AVG Internet Security 2012** termékkel együtt telepített összes összetevőről – részletek >>
- ***A Tálcaikon*** *(a képernyő jobb alsó részén, az értesítési területen)* az **AVG Internet Security 2012 aktuális állapotát jeleníti meg** – részletek >>
- ***Az AVG minialkalmazás*** *(Windows oldalsáv, támogatott rendszerek: Windows Vista/7)* gyors hozzáférést biztosít a vizsgálathoz és a frissítésekhez az **AVG Internet Security 2012** programon belül – részletek >>

5.1. System (Rendszer) menü

The ***Rendszer menü*** a Windows alkalmazásokban található normál navigációs menü. Vízszintesen helyezkedik el az **AVG Internet Security 2012** főablak legfelső részén. Használja a Rendszer menüt adott AVG összetevők, funkciók és szolgáltatások eléréséhez.

A Rendszer menü öt fő részre van osztva:

5.1.1. Fájl

- ***Kilépés*** - bezárja az **AVG Internet Security 2012** felhasználói felületet . Az AVG továbbra is fut a háttérben, és az Ön számítógépe továbbra is tökéletesen védve van!

5.1.2. Összetevők

Az Összetevők pont a rendszer menüben hivatkozásokat tartalmaz az összes telepített AVG összetevőhöz. Megnyitja ezen összetevők áttekintő paneljét:

- ***Rendszer áttekintése*** - váltás az alapértelmezett felhasználói felületre az összes telepített összetevő és állapotuk megjelenítésével
- ***A Víruskereső*** vírusokat, kémprogramokat, férgeket, trójaiakat és kéretlen fájlokat valamint kódokat keres a rendszeren, és a kártékony reklámprogramoktól is véd – részletek >>
- ***A LinkScanner*** webalapú fenyegetések ellen nyújt védelmet internetes keresés és böngészés közben – részletek >>
- ***Az E-mail védelem*** levélszemetet keres a bejövő e-mailekben, és blokkolja a vírusokat, az adathalász támadásokat és az egyéb fenyegetéseket – részletek >>
- ***A Tűzfal*** irányítja a kommunikációt egyes hálózati portokon, véd a rosszindulatú támadásoktól, valamint blokkolja a behatolási kísérleteket – részletek >>
- ***Az Anti-Rootkit*** az alkalmazásokban, illesztőprogramokban vagy könyvtárakban rejtőző veszélyes rootkiteket ellenőrzi – részletek >>
- ***A Rendszereszközök*** részletes áttekintést nyújt az AVG környezettel és az operációs rendszerrel kapcsolatban - részletek >>
- ***A PC Analyzer*** információkat nyújt a számítógép állapotáról - részletek >>
- ***Az Identity Protection*** folyamatosan védi digitális értékeit az új és ismeretlen fenyegetésekkel szemben – részletek >>
- ***A Biztonság eszköztár*** összetevővel közvetlenül a webböngészőből érhet el bizonyos AVG szolgáltatásokat – részletek >>
- ***A Távfelügyelet*** összetevő kizárólag az AVG Business Edition verzióiban érhető el, ha engedélyezi a telepítési folyamat során

5.1.3. Előzmények

- A vizsgálat eredménye – megjeleníti az AVG vizsgálati felületet, illetve A vizsgálat eredményének áttekintése panelt
- Állandó védelem észlelés – megnyit egy párbeszédpanelt a fenyegetések áttekintésével, amelyeket az Állandó védelem
- E-mail vizsgáló észlelése – megnyit egy párbeszédpanelt azon üzenetmellékletek áttekintésével, amelyeket az E-mail vizsgáló összetevő veszélyesnek talált
- Online szűrő találatok – megnyit egy párbeszédpanelt az Online szűrő szolgáltatás által a LinkScanner összetevőben észlelt fenyegetések áttekintésével
- Karantén – megnyitja a Karantént (elkülönített helyet), ahova az AVG program az összes nem javítható fertőzést helyezi. A Karanténban a fertőzött fájlok el vannak különítve, és a számítógép biztonsága garantált. Ugyanakkor a fertőzött fájlok jövőbeli javítás céljából eltárolódnak
- Eseménynapló - megnyitja az eseménynaplót az összes naplózott **AVG Internet Security 2012** eseménnyel
- Tűzfal - megnyitja a Tűzfalbeállítások ablakot a Naplók fülön a Tűzfal műveletek részletes áttekintésével

5.1.4. Eszközök

- Számítógép vizsgálata – átvált az AVG vizsgálati felületre, és elindítja a számítógép teljes vizsgálatát.
- Kiválasztott mappa vizsgálata... – Átvált az AVG vizsgálati felületre, és lehetővé teszi hogy meghatározza, mely fájlokat illetve mappákat kívánja ellenőrizni a számítógépen.
- Fájl vizsgálata... – Egyetlen, a lemez faszerkezetében kiválasztott fájl vizsgálatát teszi lehetővé.
- Frissítés – Automatikusan elindítja az **AVG Internet Security 2012** frissítését.
- ***Frissítés könyvtárból...*** – Elindítja a frissítési folyamatot a helyi lemezen található megadott mappában lévő frissítési fájlokkal. Ez az opció csak vészhelyzet esetén javasolt, pl. olyan helyzetekben, mikor nincs internetkapcsolat (*például a számítógép fertőzött, és le van csatlakoztatva az internetről; a számítógép olyan hálózathoz van csatlakoztatva, mely nem fér hozzá az internethez stb.*). A megnyíló ablakban válassza ki azt a mappát, amely tartalmazza a telepítőfájlt, és indítsa el a telepítési folyamatot.
- Haladó beállítások... – Megnyitja a Haladó AVG beállítások, párbeszédpanelt, ahol szerkesztheti az AVG Internet Security 2012 beállításait. Általában nem érdemes módosítani a szoftvergyártó által megadott alapértelmezett beállításokat az alkalmazásban.
- Tűzfalbeállítások... – Megnyitja a Tűzfal összetevő haladó beállításainak megadásra szolgáló külön párbeszédpanelt.

5.1.5. Súgó

- ***Tartalomjegyzék*** - megnyitja az AVG súgófájlokat
- ***Online súgó*** – megnyitja az AVG webhelyén (http://www.avg.hu/) az ügyféltámogatási központ oldalát
- ***Az Ön AVG honlapja*** – megnyitja az AVG webhelyét (http://www.avg.hu/)
- ***Vírusokról és fenyegetésekről*** – megnyitja az online Vírusenciklopédiát, ahol részletes információkat találhat az észlelt vírussal kapcsolatban
- ***Újraaktivál*** - megnyitja az ***AVG aktiválása*** panelt azokkal az adatokkkal, amiket megadott az AVG testreszabása panelen a telepítési folyamat során. Ezen a panelen megadhatja a licenckódot, hogy lecserélje az értékesítési számot (*az a szám, amivel telepítette az AVG-t*), vagy hogy lecserélje a régi licenckódot (*pl. mikor frissíti az új AVG terméket*).
- ***Regisztrálás most*** – csatlakozik az AVG webhelyének regisztrációs oldalához (http://www.avg.hu/). Töltse ki a regisztrációs adatokat; csak regisztrált ügyfelek jogosultak az ingyenes AVG műszaki terméktámogatásra.

Megjegyzés: *Ha az* **AVG Internet Security 2012** *próbaverzióját használja, akkor az utolsó két lépés a* ***Vásárlás most*** *és az* ***Aktiválás*** *lesz, amelyek segítségével megvásárolhatja a program teljes verzióját. Az értékesítési számmal telepített* **AVG Internet Security 2012** *esetében ezen lépések a következők:* ***Regisztrálás*** *és* ***Aktiválás***.

- ***Az AVG névjegye*** – megnyitja az ***Információk*** panelt öt füllel, ahol megtalálhatja a program nevét, a program és a vírusadatbázis verzióját, a rendszerinformációkat, a licencmegállapodást és az ***AVG Technologies CZ*** kapcsolatfelvételi adatait.

5.1.6. Támogatás

A ***Támogatás*** hivatkozás egy új ***Információ*** párbeszédpanelt nyit meg, amelyen az összes szükséges információ megtalálható a segítségkéréshez. A párbeszédpanel a telepített AVG program alapvető adatait (*program / adatbázis-verzió*), a licencadatokat és a gyorstámogatási hivatkozások listáját tartalmazza.

Az ***Információ*** párbeszédpanel hat lapra van osztva:

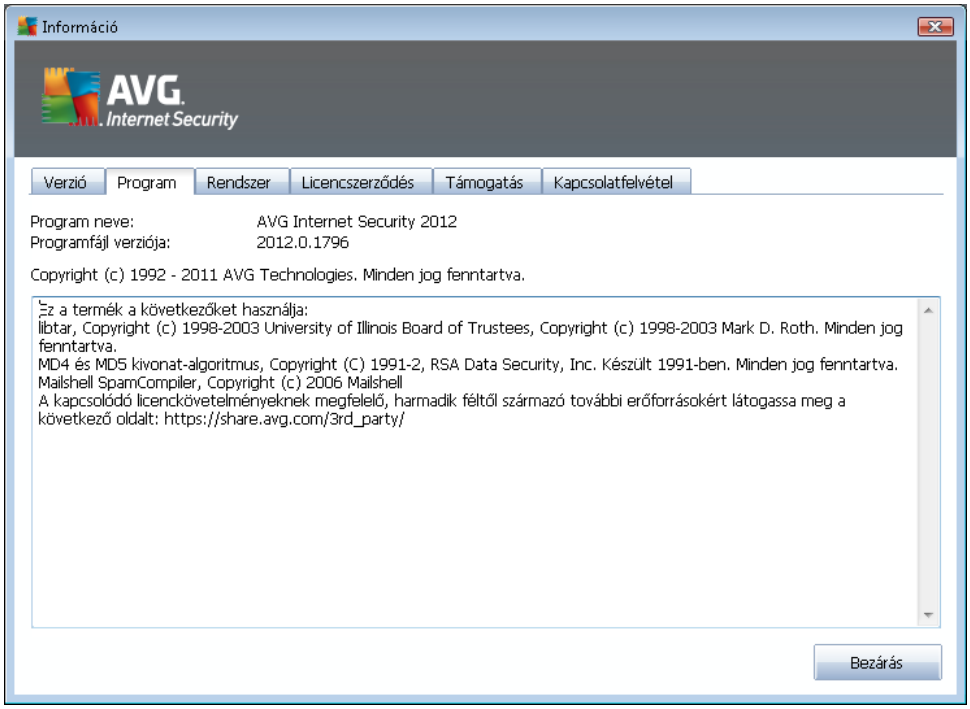
A ***Verzió*** lap három részre van osztva:

- ***Támogatási információk*** – Információkat nyújt az **AVG Internet Security 2012** verziójáról, a vírusadatbázis verziójáról, a Levélszemétszűrő adatbázisának verziójáról és a LinkScanner verziójáról.

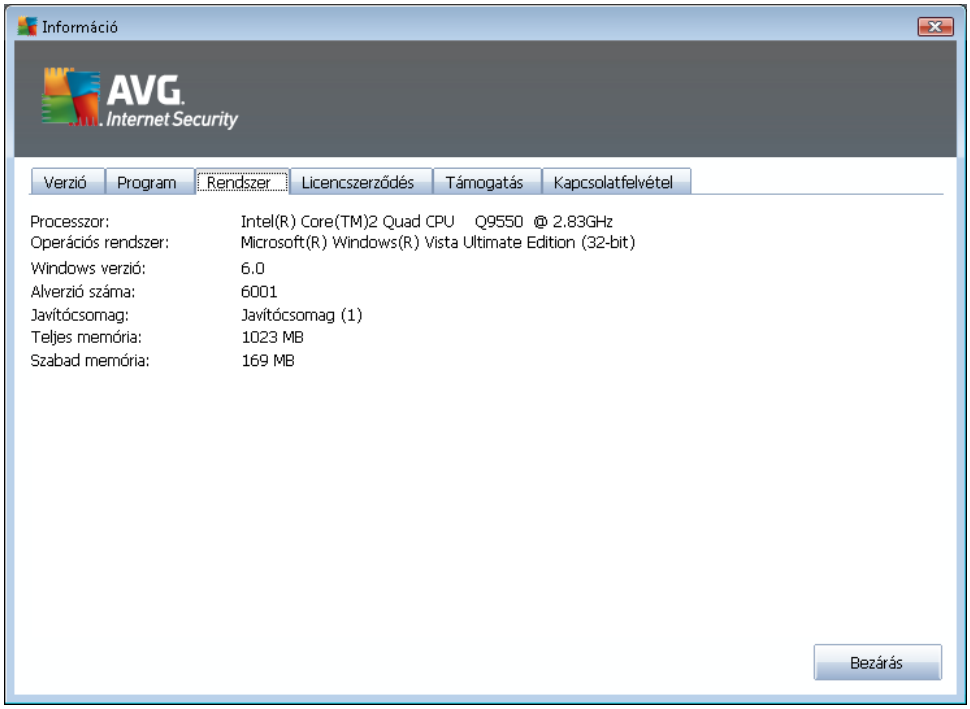
- ***Felhasználói adatai*** – A licencet birtokló felhasználóval és vállalattal kapcsolatos adatok.

- ***Licenc részletes adatai*** – Az Ön licencével kapcsolatos információk *(a termék neve, a licenc típusa és száma, a licenc lejáratának dátuma és az engedélyezett munkaállomások száma*). Az itt található ***Regisztráció*** hivatkozásra kattintva regisztrálhatja az **AVG Internet Security 2012** terméket az interneten keresztül. Ezáltal teljes körűen használhatja az AVG műszaki támogatását. Az ***Újraaktiválás*** hivatkozásra kattintva megnyílik az ***AVG aktiválása*** párbeszédpanel. Írja be a licenckódját a megfelelő mezőbe, felülírva az értékesítési számot *(amit az AVG Internet Security 2012 telepítése során használt)*, vagy lecserélve az aktuális licenckódot egy újabbra *(például amikor egy bővebb szolgáltatásokat nyújtó AVG termékre frissít).*

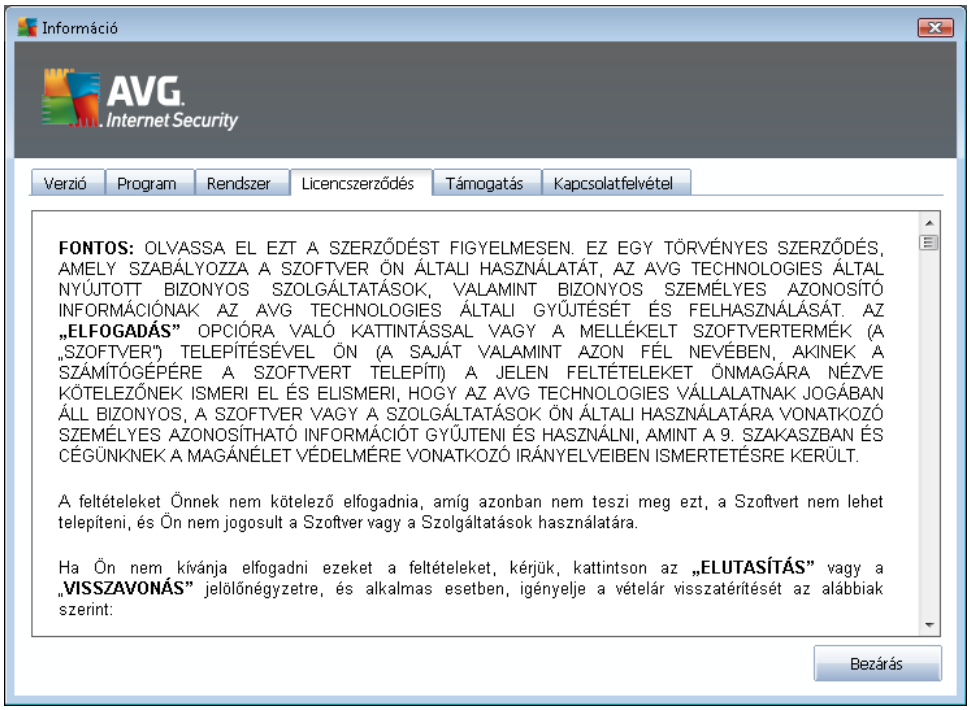
A ***Program*** fülön információt talál az **AVG Internet Security 2012** programfájl verziójáról és a termékben használt, harmadik féltől származó kódról:



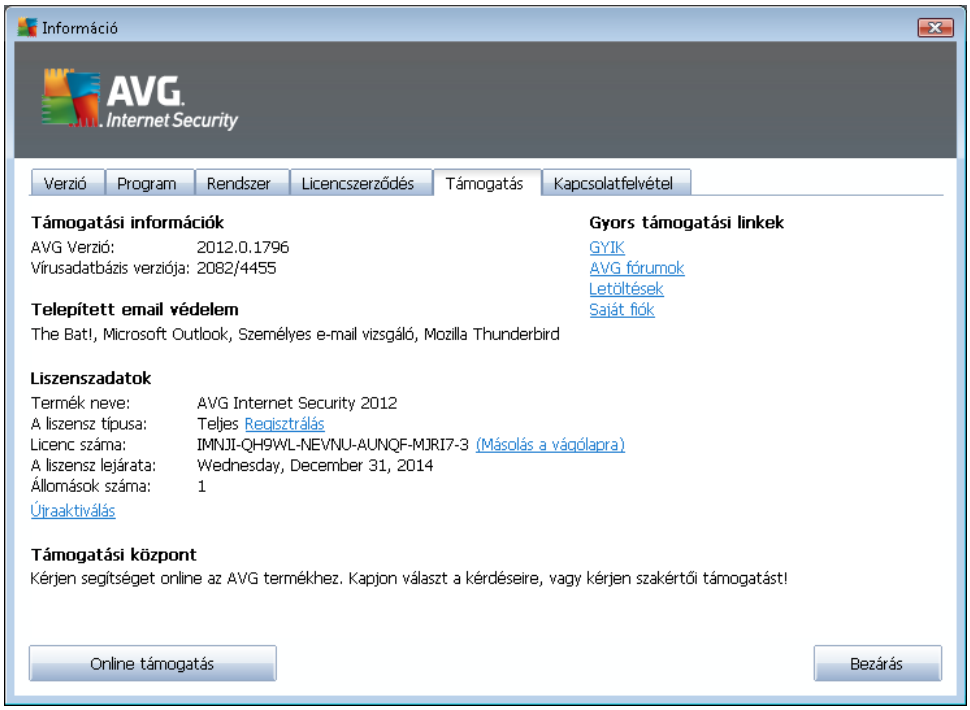
A ***Rendszer*** lap az operációs rendszer paramétereinek listáját jeleníti meg *(processzortípus, operációs rendszer és annak verziója, alverzió száma, használt szervizcsomagok, teljes memória mérete és a szabad memória mérete)*:



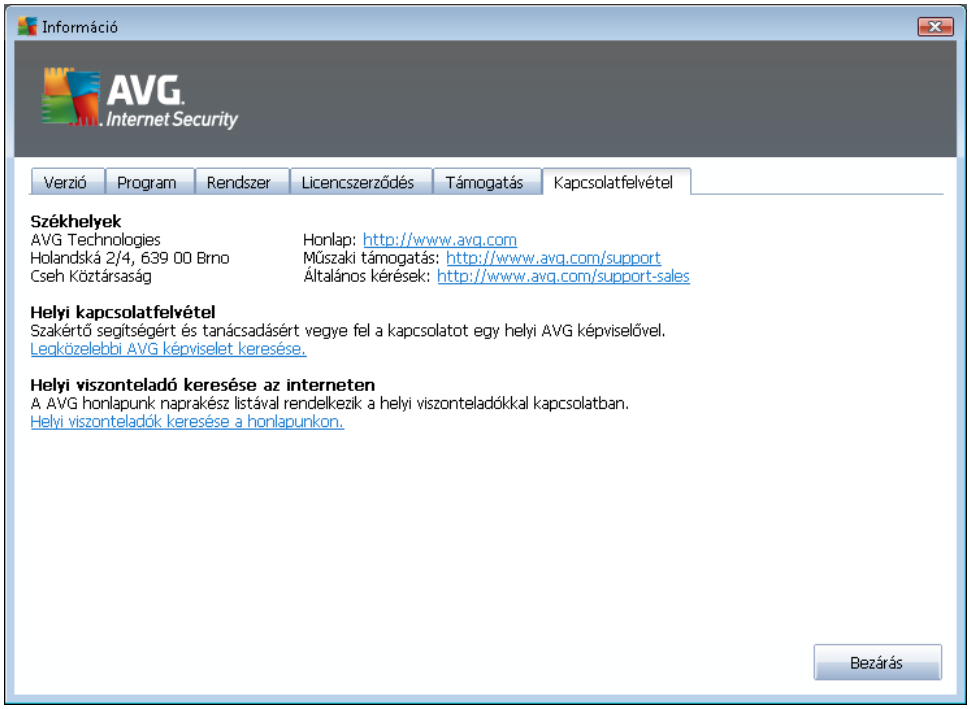
A ***Licencszerződés*** lapon megtekinthető az Ön és az AVG Technologies vállalat között létrejött szerződés teljes szövege:



A ***Támogatás*** lap felsorolja az összes lehetőséget az ügyfélszolgálat eléréséhez. Továbbá hivatkozásokat biztosít az AVG webhelyéhez (http://www.avg.hu/), AVG fórumokhoz, a GYIK részhez stb. Ezenkívül olyan információkat is talál itt, amelyek az ügyféltámogatási csapat megkeresésekor lehetnek hasznosak:



A ***Kapcsolatfelvétel*** lap felsorolja az AVG Technologies elérhetőségeit, illetve az AVG helyi képviseleteinek és viszonteladóinak elérhetőségét:



5.2. Biztonsági állapot információk

A ***Biztonsági állapot információk*** nevű rész az **AVG Internet Security 2012** főablak felső részén helyezkedik el. Itt mindig információkat találhat az **AVG Internet Security 2012** aktuális biztonsági állapotáról. Tekintse át az ebben a részben esetlegesen megjelenő ikonok listáját és jelentésüket:

- A zöld ikon azt jelzi, hogy az ***AVG Internet Security 2012 teljesen működőképes***. A számítógép teljesen védett, a rendszer naprakész, és a telepített összetevők megfelelően működnek.

- A narancsszínű ikon figyelmeztet, hogy ***egy vagy több összetevő rosszul van konfigurálva***, ezért ellenőrizni kell ezek beállításait. Nincs súlyos hiba az **AVG Internet Security 2012** működésében, és elképzelhető, hogy Ön kapcsolta ki az egyik összetevőt valamilyen okból. A védelme továbbra is garantált. Azonban fordítson figyelmet a problémás összetevő beállításaira! A név a ***Biztonsági állapot információk*** részenfog megjelenni.

A narancssárga ikon akkor is megjelenik, ha valamiért úgy dönt, hogy figyelmen kívül hagyja egy összetevő hibás állapotát. ***Az Összetevő állapotának mellőzése*** lehetőség a *jobb kattintással megnyitható* helyi menüből érhető el, az **AVG Internet Security 2012** főablakában, az adott összetevő áttekintésénél. Ezt a lehetőséget választva jelezheti, hogy

tisztában van az összetevő hibás állapotával, de saját elhatározásból ebben az állapotban kívánja tartani az **AVG Internet Security 2012** szoftvert, és nem szeretné, hogy az értesítési terület ikon figyelmeztesse erre. Elképzelhető, hogy bizonyos helyzetekben használnia kell, de javasoljuk, hogy amint lehetséges, kapcsolja ki az ***Összetevő állapotának mellőzése*** lehetőséget.

– A vörös ikon azt jelzi, hogy az ***AVG Internet Security 2012 kritikus állapotban van***! Egy vagy több összetevő nem működik megfelelően, és az **AVG Internet Security 2012** nem tudja megvédeni a számítógépet. Azonnal javítsa ki a jelentett problémát. Ha nem tudja egyedül kijavítani a hibát, akkor vegye fel a kapcsolatot az AVG műszaki támogatás csapattal.

Ha az AVG Internet Security 2012 szoftver nincs optimális teljesítményre állítva, akkor egy új Javítás (vagy Összes javítása, ha több problémáról van szó) gomb jelenik meg a biztonsági állapottal kapcsolatos információk mellett. Kattintson erre a gombra az automatikus programlefoglalási és konfigurációs folyamat elindításához. Így könnyen optimalizálható az AVG Internet Security 2012 szoftver teljesítménye, és garantálható a lehető legnagyobb biztonság.

Különösen javasolt, hogy figyelmet fordítson a ***Biztonsági állapot információk*** részre, és probléma esetén azonnal javítsa a hibát. Különben biztonsági kockázatnak teszi ki számítógépét!

Megjegyzés: *Az AVG Internet Security 2012 állapota bármikor ellenőrizhető az értesítési terület ikonjánál.*

5.3. Gyorshivatkozások

A Gyorshivatkozások az **AVG Internet Security 2012** felhasználó felületének bal oldalán találhatók. Ezek a gyorshivatkozások lehetővé teszik, hogy azonnal hozzáférjen az alkalmazás legfontosabb és leggyakrabban használt funkcióihoz, amilyenek például a vizsgálat és a frissítés. Ezek a gyorshivatkozások bármikor elérhetők a felhasználói felület összes párbeszédpaneléről:

A Gyorshivatkozások grafikusan három szakaszra vannak osztva:

- ***Áttekintés*** – Használja ezt a hivatkozást bármely éppen megnyitott AVG párbeszédpanelről az alapértelmezett ablakra váltáshoz, amely az összes telepített összetevő áttekintését tartalmazza. *(A részletekért tekintse meg az Összetevők áttekintése című fejezetet)*

- ***Vizsgálat indítása*** – Alapértelmezett állapotban ez a gomb információt nyújt a legutolsó elindított vizsgálatról *(például megadja a vizsgálat típusát és az utolsó vizsgálat dátumát)*. Kattintson a ***Vizsgálat indítása*** parancsra ugyanannak a vizsgálatnak a végrehajtásához. Ha egy másik vizsgálatot kíván elindítani, kattintson a ***Vizsgálati beállítások*** hivatkozásra. Ekkor megnyílik az AVG vizsgálati felület, ahonnan közvetlenül indíthat vizsgálatokat, és ütemezheti azokat, vagy szerkesztheti a paramétereiket. *(A részletekért tekintse meg az AVG vizsgálat című fejezetet)*

- ***Azonnali frissítés*** – Ez a hivatkozás megjeleníti a legutóbbi frissítés dátumát és időpontját. A frissítési folyamat azonnali futtatásához kattintson erre a gombra, és kövesse nyomon az állapotát. *(A részletekért tekintse meg az AVG frissítések című fejezetet)*

A ***Gyorshivatkozások*** mindig elérhetőek az AVG felhasználói felületről. Ha egy gyorshivatkozást használ egy adott folyamat futtatásához – legyen az akár egy vizsgálat, akár egy frissítés – az alkalmazás egy új párbeszédpanelre vált, de a gyorshivatkozások továbbra is elérhetőek maradnak. Ezenkívül a futó folyamat grafikusan is meg van különböztetve a navigációs területen, így teljes irányítással rendelkezik az összes elindított folyamat felett, amely az **AVG Internet Security 2012** programban fut az adott időben.

5.4. Összetevők áttekintése

Összetevők áttekintésének szakaszai

Az ***Összetevők áttekintése*** szakasz az **AVG Internet Security 2012** felhasználói felület központi részén található. A felület két részből áll:

- ***A Telepített összetevők áttekintése*** az összes telepített összetevő grafikus paneljét tartalmazza. Az egyes panelek az összetevő ikonjával vannak megjelölve, és arról biztosítanak adatokat, hogy az adott összetevő aktív vagy inaktív éppen.

- ***Az Összetevő leírása*** ezen párbeszédpanel alsó részén található. A leírás röviden ismerteti az összetevő alapvető működését. Továbbá információkat nyújt a kiválasztott összetevő aktuális állapotával kapcsolatosan.

Telepített összetevők listája

Az **AVG Internet Security 2012 termékben** az ***Összetevők áttekintése*** rész a következő összetevőkről nyújt információkat:

- ***A Víruskereső*** vírusokat, kémprogramokat, férgeket, trójaiakat és kéretlen fájlokat valamint kódokat keres a rendszeren, és a kártékony reklámprogramoktól is véd – részletek >>

- ***A LinkScanner*** webalapú fenyegetések ellen nyújt védelmet internetes keresés és böngészés közben – részletek >>

- ***Az E-mail védelem*** levélszemetet keres a bejövő e-mailekben, és blokkolja a vírusokat, az adathalász támadásokat és az egyéb fenyegetéseket – részletek >>

- ***A Tűzfal*** irányítja a kommunikációt egyes hálózati portokon, véd a rosszindulatú támadásoktól, valamint blokkolja a behatolási kísérleteket – részletek >>
- ***Az Anti-Rootkit*** az alkalmazásokban, illesztőprogramokban vagy könyvtárakban rejtőző veszélyes rootkiteket ellenőrzi – részletek >>
- ***A Rendszereszközök*** részletes áttekintést nyújt az AVG környezettel és az operációs rendszerrel kapcsolatban - részletek >>
- ***A PC Analyzer*** információkat nyújt a számítógép állapotáról - részletek >>
- ***Az Identity Protection*** folyamatosan védi digitális értékeit az új és ismeretlen fenyegetésekkel szemben – részletek >>
- ***A Biztonság eszköztár*** összetevővel közvetlenül a webböngészőből érhet el bizonyos AVG szolgáltatásokat – részletek >>

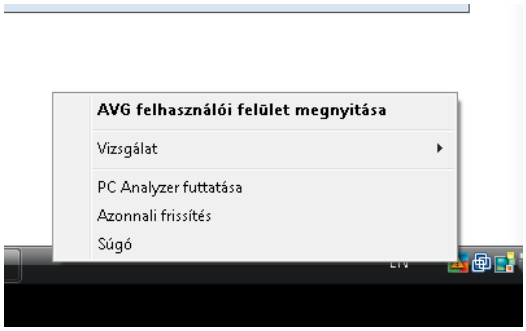
- ***A Távfelügyelet*** összetevő kizárólag az AVG Business Edition verzióiban érhető el, ha engedélyezi a telepítési folyamat során

Elérhető műveletek

- ***Helyezze az egérmutatót bármely összetevő ikonjára*** az összetevők áttekintésében történő kiemeléshez. Ezzel egy időben az összetevő alapvető működésének leírása megjelenik a felhasználói felület alsó részén.
- ***Ha egyszer kattint bármely összetevő ikonjára***, akkor megnyílik az összetevő saját felülete az alapvető statisztikai adatokkal.
- ***Kattintson a jobb gombbal az összetevő ikonjára*** a helyi menü számos lehetőséggel kibővített megjelenítéséhez:
  - ***Megnyitás*** – Kattintson erre a lehetőségre az összetevő saját párbeszédpaneljének megnyitásához *(pont, mintha az összetevő ikonjára kattintana egyszer)*.
  - ***Az összetevő állapotának mellőzése*** – Ezt a lehetőséget választva jelezheti, hogy tudatában van az összetevő hibaállapotának, de saját elhatározásából fenn kívánja tartani ezt az állapotot, és nem szeretné, hogy a tálcaikon figyelmeztesse erre.
  - ***Megnyitás a Speciális beállításokban ...*** – Ez a lehetőség csak bizonyos összetevők esetén érhető el; amelyek lehetőséget nyújtanak a speciális beállítások számára.

5.5. Tálcaikon

Az AVG tálcaikon *(a Windows tálcán a képernyő jobb alsó sarkában található)* jelzi az **AVG Internet Security 2012** alkalmazás aktuális állapotát. Ez mindig látható a tálcán, attól függetlenül, hogy az **AVG Internet Security 2012** felhasználói felülete meg van-e nyitva:



AVG tálcaikon megjelenése

- Ha színes, és semmilyen egyéb elem nem látható rajta, az azt jelzi, hogy az **AVG Internet Security 2012** összetevők aktívak és tökéletesen működőképesek. Az ikon akkor is így jelenhet meg, ha egy összetevő nem működik tökéletesen, de a felhasználó úgy döntött, hogy figyelmen kívül hagyja az adott összetevő állapotát. *(Dönthet úgy, hogy figyelmen kívül hagyja az összetevő állapotát. Ezzel jelzi, hogy tisztában van az összetevő hibaállapotával, de saját elhatározásból ebben az állapotban kívánja tartani, és nem szeretné, hogy a program figyelmeztesse erre.*

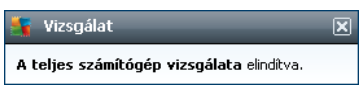
- A felkiáltójellel kiegészített ikon azt jelzi, hogy egy *(vagy akár több)* összetevő hibaállapotban van. Mindig ügyeljen az ilyen figyelmeztetésekre, és próbálja meg elhárítani a nem megfelelően beállított összetevők konfigurációs problémáit. Az alkalmazás felhasználói felületének megnyitásához és az összetevő beállításainak módosításához kattintson duplán a tálcaikonra. Részletes információkért azzal kapcsolatban, hogy melyik összetevő van hibaállapotban, tekintse meg a biztonsági állapot információk nevű szakaszt.

- A tálcaikon ezenfelül megjelenhet színesen, egy villogó vagy forgó fénynyalábbal is. Az így kinéző ikon azt jelzi, hogy éppen frissítési folyamat zajlik.

- A színes ikonon megjelenhet egy nyíl is, ami azt jelenti, hogy az **AVG Internet Security 2012** éppen vizsgálatot futtat.

AVG tálcaikon információk

Az AVG tálcaikon további információkat nyújt az aktuális **AVG Internet Security 2012** műveletekről és a program esetleges állapotváltozásairól (*ütemezett vizsgálat vagy frissítés automatikus indítása, tűzfalprofil váltása, összetevő állapotváltozása, hibaállapot stb.*) a tálcaikonról megnyíló előugró ablakokban:



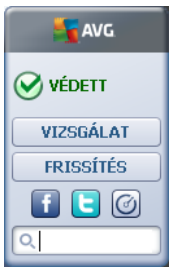
Az AVG tálcaikonról elérhető műveletek

Az AVG tálcaikon gyorshivatkozásként is szolgál az **AVG Internet Security 2012** felhasználói felületének azonnali eléréséhez. A felület megnyitásához csak kattintson duplán az ikonra. Kattintson a jobb gombbal az ikonra a helyi menü megnyitásához, amely a következő lehetőségeket tartalmazza:

- ***AVG felhasználói felület megnyitása*** – Kattintson ide az **AVG Internet Security 2012** felhasználói felületének megnyitásához.
- ***Vizsgálatok*** – Kattintson ide az előre meghatározott vizsgálatok (*Számítógép teljes vizsgálata*, *Kiválasztott fájlok vagy mappák ellenőrzése*, *Anti-Rootkit vizsgálat*) helyi menüjének megnyitásához, majd válassza ki a kívánt vizsgálatot – ekkor az azonnal elindul.
- ***Tűzfal*** – Kattintson ide a Tűzfal beállítások helyi menüjének megnyitásához, ahol módosíthatja a főbb paramétereket, például a Tűzfal állapota (*Tűzfal engedélyezve/Tűzfal letiltva/Vészhelyzet mód*), a Játék módra váltás és a Tűzfal profilok beállításokat.
- ***PC Analyzer*** – Kattintson ide a PC Analyzer összetevő felhasználói felületének megnyitásához.
- ***Futó vizsgálatok*** – Ez az elem csak akkor jelenik meg, ha egy vizsgálat éppen fut a számítógépen. A vizsgálatnál beállíthatja annak prioritását, illetve leállíthatja vagy szüneteltetheti azt. Továbbá a következő műveletek érhetők itt el: *Összes vizsgálat prioritásának beállítása, Összes vizsgálat szüneteltetése* vagy *Összes vizsgálat leállítása*.
- ***Frissítés most*** – Elindítja az azonnali frissítést.
- ***Súgó*** – Megnyitja a súgófájlt a kezdőlapon.

5.6. AVG minialkalmazás

Az AVG minialkalmazás a Windows asztalon jelenik meg (*Windows oldalsáv*). Ez az alkalmazás csak a Windows Vista és a Windows 7 rendszereken támogatott. ***Az AVG minialkalmazás*** azonnali hozzáférést biztosít a legfontosabb **AVG Internet Security 2012** szolgáltatásokhoz, pl. vizsgálat és frissítés:

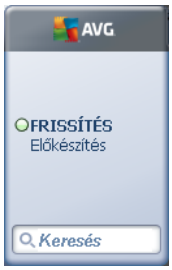


Gyors hozzáférés a vizsgálathoz és a frissítéshez

Ha szükséges, az ***AVG minialkalmazás*** lehetővé teszi, hogy azonnal elindítson egy vizsgálatot vagy egy frissítést:

- ***Vizsgálat indítása*** – Kattintson a ***Vizsgálat indítása*** hivatkozásra a Vizsgálat a teljes számítógépen funkció közvetlen elindításához. A vizsgálati folyamat állapotát a minialkalmazás egy külön felületén figyelheti. A rövid statisztikai áttekintés információkat nyújt a vizsgált objektumok, az észlelt fenyegetések és a javított fenyegetések számával kapcsolatban. A vizsgálat során bármikor szüneteltetheti vagy leállíthatja a folyamatot. A vizsgálati eredményekhez tartozó részletes adatokért tekintse meg A vizsgálat eredményének áttekintése párbeszédpanelt, amely közvetlenül a minialkalmazásból nyitható meg a ***Részletek mutatása*** gombra kattintva *(az eredmények az Oldalsáv minialkalmazások vizsgálata területen láthatók)*.

- ***Azonnali frissítés*** – Kattintson az ***Azonnali frissítés*** hivatkozásra az **AVG Internet Security 2012** közvetlen frissítéséhez a minialkalmazásból:



Közösségi hálózatok elérése

Az AVG minialkalmazás tartalmaz egy gyorshivatkozást a főbb közösségi hálózatok eléréséhez is. Használja a megfelelő gombot, hogy csatlakozzon az AVG közösségekhez a Twitter, Facebook, és LinkedIn oldalakon:

- ***Twitter link*** - megnyit egy új ***AVG minialkalmazást***, amelyen megtekintheti az AVG legújabb bejegyzéseit a Twitteren. Kattintson az ***AVG Twitter bejegyzések megtekintése*** linkre, amely egy új böngészőablakot nyit meg, és átirányítja Önt közvetlenül a Twitter weboldalára, ahol megtekintheti az AVG kapcsolódó bejegyzéseit:

- ***Facebook link*** - megnyitja a böngészőt a Facebook oldalával, ahol megtekintheti az ***AVG közösségi*** oldalát

- ***LinkedIn*** – Ez a lehetőség csak hálózati telepítés esetén érhető el (*például ha az AVG Business Edition verzióját telepítette*). A rendszer megnyitja a böngészőt az ***AVG SMB Community*** webhelyénél a LinkedIn közösségi oldalon.

A minialkalmazással elérhető egyéb funkciók

- ***PC Analyzer*** – Megnyitja a PC Analyzer összetevő felhasználói felületét

- ***Keresődoboz*** – Írjon be egy kulcsszót, és a találatok azonnal megjelennek az alapértelmezett böngésző egy újonnan megnyíló ablakában

6. AVG összetevők

6.1. Víruskereső

A ***Víruskereső*** összetevő az **AVG Internet Security 2012** sarokköve, amely egyesíti egy biztonsági program számos alapvető funkcióját:

- Vizsgálati motor
- Állandó védelem
- A kémprogramok elleni védelem

6.1.1. Vizsgálati motor

A ***Víruskereső*** összetevő alapjául szolgáló keresőmotor minden fájlt illetve műveletet megvizsgál *(fájlok megnyitása/bezárása stb.)*, hogy nem talál-e ismert vírusokat. A felismert vírusokat a program elzárja minden fájlművelettől, ezután pedig megsemmisíti vagy karanténba helyezi azokat.

Az AVG Internet Security 2012 fontos funkciója, hogy minden ismert vírus futását ellehetetleníti a számítógépen.

Észlelési módszerek

A legtöbb víruskereső szoftver heurisztikus keresésre is képes, amelynek során a program vírusra utaló tulajdonságokat, úgynevezett víruskarakterisztikákat keres az egyes fájlokban. Ez azt jelenti, hogy a víruskereső program felismerhet teljesen új, idáig ismeretlen vírusokat is, ha az tartalmaz bizonyos – már létező vírusokra jellemző – tulajdonságokat. A ***Víruskereső*** a következő észlelési módszereket alkalmazza:

- *Keresés* – Egy adott vírusra jellemző minta keresése
- *Heurisztikus elemzés* – A vizsgált objektum utasításainak dinamikus emulálása virtuális számítógépes környezetben
- *Általános azonosítás* – Az adott vírusra/víruscsoportra jellemző utasítások azonosítása

Mivel egyetlen technológia nem feltétlenül elegendő egy vírus megkereséséhez és azonosításához, a ***víruskereső*** program többféle technológiát ötvöz a számítógép védelmének érdekében. **Az AVG Internet Security 2012** képes a rendszer nemkívánatos végrehajtható alkalmazásainak és DLL könyvtárainak elemzésére és azonosítására is. Az ilyen fenyegetéseket *(többféle kémprogram, reklámprogram stb.)* nemkívánatos alkalmazásoknak nevezik. Ezenkívül az **AVG Internet Security 2012** megvizsgálja a beállításjegyzéket is, ahol gyanús bejegyzéseket, ideiglenes internetes fájlokat és nyomkövető cookie-kat keres, és lehetőséget nyújt a kártékony elemek fertőzésként történő kezelésére.

Az AVG Internet Security 2012 folyamatos védelmet biztosít számítógépének.

6.1.2. Állandó védelem

Az AVG Internet Security 2012 úgy nevezett állandó védelem formájában nyújt folyamatos védelmet. A ***Víruskereső*** minden egyes megnyitott, mentett vagy másolt fájlt megvizsgál *(megadott kiterjesztéssel rendelkezőt vagy kiterjesztés nélkülit)*. Védi a számítógép rendszerterületeit és a cserélhető adathordozókat (*flash meghajtó stb.*). Ha a rendszer vírust észlel egy fájl elérése közben, akkor megszakítja az éppen végrehajtott műveletet, és nem engedi, hogy a vírus működésbe lépjen. Jellemzően a felhasználó észre sem veszi a folyamatot, hiszen az állandó védelem „a háttérben" fut. Csak akkor kap értesítést, ha a program fenyegetést talál; ezzel egy időben a ***Víruskereső*** megakadályozza, hogy a fenyegetés működésbe lépjen, valamint eltávolítja azt.

Az Állandó védelem betöltése a számítógép memóriájába a rendszer indításakor történik, és különösen fontos, hogy állandóan be is legyen kapcsolva!

6.1.3. A kémprogramok elleni védelem

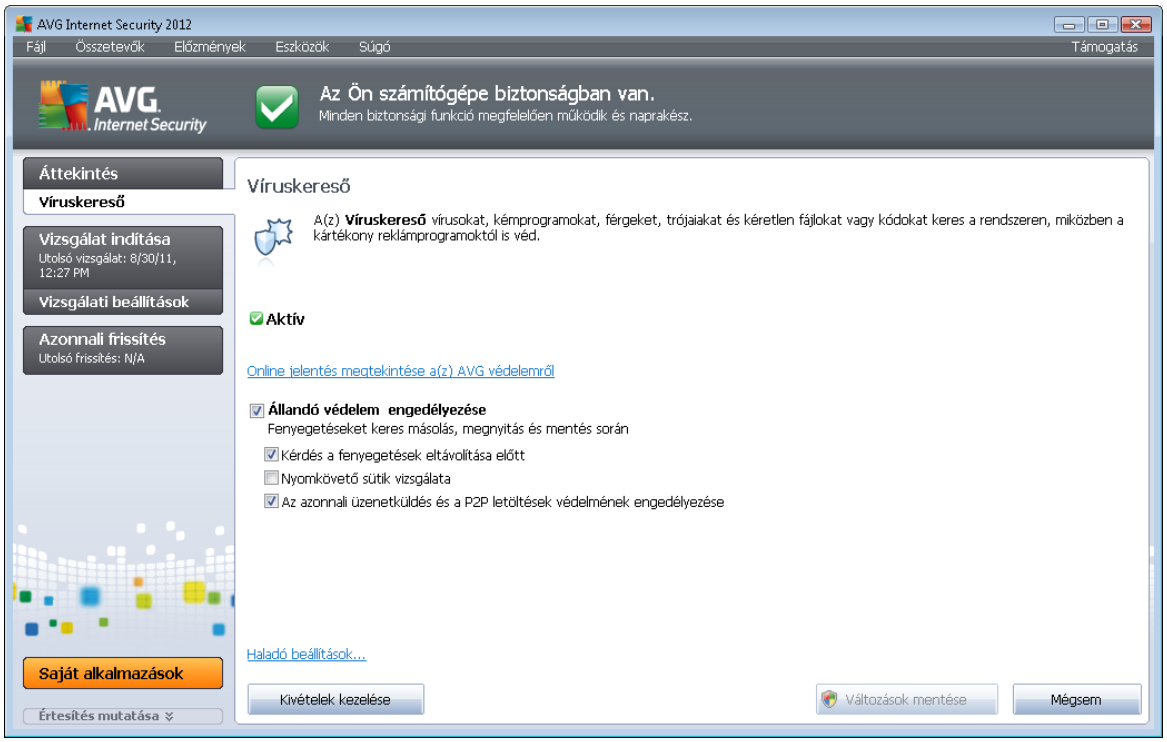
A Kémprogram-elhárító egy kémprogram-adatbázist tartalmaz, amely az ismert kémprogram-definíciók azonosítására szolgál. Az AVG kémprogram szakértői azon dolgoznak, hogy minél hamarabb azonosítsák és leírják a legújabb kémprogram-mintákat, és hozzáadják azokat az adatbázishoz. A frissítési folyamat során ezek a definíciók letöltődnek a számítógépére, így Ön mindig megbízható védelemmel rendelkezik a legújabb kémprogram-típusokkal szemben. ***A Kémprogram-elhárító*** lehetővé teszi a számítógépen lévő káros programok/kémprogramok megkeresését. A vizsgálat során a program a még „szunnyadó és inaktív", azaz a letöltött, de még nem működő káros programokat is azonosítja.

Mi az a kémprogram?

A kémprogramok a káros programok olyan típusaként azonosíthatók, amelyek a felhasználó tudta vagy beleegyezése nélkül adatokat gyűjtenek össze a felhasználó számítógépéről. Bizonyos kémprogramok telepítése szándékosan is történhet. Ezek gyakran hirdetéseket, felugró ablakokat és más kellemetlen szoftvereket tartalmaznak. A fertőzések fő forrását jelenleg a potenciálisan veszélyes tartalmat hordozó weblapok jelentik. A terjedés más módon is történhet: gyakran előfordul, hogy a rosszindulatú programok e-mailben terjednek, vagy férgek és vírusok közvetítik őket. A védelem legfontosabb eleme egy háttérben működő ellenőrzőprogram, a ***Kémprogram-kereső***, amely az alkalmazásokat futásuk közben a háttérben ellenőrzi.

6.1.4. Víruskereső felület

A ***Víruskereső*** összetevő felhasználói felülete rövid információkat nyújt az összetevő működéséről, az aktuális állapotáról *(Aktív)*, illetve az összetevő alapvető konfigurációs lehetőségeiről:



Beállítási lehetőségek

A párbeszédpanel a ***Víruskereső*** összetevő néhány alapvető beállítási lehetőségét tartalmazza. Az alábbiakban ezek rövid leírását találja:

- ***Az AVG általi védelméről készült online jelentés megtekintése*** – A hivatkozás az AVG webhely (http://www.avg.hu/) egy adott oldalára irányítja át. Ezen a webhelyen részletes statisztikai áttekintést talál az **AVG Internet Security 2012** a számítógépen egy adott időtartamon belül, valamint összességében végzett tevékenységeiről.

- ***Állandó védelem engedélyezése*** – Ez a beállítás lehetővé teszi, hogy könnyen ki-/és bekapcsolja az állandó védelmet. Az Állandó védelem a fájlokat másolásukkor, megnyitásukkor és mentésükkor vizsgálja. Ha a rendszer fenyegetést észlel, akkor azonnal riaszt. Alapértelmezés szerint a funkció be van kapcsolva, és javasoljuk, hogy hagyja így. Ha az állandó védelem be van kapcsolva, eldöntheti, hogy az esetleges észlelt fertőzéseket hogyan kezelje a rendszer:

  - ***Az összes fenyegetés automatikus eltávolítása*/*Kérdés a fenyegetések eltávolítása előtt*** – Válassza ki az egyik beállítást. Ez a beállítás nincsen hatással a biztonsági szintre, és csak az Ön személyes preferenciáit tükrözi.

- ***Nyomkövető sütik vizsgálata*** – Az előző beállításoktól függetlenül meghatározhatja, hogy kívánja-e vizsgálni a nyomkövető cookie-k jelenlétét. *(A cookie-k olyan szöveges adatcsomagok, amelyeket a kiszolgáló küld a webböngészőnek, illetve amelyeket a webböngésző küld vissza a kiszolgálónak, ha újra csatlakozik ahhoz. A HTTP cookie-kat hitelesítéshez, nyomkövetéshez és bizonyos felhasználói adatok – például webhely-preferenciák vagy online vásárlás esetén a kosár tartalma – gyűjtéséhez használják.* Bizonyos esetekben bekapcsolhatja ezt a funkciót a maximális biztonsági szint eléréséhez, azonban alapértelmezés szerint ki van kapcsolva.

- ***Azonnali üzenetküldés védelem engedélyezése*** – Jelölje be ezt a lehetőséget, ha meg szeretne bizonyosodni arról, hogy az azonnali üzenetküldésen alapuló kommunikáció (*például ICQ, MSN Messenger stb.*) vírusmentesek.

- ***Haladó beállítások***... – Kattintson a hivatkozásra az **AVG Internet Security 2012** Haladó beállítások felületet tartalmazó párbeszédpaneljének megnyitásához. Itt részletesen megadhatja az összetevő beállításait. Kérjük, vegye figyelembe, hogy az **AVG Internet Security 2012** alapértelmezett beállításaival az összes összetevő optimális teljesítményt nyújt maximális biztonság mellett. Javasoljuk, hogy tartsa meg az alapértelmezett beállításokat.

Vezérlőgombok

A párbeszédpanelen a következő vezérlőgombokat használhatja:

- ***Kivételek kezelése*** – Megnyit egy Állandó védelem – Kivételek elnevezésű új párbeszédpanelt. Ez a párbeszédpanel a főmenüből is elérhető a következő úton: Haladó beállítások / Víruskereső / Állandó védelem / Kivételek *(részletes leírásért tekintse meg a megfelelő fejezetet)*. A párbeszédpanelen megadhatja azokat a fájlokat és mappákat, amelyeket ki szeretne hagyni az Állandó védelem vizsgálatból. Ha nincs rá külön indoka, akkor nem ajánlott elemeket kihagyni a vizsgálatból. A párbeszédpanel a következő vezérlőgombokat tartalmazza:

  - *Elérési út hozzáadása* – Megadhatja a vizsgálatból kihagyni kívánt könyvtárat *(vagy könyvtárakat)*. A könyvtárakat a helyi lemez navigációs fájáról választhatja ki egyesével.

  - *Fájl hozzáadása* – Megadhatja a vizsgálatból kihagyni kívánt fájlokat. A fájlokat a helyi lemez navigációs fájáról választhatja ki egyesével.

  - *Elem hozzáadása* – Lehetőséget nyújt a kijelölt fájl vagy mappa elérési útjának szerkesztésére.

  - *Elem eltávolítása* – Lehetőséget nyújt a kijelölt elem elérési útjának törlésére a listából.

- ***Változások mentése*** – Az összetevő beállításaiban a párbeszédpanelen elvégzett változtatások mentése és visszatérés az **AVG Internet Security 2012 fő** felhasználói felületéhez (*összetevők áttekintése*).

- ***Mégse*** – Az összetevő beállításai ezen a párbeszédpanelen elvégzett módosításainak visszavonása. A módosításokat nem menti a program. Ugyanakkor visszatér az **AVG Internet Security 2012 fő** felhasználói felületéhez (*összetevők áttekintése*).

6.1.5. Állandó védelem észlelései

A program fenyegetést észlelt.

Az Állandó védelem a fájlokat másolásukkor, megnyitásukkor és mentésükkor vizsgálja. Ha a rendszer fenyegetést észlel, akkor azonnal riaszt a következő ablakkal:

Ezen a panelen adatokat találhat azon fájlokról, amelyeket fertőzöttnek minősített a program (*Fájlnév*), továbbá itt jelenik meg a fertőzés neve (*Fenyegetés neve*), illetve egy, a Vírusenciklopédia adatbázisra mutató hivatkozás, ahol részletes adatokat talál a fertőzésről (*További információk*).

Ezután döntenie kell, hogy mit kíván tenni. Számos lehetőség közül választhat. ***Vegye figyelembe, hogy bizonyos esetekben (a fertőzött fájl típusától és helyétől függően) nem minden lehetőség áll rendelkezésre.***

- ***Eltávolítás gyakorlott felhasználóként*** – jelölje be, ha általános felhasználóként nem rendelkezik elegendő joggal a fenyegetés eltávolításához. A gyakorlott felhasználók kiterjedt hozzáférési jogokkal rendelkeznek, és ha a fenyegetés egy bizonyos rendszermappában található, akkor elképzelhető, hogy be kell jelölnie ezt az opciót az eltávolításhoz.

- ***Javítás*** - ez a gomb csak akkor jelenik meg, ha az észlelt fertőzés javítható. Eltávolítja a fertőzést a fájlból, majd visszaállítja azt az eredeti állapotába. Ha maga a fájl egy vírus, akkor használja ezt a funkciót a törléshez *vagyis a Karanténba történő áthelyezéshez)*

- ***Áthelyezés karanténba*** – A program áthelyezi a vírust a karanténba

- ***Ugrás a fájlhoz*** - ez az opció átirányítja Önt a gyanús objektum pontos helyére (*megnyit egy új Windows Intéző ablakot*)

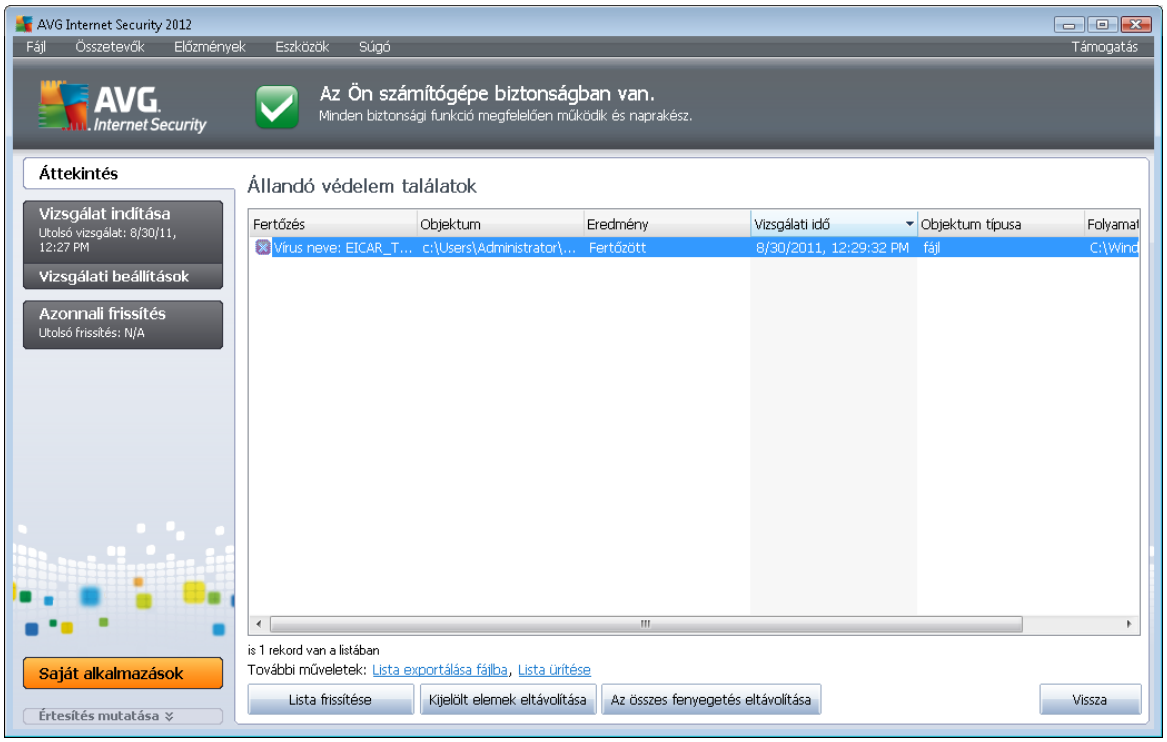
- ***Mellőzés*** - NE használja ezt az opciót, csak akkor, ha feltétlenül szükséges!

Megjegyzés: *Előfordulhat, hogy az észlelt objektum mérete túllépi a karantén szabad helyének méretét. Ebben az esetben egy figyelmeztető üzenet jelenik meg, ha Ön fertőzött objektumot próbál áthelyezni a karanténba. A karantén mérete módosítható. Ezt az értéket a merevlemez valódi méretének adott százalékában határozhatja meg. A karantén méretének növeléséhez menjen a Karantén párbeszédpanelre az AVG Haladó beállítások részen a "Karantén méretének korlátozása" opcióra.*

A panel alsó részén található a ***Részletek megjelenítése*** hivatkozás. Kattintson rá, ekkor részletes adatok jelennek meg a fertőzés észlelésekor futó folyamatról, illetve a folyamat azonosításáról.

Állandó védelem észlelései – áttekintés

Az Állandó védelem által észlelt fenyegetés összes áttekintése megtalálható az ***Állandó védelem észlelés*** panelen, amely a rendszermenü Előzmények/ Állandó védelem találatok részén található:



Az ***Állandó védelem találatok*** megmutatja az Állandó védelem által azonosított és veszélyesnek minősített elemeket, melyek javítva lettek vagy át lettek helyezve a Karanténba. Minden észlelt objektumnál a következő információk állnak rendelkezésre:

- ***Fertőzés*** - az észlelt objektum leírása (neve)
- ***Objektum*** - az objektum helye
- ***Eredmény*** - az észlelt objektumon végzett művelet

- ***Észlelési idő*** - megmutatja az objektum azonosításának dátumát és idejét
- ***Objektum típusa*** - az észlelt objektum típusa
- ***Folyamat*** - milyen művelet váltotta ki a potenciálisan veszélyes objektum megjelenését illetve észlelését

A panel alsó részén, a lista alatt, információkat találhat az észlelt objektumok összes számával kapcsolatban. Exportálhatja az észlelt elemek teljes listáját egy fájlba (***Lista exportálása fájlba***), és törölheti az elemek összes bejegyzését is (***Lista törlése***). A ***Lista frissítése*** gomb frissíteni fogja a ***Rezidens védelem*** által észlelt fenyegetések listáját. A ***Vissza*** gombra kattintva visszatérhet az alapértelmezett AVG fő párbeszédpanelre (*összetevők áttekintése*).

6.2. LinkScanner

A LinkScanner védi Önt napjaink gyorsan felbukkanó és eltűnő online fenyegetéseitől. Ezen fenyegetések rejtve lehetnek bármilyen szervezet weboldalán (a kormányzatoktól kezdve, a nagy és jól ismert márkákon át, egészen a kisvállalkozásokig), és ritkán maradnak ugyanazon a weboldalon 24 óránál tovább. ***A LinkScanner*** elemzi a linkek mögött lévő, megtekintendő weboldalak tartalmát, és biztosítja, hogy Ön már akkor biztonságban legyen, mielőtt még rákattintana az adott linkre.

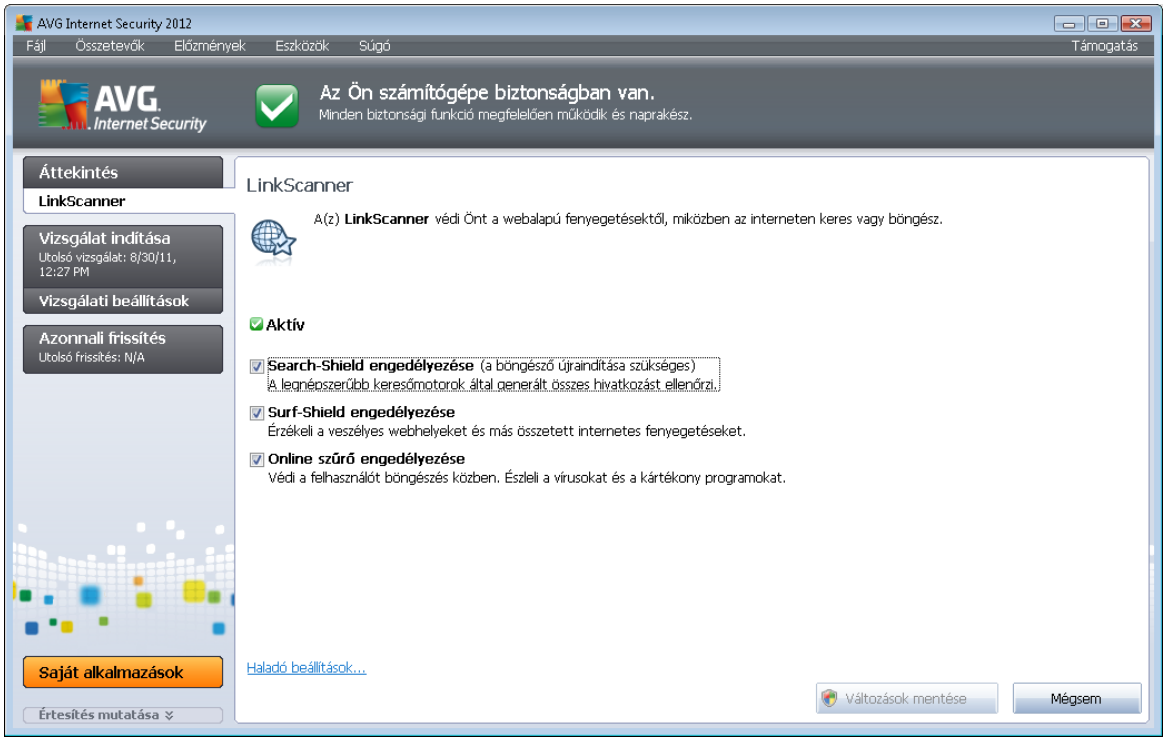
A LinkScanner nem a kiszolgálóplatformok védelmére szolgál!

A ***LinkScanner*** technológia a következő fő szolgáltatásokat tartalmazza::

- A Kereső védelem olyan webhelyek listáját tartalmazza (URL-címek), amelyek veszélyesnek minősülnek. Ha Google, Yahoo!, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask vagy Seznam keresőmotorral keres, a rendszer a lista alapján ellenőrzi a keresési eredményeket, és megjelenít egy értékelő ikont mellettük *(Yahoo! keresési eredmények esetében csak „veszélyes webhely” értékelő ikon jelenik meg)*.
- A Böngészés védelem a meglátogatott webhelyek tartalmát azok címétől függetlenül ellenőrzi. Ha bizonyos webhelyeket a Keresés védelem *nem észlel (például ha új veszélyes webhely jön létre, vagy ha egy korábban jóindulatú webhely megfertőződik)*, akkor a Böngészés védelem észleli és letiltja a meglátogatni kívánt gyanús tartalmakat.
- Az Online szűrő valós idejű védelmet nyújt az internet böngészése során. Megvizsgálja a meglátogatni kívánt weblapokat és az esetlegesen beágyazott fájlokat, mielőtt azok megjelennének a webböngészőben vagy letöltődnének a számítógépre. Az Online szűrő észleli a megnyitni kívánt weblapba ágyazott vírusokat és kémprogramokat, valamint azonnal megakadályozza azok letöltését, így semmilyen fenyegetés nem érheti a számítógépet.
- ***Az AVG Accelerator*** folyamatosabb online videolejátszást tesz lehetővé, és megkönnyíti a további letöltéseket. Amikor videogyorsítás van folyamatban, a rendszertálcán megjelenik egy felugró ablak.

6.2.1. LinkScanner felület

A LinkScanner összetevő főablaka rövid leírást nyújt az összetevő működéséről, és információkat biztosít az összetevő aktuális állapotáról *(Aktív)*:



A párbeszédpanel alsó részén az összetevő néhány alapvető beállítása található:

- ***Keresés védelem*** engedélyezése – (*alapértelmezés szerint be van kapcsolva*): Csak abban az esetben törölje a jelölőnégyzet bejelölését, ha a Keresés védelem funkciót feltétlenül szükséges kikapcsolni.

- ***Böngészés védelem*** engedélyezése – (*alapértelmezés szerint be van kapcsolva*): Aktív (*valós idejű*) védelem kockázatos weboldalak ellen. Az ismert kártékony oldalak és veszélyes tartalmuk megjelenítése a webböngészőben, illetve *bármely más, HTTP-t használó alkalmazásban is* le lesz tiltva.

- ***Online szűrő*** engedélyezése – (*alapértelmezés szerint be van kapcsolva*): Lehetséges vírusok és kémprogramok valós idejű keresése a megnyitni kívánt weboldalakon. Amennyiben a program ilyeneket észlel, a letöltés azonnal leáll, hogy semmilyen fenyegetés ne férhessen hozzá a számítógépéhez.

6.2.2. Kereső védelem észlelései

Ha a ***Kereső védelemmel*** keres az interneten, akkor a rendszer az összes népszerű keresőmotorból (*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg és SlashDot*) származó találatnál veszélyes vagy gyanús linkeket keres. Ezen hivatkozások ellenőrzésével, illetve a veszélyesek megjelölésével a LinkScanner figyelmezteti Önt, még mielőtt egy veszélyes vagy gyanús hivatkozásra kattintana. Így biztos lehet benne, hogy mindig csak biztonságos webhelyeket látogat majd meg.

Miközben a program elemzi a hivatkozásokat a keresési eredmények oldalon, egy grafikus jel fog megjelenni az egyes elemek mellett, jelezvén, hogy az ellenőrzés folyamatban van. Miután az értékelés befejeződött, az információs ikonok jelennek meg:

 A hivatkozott oldal biztonságos (*ez az ikon nem jelenik meg a biztonságos Yahoo! JP találatok*).

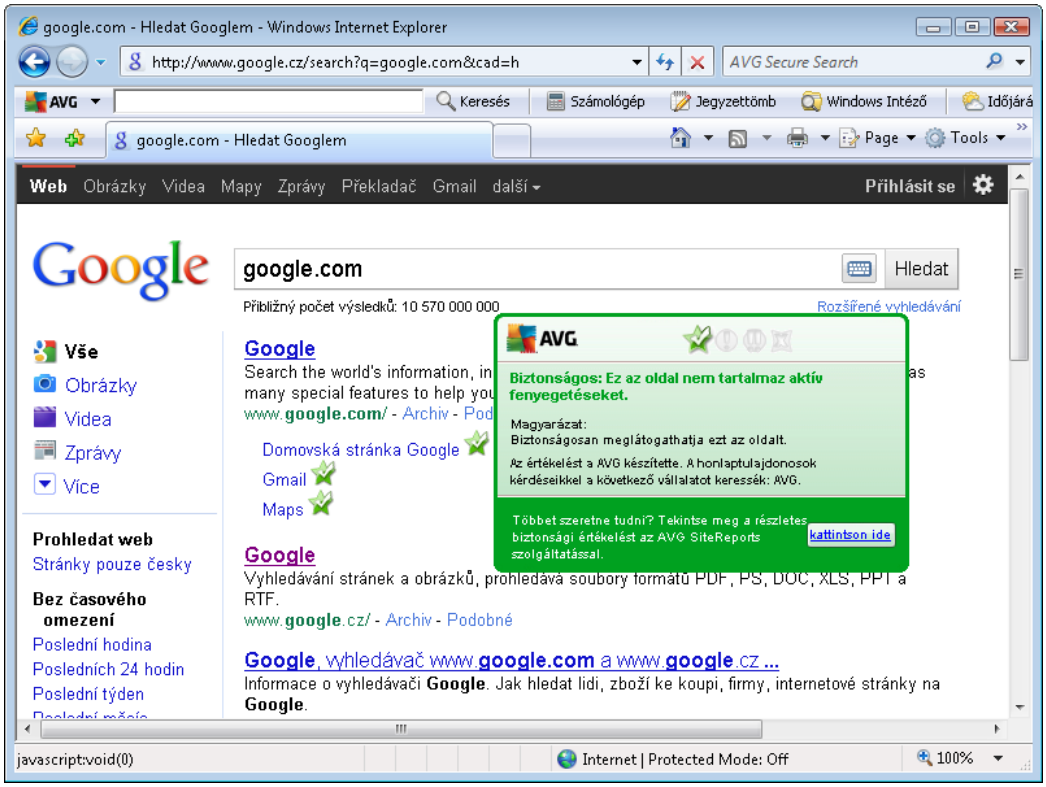
 A linkelt oldal nem tartalmaz fenyegetést, de gyanús (*kérdéses eredet vagy cél, ezért nem javasoljuk például internetes vásárlásokhoz).*).

 Maga a linkelt oldal biztonságos lehet, de hivatkozásokat tartalmaz határozottan veszélyes oldalakra; vagy gyanús kódot használ, bár közvetlen fenyegetést nem jelent.

 A linkelt oldal aktív fenyegetést jelent! Saját biztonsága érdekében nem engedélyezett az oldal meglátogatása.

 A linkelt oldal nem elérhető, ezért nem lehet ellenőrizni.

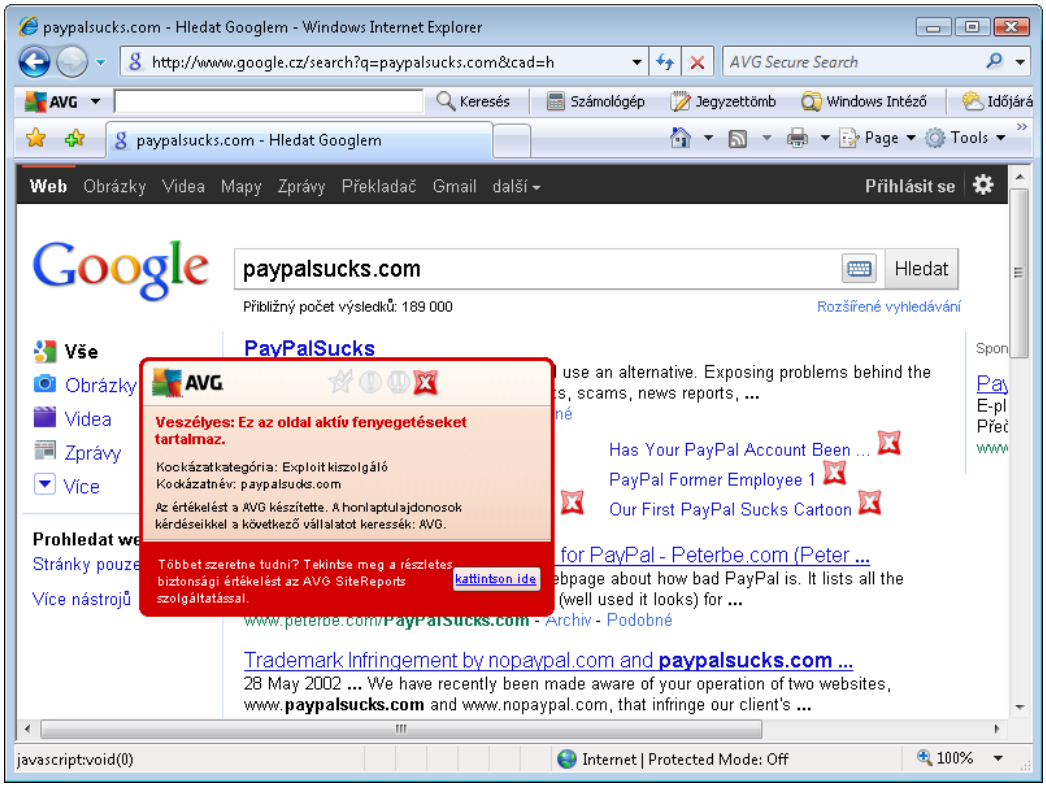
Ha ráviszi az egérmutatót egy adott információs ikonra, akkor részletek jelennek meg a kérdéses hivatkozással kapcsolatban. A fenyegetésről további részletek is rendelkezésre állnak (*ha vannak*):



6.2.3. Böngészés védelem észlelései

Ez a hatékony védelem blokkolni fogja bármilyen megnyitandó káros weboldal tartalmát, és megelőzi, hogy azok letöltődjenek a számítógépre. Ha egy veszélyes weboldalra mutató hivatkozásra kattint vagy annak címét írja be, akkor a program automatikusan letiltja az oldal megnyitását, és ezáltal megvédi Önt a véletlen megfertőződéstől. Fontos, hogy ne felejtse el, hogy a káros weboldalak már azzal megfertőzhetik a számítógépet, ha egyszerűen csak felkeresi azokat, ezért ha olyan veszélyes weboldalt látogatna meg, amely biztonsági réseket próbál kihasználni, vagy egyéb komoly fenyegetést tartalmaz, akkor a LinkScanner nem engedélyezi annak megjelenítését a böngészőben.

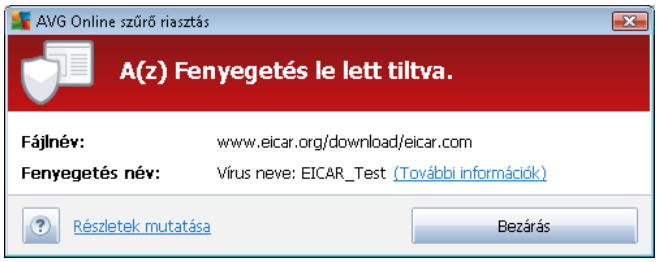
Ha káros weboldalt látogat meg, akkor a LinkScanner egy ehhez hasonló figyelmeztetést jelenít meg a böngészőben:



Az ilyen weboldalakra belépni rendkívül kockázatos és nem javasolt.

6.2.4. Online szűrő észlelései

Az Online szűrő ellenőrzi a meglátogatandó weboldalakat (és az esetlegesen beágyazott dokumentumokat), mielőtt azok megjelennének a webböngészőben vagy letöltődnének a számítógépre. Ha fenyegetést észlel, akkor azonnal riaszt a következő ablakkal:

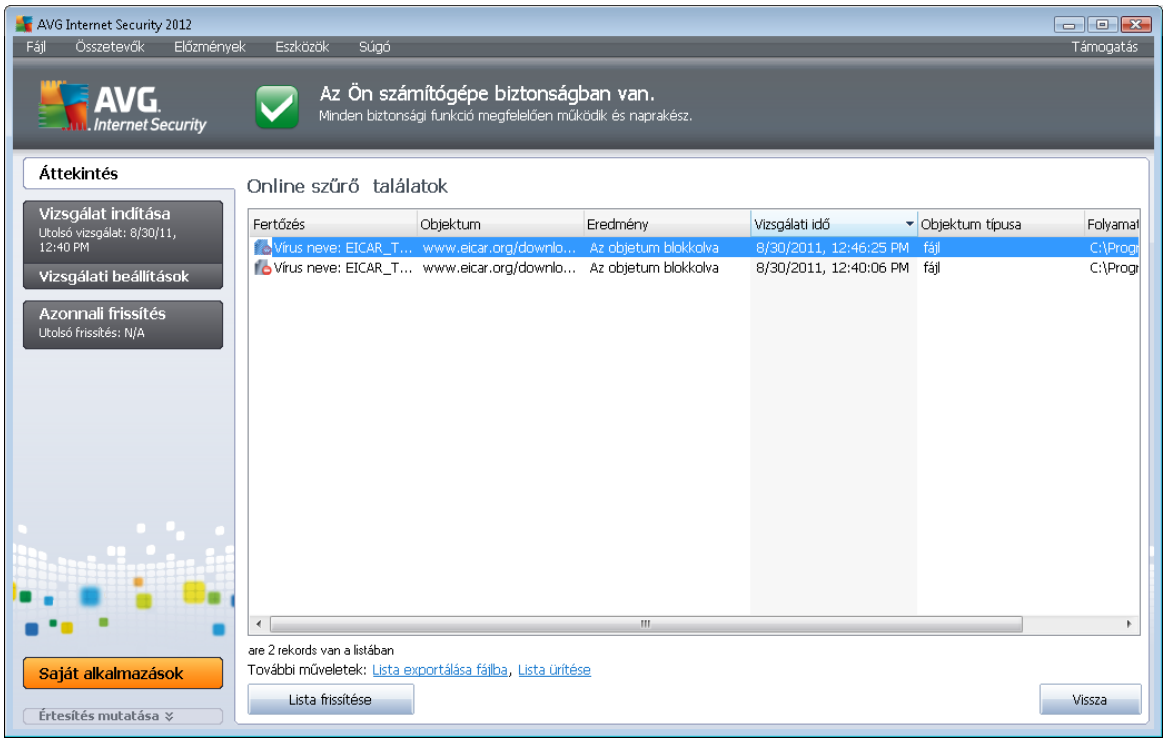


Ezen a panelen adatokat találhat azokról fájlokról, amelyeket fertőzöttnek minősített a program (*Fájlnév*), továbbá itt jelenik meg a fertőzés neve (*Fenyegetés neve*), illetve egy, a Vírusenciklopédia adatbázisra mutató hivatkozás, ahol részletes adatokat talál a fertőzésről (*ha van ilyen*). A párbeszédpanel a következő gombokat tartalmazza:

- ***Részletek megjelenítése*** - kattintson a ***Részletek megjelenítése*** gombra egy új felbukkanó ablak megnyitásához, ahol információkat találhat a fertőzés észlelésekor futó folyamatról, illetve a folyamat azonosításáról.

- ***Bezár*** - kattintson erre a gombra a panel bezárásához.

A gyanús oldal nem lesz megnyitva, és a program a fenyegetést naplózza az ***Online szűrő találatokban*** - az észlelt fenyegetések áttekintése a rendszermenü Előzmények / Online szűrő találatok részen érhető el.



Minden észlelt objektumnál a következő információk állnak rendelkezésre:

- ***Fertőzés*** - az észlelt objektum leírása (*neve*)
- ***Objektum*** - az objektum forrása (*weboldal*)
- ***Eredmény*** - az észlelt objektumon végzett művelet
- ***Észlelési idő*** - azon dátum és időpont, amikor a program észlelte és letiltota a fenyegetést
- ***Objektum típusa*** - az észlelt objektum típusa
- ***Folyamat*** - milyen művelet váltotta ki a potenciálisan veszélyes objektum megjelenését illetve észlelését

A panel alsó részén, a lista alatt, információkat találhat az észlelt objektumok összes számával kapcsolatban. Exportálhatja az észlelt elemek teljes listáját egy fájlba (***Lista exportálása fájlba***), és törölheti az elemek összes bejegyzését is (***Lista törlése***).

Vezérlőgombok

- ***Lista frissítése*** – frissíti az ***Online szűrő***

- ***Vissza*** – visszatérés az alapértelmezett AVG fő párbeszédpanelre *(összetevők áttekintése)*

6.3. E-mail védelem

A leggyakoribb vírusok és trójaiak emailen keresztül terjednek. Az adathalászat és a levélszemét egyre nagyobb kockázatot jelent. Az ingyenes email postafiókokra nagyobb valószínűséggel érkezik kártékony email (*mivel azok ritkán használnak levélszemétszűrő technológiát*), és az otthoni felhasználók gyakran megbíznak az ilyen emailekben. Az otthoni felhasználók ismeretlen weboldalakat böngésznek, és online adatlapokat töltenek ki személyes adataikkal (*pl. email cím*). Ez szintén növeli az emailen keresztül történő támadás veszélyét. A vállalatok gyakran céges emaileket használnak, és például levélszemétszűrőt alkalmaznak a kockázat csökkentéséhez.

Az ***E-mail védelem*** összetevő felelős az összes küldött vagy fogadott e-mail vizsgálatáért. Ha vírust észlel egy e-mailben, akkor azonnal áthelyezi azt a karanténba. Az összetevő képes kiszűrni bizonyos típusú e-mail mellékleteket, és tanúsítási szöveget fűz hozzá a vírusmentes üzenetekhez. ***Az E-mail védelem*** két fő funkcióval rendelkezik:

- E-mail vizsgáló

- Levélszemétszűrő

6.3.1. E-mail vizsgáló

A személyes e-mail vizsgáló összetevő automatikusan ellenőrzi a bejövő/kimenő üzeneteket. Használhatja olyan levelezőprogramokkal, amelyeknek nincsen saját bővítménye az AVG-ben (*de olyan programokkal is használhatja, amelyekhez az AVG külön bővítményt biztosít, pl. Microsoft Outlook vagy The Bat*). Elsősorban a következő levelezőprogramokkal használható: Outlook Express, Mozilla, Incredimail, stb.

Az AVG telepítése során a program automatikus kiszolgálókat állít be az e-mailek ellenőrzéséhez: egyet a bejövő e-mailek ellenőrzéséhez és egyet a kimenő e-mailek ellenőrzéséhez. Ezen két szerver használatával az e-mailek automatikusan ellenőrizve lesznek a 110-es és a 25-ös porton (*a bejövő/kimenő e-mailek szabványos portjai*).

Az E-mail vizsgáló közvetítő szerepet játszik az e-mail kliens és az e-mail szerverek között.

- ***Bejövő levél:*** Ha üzenet érkezik a szerverről, az ***E-mail vizsgáló*** összetevő ellenőrzi azt, eltávolítja a fertőzött mellékleteket, és tanúsítványt ad hozzá. Az észlelésük után a program a vírusokat azonnal a karanténba helyezi. Az üzenetet ezután átadja a levelezőprogramnak.

- ***Kimenő levél:*** Az üzenet a levelezőprogramból az E-mail vizsgálóhoz kerül, amely ellenőrzi azt, majd továbbküldi az üzenetet az SMTP kiszolgálóra (*a kimenő e-mailek vizsgálata alapértelmezés szerint le van tiltva, ezt külön kapcsolhatja be*).

Az E-mail vizsgáló használata nem javasolt kiszolgálóplatformokon.

6.3.2. Levélszemétszűrő

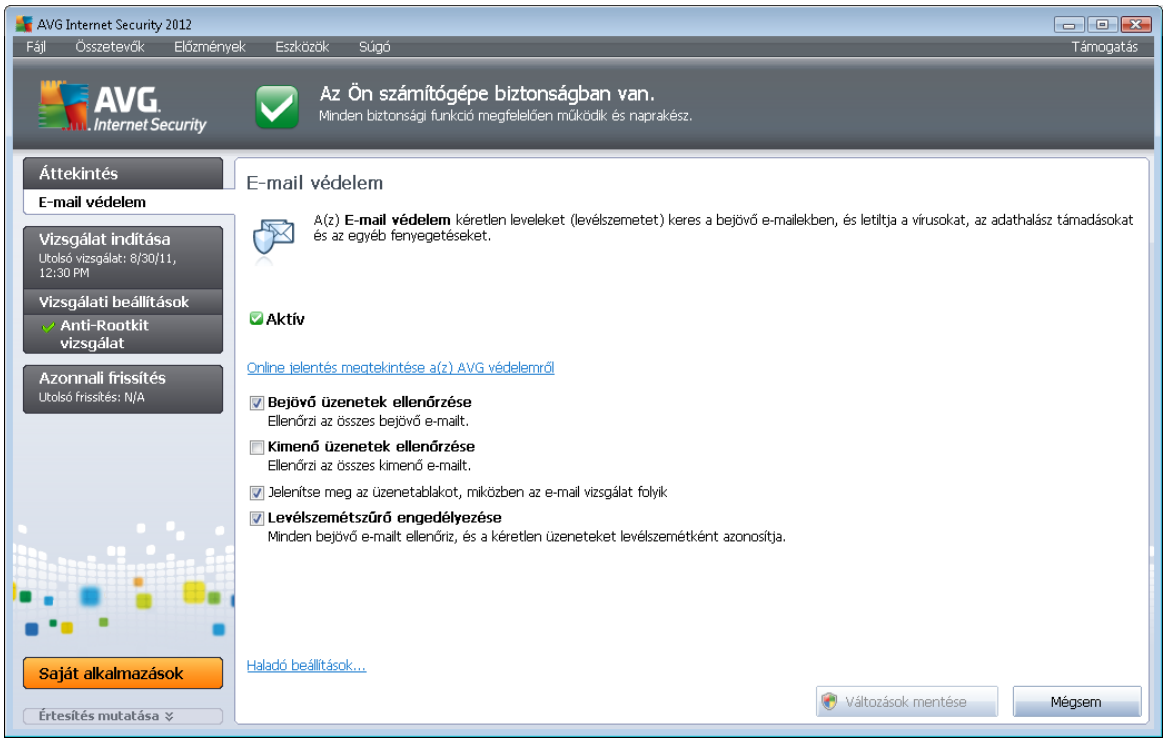
Hogyan működik a Levélszemétszűrő?

A Levélszemétszűrő minden bejövő e-mailt ellenőriz, és a kéretlen üzeneteket levélszemétként azonosítja. ***A Levélszemétszűrő*** módosítani tudja az (*előtte levélszemétként azonosított*) e-mailek tárgyát úgy, hogy egy különleges szöveges karakterláncot fűz hozzá. Ezután könnyen szűrheti e-mailjeit a levelezőprogramban. ***A Levélszemétszűrő*** összetevő többféle elemzési módszerrel dolgozza fel az egyes e-maileket, így maximális védelmet nyújt a kéretlen üzenetek ellen. ***A Levélszemétszűrő*** rendszeresen frissített adatbázist használ a levélszemét észleléséhez. Használhat RBL-kiszolgálót (*ismert levélszemétküldők e-mail címeinek nyilvános adatbázisa*), és manuálisan is hozzáadhatja az e-mail címeket az Engedélyezettek listájához (*soha nem levélszemét*) és a Feketelistához (*mindig levélszemét*).

Mi az a levélszemét?

A levélszemét általában azokat a kéretlen leveleket jelenti, melyek valamilyen terméket vagy szolgáltatást reklámoznak. Ezeket nagy tömegben, egyszerre sok e-mail címre küldik el, megtöltve ezzel a' postaládákat. A levélszemét nem vonatkozik a jogszerűen küldött kereskedelmi e-mailekre, amelyeket a felhasználó beleegyezésével küldenek. A levélszemét nem csak bosszantó, de gyakran átverések, vírusok és káros tartalmak forrása.

6.3.3. E-mail védelem felület



Az ***E-mail védelem*** párbeszédpanelen egy rövid szöveget talál, amely az összetevő funkcióját írja

le, valamint a jelenlegi állapotára vonatkozó információkat ad meg *(Aktív).* Az ***AVG általi védelméről készült online jelentés megtekintése*** hivatkozás segítségével az **AVG Internet Security 2012** termék tevékenységeinek és észleléseinek részletes statisztikáit tekintheti meg az AVG webhely erre szolgáló oldalán (http://www.avg.hu/).

Alapvető E-mail védelmi beállítások

Az ***E-mail védelem*** párbeszédpanelen szerkesztheti az összetevő működésének néhány alapvető tulajdonságát:

- ***Bejövő üzenetek ellenőrzése*** *(alapértelmezett állapotban bekapcsolva)* – Jelölje be ezt az elemet annak megadásához, hogy az e-mail fiókba érkező összes üzenetet ellenőrizze a program.
- ***Kimenő üzenetek ellenőrzése*** *(alapértelmezett állapotban kikapcsolva)* – Jelölje be ezt az elemet a postafiókból elküldött összes e-mail vírusmentességének vizsgálatához.
- ***Jelenítse meg az üzenetablakot, miközben az e-mail vizsgálat folyik*** *(alapértelmezett állapotban bekapcsolva)* – Jelölje be ezt az elemet, ha azt szeretné, hogy megjelenjen egy párbeszédpanel az AVG ikon felett a rendszertálcán az e-mailek vizsgálata közben.
- ***Levélszemétszűrő*** *engedélyezése (alapértelmezett állapotban bekapcsolva)* – Jelölje be ezt az elemet, ha a bejövő e-mail üzeneteit szűrni szeretné, hogy ne kapjon kéretlen e-maileket.

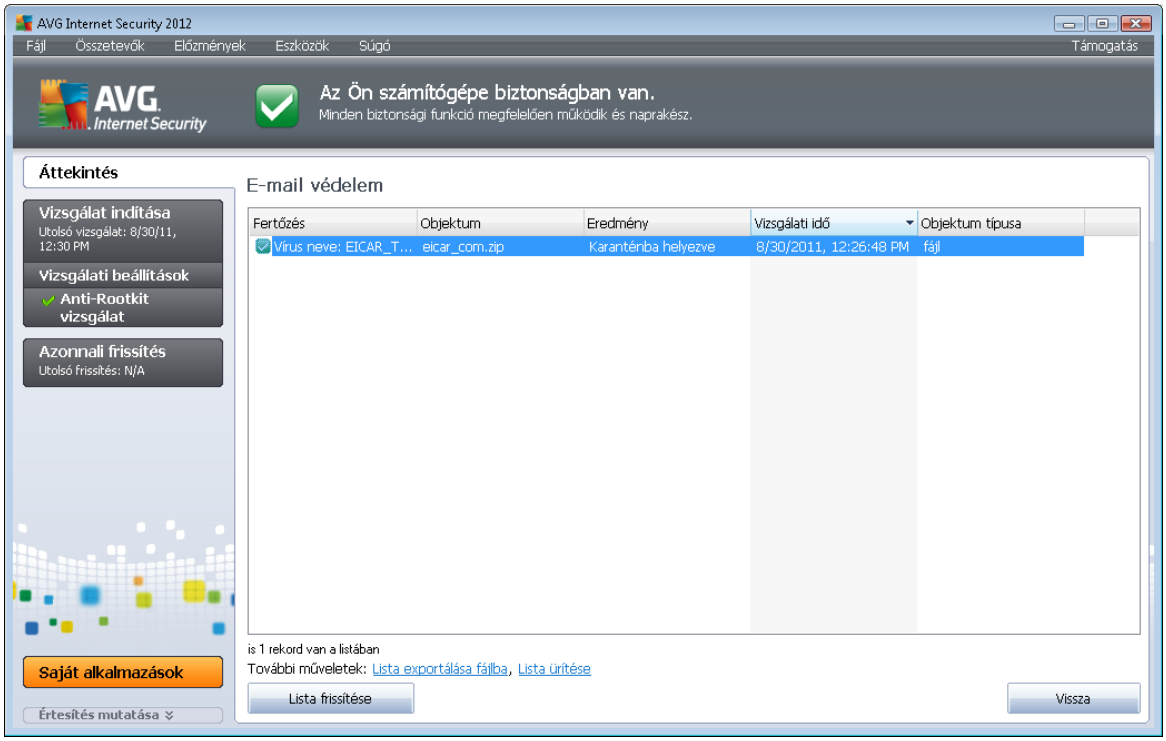
A szoftver gyártója minden AVG összetevőt az optimális teljesítmény elérésére állított be. Ne változtassa meg az AVG beállításokat, hacsak nem feltétlenül szükséges. Bármely változtatást gyakorlott felhasználónak kell végeznie. Ha meg kell változtatnia az AVG beállításait, akkor válassza az Eszközök/Haladó beállítások menüt, majd módosítsa az elemeket a megnyíló Haladó AVG beállítások ablakban.

Vezérlőgombok

Az ***E-mail védelem*** párbeszédpanel vezérlőgombjai a következők:

- ***Változások mentése*** – nyomja meg ezt a gombot a változtatások mentéséhez és alkalmazásához
- ***Mégse*** – nyomja meg ezt a gombot, ha az alapértelmezett AVG főablakhoz szeretne visszatérni (*összetevők áttekintése*)

6.3.4. Az E-mail védelem észlelései



Az ***E-mail vizsgáló észlelés*** párbeszédpanelen (*ez a rendszermenü Előzmények / E-mail vizsgáló észlelés menüpontját választva érhető el*) az E-mail védelem összetevő által rögzített összes észlelés megtekinthető. Minden észlelt objektumnál a következő információk állnak rendelkezésre:

- ***Fertőzés*** - az észlelt objektum leírása (neve)
- ***Objektum*** - az objektum helye
- ***Eredmény*** - az észlelt objektumon végzett művelet
- ***Észlelési idő*** - megmutatja a gyanús objektum azonosításának dátumát és idejét
- ***Objektum típusa*** - az észlelt objektum típusa

A panel alsó részén, a lista alatt, információkat találhat az észlelt objektumok összes számával kapcsolatban. Exportálhatja az észlelt elemek teljes listáját egy fájlba (***Lista exportálása fájlba***), és törölheti az elemek összes bejegyzését is (***Lista törlése***).

Vezérlőgombok

A vezérlőgombok az ***E-mail vizsgáló*** felületen a következők:

- ***Lista frissítése*** – Frissíti az észlelt fenyegetések listáját.

- ***Vissza*** – Visszalépés az előző párbeszédpanelre.

6.4. Tűzfal

A tűzfal olyan rendszer, amely a hálózati adatforgalom blokkolásával, illetve engedélyezésével érvényt szerez a beállított hozzáférés-vezérlési házirendeknek. A ***tűzfal*** szabályokat tartalmaz, amelyek védik a belső hálózatot a kívülről *(jellemzően az internetről)* érkező támadásokkal szemben, ezenkívül a tűzfal minden egyes hálózati porton figyeli a kommunikációt. Miután a tűzfal összevetette a kommunikációt a megadott szabályokkal, vagy engedélyezi, vagy blokkolja azt. Ha a ***tűzfal*** behatolási kísérletet észlel, akkor „blokkolja" azt, és nem engedi meg a behatolónak, hogy hozzáférjen a számítógéphez.

A ***tűzfal*** úgy van konfigurálva, hogy engedélyezze vagy tiltsa a belső/külső kommunikációt (mindkét irányban) a megadott portokon és alkalmazásoknál. Például a tűzfalat be lehet úgy állítani, hogy a bejövő és kimenő adatokat csak a Microsoft Explorer-ben engedélyezze. Ilyenkor más webböngészőkben az adatforgalom nem engedélyezett.

A ***tűzfal*** megakadályozza, hogy személyes adatai az Ön engedélye nélkül hagyják el a számítógépet. A tűzfal azt is szabályozza, hogy a számítógép hogyan bonyolítsa le az adatcserét a helyi hálózaton vagy az interneten található más számítógépekkel. Egy szervezeten belül az egyes számítógépekre telepített ***tűzfal*** a szervezeten belül dolgozók által indított támadásokkal szemben is megvédi a számítógépeket.

Azok a számítógépek, amelyeket nem védenek tűzfallal, könnyen áldozatul eshetnek a hackerek és adattolvajok támadásainak.

Javaslat: *Általában nem ajánlott, hogy egynél több tűzfalat telepítsen a számítógépre. A számítógép biztonsága nem garantált, ha több tűzfalat használ egyszerre. Ugyanis elképzelhető, hogy a két alkalmazás ütközik egymással. Javasoljuk, hogy a számítógépen csak egyetlen tűzfalat használjon, és kapcsolja ki a többit, így csökkentheti egy esetleges szoftverütközés vagy abból adódó probléma kockázatát.*

6.4.1. Tűzfal alapelvek

Az **AVG Internet Security 2012** ***Tűzfal*** összetevője vezérli a számítógép egyes hálózati portjain keresztülhaladó összes adatforgalmat. A ***Tűzfal*** a megadott szabályok alapján elemzi azokat az alkalmazásokat, amelyek a számítógépen futnak *(és amelyek csatlakozni szeretnének az internethez vagy a helyi hálózathoz)*, továbbá azokat, amelyek kívülről próbálnak csatlakozni a számítógéphez. A ***Tűzfal*** ezután engedélyezi vagy megtiltja az egyes alkalmazásoknak a kommunikációt a hálózati portokon. Alapértelmezés szerint, ha az alkalmazás ismeretlen *(vagyis nem rendelkezik meghatározott Tűzfal szabállyal)*, akkor a ***Tűzfal*** rákérdez, hogy engedélyezze vagy letiltsa a kommunikációs próbálkozást.

Az AVG tűzfalának használata kiszolgálóplatformokon nem javasolt.

Mi a feladata az AVG tűzfalnak:

- Ismert alkalmazások kommunikációs próbálkozásainak automatikus engedélyezése vagy tiltása, illetve megerősítés kérése

- Teljes profilok használata előre meghatározott szabályokkal az Ön igényei szerint
- Profilok váltása automatikusan különböző hálózatokra történő csatlakozáskor, illetve különböző hálózati adapterek használatakor

6.4.2. Tűzfal profilok

A Tűzfal lehetővé teszi, hogy meghatározzon bizonyos biztonsági szabályokat az alapján, hogy a számítógép egy tartományon belül helyezkedik el, különálló számítógép vagy notebook. E lehetőségek mindegyike más és más védelmi szintet kíván, és a szinteket a megfelelő profilok fedik le. Röviden a Tűzfal profil a Tűzfal összetevő egy bizonyos konfigurációja, ahol számos előre meghatározott beállítást használhat.

Elérhető profilok

- ***Mind engedélyezése*** -olyan Tűzfal rendszerprofil, melyet a gyártó előre beállított és mindig elérhető. Ha ez a profil aktiválva van, akkor minden hálózati kommunikáció engedélyezett, és nincs biztonsági szabály alkalmazva, hasonlóan mint ha a Tűzfal védelem ki lenne kapcsolva (minden alkalmazás engedélyezett, de az adatcsomagok továbbra is ellenőrizve lesznek – a szűrés teljes kikapcsolásához tiltsa le a Tűzfalat). Ezt a rendszerprofilt nem lehet másolni, törölni vagy a beállításait módosítani.
- ***Mind tiltása*** – olyan Tűzfal rendszerprofil, melyet a gyártó előre beállított és mindig elérhető. Ha ez a profil aktiválva van, akkor minden hálózati kommunikáció blokkolva lesz, a számítógép nem lesz elérhető külső hálózatok számára, és nem is tud kifelé kommunikálni. Ezt a rendszerprofilt nem lehet másolni, törölni vagy a beállításait módosítani.
- ***Egyéni profilok*** – az egyéni profilok lehetővé teszik, hogy kihasználja az automatikus profilváltás nyújtotta előnyöket, amely különösen akkor hasznos, ha gyakran csatlakozik különböző hálózatokra *(pl. notebook használata esetén).* Az egyéni profilok automatikusan létrejönnek az **AVG Internet Security 2012** telepítése után, és tartalmazzák a Tűzfal házirendekre vonatkozó egyedi követelményeket. A következő egyéni profilok állnak rendelkezése:
    - ***Közvetlen csatlakozás az internetre*** – külön védelemmel nem rendelkező általános, otthoni asztali számítógépekhez vagy notebookokhoz javasolt, amelyek közvetlenül csatlakoznak az internethez. Ez a beállítás ajánlott abban az esetben is, amikor notebook számítógépét különféle ismeretlen és valószínűleg nem biztonságos hálózatokhoz (*például internetkávézóban, hotelszobában stb.*) csatlakoztatja. A profil legszigorúbb tűzfal házirendje biztosítja az ilyen számítógépek megfelelő védelmét.
    - ***Tartományba rendelt számítógép*** – Helyi hálózaton lévő számítógépekhez, jellemzően iskolában vagy munkahelyen használható. A szabály feltételezi, hogy a hálózatot professzionálisan felügyelik és védik, így a biztonsági szint alacsonyabb lehet a fentebb említett esetéknél, így engedélyezheti a hozzáférést a megosztott mappákhoz, lemezmeghajtókhoz stb.
    - ***Kisebb otthoni vagy irodai hálózat*** – Kis méretű hálózaton lévő számítógépekhez,

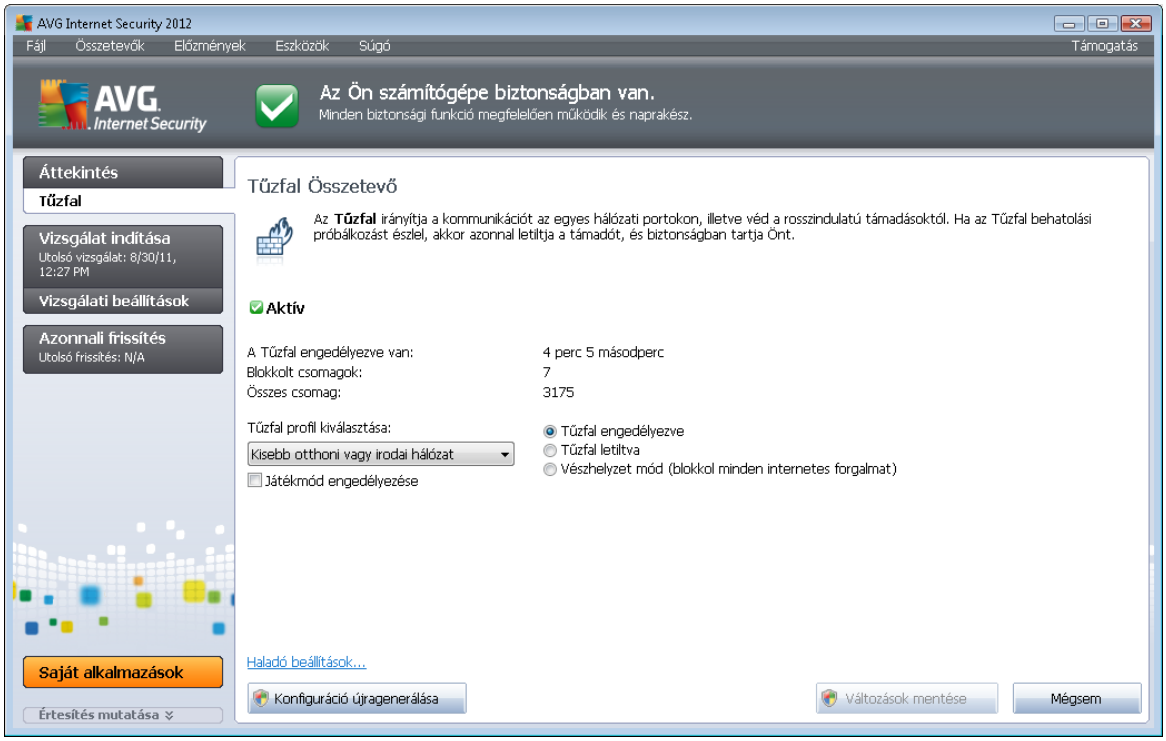
jellemzően otthon vagy kisvállalkozások irodáiban használható. Jellemzően az ilyen hálózatok nem rendelkeznek „központi” rendszergazdával, mindössze néhány csatlakoztatott számítógépet tartalmaznak, illetve gyakran megosztják a nyomtatókat, lapolvasókat és más hasonló eszközöket, és a tűzfal szabálynak ennek megfelelően kell működnie.

Profilváltás

A Profilváltás funkció lehetővé teszi a Tűzfal számára, hogy automatikusan váltson az adott profilra egy bizonyos hálózati adapter használatakor vagy egy bizonyos típusú hálózatra történő kapcsolódáskor. Ha nincs profil hozzárendelve a hálózati területhez, akkor a következő kapcsolódáskor a Tűzfal egy párbeszédpanelen megkérdezi, hogy kíván-e hozzárendelni egy profilt. Profilokat rendelhet hozzá minden helyi hálózati csatolóhoz vagy területhez, és meghatározhat beállításokat a Környezet- és adapterprofilok panelen, ahol le is tilthatja az adott funkciót, ha nincs rá szüksége (*ekkor minden kapcsolatnál az alapértelmezett profilt használja a tűzfal*).

Különösen a notebook-ot és különböző típusú hálózatokat használók fogják hasznosnak találni ezt a funkciót. Ha asztali számítógéppel rendelkezik, és csak egyféle típusú kapcsolatot használ (*pl. kábelen keresztül csatlakozik az internetre*), akkor nem kell foglalkoznia a profilváltással, mivel valószínűleg soha nem fogja azt kihasználni.

6.4.3. Tűzfal felület



A fő, ***Tűzfal összetevő*** nevű párbeszédpanel alapvető információt nyújt az összetevő funkcióiról, állapotáról *(Aktív)* és egy rövid áttekintést az összetevő statisztikájáról:

- ***A Tűzfal működik ... óta*** – A Tűzfal utolsó indítása óta eltelt idő
- ***Blokkolt csomagok*** – Az összes ellenőrzött adatcsomagból blokkolt csomagok száma
- ***Összes csomag*** – A Tűzfal futása során ellenőrzött összes adatcsomag száma

Alap tűzfalbeállítások

- ***Tűzfal profil kiválasztása*** – A legördülő menüből válasszon ki egyet a meghatározott profilokból (*az egyes profilok részletes leírását és azok javasolt használatának bemutatását a Tűzfal profilok című fejezetben találja*)
- ***Játékmód engedélyezése*** – Jelölje be ezt a lehetőséget annak biztosításához, hogy ha teljes képernyős alkalmazásokat (*játékokat, prezentációkat, filmeket stb.*) futtat, akkor a Tűzfal nem kérdez rá arra, hogy Ön engedélyezi-e vagy letiltja az ismeretlen alkalmazások kommunikációját. Ha egy ismeretlen alkalmazás megpróbál kommunikálni a hálózaton, a Tűzfal automatikusan engedélyezi vagy letiltja a kommunikációt az aktuális profilbeállításoknak megfelelően. ***Megjegyzés:*** Ha a Játék mód be van kapcsolva, akkor a rendszer az összes ütemezett feladatot (vizsgálatot, frissítést) elhalasztja az alkalmazás bezárásáig.
- Továbbá ebben az alapvető beállítások megadására szolgáló részben három alternatív lehetőség közül is választhat a Tűzfal összetevő aktuális állapotának meghatározásához:
  - ***Tűzfal engedélyezve*** *(alapértelmezett állapot)* – Válassza ezt a lehetőséget azon alkalmazások kommunikációjának engedélyezéséhez, amelyek „engedélyezett” minősítést kaptak a kiválasztott Tűzfal profilban definiált szabálykészletben.
  - ***Tűzfal letiltva*** – Ez a lehetőség teljesen kikapcsolja a tűzfalat , és a rendszer minden hálózati forgalmat ellenőrzés nélkül engedélyez.
  - ***Vészhelyzet mód (blokkol minden internetes adatforgalmat)*** – Válassza ezt a lehetőséget, ha minden adatforgalmat le kíván tiltani minden porton. A Tűzfal ekkor továbbra is működik, de minden adatforgalom megszakad.

Megjegyzés: *A szoftver szállítója beállította az összes AVG Internet Security 2012 összetevőt, hogy azok optimális teljesítményt nyújtsanak. Ne változtassa meg az AVG beállításokat, hacsak nem feltétlenül szükséges. Bármely változtatást hozzáértő felhasználónak kell végeznie. Ha meg kell változtatnia a Tűzfal beállításait, akkor válassza az* ***Eszközök / Tűzfal beállítások*** *menüt, majd módosítsa az opciókat a megnyíló Tűzfal beállítások ablakban.*

Vezérlőgombok

- ***Konfiguráció újragenerálása*** - nyomja meg ezt a gombot az aktuális Tűzfal konfiguráció felülírásához, illetve az alapállapotra történő visszaállításhoz az automatikus észlelés szerint.
- ***Változások mentése*** – Kattintson erre a gombra a mentéshez és a változtatások

alkalmazásához.

- ***Mégse*** – Kattintson erre a gombra, ha az alapértelmezett AVG párbeszédpanelre szeretne visszatérni (*összetevők áttekintése*).

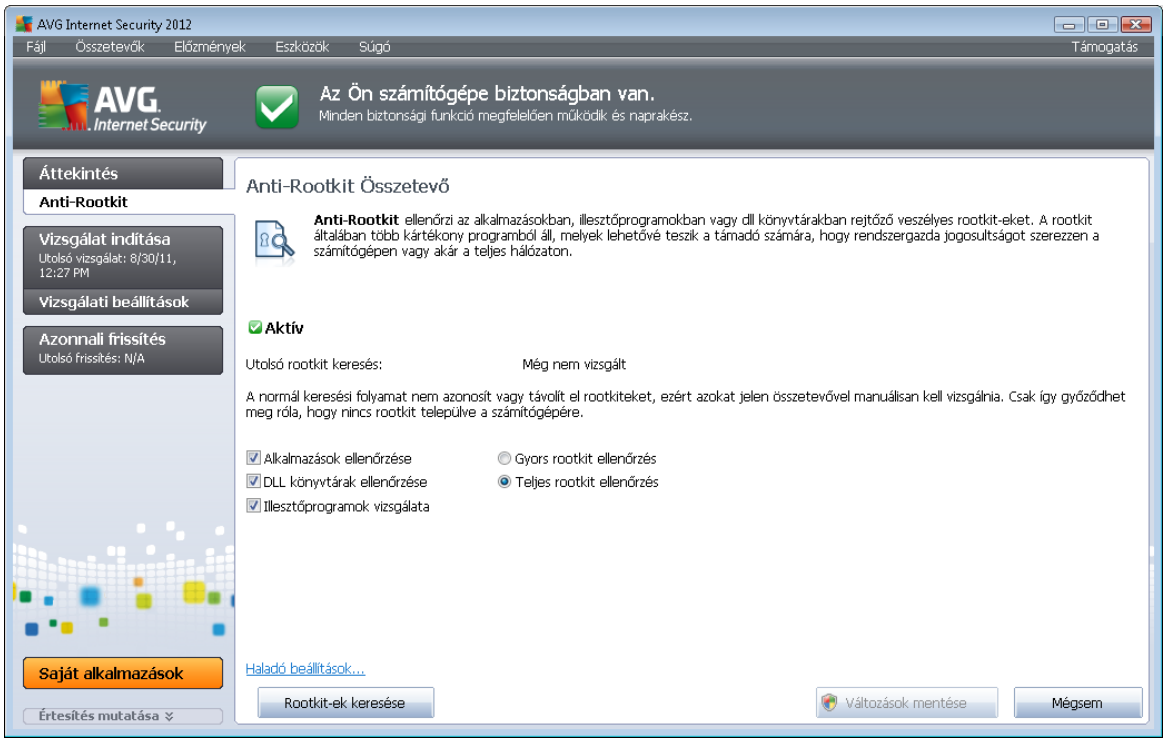
6.5. Anti-Rootkit

Az Anti-Rootkit egy speciális eszköz, amely felismeri és hatékonyan eltávolítja a veszélyes rootkiteket, azaz az olyan programokat és technológiákat, amelyek rosszindulatú szoftverek jelenlétét leplezhetik a számítógépen. ***Az Anti-Rootkit*** előre meghatározott szabályok alapján képes észlelni a rootkiteket. Vegye figyelembe, hogy a program az összes rootkitet észleli *(nem csak a fertőzötteket)*. Ha az ***Anti-Rootkit*** rootkitet talál, akkor az nem feltétlenül jelenti azt, hogy az adott rootkit veszélyes. Bizonyos esetekben a rootkitek illesztőprogramok vagy legitim alkalmazások részei.

Mi az a rootkit?

A rootkit olyan program, amelyet arra terveztek, hogy átvegye az irányítást a számítógép felett annak tulajdonosának vagy jogos használójának hozzájárulása nélkül. Hardverhez való hozzáférés ritkán szükséges, mivel a rootkit az azon futó operációs rendszer feletti irányítást veszi át. A rootkitek jellemzően leplezik jelenlétüket a rendszeren az operációs rendszer normál biztonsági mechanizmusának kijátszásával vagy megkerülésével. Gyakran egyúttal trójaiak is, és elhitetik a felhasználóval, hogy biztonságosan futtathatók a számítógépen. Az ehhez használt módszerek a következők lehetnek: futó folyamatok elrejtése a figyelőprogramoktól, fájlok vagy rendszeradatok elrejtése az operációs rendszeren.

6.5.1. Anti-Rootkit felület



Az ***Anti-Rootkit*** párbeszédablak rövid leírást tartalmaz az összetevő működéséről, tájékoztat az összetevő aktuális állapotáról *(Aktív)*, illetve megjeleníti az ***Anti-Rootkit*** vizsgálat futtatásának legutóbbi időpontját (***Legutóbbi rootkit keresés***). Az ***Anti-Rootkit*** párbeszédpanel tartalmazza az Eszközök/Haladó beállítások linket. Használja ezt a hivatkozást az ***Anti-Rootkit*** összetevő haladó beállításainak eléréséhez.

A szoftver gyártója minden AVG összetevőt az optimális teljesítmény elérésére állított be. Ne változtassa meg az AVG beállításokat, hacsak nem feltétlenül szükséges. Bármely változtatást gyakorlott felhasználónak kell végeznie.

Alapvető Anti-Rootkit beállítások

A párbeszédpanel alsó részén megadhatja a rootkitek keresésének néhány alapvető beállítását. Először is jelölje be, hogy mely objektumokat kell ellenőrizni:

- ***Alkalmazások ellenőrzése***
- ***DLL könyvtárak ellenőrzése***
- ***Illesztőprogramok keresése***

Ezután kiválaszthatja a rootkit vizsgálati módot:

- ***Gyors rootkit vizsgálat*** – Az összes futó folyamatot, a betöltött illesztőprogramokat és a rendszermappát (*általában c:\Windows*) ellenőrzi.
- ***Teljes rootkit vizsgálat*** – Az összes futó folyamatot, a betöltött illesztőprogramokat, a rendszermappát (*általában c:\Windows*), valamint az összes helyi lemezt (*a flash memóriákat is, de a floppy-/CD-meghajtókat nem*) ellenőrzi.

Vezérlőgombok

- ***Rootkitek keresése*** – Mivel a rootkitek vizsgálata nem része A teljes számítógép vizsgálata funkciónak, ezért azt az ***Anti-Rootkit*** felületről indíthatja ezzel a gombbal.
- ***Változások mentése*** – Kattintson erre a gombra az összes változás mentéséhez, és az alapértelmezett AVG fő párbeszédpanelre (*összetevők áttekintése*) történő visszatéréshez.
- ***Mégse*** – Kattintson erre a gombra, ha a végzett módosítások mentése nélkül az alapértelmezett AVG fő párbeszédpanelre szeretne visszatérni (*összetevők áttekintése*).

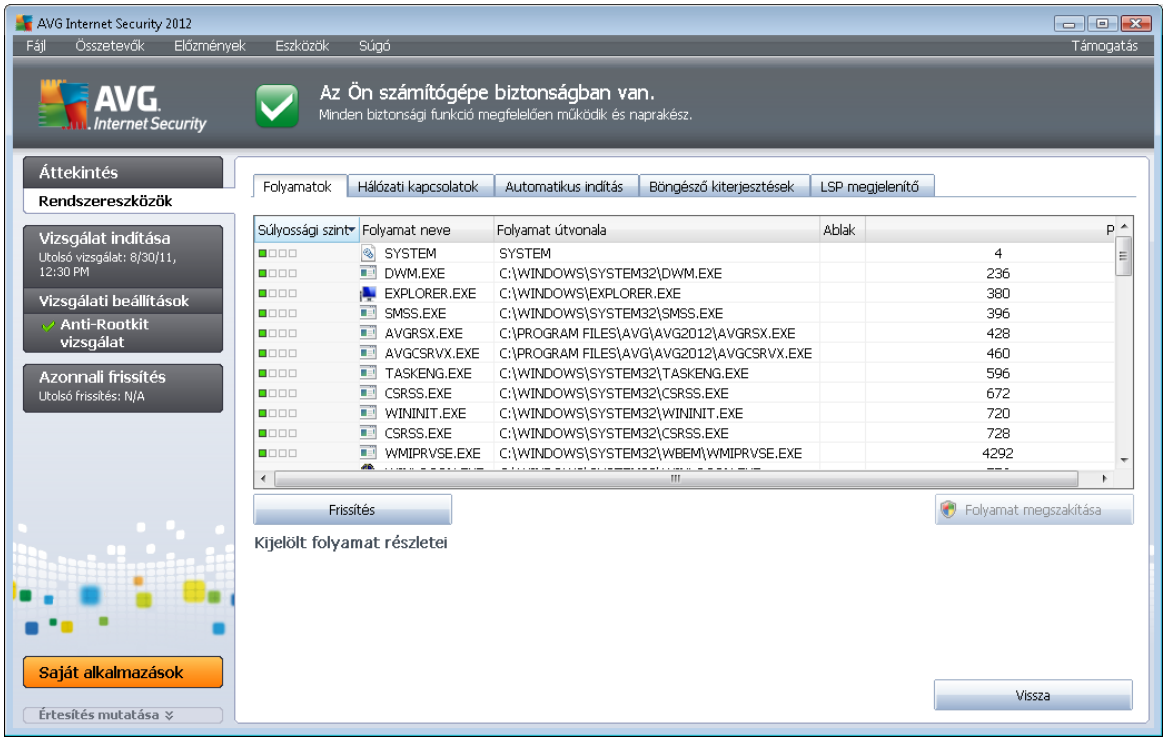
6.6. Rendszereszközök

A Rendszereszközök rész a **AVG Internet Security 2012** környezet és az operációs rendszer részletes összefoglaló információit jeleníti meg. Az összetevő a következő elemek áttekintését jeleníti meg:

- Folyamatok - a számítógépen jelenleg aktív (*pl. futó alkalmazások*) folyamatok listája
- Hálózati kapcsolatok - a jelenleg aktív kapcsolatok listája
- Automatikus indítás - a Windows rendszer indításakor automatikusan elinduló alkalmazások listája
- Böngészőkiterjesztések - az internetböngészőben telepített bővítmények (*pl. alkalmazások*)
- LSP böngésző - réteges szolgáltató (*LSP*listája)

Bizonyos részleteket szerkeszteni is lehet, de ezt csak gyakorlott felhasználóknak javasoljuk!

6.6.1. Folyamatok



A ***Folyamatok*** panel a számítógépen jelenleg aktív folyamatokat listázza (*azaz. futó alkalmazások*). A lista több oszlopból áll:

- ***Súlyossági szint*** -)az adott folyamat kockázati szintjének grafikus értékelése egy négyszintű skálán a legkevésbé fontosabbtól (■□□□)a legfontosabbikig (■■■■)
- ***Folyamat neve*** - az aktív folyamat nevét jelzi
- ***Folyamat elérési útvonala*** - az aktív folyamat tényleges elérési útját jelzi
- ***Ablak*** - az alkalmazásablak nevét jelzi, ha van ilyen

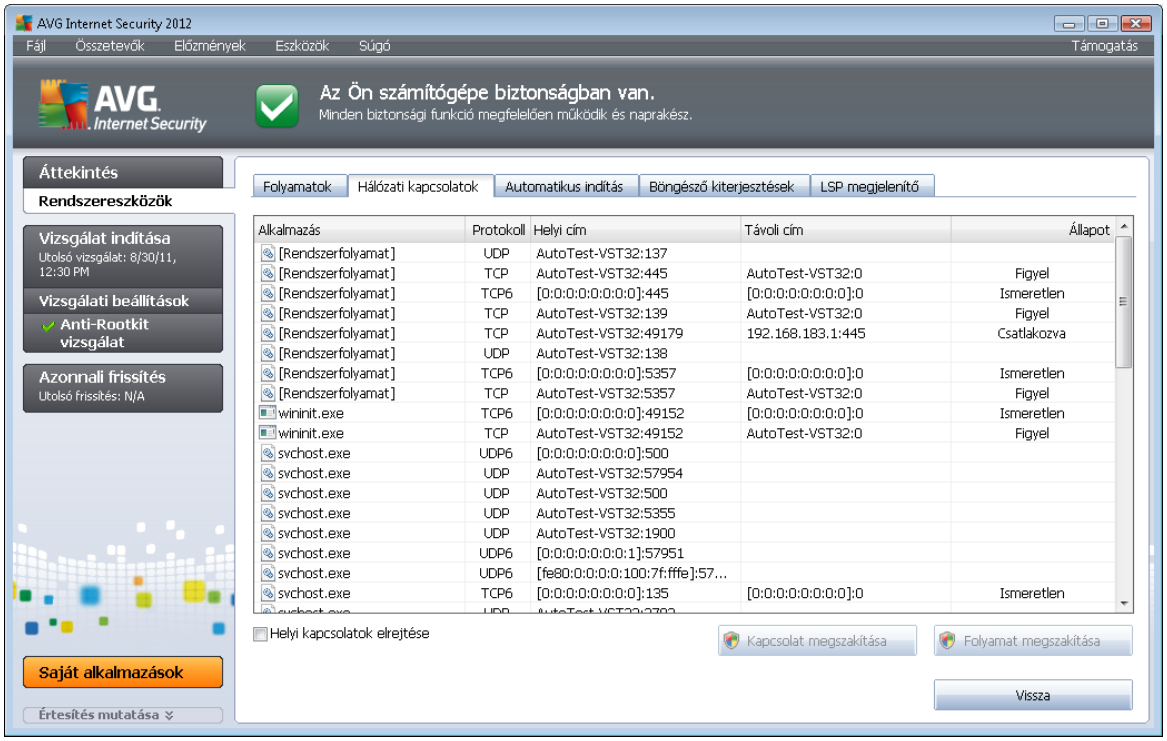
- ***PID*** - a folyamatazonosító szám a Windows rendszerben használt belső folyamatazonosító, amely a folyamatok egyértelmű azonosítására szolgál

Vezérlőgombok

A ***Folyamatok*** lapon található vezérlőgombok a következők:

- ***Frissítés*** - frissíti a folyamatok listáját az aktuális állapotnak megfelelően
- ***Folyamat megszakítása*** - kiválaszthat egy vagy több alkalmazást, és leállíthatja azokat ezen gomb segítségével. ***Az alkalmazások leállítása csak akkor javasolt, ha meg van győződve róla, hogy azok valódi veszélyeket rejtenek!***
- ***Mégse*** – Ide kattintva az alapértelmezett AVG fő párbeszédpanelre (*összetevők áttekintése*) térhet vissza

6.6.2. Hálózati kapcsolatok



A ***Hálózati kapcsolatok*** panel a jelenleg aktív kapcsolatokat tartalmazza. A lista a következő oszlopokból áll:

- ***Alkalmazás*** - a kapcsolathoz tartozó alkalmazás neve (*a Windows 2000 kivételével, ahol ezen adat nem érhető el*)
- ***Protokoll*** - a kapcsolathoz használt átviteli protokoll típusa:

- TCP – az internet protokollal (IP) együtt használatos protokoll, amely az adatok interneten történő továbbítására szolgál
- UDP – a TCP protokoll egyik alternatívája

- ***Helyi cím*** - a helyi számítógép IP-címe és a használt port száma
- ***Távoli cím*** - a távoli számítógép IP-címe és a használt port száma. Ha lehetséges, a program a távoli számítógép nevét is megállapítja.
- ***Állapot*** - megmutatja a legvalószínűbb aktuális állapotot (*Csatlakoztatva, A kiszolgálónak kell bezárnia, Figyelés, Aktív bezárás vége, Passzív bezárás, Aktív bezárás*)

A csak külső kapcsolatok listázásához jelölje be a ***Helyi kapcsolatok elrejtése*** jelölőnégyzetet a párbeszédpanel alsó részén a lista alatt.

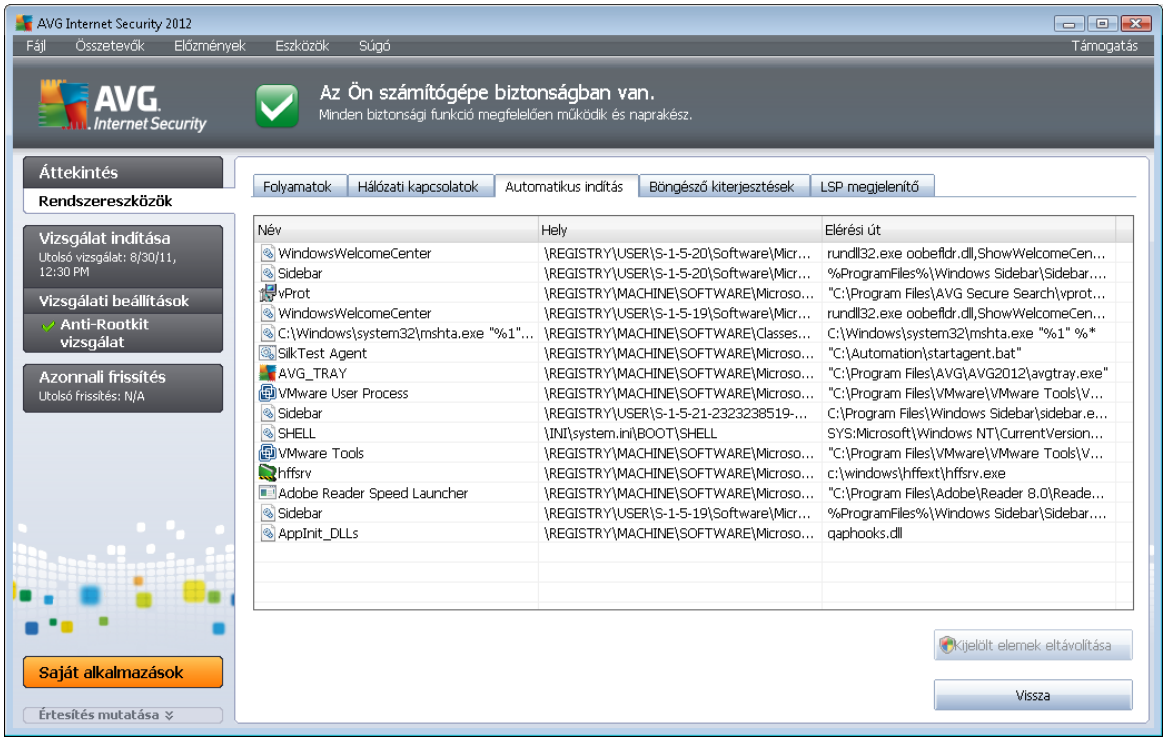
Vezérlőgombok

A ***Hálózati kapcsolatok*** lapon a következő vezérlőgombok érhetők el:

- ***Kapcsolat megszakítása*** - bezár egy vagy több kapcsolatot a listában
- ***Folyamat megszakítása*** - bezár egy vagy több kapcsolathoz tartozó alkalmazást a listában
- ***Vissza*** – Visszatérés az alapértelmezett AVG fő párbeszédpanelre (összetevők áttekintése).

Időnként lehetséges, hogy csak a csatlakoztatva állapotú alkalmazásokat lehet leállítani. A kapcsolatok leállítását csak akkor ajánljuk, ha meg van győződve róla, hogy azok valódi veszélyt rejtenek!

6.6.3. Automatikus indítás



Az ***Automatikus indítás*** panel megjeleníti az összes olyan alkalmazást, mely a Windows rendszer indításakor elindul. Rendkívül gyakran előfordul, hogy a káros programok automatikusan hozzáadják magukat a beállításjegyzékben található indítási bejegyzéshez.

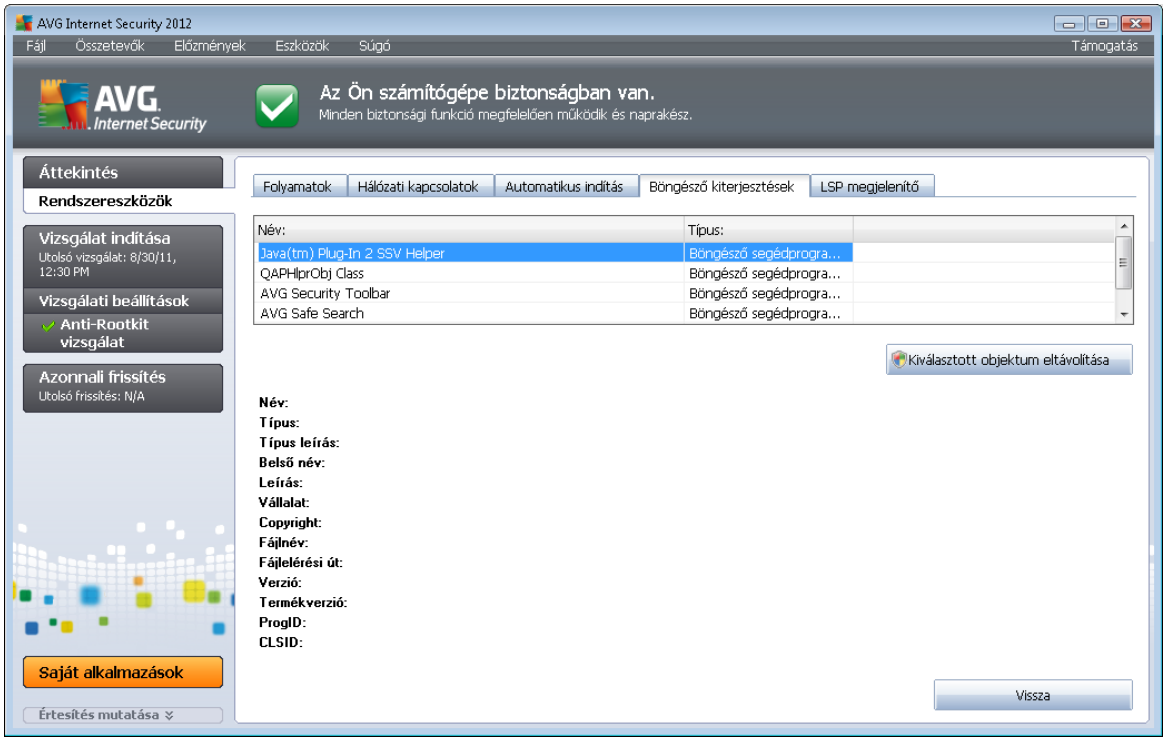
Vezérlőgombok

Az ***Automatikus indítás*** lapon a következő vezérlőgombok érhetők el:

- ***Kijelölt elemek eltávolítása*** – Kattintson erre a gombra az egy vagy több kijelölt bejegyzés törléséhez.
- ***Vissza*** – Visszatérés az alapértelmezett AVG fő párbeszédpanelre *(összetevők áttekintése).*

A listában szereplő alkalmazásokat csak akkor ajánlatos törölni, ha meg van győződve róla, hogy azok valódi veszélyeket rejtenek.

6.6.4. Böngésző kiterjesztések



A ***Böngésző kiterjesztések*** panel az internetböngészőben telepített bővítmények (*alkalmazások*) listáját jeleníti meg. A listában a szabályos bővítmények és a lehetséges rosszindulatú programok egyaránt előfordulhatnak. Kattintson egy objektumra a listában a kiválasztott bővítménnyel kapcsolatos részletes információkért, amelyek a panel alsó részén jelennek meg.

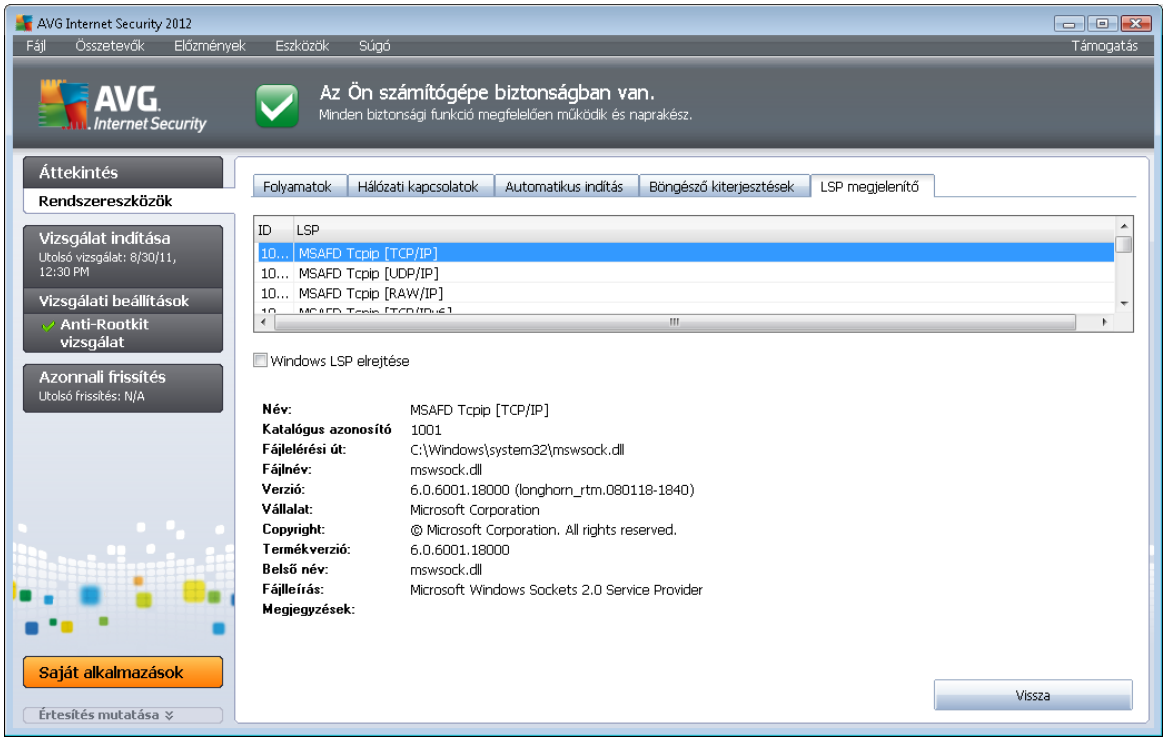
Vezérlőgombok

A ***Böngésző kiterjesztések*** lapon található vezérlőgombok a következők:

- ***Kiválasztott objektum eltávolítása*** - eltávolítja a kijelölt bővítményt a listából. ***a listában szereplő bővítményeket csak akkor ajánlatos törölni, ha meg van győződve róla, hogy azok valódi veszélyt rejtenek!***

- ***Vissza*** – Visszatérés az alapértelmezett AVG fő párbeszédpanelre *(összetevők áttekintése).*

6.6.5. LSP megjelenítő



Az ***LSP nézőke*** panel megjeleníti a réteges szolgáltatók (LSP) listáját.

A ***réteges szolgáltató*** (LSP) a Windows operációs rendszer hálózati szolgáltatásaihoz kapcsolódó rendszerillesztő. A program hozzáfér a számítógép összes bejövő és kimenő adatához, és módosíthatja is ezeket. Bizonyos LSP programokra feltétlenül szükség van ahhoz, hogy a Windows kapcsolódni tudjon más számítógépekhez, speciálisan az internethez is. Bizonyos rosszindulatú alkalmazások azonban képesek arra, hogy LSP programként telepítsék magukat, és így hozzáférhetnek a számítógép által továbbított összes adathoz. A következő áttekintés a lehetséges LSP veszélyforrások ellenőrzésében segít.

Bizonyos esetekben a hibás LSP programok javítása is lehetséges(*például ha a fájl el lett távolítva, de a regisztrációs bejegyzések érintetlenek maradtak*). A javítható LSP program felfedezésekor új gomb jelenik meg, mellyel a hiba kijavítható.

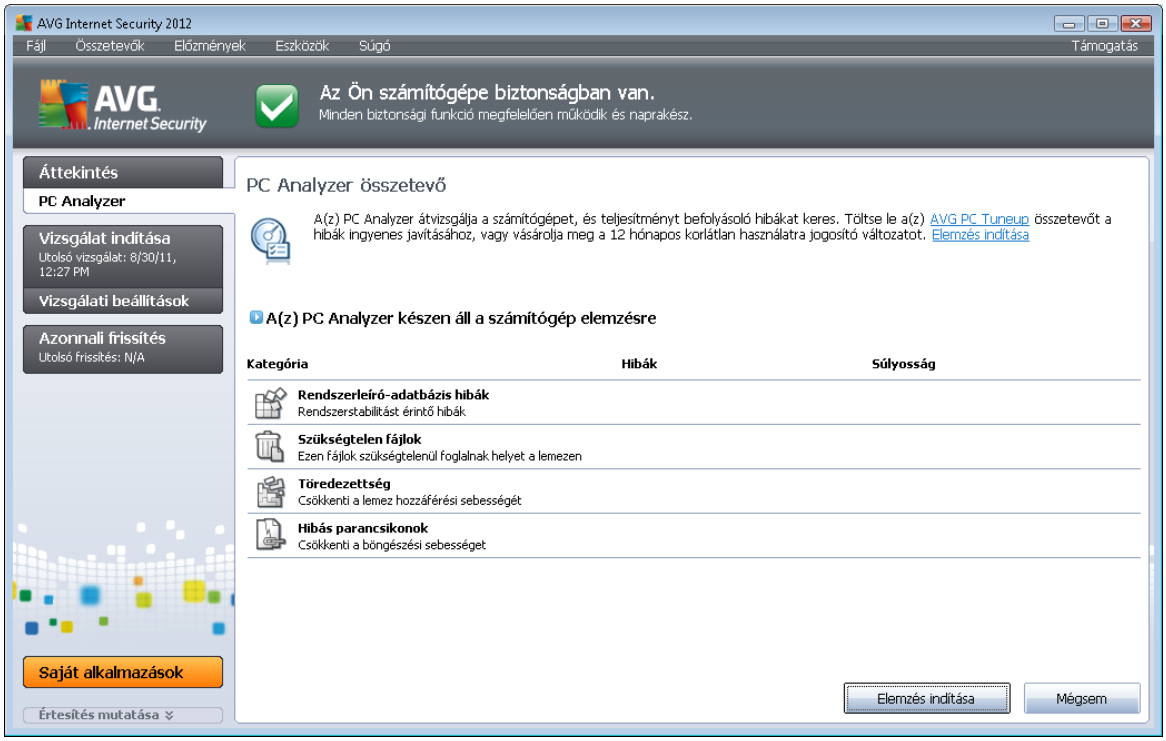
Vezérlőgombok

Az ***LSP megjelenítő*** lapon található vezérlőgombok a következők:

- ***Windows LSP elrejtése*** – A Windows LSP a listában való megjelenítéséhez törölje az elem jelölését.
- ***Vissza*** – Visszatérés az alapértelmezett AVG fő párbeszédpanelre (*összetevők áttekintése*).

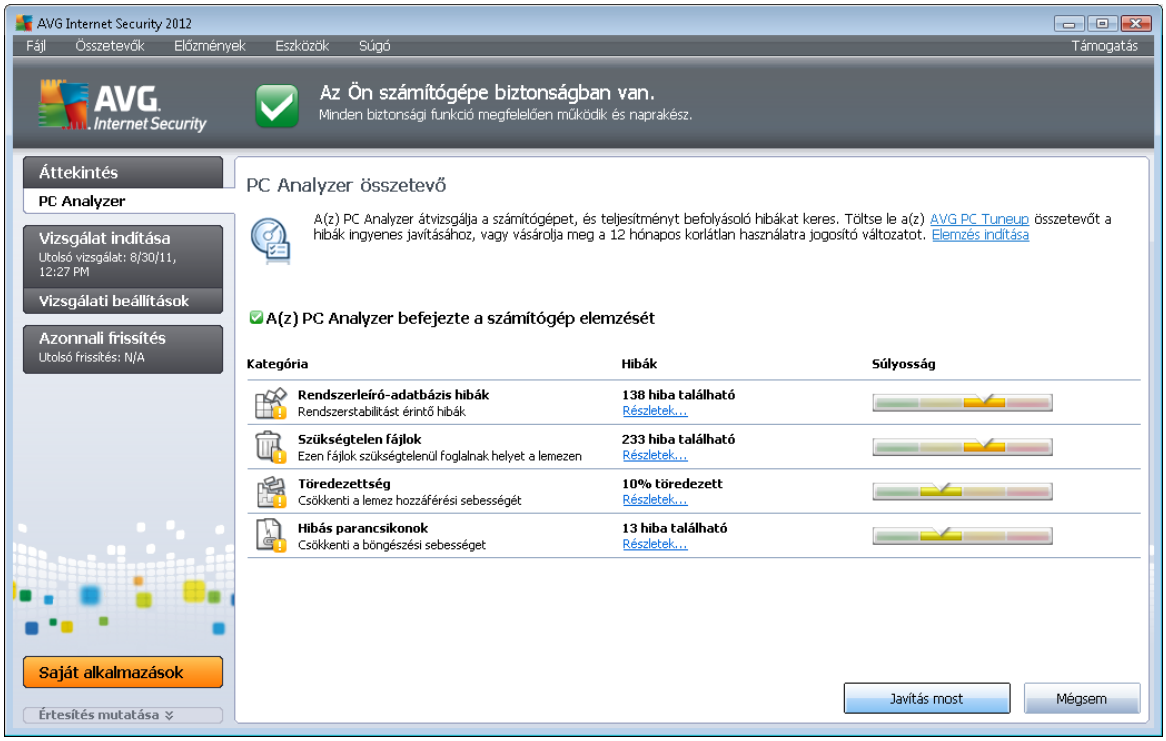
6.7. PC Analyzer

A ***PC Analyzer*** összetevő hibákat keres a rendszeren és megmutatja, hogy milyen tényezők csökkentik a számítógép teljesítményét. A felhasználói felületen a következő négy kategóriát láthatja: beállításjegyzék hibái, felesleges fájlok, töredezettség és megszakadt parancsikonok:



- ***A Rendszerleíró adatbázis hibái*** megjelenítik a Windows Rendszerleíró adatbázisában szereplő hibákat. Mivel a rendszerleíró adatbázis javítása szaktudást igényel, nem javasoljuk, hogy Ön próbálja azt egyedül kijavítani.
- ***A Szükségtelen fájlok*** rész megjeleníti a leginkább szükségtelen fájlokat. Ezek jellemzően ideiglenes fájlok, valamint a Lomtár elemei.
- ***A Töredezettség*** funkció kiszámítja a merevlemez töredezettségének százalékos mértékét (a töredezettséget az okozza, hogy már sokat használta a merevlemezt, ezért a fájlok a fizikai lemezen több apró darabban, szétszórva helyezkednek el). Használjon töredezettségmentesítő eszközt a hiba javításához.
- ***A Hibás parancsikonok*** rész megjeleníti a nem működő pl. nem létező helyekre mutató parancsikonokat.

A rendszer elemzésének indításához nyomja meg az ***Elemzés*** gombot. Ekkor figyelheti az elemzési folyamatot, majd az eredményeket megtekintheti a diagramon:



Az eredmények megjelenítik az észlelt rendszerhibák számát (***Hibák***) a vizsgált kategóriák szerint csoportosítva. Az eredmények grafikus formában is megjelennek a ***Súlyossági szint*** oszlopon.

Vezérlőgombok

- ***Elemzés indítása*** (*az elemzés indítása előtt jelenik meg*) – Kattintson erre a gombra a számítógép elemzésének azonnali indításához
- ***Javítás*** (*az elemzés befejezése előtt jelenik meg*) – Kattintson erre a gombra az AVG webhelyére (http://www.avg.hu/) ugráshoz, ahol részletes és naprakész információkat tekinthet meg a ***PC Analyzer*** összetevőről
- ***Mégse*** – Kattintson erre a gombra a folyamatban lévő elemzés leállításához, és az alapértelmezett AVG fő párbeszédpanelre (*összetevők áttekintése*) történő visszatéréshez az elemzés befejezése után

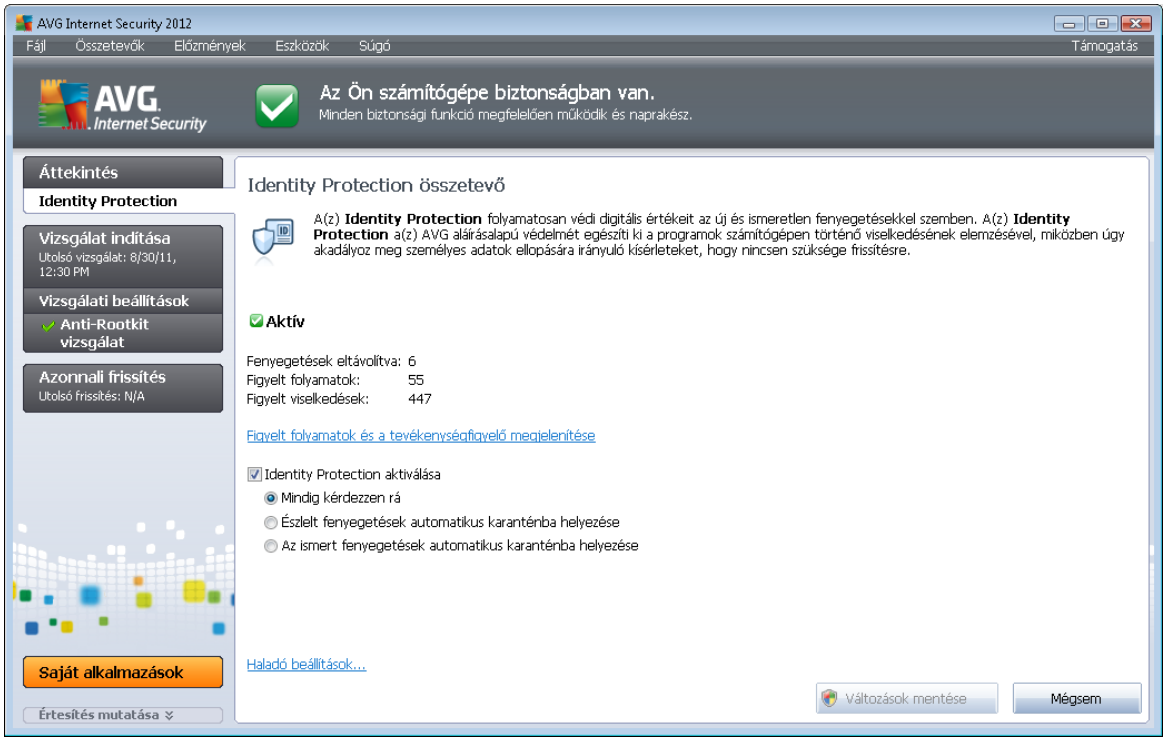
6.8. Identity Protection

Az Identity Protection olyan, káros programoktól védő összetevő, amely mindenféle káros program (*kémprogramok, robotprogramok, személyes adatokat eltulajdonító programok stb.*) ellen véd, viselkedésalapú technológiát használ, és azonnali védelmet biztosít a legújabb vírusok ellen. ***Az Identity Protection*** megakadályozza, hogy tolvajok jelszavakat, banki adatokat, hitelkártyaszámokat és egyéb személyes digitális adatokat lopjanak el különféle rosszindulatú szoftverek (*káros programok*) segítségével. A program meggyőződik arról, hogy minden, a számítógépen futó alkalmazás megfelelően működjön. ***Az Identity Protection*** folyamatosan észleli és letiltja a gyanús viselkedést, és megvédi a számítógépet a legújabb káros programoktól.

Az Identity Protection valósidejű védelmet nyújt a számítógép számára az új és ismeretlen fenyegetések ellen. Figyeli az összes folyamatot *(beleértve a rejtetteket is)* és a több mint 285 különféle viselkedési mintát, annak megállapításához, hogy zajlik-e gyanús tevékenység a rendszeren. Ezért olyan fenyegetéseket is képes azonosítani, amelyek még nem szerepelnek a vírusadatbázisban. Ha ismeretlen kód jut el a számítógépre, a program azonnal elkezdi figyelni, nem káros tevékenységeket hajt-e végre, és nyomon követi a viselkedését. Ha a fájl kártékonynak bizonyul, az ***Identity Protection*** áthelyezi a kódot a karanténba, majd visszaállítja a rendszert érintő összes rosszindulatú módosítást *(kódbeszúrás, beállításjegyzék módosításai, portok megnyitása stb.)*. Nem kell vizsgálatot indítania a védelem biztosításához. Ez a technológia rendkívül proaktív, ritkán van szüksége frissítésekre, és mindig készenlétben áll.

Az Identity Protection kiegészítő védelmet biztosít a víruskereső mellett. Ajánlott mindkét összetevőt telepíteni a számítógép teljes körű védelme érdekében.

6.8.1. Identity Protection felület



Az Identity Protection párbeszédpanelen az összetevő alapvető működéséről és állapotáról *(aktív)* szóló rövid leírás, valamint néhány statisztikai adat található:

- ***Eltávolított fenyegetések –*** megadja a kártékony programként észlelt és eltávolított alkalmazások számát
- ***Figyelt folyamatok*** - az IDP által figyelt, jelenleg futó alkalmazások száma
- ***Figyelt viselkedések*** - a figyelt alkalmazásokkal futó műveletek száma

Alább találhatja a Figyelt folyamatok és az aktivitási figyelő megjelenítése linket, amely a Rendszereszközök összetevő felhasználói felületére irányítja Önt, ahol megtekintheti az összes

figyelt folyamat részletes áttekintését.

Identity Protection alapvető beállításai

A párbeszédpanel alsó részén szerkesztheti az összetevő működésének bizonyos alapszintű beállításait:

- ***Identity Protection aktíválása*** - (*alapállapotban bekapcsolva*): jelölje az IDP összetevő aktiválásához és a további beállítások megnyitásához.

Bizonyos esetekben az ***Identity Protection*** egyes legitim fájlokat gyanúsnak vagy veszélyesnek minősíthet. Mivel az ***Identity Protection*** a fenyegetéseket a viselkedés alapján észleli, előfordulhat, hogy a termék olyankor is tévesen riaszt, amikor bizonyos programok billentyűleütéseket figyelnek, vagy programokat és drivereket telepítenek a számítógépre. Válassza ki az alábbi beállítások egyikét, amely meghatározza az ***Identity Protection*** összetevő viselkedését riasztás során:

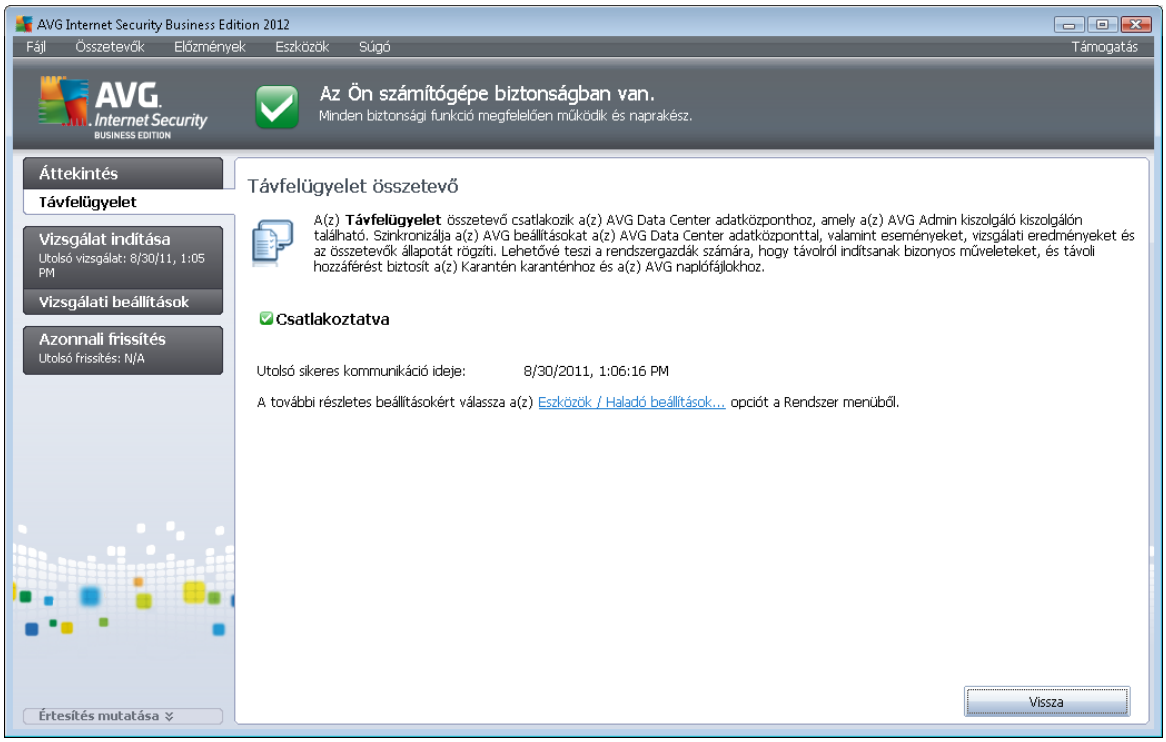
  - ***Mindig legyen kérdés*** - ha egy alkalmazás kártevőként lett azonosítva, akkor a rendszer rákérdez, hogy letiltsa-e azt (*ez az opció alapállapotban be van kapcsolva, és ne is módosítsa ezt a beállítást, kivéve, ha feltétlenül szükséges*)
  - ***Az észlelt fenyegetések automatikus karanténba helyezése*** - a kártevőként észlelt összes alkalmazást a program automatikusan letiltja
  - ***Ismert fenyegetések automatikus karanténba helyezése*** - azon alkalmazások, amelyek biztosan kártevők, le lesznek tiltva

Vezérlőgombok

A vezérlőgombok az ***Identity Protection*** felületen a következők:

- ***Változások mentése*** – nyomja meg ezt a gombot a változtatások mentéséhez és alkalmazásához
- ***Mégse*** – nyomja meg ezt a gombot, ha az alapértelmezett AVG főablakhoz ***szeretne visszatérni*** (*összetevők áttekintése*)

6.9. Távfelügyelet



A ***Távfelügyelet*** összetevő csak akkor jelenik meg az **AVG Internet Security 2012** felhasználói felületén, ha telepítette a termék Business Edition kiadását *(a telepítéshez használt licenccel kapcsolatos információk beszerzéséhez tekintse meg a Verzió lapot az Információ párbeszédpanelen, amelyet a Támogatás rendszermenü elemből nyithat meg)*. A ***Távfelügyelet összetevő*** párbeszédpanelen láthatja, hogy az összetevő aktív-e, illetve csatlakozott-e a kiszolgálóhoz. A ***Távfelügyelet*** összetevő összes beállítását a ***Haladó beállítások / Távfelügyelet*** részen végezheti el.

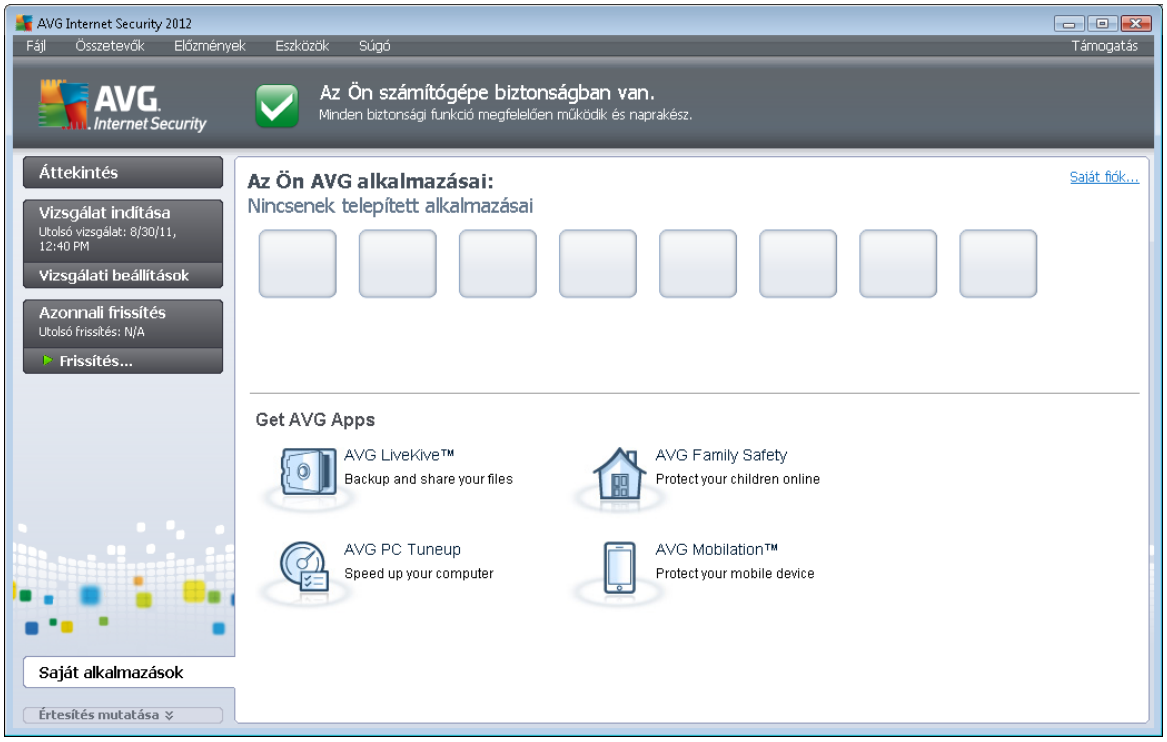
Az AVG Távfelügyelet összetevő beállításaival és szolgáltatásaival kapcsolatos részletes leírásért forduljon az összetevőről szóló dokumentációhoz. Ez a dokumentáció letölthető az AVG webhelyéről (http://www.avg.hu/), a ***Támogatási központ / Letöltés / Dokumentáció*** részről.

Vezérlőgombok

- ***Vissza*** – Kattintson erre a gombra, ha az alapértelmezett AVG fő párbeszédpanelre szeretne visszatérni (*összetevők áttekintése*).

7. Saját alkalmazások

A LiveKive, a Family Safety és a PC Tuneup alkalmazások elérhetők önálló AVG termékként, valamint az **AVG Internet Security 2012** csomag opcionális részeként is. ***Az Ön AVG alkalmazásai*** párbeszédpanelen *(az AVG fő párbeszédpanelen a Saját alkalmazások gombra kattintva közvetlenül elérhető)* áttekintheti a már telepített és az opcionálisan telepíthető alkalmazásokat:



7.1. LiveKive

A LiveKive összetevő online adatmentésre szolgál. Az adatokat biztonságos kiszolgálókon tárolja a rendszer. ***A LiveKive*** automatikusan menti az összes fájlt, képet és zenét egyetlen biztonságos helyre, és lehetővé teszi, hogy megossza azokat a családjával és barátaival, illetve hozzáférjen azokhoz bármilyen internetezésre alkalmas eszközzel, például iPhone és Androidos készülékekkel. ***A LiveKive*** funkciói:

- Biztonsági intézkedés arra az esetre, ha a számítógépe és/vagy merevlemeze megsérülne
- Bármilyen olyan eszközzel hozzáférhet az adataihoz, amely csatlakozik az internethez
- Egyszerű rendszerezés
- Megosztás erre feljogosított felhasználókkal

Részletes információkért látogasson el a megfelelő AVG weboldalra, ahol azonnal le is töltheti az összetevőt. Ehhez használhatja a Saját alkalmazások párbeszédpanelen található LiveKive hivatkozást.

7.2. Family Safety

A Family Safety segít megvédeni a gyermekeit a nem megfelelő webhelyektől, médiatartalmaktól és online keresésektől, illetve jelentésekkel szolgál az online tevékenységeikről. Minden egyes felhasználó esetében megadhatja a kívánt védelmi szintet, és külön-külön figyelheti a felhasználók tevékenységét az egyedi bejelentkezéseken keresztül.

Részletes információkért látogasson el a megfelelő AVG weboldalra, ahol azonnal le is töltheti az összetevőt. Ehhez használhatja a Family Safety hivatkozást a Saját alkalmazások párbeszédpanelen.

7.3. PC Tuneup

A PC Tuneup alkalmazás részletes rendszerelemzésre szolgáló eszköz, amely meghatározza, hogy miként javítható a számítógép sebessége és teljesítménye. ***A PC Tuneup*** funkció többek között az alábbiakat tartalmazza:

- Merevlemez tisztító – Eltávolítja a felesleges fájlokat, amelyek lelassítják a számítógépet.
- Disk Defrag – Töredezettségmentesíti a lemezmeghajtókat és optimalizálja a rendszerfájlok elhelyezését.
- Registry Cleaner – Kijavítja a beállításjegyzék hibáit a számítógép stabilitásának növelése érdekében.
- Registry Defrag – Tömöríti a beállításjegyzéket, megszüntetve ezáltal a memóriaigényes réseket.
- Disk Doctor – Megkeresi a rossz szektorokat, elveszett szektorcsoportokat és könyvtárhibákat, majd kijavítja azokat.
- Internet Optimizer – Átalakítja az általános beállításokat egy adott internetkapcsolathoz.
- Nyomtörlő – Eltávolítja a számítógép és az internethasználat előzményét.
- Disk Wiper – Végleges törlést hajt végre a szabad lemezterületen, hogy ne lehessen visszaállítani az érzékeny adatokat.
- File Shredder – Törli egy lemez vagy USB-memória kijelölt fájljait úgy, hogy azokat később ne lehessen visszaállítani.
- File Recovery – Visszaállítja a lemezekről, USB-memóriából vagy fényképezőgépről véletlenül törölt fájlokat.
- Duplicate File Finder – Segít megkeresni és eltávolítani a több példányban létező fájlokat, amelyek feleslegesen foglalják a lemezterületet.
- Services Manager – Letiltja a felesleges szolgáltatásokat, amelyek lelassítják a számítógépet.
- Startup Manager – Lehetővé teszi, hogy a felhasználó beállítsa azokat a programokat,

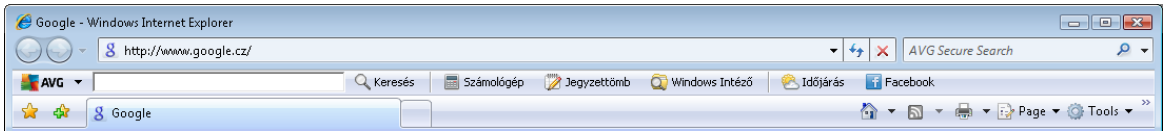
amelyek a Windows indításakor automatikusan elindulnak.

- Uninstall Manager – Teljesen eltávolítja azokat a programokat, amelyekre már nincs szüksége.
- Tweak Manager – Lehetővé teszi, hogy a felhasználó rejtett Windows beállítások százainak finomhangolását végezze el.
- Task Manager – Felsorolja az összes futó folyamatot, szolgáltatást és zárolt fájlt.
- Disk Explorer – Megmutatja, hogy mely fájlok foglalják a legtöbb helyet a számítógépen.
- System Information – Részletes információt szolgáltat a telepített hardverekről és szoftverekről.

Részletes információkért látogasson el a megfelelő AVG weboldalra, ahol azonnal le is töltheti az összetevőt. Ehhez használhatja a PC Tuneup hivatkozást a Saját alkalmazások párbeszédpanelen.

8. AVG Biztonság eszköztár

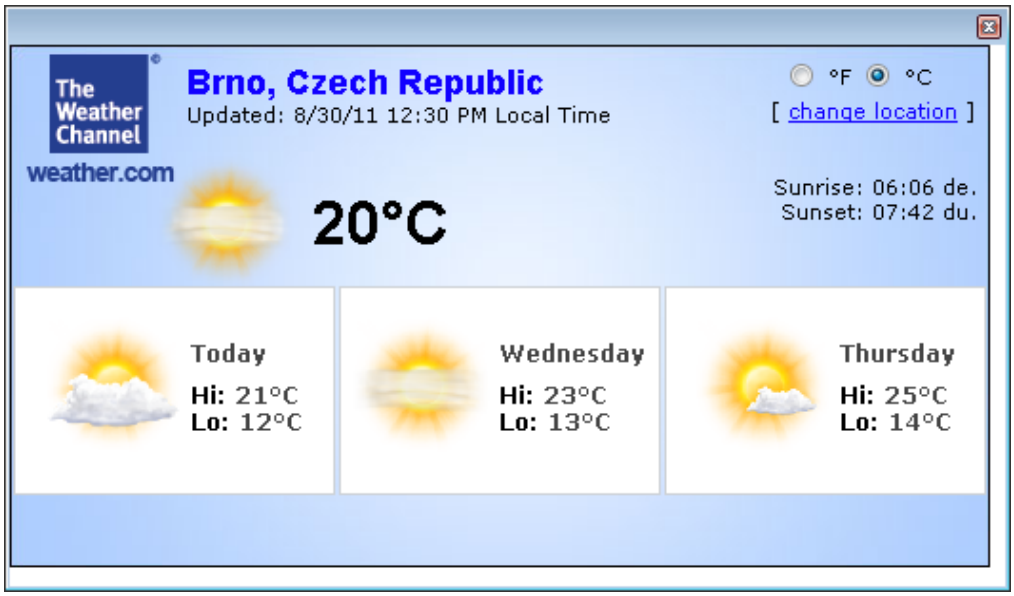
Az AVG Biztonság eszköztár egy olyan eszköz, amely szorosan együttműködik a LinkScanner összetevővel, és maximális biztonságot garantál, miközben az interneten böngészik. Az **AVG Internet Security 2012** terméken belül az ***AVG Biztonság eszköztár*** telepítése opcionális. A telepítési folyamat során kiválaszthatta, hogy mely összetevők legyenek telepítve. ***Az AVG Biztonság eszköztár*** közvetlenül elérhető a webböngészőből. Jelenleg a támogatott internetböngészők a következők: Internet Explorer (*6.0 és újabb verziók*) és/vagy Mozilla Firefox (*3.0 és újabb verziók*). A többi böngésző nem támogatott *(ha más böngészőt használ, például az Avant böngészőt, akkor a program nem várt módon viselkedhet)*.



Az AVG Biztonság eszköztár az alábbi elemeket tartalmazza:

- ***Az AVG embléma*** a legördülő menüvel:
  - ***AVG biztonságos keresés használata*** - Lehetővé teszi, hogy közvetlenül az ***AVG biztonsági eszköztárról*** keressen az ***AVG biztonságos keresési*** motorja segítségével. Minden keresési eredményt folyamatosan ellenőriz a Kereső védelem szolgáltatás, így teljes biztonságban érezheti magát böngészés közben.
  - ***Aktuális fenyegetettségi szint*** – Megnyitja a víruslabor weboldalát, ahol grafikus formában ellenőrizheti az aktuális internetes fenyegetettségi szintet.
  - ***AVG Víruslabor*** – Megnyitja a ***Webhelyjelentések*** oldalt az AVG webhelyén (http://www.avg.hu/), ahol név szerint kereshet az adott fenyegetések között, illetve részletes információkat kaphat róluk.
  - ***Eszköztár súgó*** – Egy online súgót nyit meg, amely az ***AVG Biztonság eszköztár*** összes funkcióját tartalmazza.
  - ***Visszajelzés küldése a termékről*** – Egy weboldal nyílik meg egy űrlappal, amelyet kitölthet és elmondhatja véleményét az ***AVG Biztonság eszköztár*** eszközről.
  - ***Névjegy...*** – Egy új, a jelenleg telepített ***AVG Biztonság eszköztár*** verzióval kapcsolatos adatokat tartalmazó ablakot nyit meg.
- ***Keresési mező*** – Keressen az interneten az ***AVG Biztonság eszköztár*** segítségével, hogy teljesen biztonságban és kényelemben tudhassa magát a 100 százalékban biztonságos keresési eredményeknek köszönhetően. Írja be a kulcsszót vagy a kívánt kifejezést a keresőmezőbe, és kattintson a ***Keresés*** gombra *(vagy nyomja le az Enter billentyűt)*. Az összes keresési eredményt folyamatosan ellenőrzi a Kereső védelem szolgáltatás *(ez a LinkScanner összetevőn belül található)*.
- Gyorsgombok az alábbi alkalmazások gyors eléréséhez: ***Számológép***, ***Jegyzettömb***, ***Windows Intéző***

- ***Időjárás*** – Ezzel a gombbal egy új párbeszédpanelt nyit meg, amely a földrajzi helyének megfelelő aktuális időjárásról nyújt információt, valamint megjeleníti a következő két napra vonatkozó előrejelzést. Ez az információ rendszeresen, 3-6 óránként frissül. A párbeszédpanelen manuálisan módosíthatja a kívánt helyszínt, és kiválaszthatja, hogy a hőmérsékletet Celsius vagy Fahrenheit fokban szeretné látni.



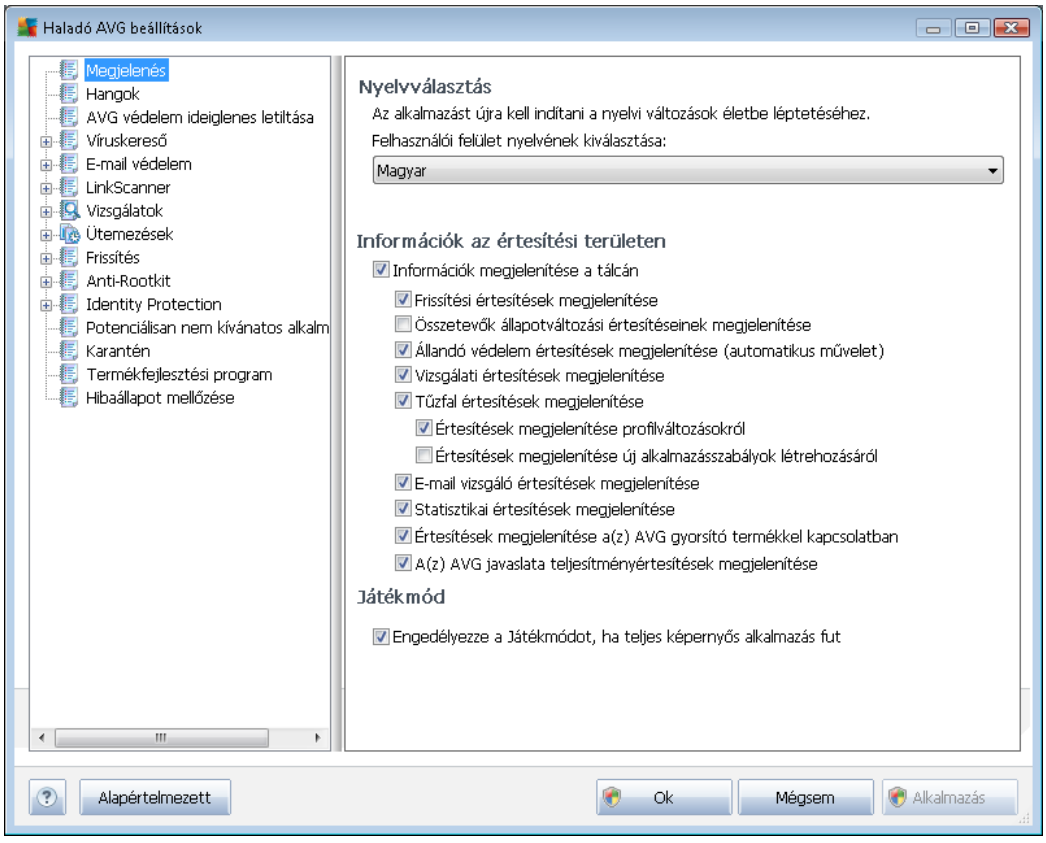
- ***Facebook*** – Ezzel a gombbal a Facebook közösségi hálózathoz csatlakozhat közvetlenül az ***AVG Biztonság eszköztárból***. *viselkedés*.

9. AVG Haladó beállítások

Az **AVG Internet Security 2012** egy új ablakot nyit meg ***Haladó AVG beállítások*** néven. Az ablak két részre van osztva: a bal oldali rész fastruktúrába osztott navigációt tesz lehetővé a program beállítási lehetőségei között. Válassza ki a módosítandó összetevőt (*vagy adott részét*), ekkor megnyílik az adott elemhez tartozó szerkesztőablak a jobb oldalon.

9.1. Megjelenés

A navigációs fa első eleme a ***Megjelenés***. Ez az **AVG Internet Security 2012** felhasználói felület általános beállításainak, valamint az alkalmazás viselkedését befolyásoló néhány alapvető beállításnak a megadását teszi lehetővé:

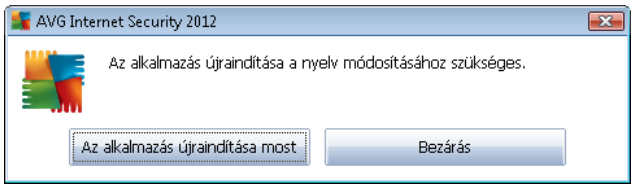


Nyelvválasztás

A ***Nyelvválasztás*** területen választható ki a használni kívánt nyelv egy legördülő menüből. Az itt kiválasztott nyelvet fogja használni az egész **AVG Internet Security 2012** felhasználói felület. A legördülő menüben csak a telepítési folyamat (*lásd az Egyéni opciók* című fejezetet) során kiválasztott nyelvek és az angol jelennek meg (*az angol nyelvet alapértelmezés szerint mindig automatikusan telepíti a program*). Az **AVG Internet Security 2012** szoftvert újra kell indítani a nyelválasztás érvényesítéséhez. Kövesse az alábbi lépéseket:

- A legördülő menüben válassza ki az alkalmazásban használni kívánt nyelvet

- A választás megerősítéséhez kattintson az ***Alkalmaz*** gombra *(a párbeszédpanel jobb alsó sarkában)*
- Kattintson az ***OK*** gombra a megerősítéshez
- Egy új párbeszédablak ugrik elő, ami tájékoztatja, hogy a nyelválasztás érvényesítéséhez újra kell indítania az **AVG Internet Security 2012**
- Kattintson ***Az alkalmazás újraindítása most*** gombra a program újraindításának engedélyezéséhez, és várja meg, amíg életbe lép a nyelváltás:



Információk az értesítési területen

Ezen a területen letilthatja az **AVG Internet Security 2012** alkalmazás állapotával kapcsolatos, a rendszertálcán megjelenő értesítéseket. Alapértelmezés szerint a rendszerértesítések megjelenítése engedélyezett. Javasoljuk, hogy ne változtasson ezen a beállításon. Rendszerértesítések tájékoztatnak például a vizsgálati vagy frissítési folyamat indulásáról, valamint az **AVG Internet Security 2012** összetevőinek állapotváltozásáról. Ezeknek a bejelentéseknek szenteljen komoly figyelmet.

Ha valamilyen okból úgy dönt, hogy nem szeretné ezeket az értesítéseket megjeleníteni, vagy csak néhányat kapcsolna be közülük *(például csak egyes AVG Internet Security 2012 összetevőkkel kapcsolatos értesítésekre kíváncsi)*, akkor ezt a következő jelölőnégyzetek bejelölésével vagy jelölésük törlésével teheti meg:

- ***Információk megjelenítése a tálcán*** *(alapértelmezés szerint bekapcsolva)* – Alapértelmezés szerint az összes értesítés megjelenik. Törölje az elem jelölését, ha minden rendszerértesítés megjelenítését ki kívánja kapcsolni. Ha be van kapcsolva, akkor kiválaszthatja, hogy milyen értesítések jelenjenek meg:
  - ***Értesítések megjelenítése a frissítésekkel*** kapcsolatban *(alapértelmezés szerint bekapcsolva)* – Meghatározza, hogy az **AVG Internet Security 2012** frissítés indításával, magával a folyamattal illetve a befejezéssel kapcsolatban jelenjenek-e meg értesítések.
  - ***Összetevők állapotváltozásával kapcsolatos értesítések megjelenítése*** *(alapértelmezés szerint kikapcsolva)* – Meghatározza, hogy az összetevők működésével/működésképtelenségével vagy lehetséges problémákkal kapcsolatban jelenjenek-e meg értesítések. Az összetevők hibaállapotának jelentésekor ez a beállítás egyenértékű az értesítési terület ikonjának **AVG Internet Security 2012** összetevőkre vonatkozó hibajelzésével.
  - ***Az Állandó védelem összetevővel kapcsolatos értesítések megjelenítése***

(automatikus művelet) *(alapértelmezés szerint bekapcsolva)* – Meghatározza, hogy a fájlok mentésével, másolásával, illetve folyamatok megnyitásával kapcsolatban jelenjenek-e meg értesítések (*ez a beállítás csak akkor működik, ha az Állandó védelem Automatikus javítás szolgáltatása be van kapcsolva*).

- ***Értesítések megjelenítése a vizsgálatokkal*** kapcsolatban*(alapértelmezés szerint bekapcsolva)* – Meghatározza, hogy az ütemezett vizsgálat indításával, magával a folyamattal illetve az eredményekkel kapcsolatban jelenjenek-e meg értesítések.

- ***A Tűzfal összetevővel kapcsolatos értesítések megjelenítése*** *(alapértelmezés szerint bekapcsolva)* – Meghatározza, hogy a Tűzfal állapotával és folyamataival kapcsolatos értesítések, például az összetevő be- és kikapcsolásával kapcsolatos figyelmeztetések, adatforgalom esetleges blokkolása stb. megjelenjenek-e vagy sem. Ez az elem további két specifikusabb kiválasztási beállítást kínál *(ezek részletes leírását ezen dokumentum Tűzfal című fejezetében találja)*:

  - ***Profilváltozásokkal kapcsolatos értesítések megjelenítése*** *(alapértelmezés szerint bekapcsolva)* – Értesítések küldése a Tűzfal profilok automatikus változásairól.

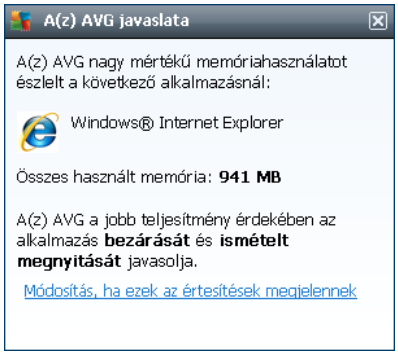
  - ***Értesítések megjelenítése új alkalmazásszabályok létrehozásáról*** *(alapértelmezés szerint kikapcsolva)* – Értesítések küldése a biztonságos elemeket tartalmazó listán szereplő alkalmazásokkal kapcsolatos Tűzfal szabályok létrehozásáról.

- ***Az E-mail vizsgáló összetevővel kapcsolatos értesítések megjelenítése*** *(alapértelmezés szerint bekapcsolva)* – Meghatározza, hogy megjelenjenek-e üzenetek a bejövő és kimenő e-mailek vizsgálatakor.

- ***Statisztikai értesítések megjelenítése*** *(alapértelmezés szerint bekapcsolva)* – Jelölje be, ha rendszeresen meg kíván jeleníteni statisztikai értesítéseket a tálcán.

- ***Az AVG Accelerator szolgáltatással kapcsolatos értesítések megjelenítése*** *(alapértelmezés szerint bekapcsolva)* – Meghatározza, hogy megjelenjenek-e az ***AVG Accelerator*** tevékenységeivel kapcsolatos értesítések. ***Az AVG Accelerator*** szolgáltatás gördülékenyebbé teszi az online videolejátszást, és megkönnyíti a további letöltéseket.

- ***AVG Advice teljesítményértesítések megjelenítése*** *(alapértelmezés szerint bekapcsolva)* – Az ***AVG Advice*** megfigyeli a támogatott internetböngészők *(Internet Explorer, Chrome, Firefox, Opera és Safari)* teljesítményét, és értesítést küld, amennyiben egy böngésző több memóriát használ az ajánlott értéknél. Ilyen esetekben a számítógép teljesítménye jelentősen visszaeshet, és javasolt újraindítani az internetböngészőt a műveletek felgyorsítása érdekében. Ha szeretne információkat kapni, hagyja bekapcsolva az ***AVG Advice teljesítményértesítések*** elemet.

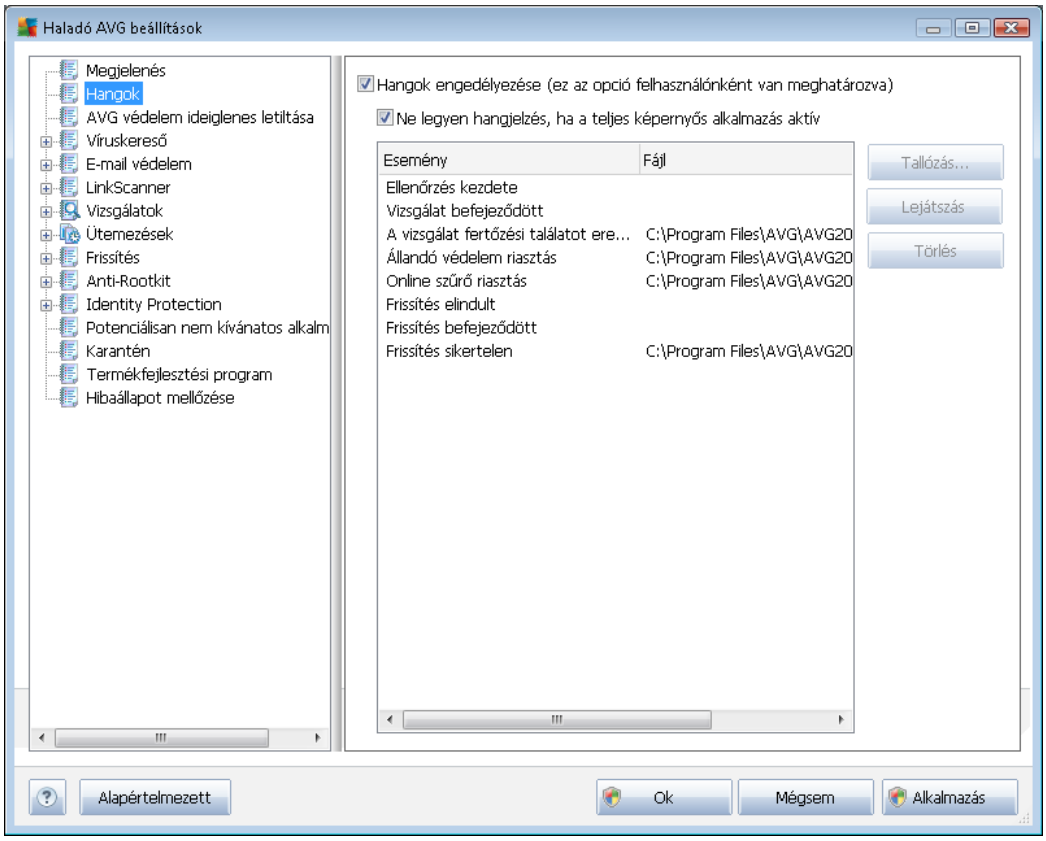


Játék mód

Az AVG ezen szolgáltatása olyan teljes képernyős alkalmazásokra lett kifejlesztve, amelyeknél az AVG esetlegesen értesítő üzeneteket jelenít meg (*pl. ha egy ütemezett vizsgálat elindul*), és ez zavaró lehet(*kis méretűre állíthatják az alkalmazást, és ronthatják a grafikus megjelenítést*). Ezen probléma elkerülése érdekében jelölje be a ***Játékmód engedélyezése teljes képernyős alkalmazások futtatásakor*** opciót(*alapbeállítás*).

9.2. Hangok

A ***Hangok*** párbeszédpanelen beállíthatja, hogy szeretne-e hangokat hozzárendelni bizonyos **AVG Internet Security 2012** műveletekhez:



A beállítások csak az aktuális felhasználói fiókra vonatkoznak, vagyis a számítógép minden egyes felhasználója külön hangbeállításokat adhat meg. Ha engedélyezni kívánja a hangjelzéseket, hagyja bejelölve a ***Hangjelzések engedélyezése*** beállítást (*a beállítás alapértelmezés szerint be van kapcsolva*), így aktív marad az összes vonatkozó műveletet tartalmazó lista. Ezenkívül érdemes lehet bejelölni a ***Ne legyen hangjelzés, ha a teljes képernyős alkalmazás aktív*** beállítást, amivel letilthatja a hangjelzéseket olyan esetekben, amikor azok zavaróak lehetnek *(részleteket a dokumentum Haladó beállítások/Megjelenés fejezetének Játék mód szakaszában talál)*.

Vezérlőgombok

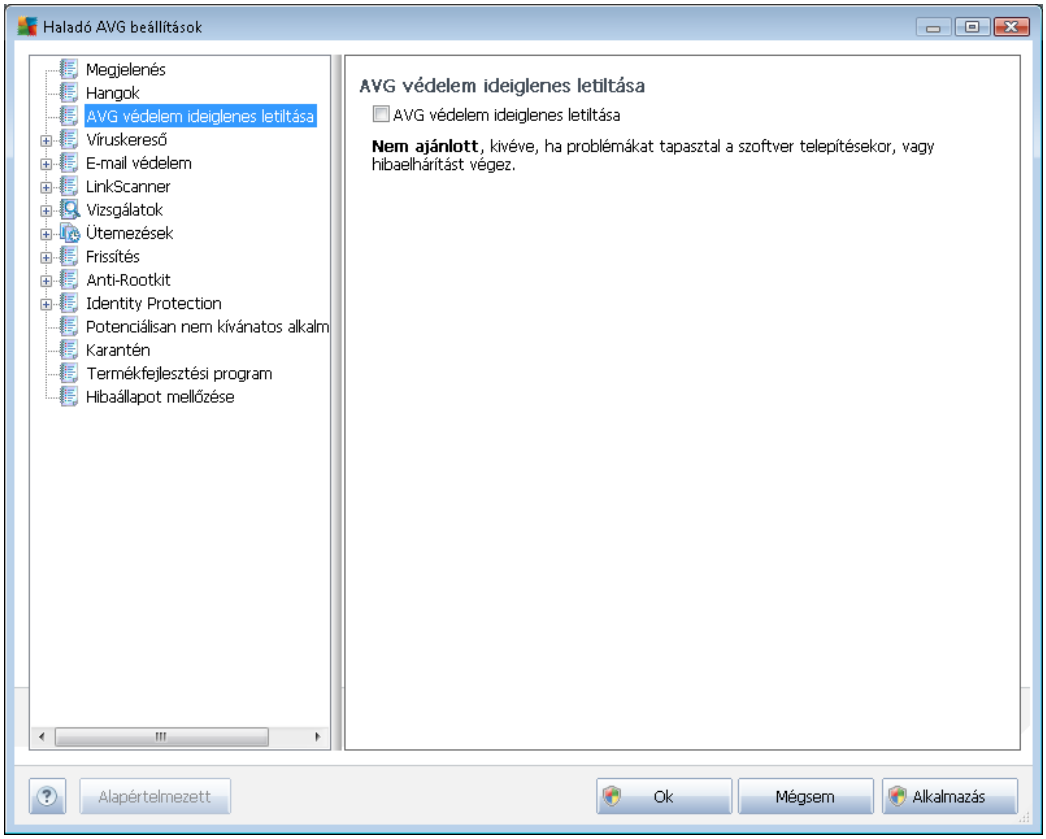
- ***Böngészés*** – Miután kiválasztotta a megfelelő eseményt a listából, a ***Tallózás*** gombra kattintva megkeresheti a számítógépen az eseményhez rendelni kívánt hangfájlt. *(Vegye figyelembe, hogy jelenleg kizárólag a *.wav formátumú fájlok támogatottak.)*
- ***Lejátszás*** – A kiválasztott hang meghallgatásához jelölje ki az eseményt a listán, majd kattintson a ***Lejátszás*** gombra.
- ***Törlés*** – Használja a ***Törlés*** gombot a hang és az adott esemény társításának

megszüntetéséhez.

9.3. Az AVG védelem ideiglenes letiltása

Az ***AVG védelem ideiglenes letiltása*** panel lehetővé teszi az **AVG Internet Security 2012** teljes védelmének kikapcsolását.

Ne feledje: ezt a beállítást csak akkor használja, ha feltétlenül szükséges.

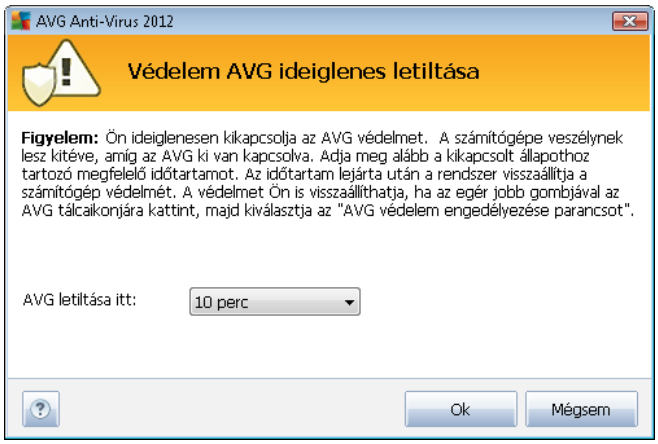


A legtöbb esetben ***nem szükséges*** kikapcsolni az **AVG Internet Security 2012** védelmet új szoftver vagy illesztőprogram telepítése előtt, még akkor sem, ha a telepítő vagy a varázsló javasolja a futó programok és alkalmazások bezárását a telepítési folyamat zavartalansága érdekében. Ha problémákat észlel a telepítések során, akkor először kapcsolja ki az állandó védelmet *(*Állandó védelem engedélyezése). Ha ideiglenesen ki kell kapcsolnia az **AVG Internet Security 2012** védelmet, akkor mielőbb kapcsolja azt vissza. Ha kikapcsolt víruskereső szoftverrel csatlakozik az internethez vagy egy hálózathoz, akkor a számítógépe védtelen a támadásokkal szemben.

Az AVG védelem letiltása

- Jelölje be ***Az AVG védelem ideiglenes letiltása*** jelölőnégyzetet, és erősítse meg a választást az ***Alkalmaz*** gombra kattintva
- A megnyíló ***Az AVG védelem ideiglenes letiltása*** párbeszédpanelen adja meg, mennyi

időre kívánja letiltani az **AVG Internet Security 2012** szoftvert. Alapértelmezés szerint a védelem 10 percig lesz kikapcsolva. Ez elegendő idő általános feladatok (például új szoftver telepítése) végrehajtásához. Vegye figyelembe, hogy az időtartamot maximum 15 percre állíthatja be, és az biztonsági okokból nem bírálható felül. A megadott időszak után az összes kikapcsolt összetevő automatikusan újra aktiválódik.

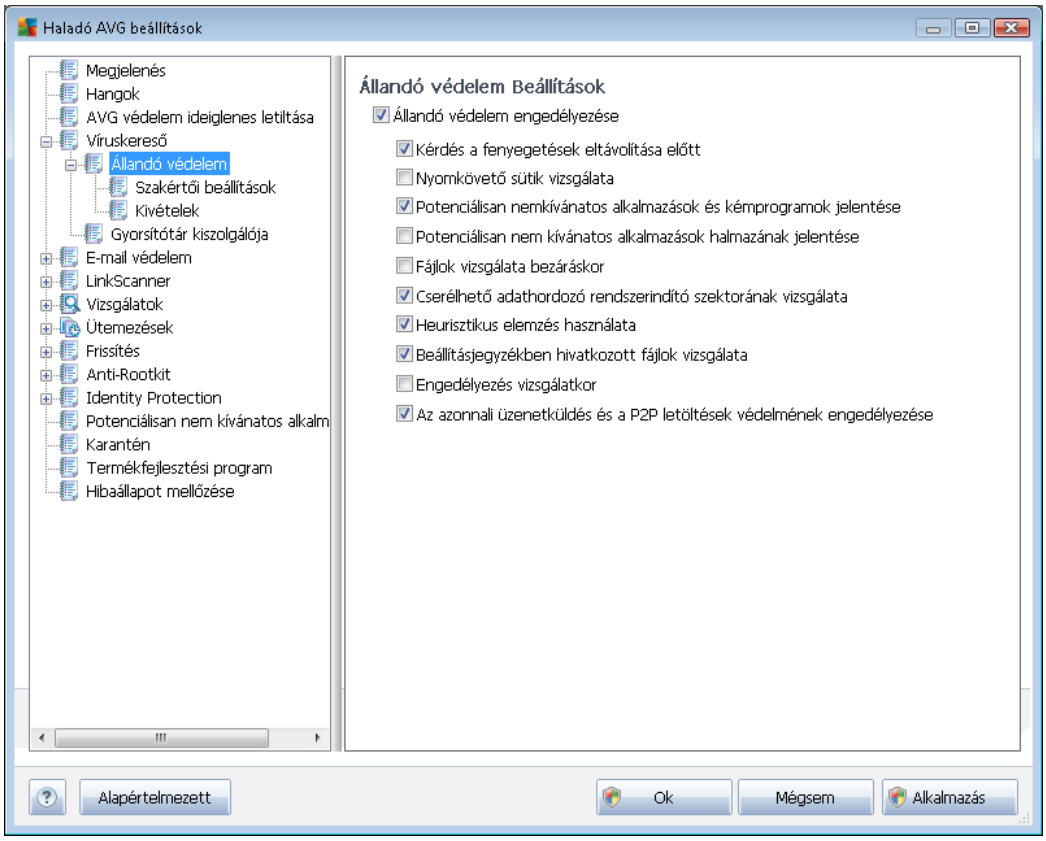


9.4. Víruskereső

Itt megadhatja a téma szövegét.

9.4.1. Állandó védelem

Az Állandó védelem összetevő a fájlok és mappák vírusokkal, kémprogramokkal és káros programokkal szembeni folyamatos védelmét biztosítja.



Az ***Állandó védelem beállítások*** párbeszédpanelen be- és kikapcsolhatja az állandó védelem funkciót az ***Állandó védelem engedélyezése*** elem segítségével (*alapértelmezés szerint be van kapcsolva*). Továbbá kiválaszthatja, hogy az állandó védelem mely funkciói legyenek aktiválva:

- ***Nyomkövető sütik vizsgálata*** (*alapértelmezés szerint ki van kapcsolva*) – Ez a paraméter határozza meg, hogy a program felismerje-e a cookie-kat a vizsgálat során. (*A HTTP cookie-kat hitelesítéshez, nyomkövetéshez és bizonyos felhasználói adatok – például webhely-preferenciák vagy online vásárlás esetén a kosár tartalma – gyűjtéséhez használják.*)

- ***Potenciálisan nemkívánatos alkalmazások és kémprogramok jelentése*** (*alapértelmezés szerint bekapcsolva*) – Jelölje be a Kémprogram-elhárító motor aktiválásához, illetve kémprogramok és vírusok kereséséhez. A kémprogramok külön kártevő kategóriát képviselnek: komoly biztonsági kockázatot jelentenek, mégis nagy részüket a felhasználók szándékosan telepítik. Javasoljuk, hogy tartsa bekapcsolva ezt a funkciót a számítógép megfelelő biztonsága érdekében.

- ***Potenciálisan nem kívánatos alkalmazások jelentése*** (*alapértelmezés szerint kikapcsolva*) – Jelölje be a kémprogramok: olyan speciális változatainak észleléséhez, amelyek ártalmatlanok amikor közvetlenül a gyártótól kapja azokat, de később kártékony

célokra is használhatók. Ezzel tovább növelheti a számítógép biztonságát. A szolgáltatás legitim programokat is letilthat, ezért a funkció alapállapotban ki van kapcsolva.

- ***Fájlok vizsgálata bezáráskor*** (*alapértelmezés szerint kikapcsolva*) – A program bezáráskor történő vizsgálatakor az AVG vizsgálja az aktív objektumokat (például alkalmazásokat, dokumentumokat) megnyitáskor és bezáráskor, így védelmet biztosít kifinomultabb vírusokkal szemben is.

- ***Cserélhető adathordozó rendszerindító szektorának vizsgálata*** (*alapértelmezés szerint bekapcsolva*)

- ***Heurisztikus elemzés használata*** (*alapértelmezés szerint bekapcsolva*) – A program heurisztikus elemzést használ a vizsgálat során, vagyis *dinamikusan emulálja a vizsgált objektum utasításait egy virtuális számítógépes környezetben*.

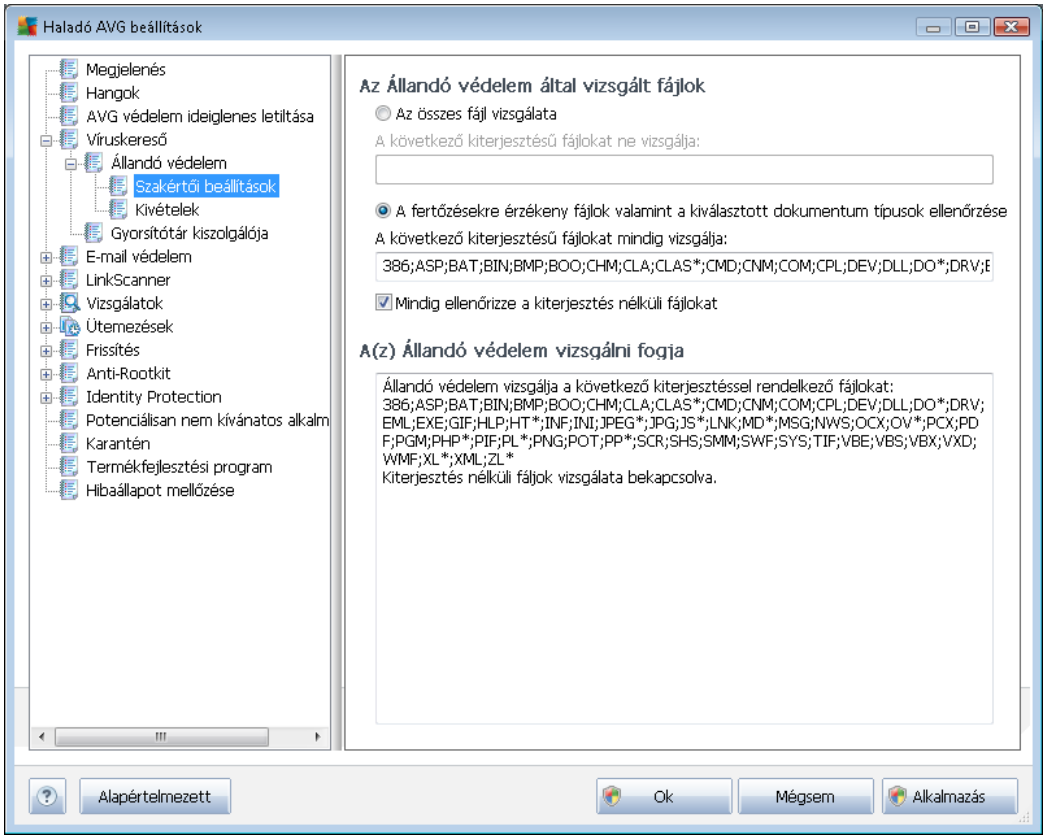
- ***Összes fenyegetés automatikus eltávolítása*** (*alapértelmezés szerint kikapcsolva*) – A program automatikusan javítja az észlelt fertőzéseket, ha van rá lehetőség. A nem javítható fertőzéseket a rendszer eltávolítja.

- ***Beállításjegyzékben hivatkozott fájlok vizsgálata*** (*alapértelmezés szerint bekapcsolva*) – Ezzel a paraméterrel beállíthatja, hogy az AVG vizsgálja meg a beállításjegyzékhez hozzáadott összes futtatható fájlt annak érdekében, hogy egy ismert fertőzés ne legyen végrehajtva a számítógép következő indításakor.

- ***Átfogó vizsgálat engedélyezése*** (*alapértelmezés szerint kikapcsolva*) – Bizonyos helyzetekben (*például extrém vészhelyzetben*) ezen lehetőség bejelölésével aktiválhatja a legátfogóbb vizsgálati algoritmust, amely a lehető legalaposabban vizsgálja át az esetlegesen fenyegetést jelentő objektumokat. Ne feledje, hogy ez a módszer meglehetősen időigényes.

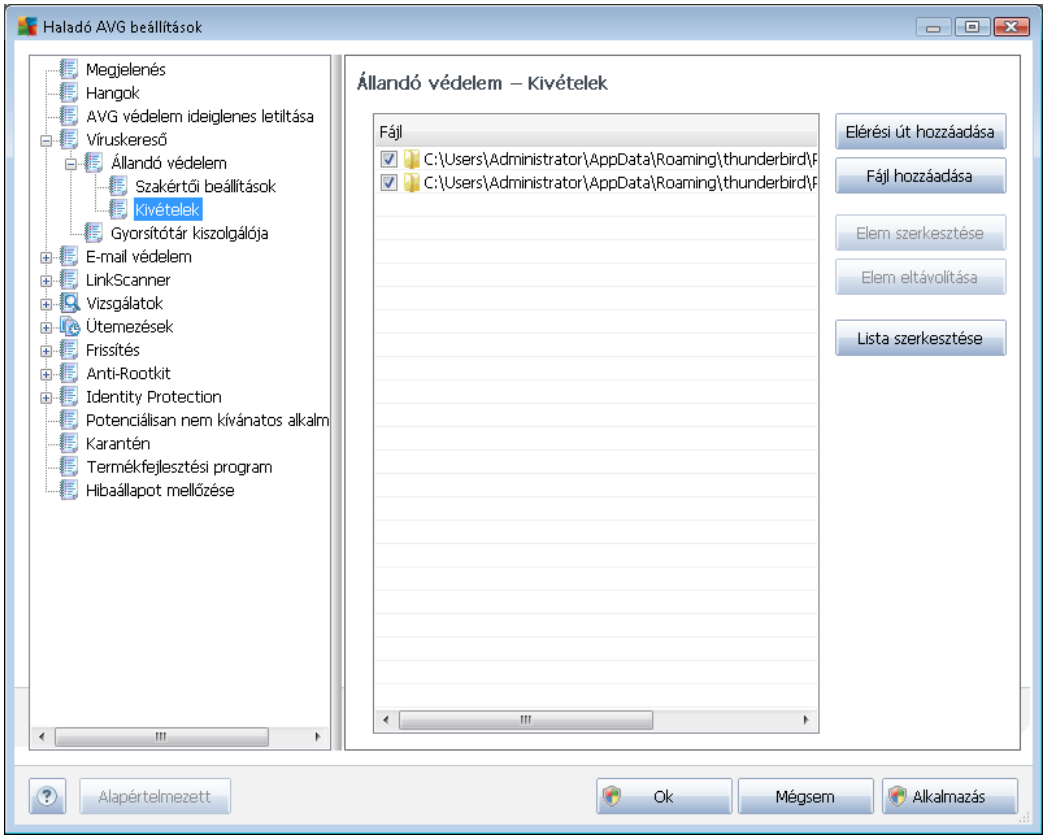
- ***Azonnali üzenetküldés védelem és P2P letöltési védelem engedélyezése*** (*alapértelmezés szerint bekapcsolva*) – Jelölje be ezt az elemet, ha meg szeretne bizonyosodni arról, hogy az azonnali üzenetküldésen alapuló kommunikáció (*például ICQ, MSN Messenger stb.*) és a P2P letöltések vírusmentesek.

Az állandó védelem által vizsgált fájlok párbeszédpanelen beállíthatja, hogy mely fájlokat (*megadott kiterjesztéssel rendelkezőket*) vizsgálja át a program:



Jelölje be a megfelelő jelölőnégyzetet aszerint, hogy ***Az összes fájl vizsgálatát*** vagy csak ***A fertőzésekre érzékeny fájlok valamint a kiválasztott dokumentum típusok ellenőrzését*** kívánja elvégezni. Ha az utóbbi lehetőséget választja, megadhatja, hogy minden fájlt vagy csak a megfertőzhető fájlokat ellenőrizze a program – továbbá meghatározhatja a kizárandó fájlok, illetve a mindenképpen vizsgálandó fájlok kiterjesztéseit is.

Az alábbi, ***Állandó védelem ellenőrzi*** nevű rész az aktuális beállításokat összegzi, és részletesen megjeleníti, hogy az ***Állandó védelem*** pontosan mit fog ellenőrizni.



Az ***Állandó védelem – Kivételek*** párbeszédpanelen lehetősége van az ***Állandó védelem*** ellenőrzése alól mentesülő fájlok és/vagy mappák megadására.

Ha nincs rá külön indoka, akkor nem ajánlott elemeket kihagyni a vizsgálatból.

Vezérlőgombok

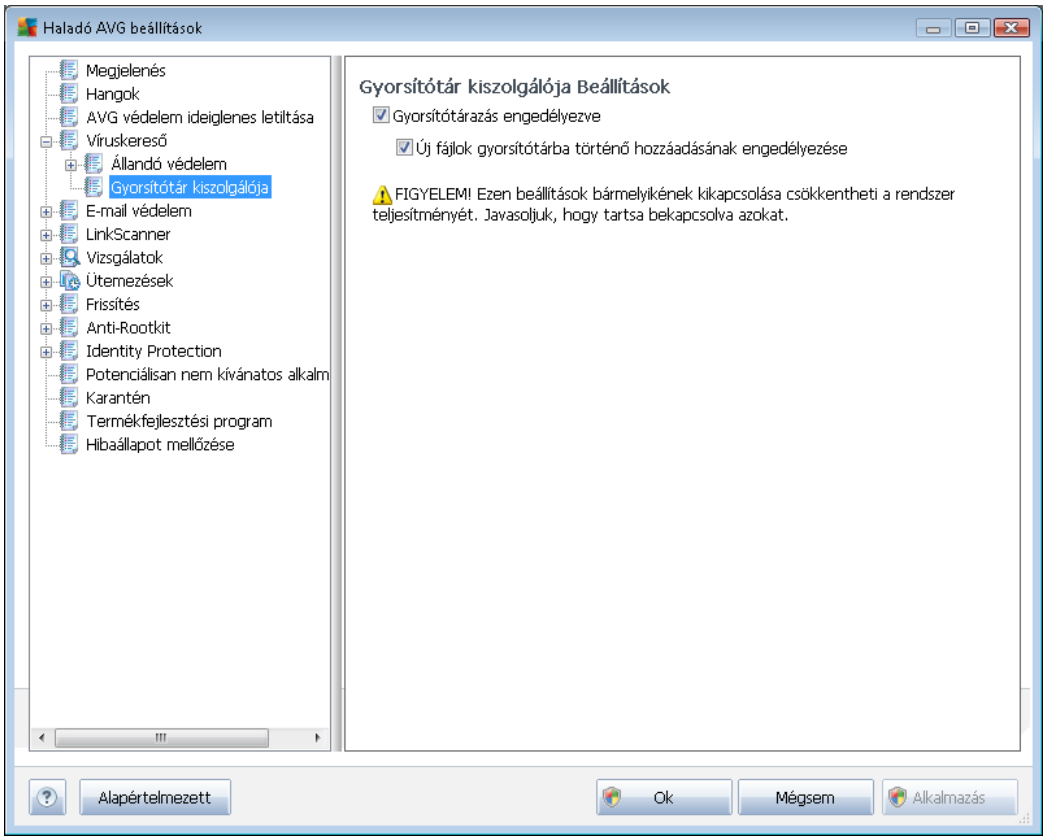
A párbeszédpanel a következő vezérlőgombokat tartalmazza:

- ***Elérési út hozzáadása*** – lehetőséget nyújt az ellenőrzés alól mentesülő könyvtárak megadására. A könyvtárakat a helyi lemezről választhatja ki (egyesével)
- ***Fájl hozzáadása*** – lehetőséget nyújt az ellenőrzés alól mentesülő fájlok megadására. A fájlokat a helyi lemezről választhatja ki (egyesével)
- ***Elem szerkesztése*** – lehetőséget nyújt a kijelölt fájl vagy mappa elérési útjának szerkesztésére
- ***Elem eltávolítása*** – lehetőséget nyújt a kijelölt elem elérési útjának törlésére a listából
- ***Lista szerkesztése*** – Lehetővé teszi a meghatározott kivételek teljes listájának szerkesztését egy új párbeszédpanelen, amely egy általános szövegszerkesztőként

működik

9.4.2. Gyorsítótár-kiszolgáló

A ***Gyorsítótár-kiszolgáló beállítások*** párbeszédpanel az **AVG Internet Security 2012** vizsgálatainak felgyorsítására szolgáló gyorsítótár-kiszolgáló műveletekre vonatkozik:



Ez gyűjti és tárolja a megbízható fájlokkal kapcsolatos adatokat (*egy fájl akkor minősül megbízhatónak, ha egy megbízható forrás digitális aláírásával rendelkezik*). Ezeket a fájlokat a program automatikusan biztonságosnak tekinti, nem szükséges ismét átvizsgálni őket, így ezeket át is ugorja a program a vizsgálatok során.

A ***Gyorsítótár-kiszolgáló beállítások*** párbeszédpanelen a következő lehetőségek érhetők el:

- ***Gyorsítótárazás engedélyezve*** (*alapállapotban bekapcsolva*) - törölje a jelölőnégyzetet a ***Gyorsítótár-kiszolgáló*** kikapcsolásához és a tár törléséhez. Vegye figyelembe, hogy a vizsgálat csökkentheti a számítógép teljesítményét, mivel a rendszer minden használatban lévő fájlt megvizsgál.

- ***Új fájlok gyorsítótárba történő hozzáadásának engedélyezése*** (*alapállapotban bekapcsolva*) - törölje a jelölőnégyzetet, ha nem szeretne több fájlt hozzáadni a gyorsítótárhoz. A rendszer megőrzi a gyorsítótárazott fájlokat a vírusadatbázis következő frissítéséig, illetve a szolgáltatás kikapcsolásáig használja azokat.

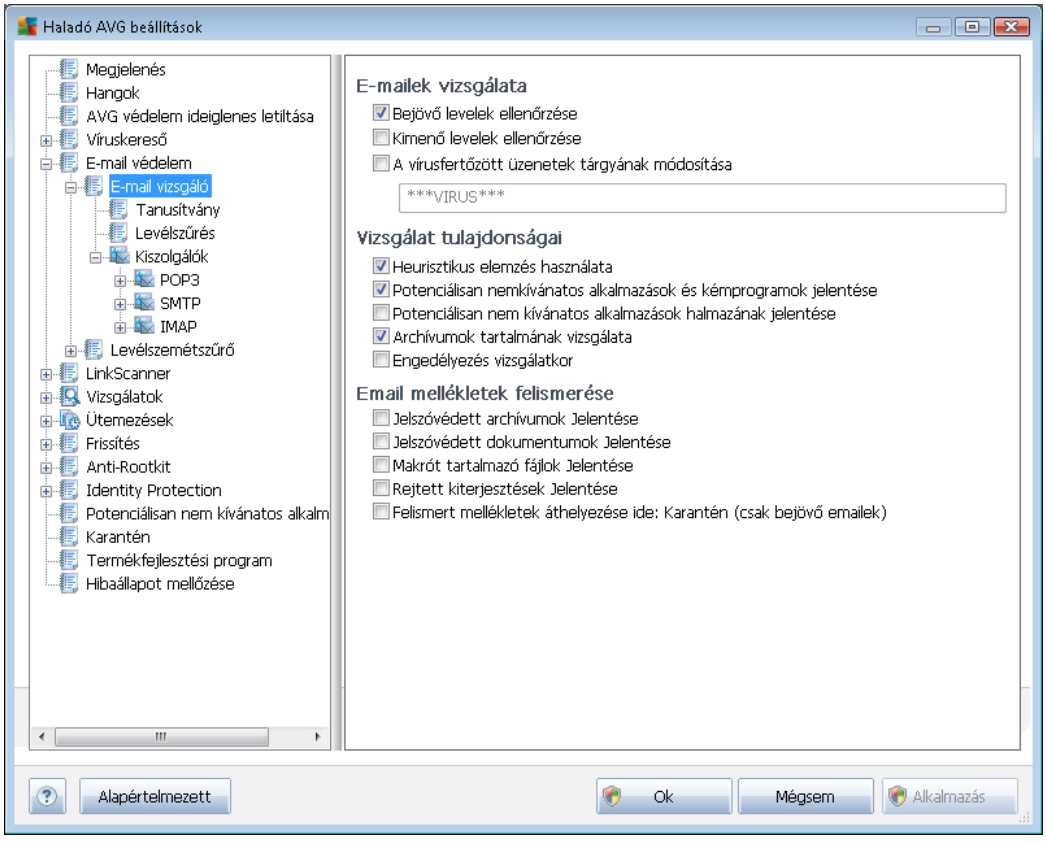
Hacsak nincsen rá nagyon nyomós indoka, azt javasoljuk, hogy tartsa meg az alapértelmezett beállítást, és hagyja bekapcsolva mindkét lehetőséget. Ellenkező esetben jelentősen csökkenhet a rendszer sebessége és teljesítménye.

9.5. E-mail védelem

Az ***E-mail védelem*** részben szerkesztheti az E-mail vizsgáló és a Levélszemétszűrő részletes konfigurációját:

9.5.1. E-mail vizsgáló

Az ***E-mail vizsgáló*** panel három részből áll:



E-mailek vizsgálata

Ezen a részen a következő alapbeállításokat adhatja meg a bejövő és/vagy kimenő üzenetekre:

- ***Bejövő e-mailek ellenőrzése*** (*alapállapotban bekapcsolva*) - használja a levelezőprogram érkező összes e-mail üzenet vizsgálatának be- vagy kikapcsolásához
- ***Kimenő e-mailek ellenőrzése*** (*alapállapotban kikapcsolva*) - használja a levelezőprogramból kimenő összes e-mail üzenet vizsgálatának be- vagy kikapcsolásához
- ***Vírusfertőzött üzenetek tárgyának módosítása*** (*alapállapotban kikapcsolva*) - ha értesítést szeretne kapni arról, hogy a vizsgált e-mail üzenet fertőzött, akkor jelölje be ezt

az elemet és adja meg a kívánt szöveget a szövegmezőben. A szöveg ekkor minden egyes fertőzött e-mail tárgyához hozzá lesz adva a könnyebb felismerhetőség és szűrés érdekében. A használatra javasolt alapérték a ***VÍRUS***.

Vizsgálat tulajdonságai

Ezen a részen meghatározhatja, hogy az e-mailek miként legyenek ellenőrizve:

- ***Heurisztika használata*** (*alapállapotban bekapcsolva*) – jelölje be a heurisztikus észlelési módszer használatához e-mail üzenetek vizsgálatakor. Ha ez az opció be van kapcsolva, akkor a mellékleteket nem csak kiterjesztés alapján szűrheti, hanem a tényleges tartalmuk alapján is. A szűrést beállíthatja a Levélszűrés panelen.

- ***Potenciálisan nemkívánatos programok és kémprogramok jelentése***- (*alapállapotban bekapcsolva*) - jelölje be a Kémprogram-elhárító motor aktiválásához, illetve kémprogramok és vírusok kereséséhez. A kémprogramok külön kártevő kategóriát képviselnek: komoly biztonsági kockázatot jelentenek, mégis nagy részüket a felhasználók szándékosan telepítik. Javasoljuk, hogy tartsa bekapcsolva ezt a funkciót a számítógép megfelelő biztonsága érdekében.

- ***Potenciálisan nem kívánatos alkalmazások jelentése*** (*alapállapotban kikapcsolva*) - jelölje be ezt a jelölőnégyzetet a kémprogramok speciális változatainak észleléséhez: olyan programok kereséséhez, amelyek ártalmatlanok, de később kártékony célokra használhatók. Ezzel tovább növelheti a számítógép biztonságát. A szolgáltatás legitim programokat is letilthat, ezért a funkció alapállapotban ki van kapcsolva.

- ***Archívumok tartalmának vizsgálata***(*alapállapotban bekapcsolva*) - jelölje be olyan archívumok tartalmának vizsgálatához, amelyek emailhez vannak csatolva.

- ***Átfogó vizsgálat engedélyezése*** (*alapállapotban kikapcsolva*) - bizonyos esetekben (*például, ha arra gyanakszik, hogy egy vírus vagy egy exploit megfertőzte*), akkor jelölje be ezt az opciót a legátfogóbb vizsgálati algoritmus bekapcsolásához, amely a számítógép nehezen fertőzhető részeit is ellenőrzi a biztonság kedvéért. Ne feledje, hogy ez a módszer meglehetősen időigényes.

Email mellékletek felismerése

Ezen a részen beállíthat további jelentéseket olyan fájlokról, melyek esetlegesen veszélyesek vagy gyanúsak. Vegye figyelembe, hogy semmilyen figyelmeztető ablak nem jelenik meg, csak egy tanúsító üzenet lesz hozzáadva az email üzenethez, és minden jelentés az E-mail vizsgáló panelen lesz megtalálható:

- ***Jelszóval védett archívumok jelentése*** – archívumok (*ZIP, RAR stb.*) melyek jelszóval védettek, nem lehet vizsgálni. Jelölje be az opciót ezen fájlok poteciálisan veszélyesnek minősítéséhez.

- ***Jelszóval védett dokumentumok jelentése*** - a jelszóval védett dokumentumokat nem lehet vizsgálni. Jelölje be az opciót ezen fájlok potenciálisan veszélyesnek minősítéséhez!

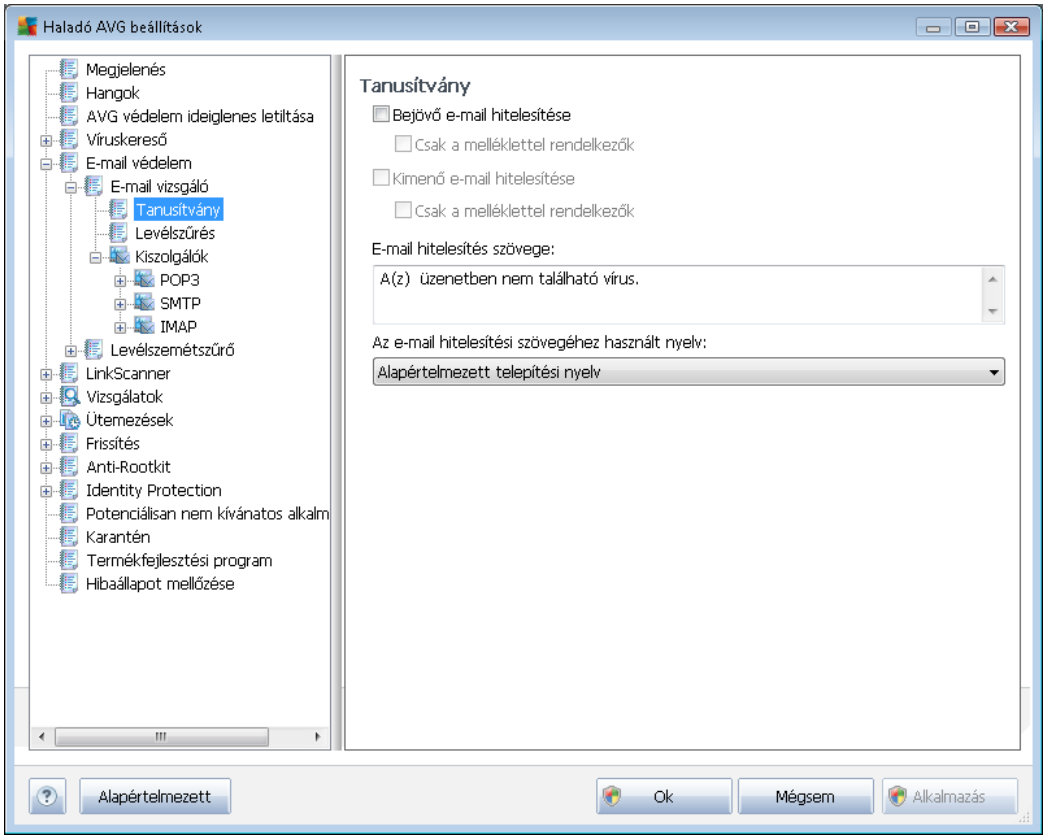
- ***Makrókat tartalmazó fájlok jelentése*** – a makró előre meghatározott műveleti lépések

folyamata, mely bizonyos feladatokat könnyít meg a felhasználó számára (az *MS Word makrók például széleskörben ismertek*). Azonban mint ilyen, a makró potenciálisan veszélyes utasításokat is tartalmazhat, ezért jelölje be ezt az opciót a makrófájlok gyanúsnak minősítéséhez!

- ***Rejtett kiterjesztések jelentése*** - a rejtett kiterjesztésű fájlok olyan gyanús "valami.txt.exe" futtatható fájlok is lehetnek, melyek ártatlan "valami.txt" szövegfájloknak álcázzák magukat. Jelölje be ezt az opciót a fájlok gyanúsnak minősítéséhez.

- ***Mellékletek áthelyezése karanténba*** - döntse el, hogy szeretne-e tájékozatást kapni e-mailben a jelszóvédett archívumokról, jelszóvédett dokumentumokról, makrókat tartalmazó fájlokról és/vagy fájlokról rejtett kiterjesztéssel, melyek egy ellenőrzött e-mailhez vannak csatolva. Ha ilyen üzenet lesz azonosítva a vizsgálat során, akkor döntse el, hogy az Karanténba kerüljön-e.

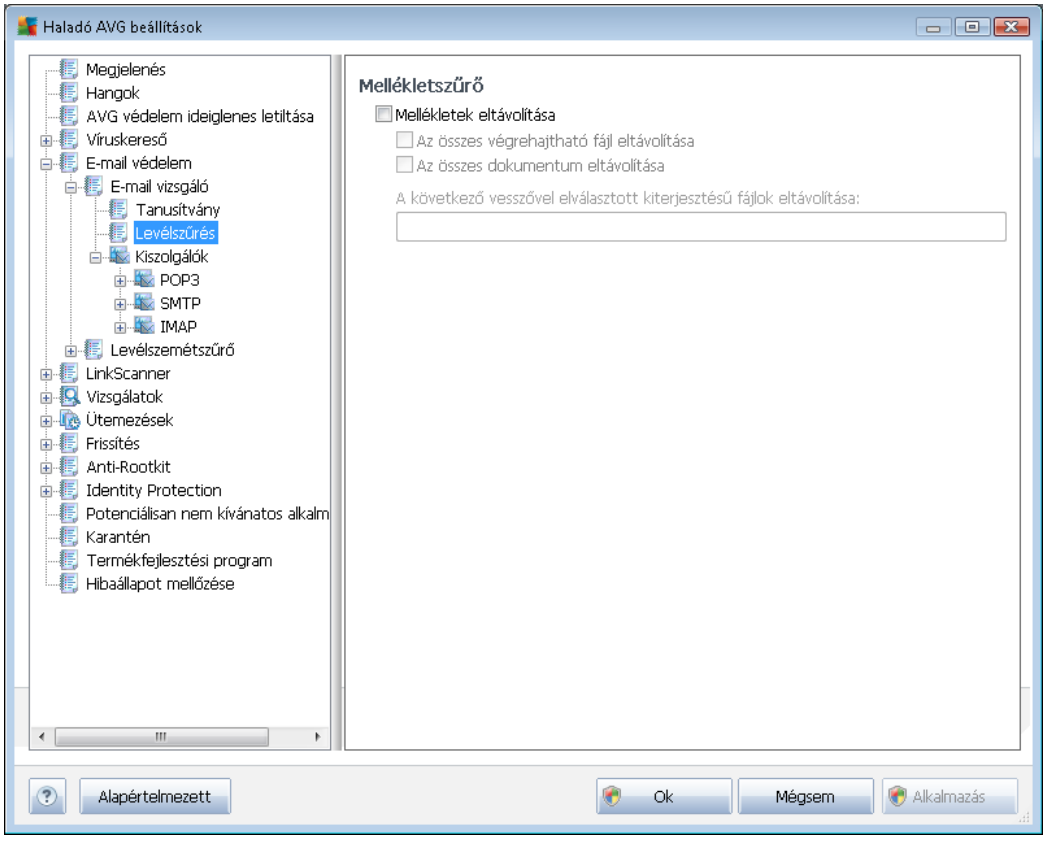
A ***Tanúsítás*** párbeszédpanelen bejelölheti az adott jelölőnégyzeteket, és így megadhatja, kér-e hitelesítést a bejövő levelek esetén (***Bejövő e-mail hitelesítése***) és/vagy a kimenő levelek esetén (***Kimenő e-mail hitelesítése***). Mindegyik lehetőség esetén később megadhatja a ***Csak a melléklettel rendelkezők*** paramétert, hogy a tanúsítványt csak a melléklettel rendelkező e-mail üzenetekhez adja hozzá a program:



Alapértelmezett állapotban a tanúsítvány szövege csak alapinformációkat tartalmaz, amely szerint *az üzenetben nem található vírus.* Azonban ez az információ bővíthető vagy módosítható az

igényeinek megfelelően: írja be a kívánt hitelesítési szöveget az ***E-mail hitelesítés szövege*** mezőbe. ***Az e-mail hitelesítési szövegéhez használt nyelv*** részben megadhatja a hitelesítés automatikusan létrehozott részének (*Az üzenetben nem található vírus*) nyelvét. Az üzenet ezután ezen a nyelven jelenik meg.

Megjegyzés: *Vegye figyelembe, hogy csak az alapértelmezett szöveg jelenik meg a kiválasztott nyelven, és a testreszabott szöveget nem fordítja le automatikusan a program.*



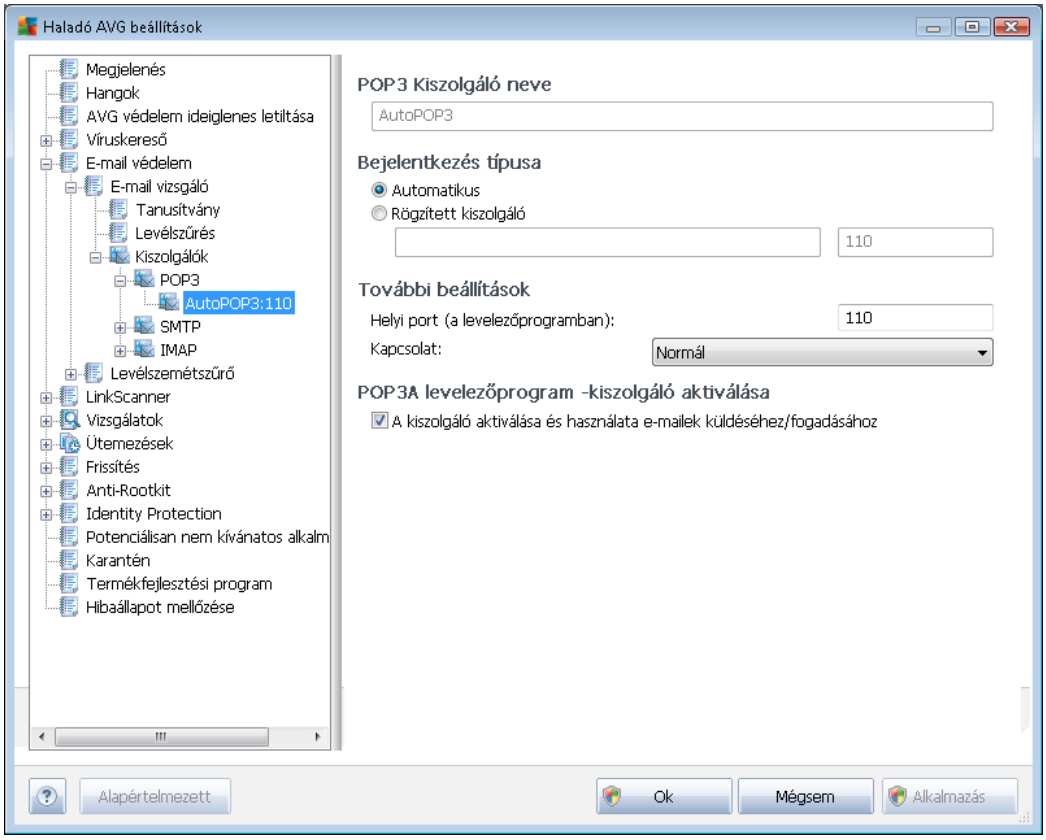
A ***Mellékletszűrő*** panel lehetővé teszi, hogy megadja az email csatolmányok vizsgálatának paramétereit. Alapállapotban a ***Mellékletek eltávolítása*** opció ki van kapcsolva. Ha úgy dönt, hogy bekapcsolja, akkor a fertőzött vagy potenciálisan veszélyesnek azonosított csatolmányok automatikusan el lesznek távolítva. Ha meg akarja határozni az eltávolítandó mellékletek különböző típusait, akkor válasszon az opciók közül:

- ***Az összes végrehajtható fájl eltávolítása*** - minden *.exe fájl törölve lesz
- ***Összes dokumentum eltávolítása*** - minden *.doc, *.docx, *.xls, *.xlsx fájl törölve lesz
- ***A vesszővel elválasztott kiterjesztésű fájlok eltávolítása*** - törli az összes meghatározott kiterjesztésű fájlt

A ***Kiszolgálók*** területen szerkesztheti az E-mail vizsgáló kiszolgálók paramétereit:

- POP3 kiszolgáló
- SMTP kiszolgáló
- IMAP kiszolgáló

Ezenkívül meghatározhat egy új kiszolgálót a bejövő és a kimenő levelek kezelésére. Ehhez kattintson az ***Új kiszolgáló hozzáadása*** gombra.



Ezen a panelen (*elérés:* ***Kiszolgálók / POP3***) megadhat egy új E-mail vizsgáló kiszolgálót a POP3 protokoll használatával a bejövő levelekhez:

- ***POP3 kiszolgáló neve*** - ebben a mezőben megadhatja az újonnan hozzáadott kiszolgálók nevét (*egy POP3 kiszolgáló hozzáadásához kattintson az egér jobb gombjával a bal oldali navigációs menü POP3 elemére*). Az automatikusan létrehozott "AutoPOP3" kiszolgálónál ez a mező ki van kapcsolva.
- ***Bejelentkezés típusa*** - megadja, hogy az E-mail vizsgáló milyen módszert határozzon a bejövő levelek levelezési kiszolgálójának meghatározására:

- ***Automatikus*** – a bejelentkezés az e-mail ügyfélprogram beállításainak megfelelően automatikusan megtörténik.

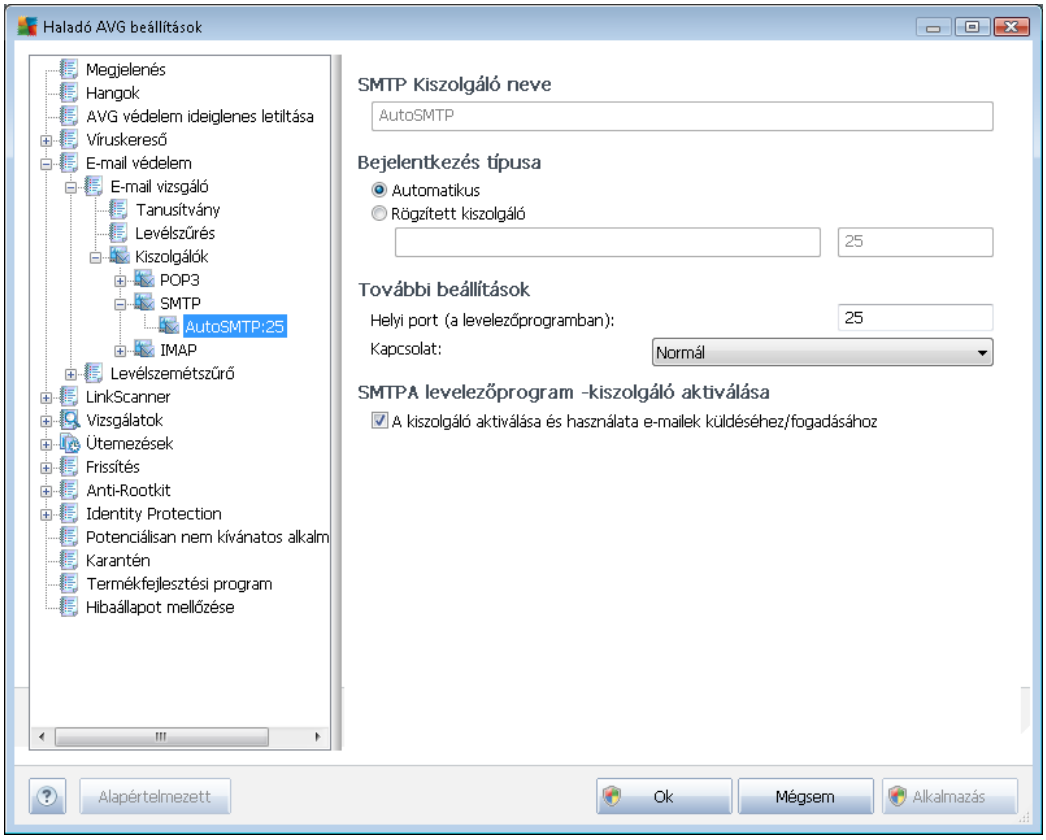
- ***Fix kiszolgáló*** – Ebben az esetben a program mindig az itt megadott kiszolgálót fogja használni. Adja meg a levelezőkiszolgáló címét vagy nevét. A bejelentkezési név nem változik. A névnél tartománynevet (*például: pop.acme.com*) vagy IP-címet (*például: 123.45.67.89*) használhat. Ha a levelezési kiszolgáló nem a standard portot használja, akkor a portot is meg lehet adni, kettősponttal elválasztva a kiszolgálónév után (*például: pop.acme.com:8200*). A POP3 kommunikáció szabványos portja 110.

- ***További beállítások*** - további paramétereket adhat meg:

  - ***Helyi port*** - meghatározza azt a portszámot, amelyet a levelező program használni fog. Ezután a levelezőprogramban is ezt a portot kell beállítani a POP3 kommunikációhoz.

  - ***Kapcsolat*** - ebben a legördülő menüben meghatározhatja, hogy milyen kapcsolatot használjon a program (*normál/SSL/SSL alapértelmezett*). Ha az SSL kapcsolatot választja, az adatok titkosítva kerülnek továbbításra, annak a veszélye nélkül, hogy egy kívülálló nyomon követhetné vagy megfigyelhetné. Ez a funkció is csak akkor áll rendelkezésre, ha a levelezési kiszolgáló támogatja.

- ***Levelezőprogram POP3-kiszolgálójának aktiválása*** - jelölje be/törölje ezt az elemet a megadott POP3-kiszolgáló aktiválásához vagy kikapcsolásához



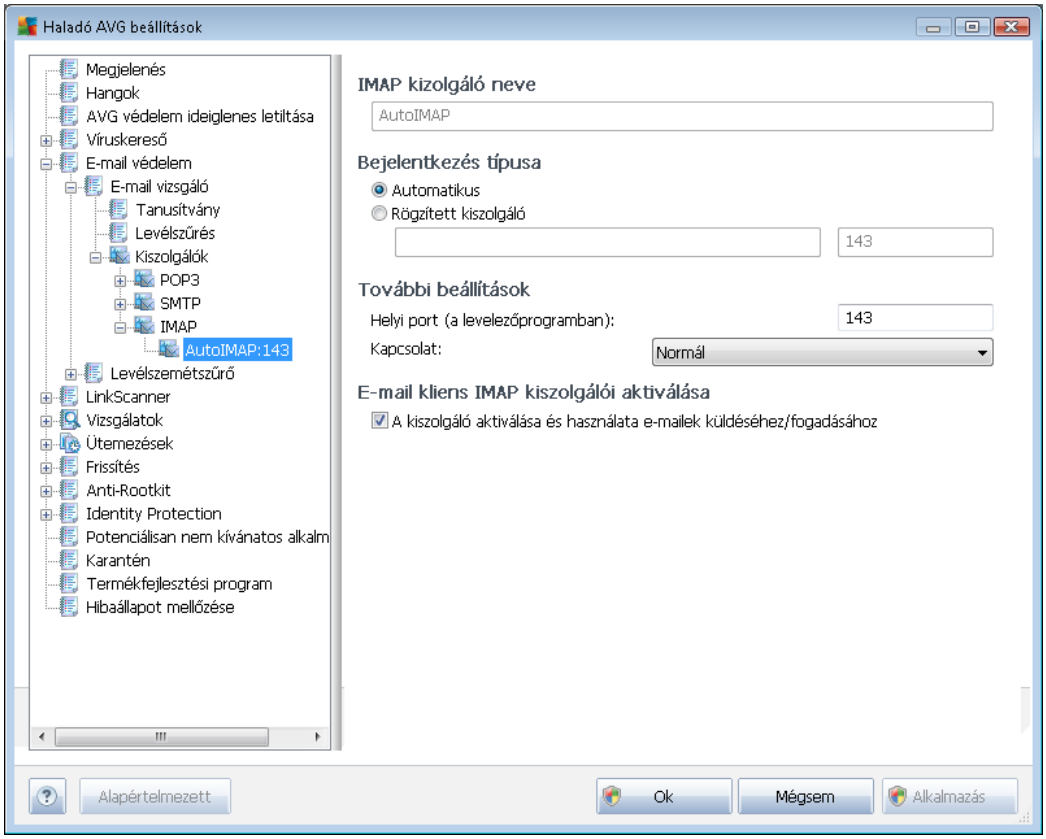
Ebben az ablakban (*megnyitva innen:* ***Kiszolgálók / SMTP***) megadhat egy új E-mail vizsgáló kiszolgálót az SMTP protokoll használatával a kimenő levelekhez:

- ***SMTP kiszolgáló neve*** - ebben a mezőben megadhatja az újonnan hozzáadott kiszolgálók nevét (*egy SMTP kiszolgáló hozzáadásához kattintson az egér jobb gombjával a bal oldali navigációs menü SMTP elemére*). Az automatikusan létrehozott "AutoSMTP" kiszolgálónál ez a mező ki van kapcsolva.
- ***Bejelentkezés típusa*** - megadja, hogy az E-mail vizsgáló milyen módszert használjon a kimenő levelek levelezési kiszolgálójának meghatározásához:
  - ***Automatikus*** – a bejelentkezés az e-mail ügyfélprogram beállításainak megfelelően automatikusan megtörténik
  - ***Fix kiszolgáló*** - ebben az esetben a program mindig az itt megadott kiszolgálót fogja használni. Adja meg a levelezőkiszolgáló címét vagy nevét. A névnél tartománynevet (*például, smtp.acme.com*), illetve IP-címet (*például, 123.45.67.89*) használhat. Ha a levelezési kiszolgáló nem a standard portot használja, akkor a portot is meg lehet adni, kettősponttal elválasztva a kiszolgálónév után (*például: smtp.acme.com:8200*). Az SMTP-kommunikáció szabványos portja a 25-ös.
- ***További beállítások*** - további paramétereket adhat meg:

- ***Helyi port*** - meghatározza azt a portszámot, amelyet a levelező program használni fog. Ezután a levelezőprogramban is ezt a portot kell beállítani az SMTP kommunikációhoz.

- ***Kapcsolat*** - ebben a legördülő menüben meghatározhatja, hogy milyen kapcsolatot használjon a program (*normál/SSL/SSL alapértelmezett*). Ha az SSL kapcsolatot választja, az adatok titkosítva kerülnek továbbításra, annak a veszélye nélkül, hogy egy kívülálló nyomon követhetné vagy megfigyelhetné a levelek tartalmát. Ez a funkció csak akkor áll rendelkezésre, ha a célként megadott levelezési kiszolgáló támogatja.

- ***Levelezőprogram SMTP-kiszolgálójának aktiválása*** – jelölje be/törölje ezt a jelölőnégyzetet a megadott SMTP-kiszolgáló aktiválásához vagy kikapcsolásához



Ebben az ablakban (megnyitva innen: ***Kiszolgálók / IMAP***) megadhat egy új E-mail vizsgáló kiszolgálót az IMAP protokoll használatával a kimenő levelekhez:

- ***IMAP kiszolgáló neve*** - ebben a mezőben megadhatja az újonnan hozzáadott kiszolgálók nevét (*egy IMAP kiszolgáló hozzáadásához kattintson az egér jobb gombjával a bal oldali navigációs menü IMAP elemére*). Az automatikusan létrehozott "AutoIMAP" kiszolgálónál ez a mező ki van kapcsolva.

- ***Bejelentkezés típusa*** - megadja, hogy az E-mail vizsgáló milyen módszert használjon a kimenő levelek levelezési kiszolgálójának meghatározásához:

- ***Automatikus*** – a bejelentkezés az e-mail ügyfélprogram beállításainak megfelelően automatikusan megtörténik

- ***Fix kiszolgáló*** - ebben az esetben a program mindig az itt megadott kiszolgálót fogja használni. Adja meg a levelezőkiszolgáló címét vagy nevét. A névnél tartománynevet (*például, smtp.acme.com*), illetve IP-címet (*például, 123.45.67.89*) használhat. Ha a levelezési kiszolgáló nem a standard portot használja, akkor a portot is meg lehet adni, kettősponttal elválasztva a kiszolgálónév után (*például: imap.acme.com:8200*). Az IMAP kommunikáció szabványos portja: 143.

- ***További beállítások*** - további paramétereket adhat meg:

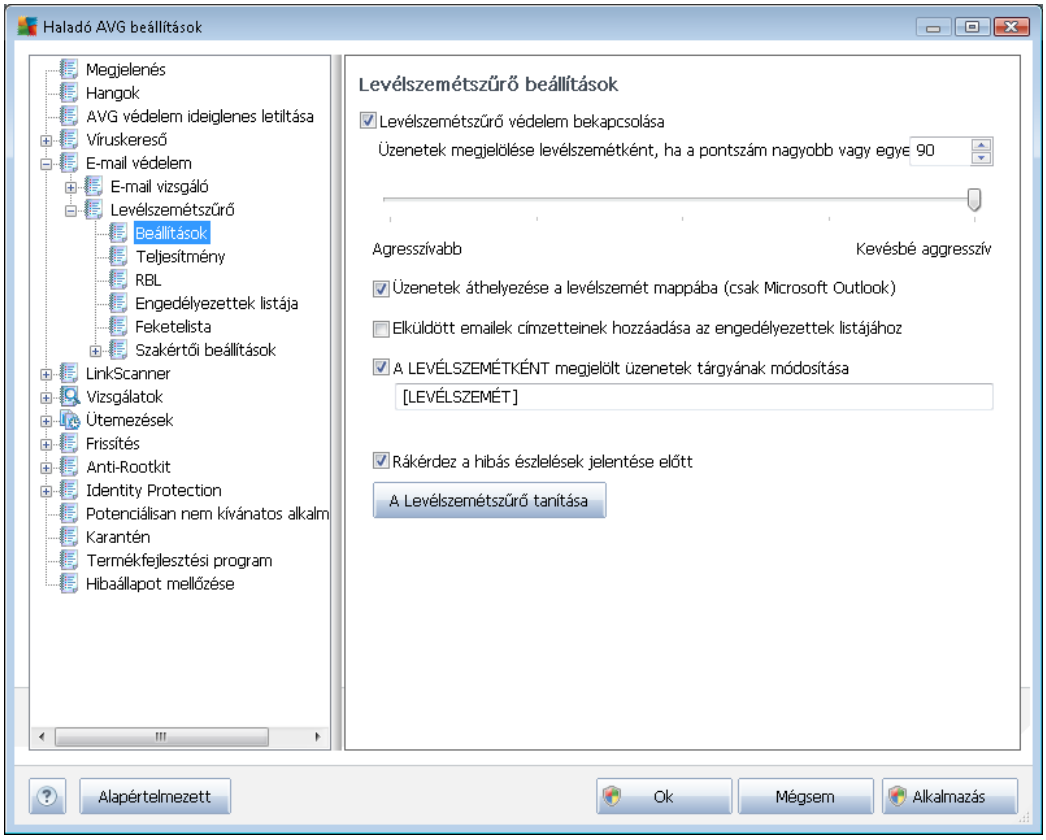
  - ***Helyi port*** - meghatározza azt a portszámot, amelyet a levelező program használni fog. Ezután a levelezőprogramban is ezt a portot kell beállítania az IMAP kommunikációhoz.

  - ***Kapcsolat*** - ebben a legördülő menüben meghatározhatja, hogy milyen kapcsolatot használjon a program (*normál/SSL/SSL alapértelmezett*). Ha az SSL kapcsolatot választja, az adatok titkosítva kerülnek továbbításra, annak a veszélye nélkül, hogy egy kívülálló nyomon követhetné vagy megfigyelhetné a levelek tartalmát. Ez a funkció csak akkor áll rendelkezésre, ha a célként megadott levelezési kiszolgáló támogatja.

- ***Levelezőprogram IMAP-kiszolgálójának aktiválása*** - jelölje be/törölje ezt a jelölőnégyzetet a megadott IMAP-kiszolgáló aktiválásához vagy kikapcsolásához

9.5.2. Levélszemétszűrő

Itt megadhatja a téma szövegét.



A ***Levélszemétszűrő beállítások*** párbeszédpanelen használja a ***Levélszemétszűrő védelem bekapcsolása*** jelölőnégyzetet a levélszemétszűrő engedélyezéséhez/letiltásához. Az opció alapállapotban be van kapcsolva, és javasoljuk, hogy ne is módosítsa azt.

A következőkben szigorú vagy kevésbé szigorú pontozási módszereket is beállíthat. ***A Levélszemétszűrő*** többféle dinamikus ellenőrzési módszer segítségével minden üzenethez társít egy pontszámot (*amely azt jelzi, hogy mennyire hasonlít az üzenet tartalma a LEVÉLSZEMÉTHEZ*) Szabályozhatja az ***Üzenet megjelölése levélszemétként, ha a pont nagyobb mint*** beállítást: vagy közvetlen érték megadásával vagy a csúszka jobbra vagy balra történő mozgatásával (*50-90 között állítható*).

Általában az 50-90 közötti értékeket javasoljuk, azonban ha bizonytalan, akkor használja a 90-et. Íme egy általános áttekintés a pontozási küszöbökről:

- ***80-90 közötti érték*** – A levélszeméthez hasonlító üzeneteket kiszűri a program. Ez a beállítás bizonyos üzeneteket tévesen is kiszűrhet.
- ***60-79 közötti érték*** - Ez már meglehetősen szigorú értéknek számít. A program minden olyan üzenetet kiszűr, amelyik levélszemét lehet. Valószínűleg egyes, nem levélszemét üzeneteket is kiszűr a rendszer.
- ***50-59 közötti érték*** – Nagyon szigorú konfiguráció. A nem levélszemét üzeneteket ugyanolyan valószínűséggel szűri ki a program, mint a levélszemetet. Ezen értékek

használatát nem javasoljuk normál használatra.

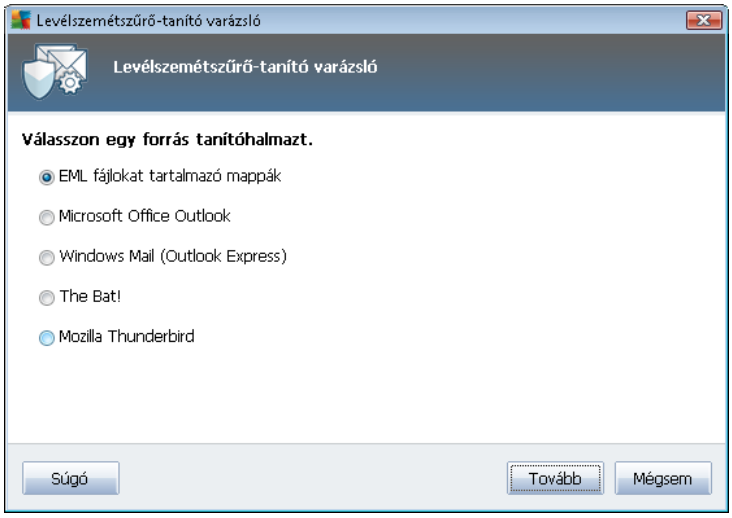
A ***Levélszemétszűrő beállítások*** párbeszédpanelen meghatározhatja, hogyan kezelje a program a levélszemétnek minősülő e-mail üzeneteket:

- ***Üzenet áthelyezése a levélszemét mappába*** - jelölje be, hogy a levélszemetek automatikusan átkerüljenek a levelezőprogram levélszemét mappájába.
- ***Az elküldött emailek címzettjeinek hozzáadása az engedélyezettek listájához*** - jelölje be ezt a négyzetet a kimenő emailek címzettjeinek megerősítéséhez, illetve annak megerősítéséhez, hogy a tőlük érkezett emailek megbízhatóak;
- ***A LEVÉLSZEMÉTKÉNT megjelölt üzenetek tárgyának módosítása*** – Jelölje be, ha az összes levélszemétként azonosított üzenetet meg szeretné jelölni egy bizonyos szóval vagy karakterrel a tárgy mezőben. A kívánt szöveget megadhatja az aktivált szövegmezőben.
- ***Rákérdez a hibás észlelések jelentése előtt*** – Csak akkor jelenik meg, ha a telepítési folyamat során beleegyezett a termékfejlesztési programban való részvételbe. Ha igen, azzal engedélyezte az észlelt fenyegetések jelentését az AVG részére. A jelentés automatikusan történik. Bejelölheti ezt a jelölőnégyzetet, ha azt szeretné, hogy a rendszer rákérdezzen az észlelt levélszemetek AVG-nek történő jelentése előtt (annak érdekében, hogy megállapíthassa, hogy az üzenet valóban levélszemétnek minősül-e).

Vezérlőgombok

A Levélszemétszűrő tanítása gomb megnyitja a Levélszemétszűrő-tanító varázslót, melyet részletesen a következő fejezetben ismerhet meg.

A ***Levélszemétszűrő-tanító varázsló*** az első lépésnél megkéri Önt, hogy válassza ki a tanításhoz használandó emaileket. Általában olyan emaileket érdemes használni, melyek helytelenül lettek LEVÉLSZEMÉTKÉNT megjelölve, vagy olyanakat, melyek annak minősülnek, de nem lettek kiszűrve.



A következő beállítások közül lehet választani:

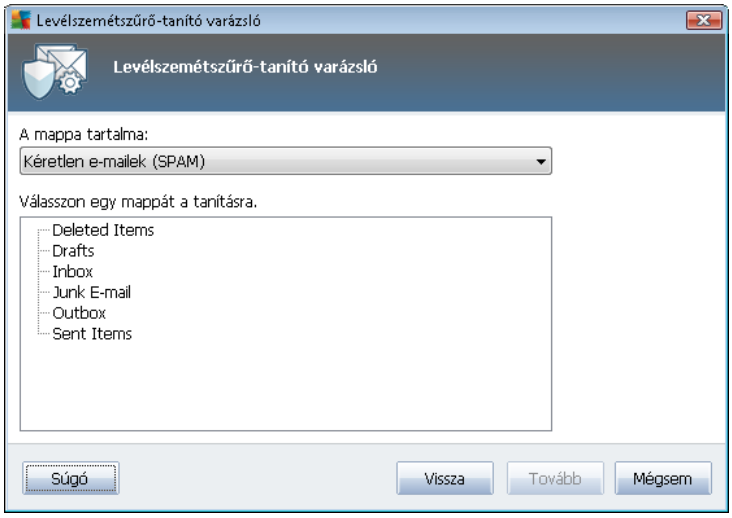
- ***Bizonyos email kliens*** - ha a felsoroltak közül valamelyik e-mail klienst használja (*MS Outlook, Outlook Express, The Bat!*), akkor egyszerűen válassza ki a megfelelő típust.
- ***EML fájlokat tartalmazó mappa*** - ha más email klienst használ, akkor először mentse az üzeneteket egy adott mappába (*.eml formátumban*), vagy győződjön meg arról, hogy tudja, hogy a levelezőprogram melyik mappában tárolja az emaileket. Ezután válassza az ***EML fájlokat tartalmazó mappa*** opciót, mely lehetővé teszi, hogy megkeresse a kívánt mappát a következő lépésben

A gyorsabb és egyszerűbb tanítási folyamat érdekében érdemes előre rendezni az emaileket külön mappákban, így majd csak a tanításhoz szükséges mappát kell kiválasztania (kéretlen vagy nem levélszemét emailek). Azonban ez nem kötelező, mivel az emaileket később is szűrheti.

Válassza ki a kívánt opciót, majd kattintson a ***Tovább*** gombra.

Az itt megjelenő panel az előző választástól függően változhat.

EML fájlokat tartalmazó mappák



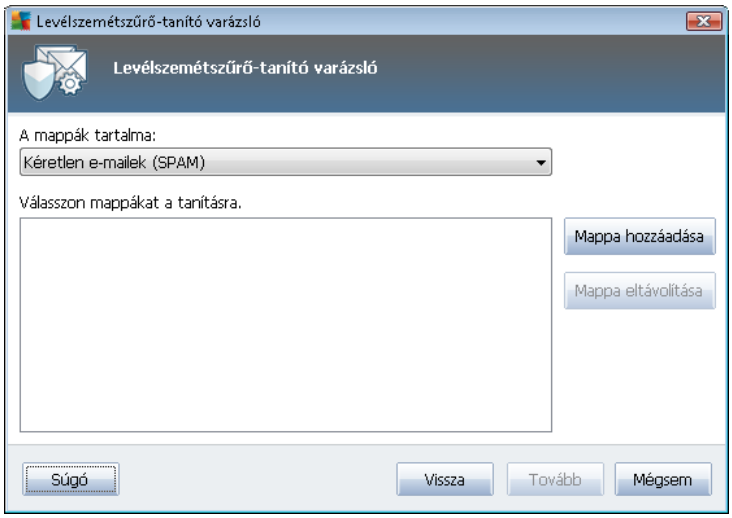
Ezen a panelen keresse meg a tanításhoz használandó mappát az üzenetekkel. Nyomja meg a ***Mappa hozzáadása*** gombot azon mappa megkereséséhez, mely tartalmazza az .eml fájlokat (*mentett emaileket*). A kiválasztott mappa megjelenik a panelen.

A ***Mappa tartalma*** legördülő menüből válassza ki az egyik opciót: hasznos üzenet (*NORMÁL*) vagy kéretlen üzenet (*LEVÉLSZEMÉT*). Vegye figyelembe, hogy az üzeneteket a következő lépésben szűrni tudja, ezért a mappáknak nem kötelező kizárólag tanításhoz használandó emaileket tartalmaznia. A szükségtelen mappákat is eltávolíthatja a listából a ***Mappa eltávolítása*** gombra történő kattintással.

Ha végzett, akkor kattintson a ***Tovább*** gombra, és lépjen az Üzenetszűrési beállítások részhez.

Bizonyos email kliens

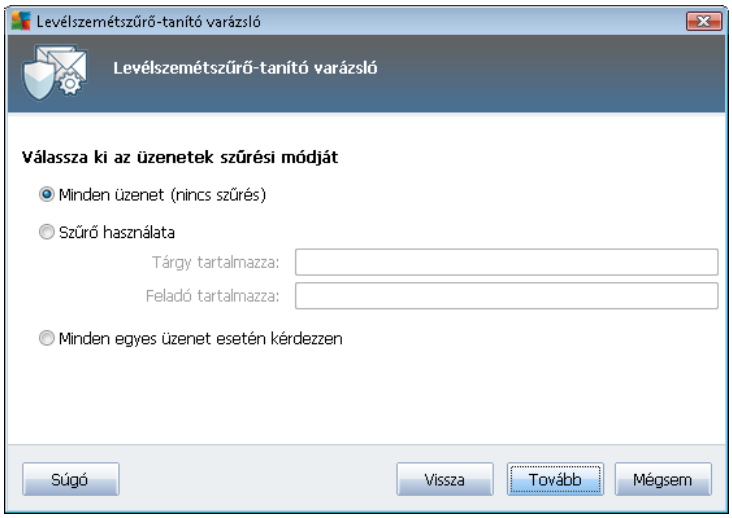
Miután megerősíti valamelyik opciót, egy új panel fog megjelenni.



Megjegyzés: *a Microsoft Office Outlook esetében először ki kell választania az MS Office Outlook profilt.*

A ***Mappa tartalma*** legördülő menüből válassza ki az egyik opciót: hasznos üzenet (*NORMÁL*) vagy kéretlen üzenet (*LEVÉLSZEMÉT*). Vegye figyelembe, hogy az üzeneteket a következő lépésben szűrni tudja, ezért a mappáknak nem kötelező kizárólag tanításhoz használandó emaileket tartalmaznia. Az adott email kliens elérési útvonala megjelenik a könyvtárfán. Keresse meg a kívánt mappát és jelölje ki az egérrel.

Ha végzett, akkor kattintson a ***Tovább*** gombra, és lépjen az Üzenetszűrési beállítások részhez.

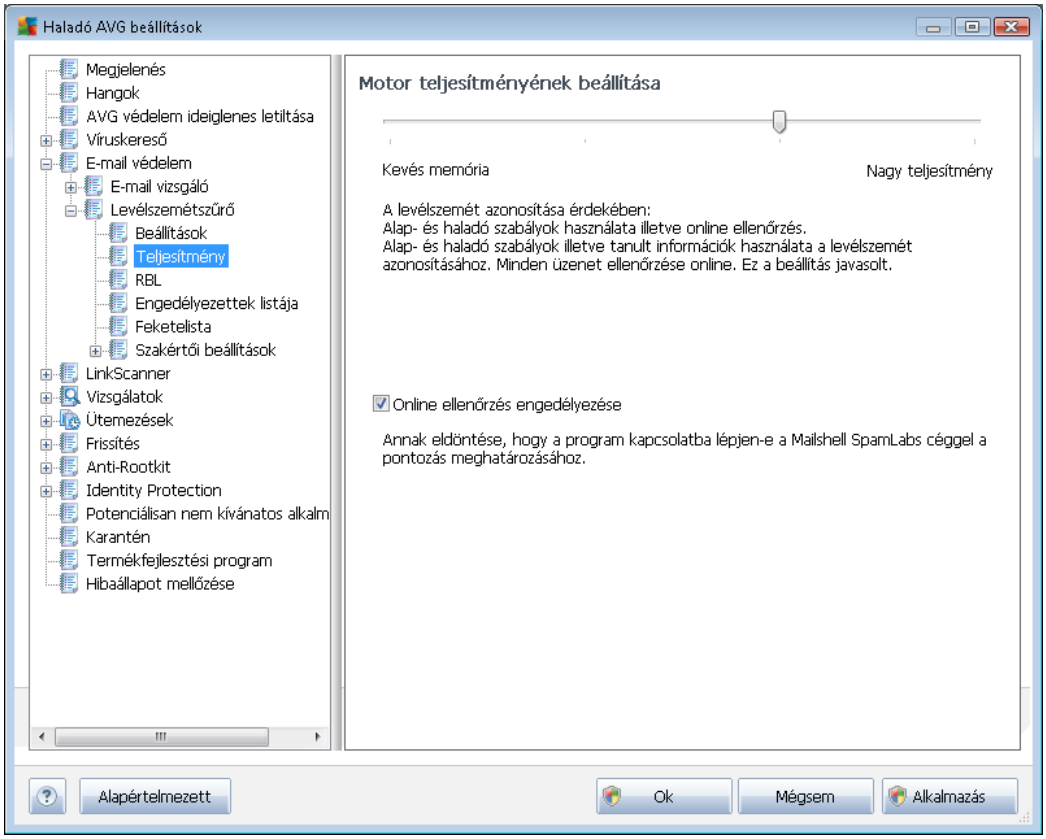


Ezen a panelen beállíthatja az üzenetek szűrését.

- ***Minden üzenet (nincs szűrés)*** – Ha biztos benne, hogy a kiválasztott mappa kizárólag tanításhoz használandó üzeneteket tartalmaz, akkor válassza a ***Minden üzenet (nincs szűrés)*** lehetőséget.
- ***Szűrő használata*** – A haladó szűréshez válassza a ***Szűrő használata*** lehetőséget. Beírhat egy, a tárgy vagy a feladó mezőben keresendő szót (*nevet*), szótöredéket vagy mondatot. Minden, a megadott kritériumoknak pontosan megfelelő üzenetet a rendszer további értesítés nélkül felhasznál a tanításhoz. Ha mindkét szövegmezőt kitölti, de csak az egyik feltételnek felel meg az üzenet, a program akkor is felhasználja.
- ***Minden egyes üzenet esetén kérdezzen*** – Ha nem biztos, hogy a mappában csak a kívánt típusú üzenetek találhatók, és ezért azt szeretné, hogy a Varázsló minden egyes e-mailnél rákérdezzen, felhasználja-e az üzenetet *(hogy eldönthesse, felhasználja-e azt tanításhoz vagy sem)*, akkor válassza a ***Minden egyes üzenet esetén kérdezzen*** lehetőséget.

Ha a megfelelő opciót kiválasztotta, akkor kattintson a ***Tovább*** gombra. Ez a panel csak tájékoztatásra szolgál, és azt mutatja, hogy a varázsló készen áll a folyamatra. A tanítás indításához kattintson a ***Tovább*** gombra újra. A tanítás elindul a korábban megadott feltételeknek megfelelően.

A ***Motor teljesítményének beállítása*** párbeszédpanelen (*a bal oldali navigációs tábla* ***Teljesítmény*** *eleméből érhető el*) megadhatja a ***Levélszemétszűrő*** összetevő teljesítménybeállításait:



Mozgassa a csúszkát balra vagy jobbra a teljesítményszint módosításához a ***Kevés memória*** / ***Nagy teljesítmény*** módok között.

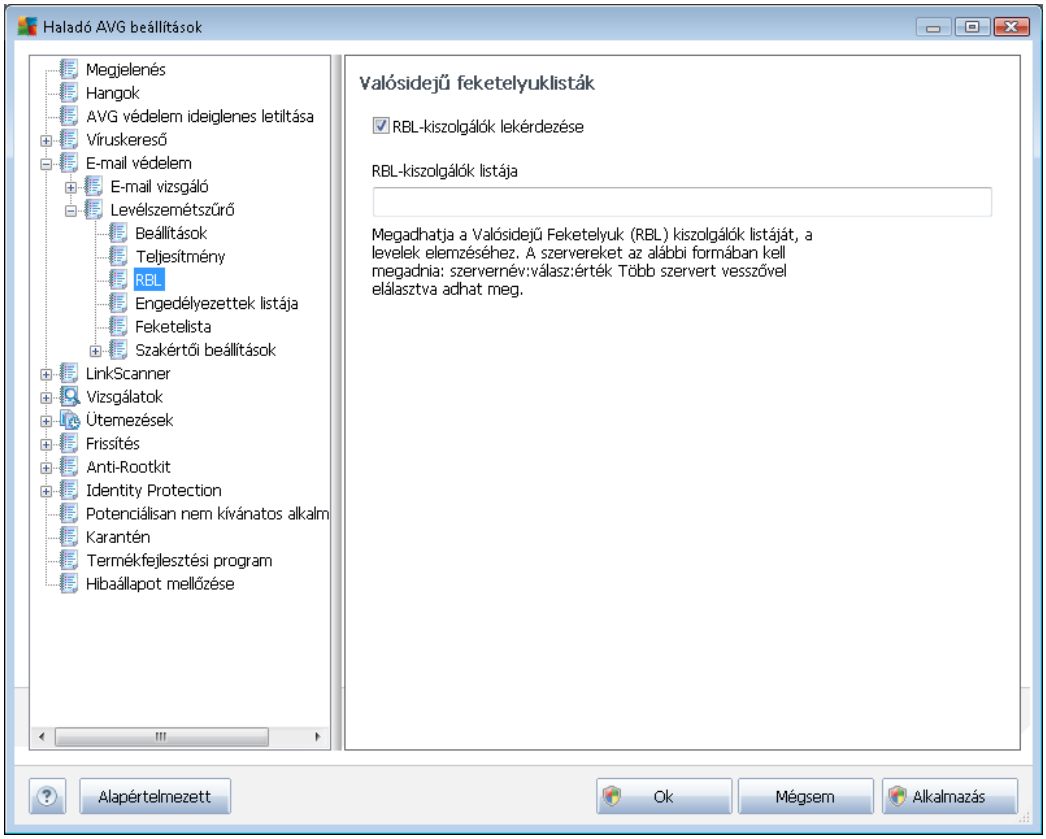
- ***Kevés memória*** – A program nem használ szabályokat a levélszemét ellenőrzése során. Kizárólag a betanított adatok alapján történik az azonosítás. Ez a mód nem ajánlott általános használatra, hacsak nem nagyon elavult a számítógép hardvert használ.

- ***Nagy teljesítmény*** – Ez a mód sok memóriát igényel. A vizsgálati folyamat során a levélszemét azonosításához a következő funkciókat használja a program: szabályok és levélszemét adatbázis-gyorsítótár, alap és haladó szabályok, levélszemétküldők IP-címei és adatbázisai.

Az ***Online ellenőrzés engedélyezése*** elem alapértelmezés szerint be van kapcsolva. Még pontosabb levélszemét azonosítást tesz lehetővé a Mailshell kiszolgálókkal való kommunikációnak köszönhetően, azaz azáltal, hogy vizsgált adatokat összeveti a Mailshell online adatbázisaival.

Általában érdemes megtartani az alapbeállításokat, és csak akkor módosítsa azokat, ha feltétlenül szükséges. A beállítások megváltoztatását csak haladó felhasználóknak ajánlunk!

Az ***RBL*** elem egy ***Valósidejű feketelyuklisták*** nevű szerkesztő párbeszédpanelt nyit meg, amelyen be- és kikapcsolhatja az ***RBL-kiszolgálók lekérdezése*** funkciót:

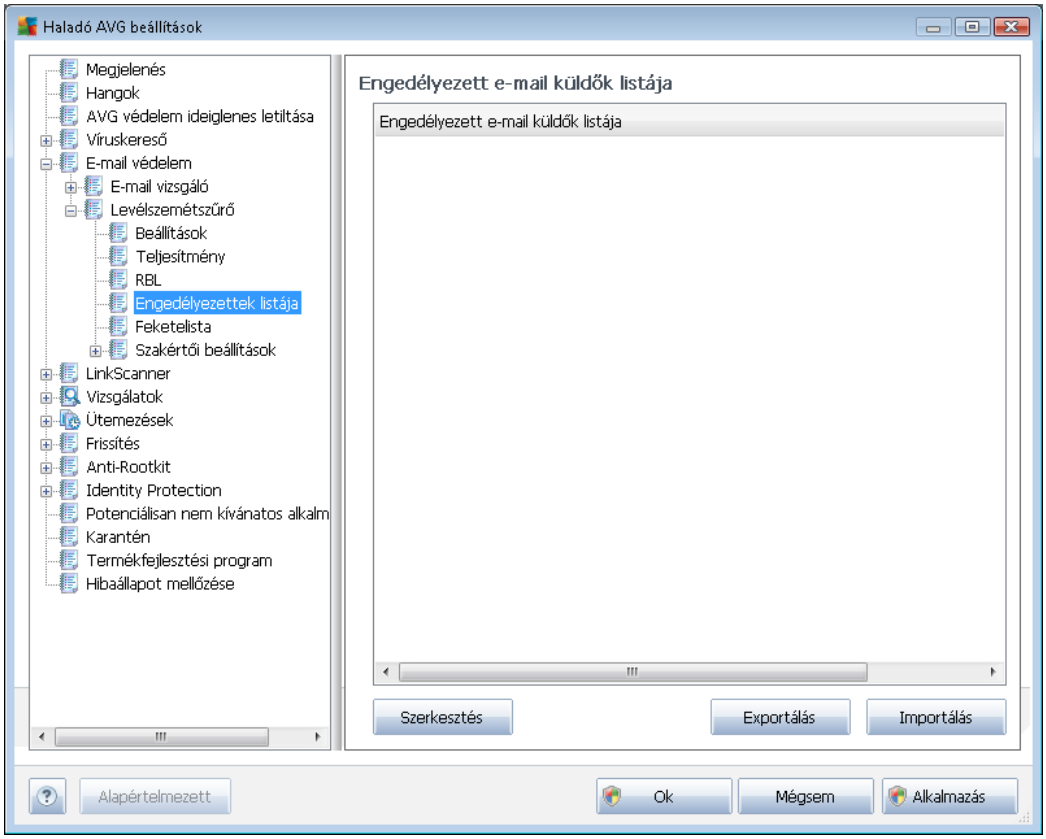


Az RBL (*valós idejű feketelyuklista*) kiszolgáló olyan tartománynév-kiszolgáló, amely egy nagy adatbázisban tárolja a világon ismertté vált levélszemétküldőket. Ha bekapcsolja ezt a funkciót, a program minden e-mailt összevet az RBL-kiszolgáló adatbázisával, és levélszemétként jelöli meg azokat, amelyek az adatbázis bármelyik bejegyzésével megegyeznek. Az RBL-kiszolgálók adatbázisába percek alatt bekerülnek a levélszemét-levelek ujjlenyomatai, ezért ez a legjobb és legpontosabb levélszemét-észlelési módszer. Ez a szolgáltatás különösen hasznos azoknak a felhasználóknak, akik nagy mennyiségű levélszemetet kapnak, mégpedig olyat, amit a Levélszemétszűrő motorja nem ismer fel.

Az ***RBL-kiszolgálók listája*** segítségével megadhatja, hogy mely RBL-kiszolgálókat kívánja használni (*ügyeljen arra, hogy a funkció engedélyezése esetén egyes rendszereknél és konfigurációknál lelassulhat az e-mail fogadás művelete, mivel minden egyes üzenetet össze kell vetni az RBL-kiszolgáló adatbázisával).*

A program nem küld személyes adatokat a kiszolgálónak.

Az ***Engedélyezettek listája*** elem megnyitja az ***Engedélyezett feladók listáját*** azon feladók e-mail címeinek és tartományneveinek globális listájával, amelyek üzenetei soha nem számítanaklevélszemétnek.



A szerkesztőfelületen összeállíthat egy listát azon feladókból, akik soha nem küldenének Önnek nem kívánatos üzeneteket (levélszemetet). A listába olyan teljes tartományneveket is felvehet (*pl. avg.com*), amelyekről soha nem fog levélszemetet kapni. Amint megvan a feladók és tartománynevek előkészített listája, megadhatja őket a következő módszerekkel: közvetlen bevitel, vagy a teljes címlista egyszerre történő importálása.

Vezérlőgombok

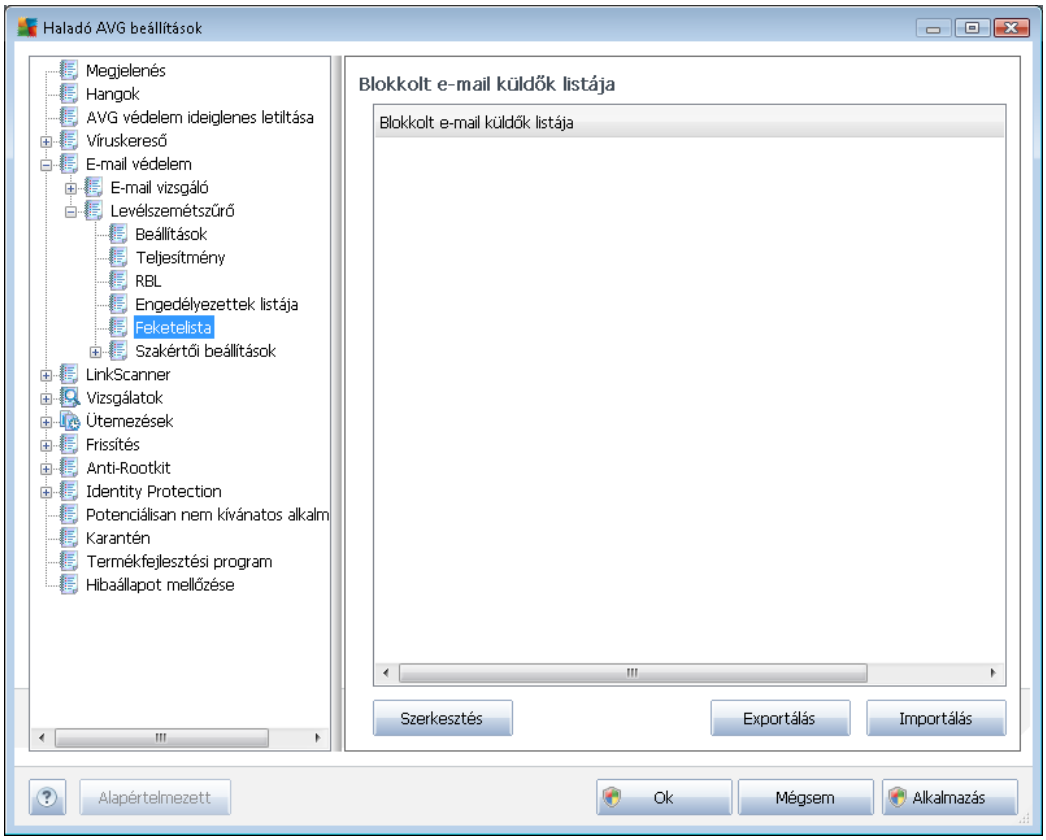
Az alábbi vezérlőgombok érhetők el:

- ***Szerkesztés*** - a gomb megnyomásával megnyit egy olyan párbeszédpanelt, ahol manuálisan megadhat egy címlistát (*használhatja a másolás és beillesztés módszerét is*). Soronként egy elemet (küldő vagy tartománynevet) illesszen be.

- ***Exportálás*** - ha valamilyen célból, például biztonsági mentés miatt exportálni szeretné a bejegyzéseket, akkor megteheti ezzel a gombbal. A program ekkor minden bejegyzést egy egyszerű szöveges fájlba másol.

- ***Importálás*** - ha az e-mail címeket és tartományneveket egy szöveges fájlba írta, ezzel a gombbal egyszerűen importálhatja a fájlt. A fájl kizárólag egyetlen elemet tartalmazhat (*cím, tartománynév*) soronként.

A ***Feketelista*** elem megnyitja a tiltott feladók e-mail címeinek és tartományneveinek globális listáját. Az ezekről a címekről érkező üzenetek mindig levélszemétnek számítanak.



Összeállíthat egy listát azon feladókból, akiktől nemkívánatos üzenetekre *(levélszemétre)* számíthat. A listába olyan teljes tartományneveket is felvehet (*például a levelszemetkuldovallalat.hu címet*), amelyekről várhatóan levélszemetet fog kapni. A felvett tartományba tartozó címekről érkező e-maileket mindig levélszemétként azonosítja a program. Amint megvan a feladók és tartománynevek előkészített listája, megadhatja őket a következő módszerekkel: közvetlen bevitel, vagy a teljes címlista egyszerre történő importálása.

Vezérlőgombok

Az alábbi vezérlőgombok érhetők el:

- ***Szerkesztés*** - a gomb megnyomásával megnyit egy olyan párbeszédpanelt, ahol manuálisan megadhat egy címlistát (*használhatja a másolás és beillesztés módszerét is*). Soronként egy elemet (*küldő vagy tartománynevet*) illesszen be.

- ***Exportálás*** - ha valamilyen célból, például biztonsági mentés miatt exportálni szeretné a bejegyzéseket, akkor megteheti ezzel a gombbal. A program ekkor minden bejegyzést egy egyszerű szöveges fájlba másol.

- ***Importálás*** - ha az e-mail címeket és tartományneveket egy szöveges fájlba írta, ezzel a gombbal egyszerűen importálhatja a fájlt.

A Haladó beállítások rész részletes beállítási lehetőségeket tartalmaz a Levélszemétszűrő összetevőhöz. Ezen beállítások módosítását csak haladó felhasználóknak ajánljuk. Jellemzően azon hálózati rendszergazdáknak, akiknek részletesen meg kell adniuk a levélszemétszűrő beállításait az e-mail kiszolgálók legjobb védelme érdekében. Ezért nincs külön súgó az egyes párbeszédablakokhoz, bár minden beállításhoz talál egy rövid leírást közvetlenül a felhasználói felület megfelelő részén.

Különösen javasoljuk, hogy ne változtassa meg ezen beállításokat, hacsak nincsen teljesen tisztában a Spamcatcher (MailShell Inc.) haladó beállításaival. A nem megfelelő módosítások gyenge teljesítményhez vagy az összetevő helytelen működéséhez vezethetnek.

Ha még mindig meg szeretné változtatni az Levélszemétszűrő beállításait haladó szinten, akkor kövesse a felhasználói felületen megjelenő utasításokat. Általában mindegyik párbeszédablakban egy adott szerkeszthető funckiót találhat - a leírás mindig megtalálható ugyanitt:

- ***Gyorsítótár*** - lenyomat, tartomány hírnév, LegitRepute

- ***Tanítás*** - maximum bejegyzés, automatikus tanítási küszöb, súlyozás

- ***Szűrés*** - nyelvi lista, országlista, engedélyezett IP-címek, blokkolt IP-címek, blokkolt országok, blokkolt karakterkészletek, hamisított feladók

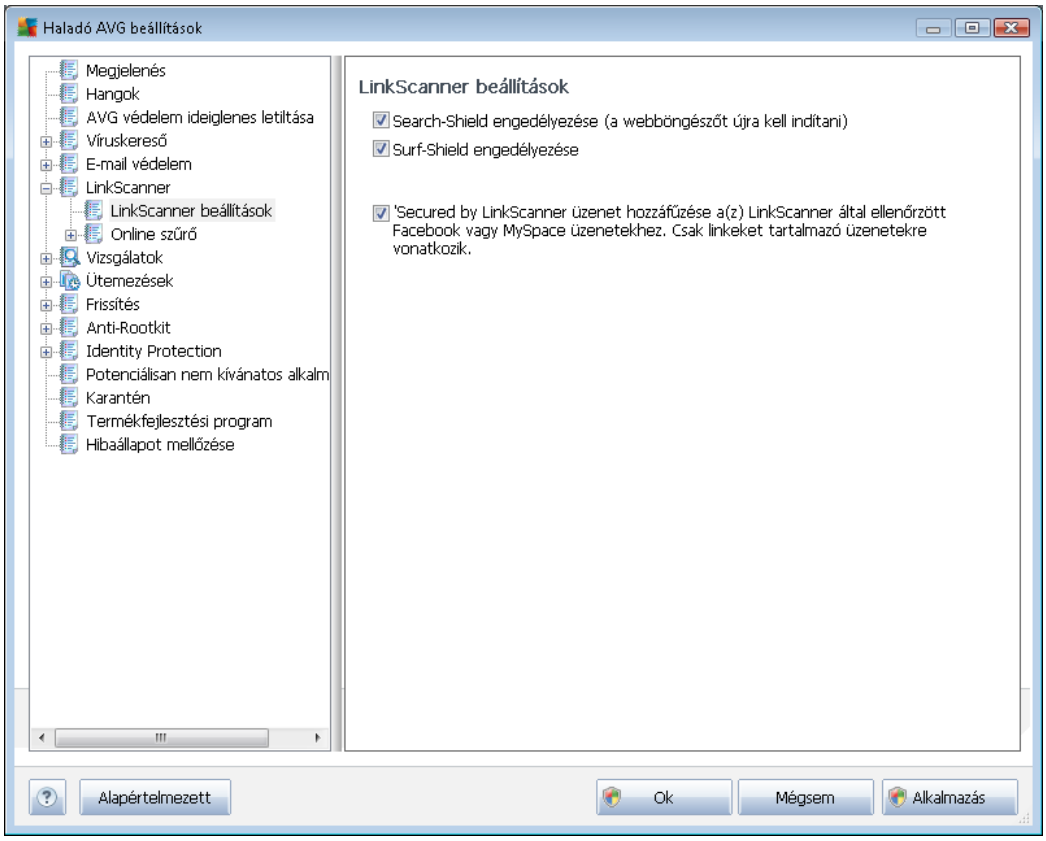
- ***RBL*** - Valósidejű feketelyuk lista kiszolgálók, több találat, küszöb, időtúllépés, maximum IP-k

- ***Internetkapcsolat*** – időtúllépés, proxykiszolgáló, proxy hitelesítése

9.6. LinkScanner

9.6.1. LinkScanner beállítások

A ***LinkScanner beállítások*** panel lehetővé teszi, hogy ki- és bekapcsolja a LinkScanner alapvető funkcióit:

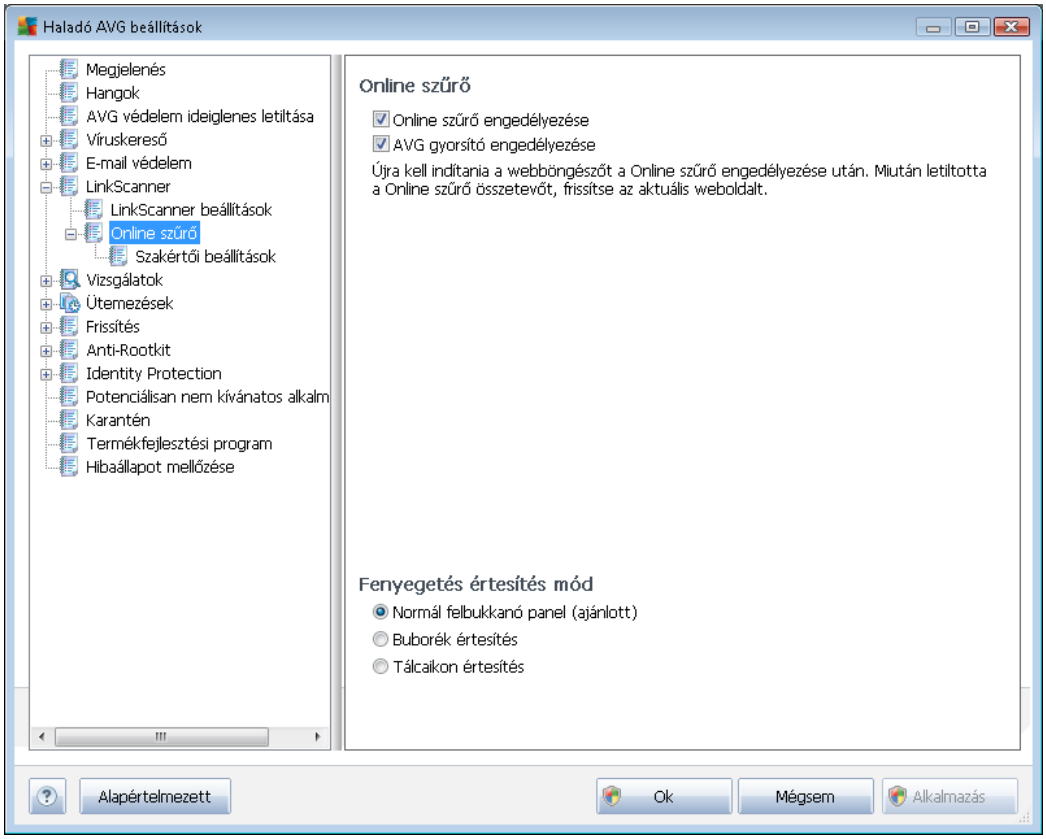


- ***Kereső védelem engedélyezése*** – (*alapállapotban bekapcsolva*): értesítések a következő keresőmotorok használatakor: Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg vagy SlashDot. A rendszer előzetesen ellenőrzi az adott webhelyek tartalmát.

- ***Böngészés védelem engedélyezése*** - (*alapállapotban bekapcsolva*): aktív (*valósidejű*) védelem kockázatos weboldalak ellen a hozzáférés során. Az ismert kártékony oldalak és veszélyes tartalmuk megjelenítése a webböngészőben, illetve *bármely más, HTTP-t használó alkalmazásban is* le lesz tiltva.

- ***'Secured by LinkScanner' üzenet hozzáadása ...*** - (*alapértelmezés szerint bekapcsolva*): jelölje be ezt az elemet, ha tanúsítási megjegyzést kíván hozzáfűzni a LinkScanner által ellenőrzött, hivatkozásokat tartalmazó azon üzenetekhez, amelyeket a Facebook és MySpace közösségi oldalakról küldött el.

9.6.2. Online szűrő



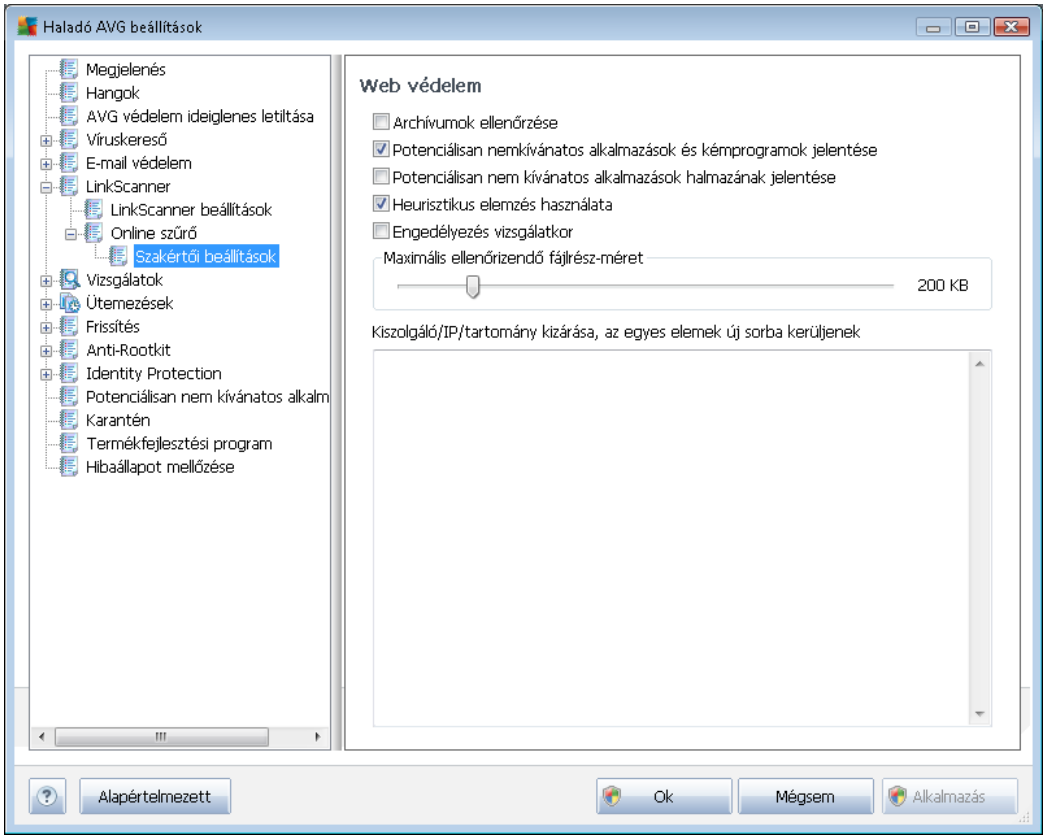
Az ***Online szűrő*** párbeszédpanel a következő beállítási lehetőségeket tartalmazza:

- ***Online szűrő engedélyezése*** *(alapértelmezés szerint bekapcsolva)* – Aktiválja/deaktiválja a teljes ***Online szűrő*** szolgáltatást. Az ***Online szűrő*** haladó beállításainak megadásához használja a következő, Webes védelem elnevezésű párbeszédpanelt.

- ***AVG Accelerator engedélyezése*** *(alapértelmezés szerint bekapcsolva)* – Aktiválja/deaktiválja az ***AVG Accelerator*** szolgáltatást, amely gördülékenyebbé teszi az online videolejátszást, és megkönnyíti a további letöltéseket.

Fenyegetés értesítés mód

A panel alsó részén válassza ki, hogy miként kíván értesítést kapni az észlelt fenyegetésekről: normál felbukkanó ablak, buborék értesítés vagy ikonjelzés a rendszerterületen.



A ***Web védelem*** ablakban szerkesztheti az összetevő beállításait a honlapok tartalmi vizsgálatának szempontjából. A szerkesztőfelület lehetővé teszi a következő alapvető opciók beállítását:

- ***Web védelem engedélyezése*** - ez az opció biztosítja, hogy az ***Online szűrő*** ellenőrizze a honlapok tartalmát. Ha az opció be van kapcsolva (*alapértelmezés szerint*), akkor a következő elemeket kapcsolhatja be és ki:
    - ***Archívumok ellenőrzése*** - (*alapállapotban kikapcsolva*): ellenőrzi a megjelenítendő oldalba ágyazott esetleges archívumok, tömörített fájlok tartalmát.
    - ***Potenciálisan nemkívánatos programok és kémprogramok jelentése –*** (*alapértelmezés szerint bekapcsolva*): jelölje be a Kémprogram-elhárító motor aktiválásához, valamint kémprogramok és vírusok kereséséhez. A kémprogramok külön kártevő kategóriát képviselnek: komoly biztonsági kockázatot jelentenek, mégis nagy részüket a felhasználók szándékosan telepítik. Javasoljuk, hogy tartsa bekapcsolva ezt a funkciót a számítógép megfelelő biztonsága érdekében.
    - ***Potenciálisan nem kívánatos alkalmazások jelentése*** - (*alapállapotban kikapcsolva*) - jelölje be ezt a jelölőnégyzetet a kémprogramok speciális változatainak észleléséhez: olyan programok kereséséhez, amelyek ártalmatlanok, de később kártékony célokra használhatók. Ezzel tovább növelheti a számítógép biztonságát. A szolgáltatás legitim programokat is letilthat, ezért a funkció alapállapotban ki van kapcsolva.

- ***Heurisztikus elemzés használata*** - (*alapállapotban bekapcsolva*): - a megjelenítendő oldal tartalmának ellenőrzése a heurisztikus elemzés módszerével (*a vizsgált objektum utasításainak dinamikus emulálása veszélytelen módon virtuális számítógépes környezetben*).

- ***Átfogó vizsgálat engedélyezése*** (*alapállapotban kikapcsolva*) - bizonyos esetekben (*például, ha arra gyanakszik, hogy a számítógépét egy vírus megfertőzte*), akkor jelölje be ezt az opciót a legátfogóbb vizsgálati algoritmus bekapcsolásához, amely a számítógép nehezen fertőzhető részeit is ellenőrzi a biztonság kedvéért. Ne feledje, hogy ez a módszer meglehetősen időigényes.

- ***Maximális ellenőrzendő fájlméret*** - ha beágyazott fájlok találhatók egy megjelenítendő weboldalban, akkor még azelőtt ellenőrizheti a tartalmukat, mielőtt azok letöltődnének a számítógépre. Azonban a nagy fájlok vizsgálata időbe telhet, és a weboldal betöltődése jelentősen lelassulhat. Használja a csúszkát az ***Online szűrővel*** vizsgálandó fájlok maximális méretének beállításához. Ha a letöltött fájl nagyobb a megadott méretnél, és az Online szűrő nem ellenőrzi, de természetesen Ön ilyenkor is védve van: ugyanis az esetleges fertőzést az ***Állandó védelem*** azonnal észleli.

- ***Kiszolgáló/IP/tartomány kizárása*** - a szövegmezőbe beírhatja egy szerver (*kiszolgáló, IP-cím, IP-cím maszkkal vagy URL*) pontos nevét vagy egy tartományt, amit az ***Online szűrőnek*** *nem kell ellenőriznie.* Csak olyan kiszolgálókat zárjon ki, amelyben teljesen biztos, hogy nem fognak veszélyes tartalmat nyújtani.

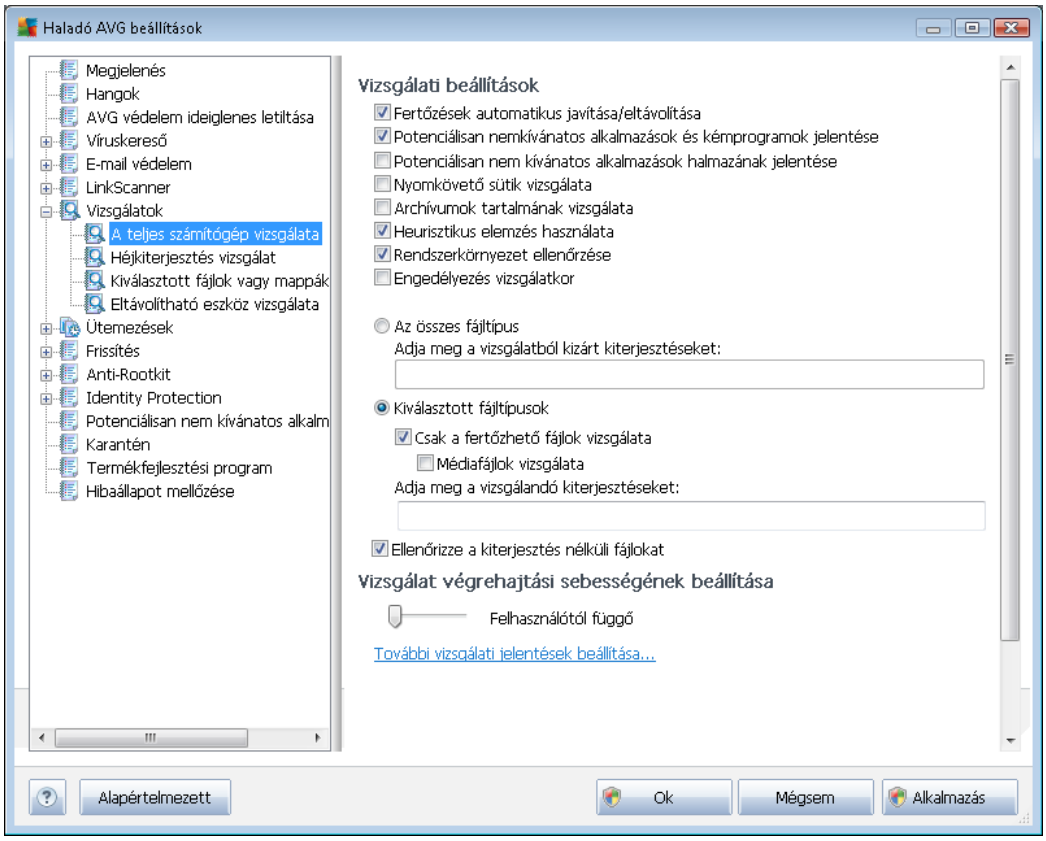
9.7. Vizsgálatok

A haladó vizsgálati beállítások négy kategóriára vannak osztva, és a szoftver gyártója által meghatározott bizonyos vizsgálati típusokra vonatkoznak:

- ***Számítógép teljes vizsgálata*** - előre beállított szolgáltatás a számítógép teljes vizsgálatához
- ***Héjkiterjesztés vizsgálat*** – egy adott objektum vizsgálata közvetlenül a Windows Intézőből
- ***Adott fájlok vagy mappák vizsgálata*** – a számítógép kiválasztott területeinek előre meghatározott, általános vizsgálata
- ***Cserélhető eszköz vizsgálata*** – a számítógéphez csatlakoztatott cserélhető eszközök vizsgálata

9.7.1. Vizsgálat a teljes számítógépen

A ***Számítógép teljes vizsgálata*** lehetővé teszi a szoftvergyártó által előre meghatározott vizsgálatok paramétereinek szerkesztését, Számítógép teljes vizsgálata:



Vizsgálati beállítások

A ***Vizsgálati beállítások*** részen a vizsgálati paraméterek listáját találhatja, melyeket tetszőlegesen be- és kikapcsolhat:

- ***Fertőzés automatikus javítása/eltávolítása*** (*alapállapotban bekapcsolva*) - ha vírust talál a vizsgálat során, akkor automatikusan javítja, amennyiben ez lehetséges. Ha a fertőzött fájl nem javítható automatikusan, az objektum át lesz helyezve a Karanténba.

- ***Potenciálisan nemkívánatos programok és kémprogramok jelentése*** - (*alapállapotban bekapcsolva*) - jelölje be a Kémprogram-elhárító motor aktiválásához, illetve kémprogramok és vírusok kereséséhez. A kémprogramok külön kártevő kategóriát képviselnek: komoly biztonsági kockázatot jelentenek, mégis nagy részüket a felhasználók szándékosan telepítik. Javasoljuk, hogy tartsa bekapcsolva ezt az opciót, mivel így növelheti a számítógép biztonságát.

- ***Potenciálisan nem kívánatos alkalmazások halmazának jelentése*** (*alapértelmezés szerint kikapcsolva*) – jelölje be ezt a jelölőnégyzetet a kémprogramok speciális

változatainak észleléséhez: olyan programok kereséséhez, amelyek ártalmatlanok, de később kártékony célokra használhatók. Ezzel tovább növelheti a számítógép biztonságát. A szolgáltatás legitim programokat is letilthat, ezért a funkció alapállapotban ki van kapcsolva.

- ***Nyomkövető sütik vizsgálata*** (*alapállapotban kikapcsolva*) - ez az opció a Kémprogram-elhárító összetevőben meghatározza, hogy a vizsgálat során felismert sütik törölve legyenek-e (*a HTTP sütiket hitelesítéshez, nyomkövetéshez és bizonyos adatok gyűjtéséhez használják a felhasználókról, pl. honlap preferenciák vagy online vásárlás során a kosár tartalma*).

- ***Archívumok tartalmának vizsgálata*** (*alapállapotban kikapcsolva*) - ez a paraméter meghatározza, hogy a vizsgálat ellenőrizze-e az archívumban tárolt fájlokat, pl. ZIP, RAR.

- ***Heurisztika használata*** (*alapállapotban bekapcsolva*) - a heurisztikus elemzés (*a vizsgált objektum utasításainak dinamikus emulációja egy virtuális környezetben*) lesz az egyik víruskeresési módszer a vizsgálat során.

- ***Rendszerkörnyezet ellenőrzése*** (*alapállapotban bekapcsolva*) - a vizsgálat a számítógép rendszerterületeit is ellenőrzi.

- ***Átfogó vizsgálat engedélyezése*** (*alapállapotban kikapcsolva*) - bizonyos esetekben (*például, ha arra gyanakszik, hogy a számítógépét egy vírus megfertőzte*), akkor jelölje be ezt az opciót a legátfogóbb vizsgálati algoritmus bekapcsolásához, amely a számítógép nehezen fertőzhető részeit is ellenőrzi a biztonság kedvéért. Ne feledje, hogy ez a módszer meglehetősen időigényes.

Döntse el, hogy a programnak mely fájlokat kell vizsgálnia

- ***Összes fájltípus*** - lehetséges megadnia kivételeket, amelyek kimaradnak a vizsgálatból (*mentés után a vesszők pontosvesszőkre változnak*).

- ***Kiválasztott fájltípusok*** - megadhatja, hogy a program csak olyan fájlokat vizsgáljon, amelyek esetlegesen fertőzőek (*a nem fertőzhető fájlok, mint pl. a sima szöveges fájlok vagy egyéb nem futtatható fájlok, nem lesznek ellenőrizve*), pl. médiafájlok (*video-, audiofájlok - ha nem jelöli be ezt a négyzetet, akkor tovább csökken a vizsgálati idő, mivel ezen fájlok általában túl nagyok, és egyébként sem valószínű, hogy vírus fertőzné meg őket*). A kiterjesztések segítségével megadhatja, hogy mely fájlokat vizsgálja a program.

- Megadhatja azt is, hogy ***a program vizsgálja a kiterjesztés nélküli fájlokat*** - ez az opció alapállapotban be van kapcsolva és javasolt, hogy tartsa is így. A kiterjesztés nélküli fájlok különösen gyanúsak, ezért mindig ellenőrizni kell őket.

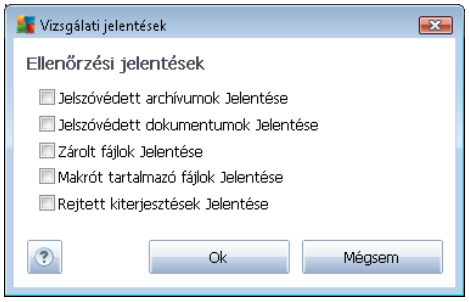
A vizsgálati sebesség beállítása

A ***Vizsgálati sebesség beállítása*** részben meghatározhatja a vizsgálat sebességét a rendszer erőforrásainak függvényében. Alapállapotban ez az érték *felhasználótól által függő* automatikus erőforráshasználatra van állítva. Ha azt szeretné, hogy a vizsgálat gyorsabban fusson, akkor kevesebb idő szükségeltetik, de a rendszererőforrások használata jelentősen megnő, és

lelassíthatja a PC-n zajló egyéb tevékenységeket (*ezt az opciót csak akkor használhatja, ha a számítógép be van kapcsolva, és senki nem dolgozik rajta jelenleg*). Másrészt csökkentheti is a rendszererőforrások használatát a vizsgálat időigényének rovására.

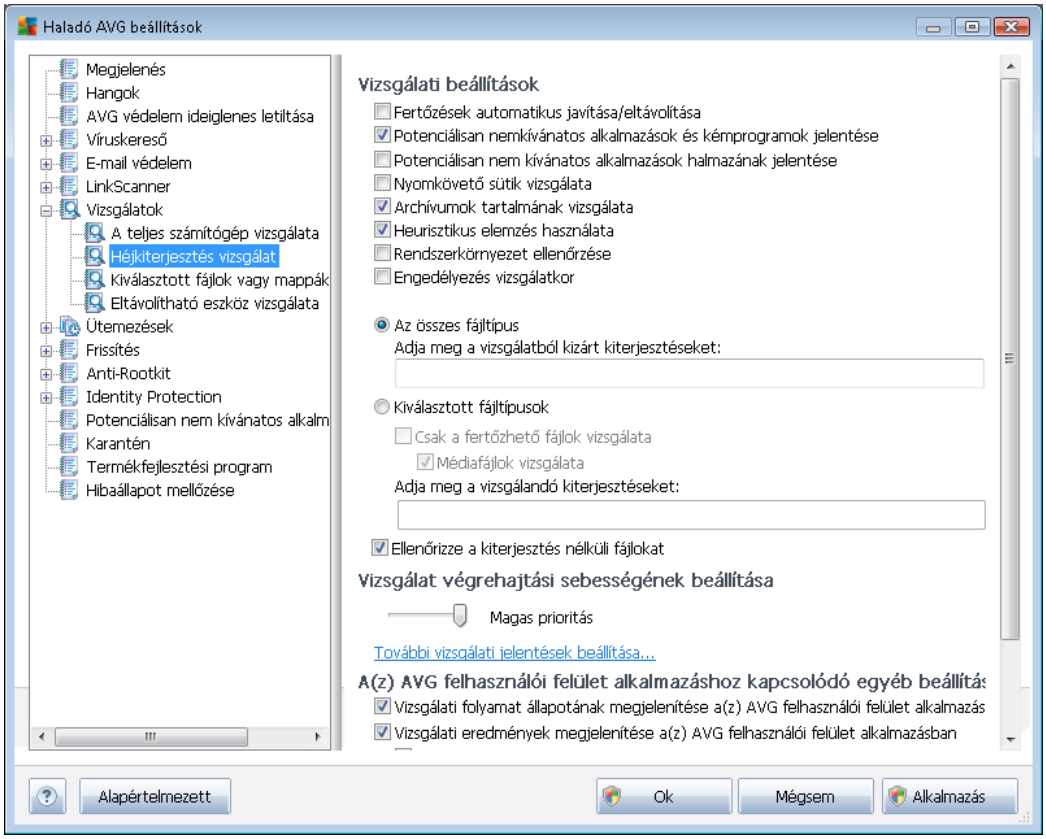
További vizsgálati jelentések beállítása...

Kattintson a ***További vizsgálati jelentések...*** hivatkozásra a ***Vizsgálati jelentések*** panel megnyitásához, ahol számos opciót jelölhet be azzal kapcsolatban, hogy a programnak mit kell jelentenie:



9.7.2. Héjkiterjesztés vizsgálat

Hasonlóan az előző Számítógép teljes vizsgálata elemhez, a ***Héjkiterjesztés vizsgálat*** is lehetővé teszi a számos gyári beállítás módosítását. Itt a beállítások egyedi objektumok Windows Intézőből történő közvetlen vizsgálatára vonatkoznak (*héjkiterjesztés*), lásd a Vizsgálat Windows Intézőben fejezetet:



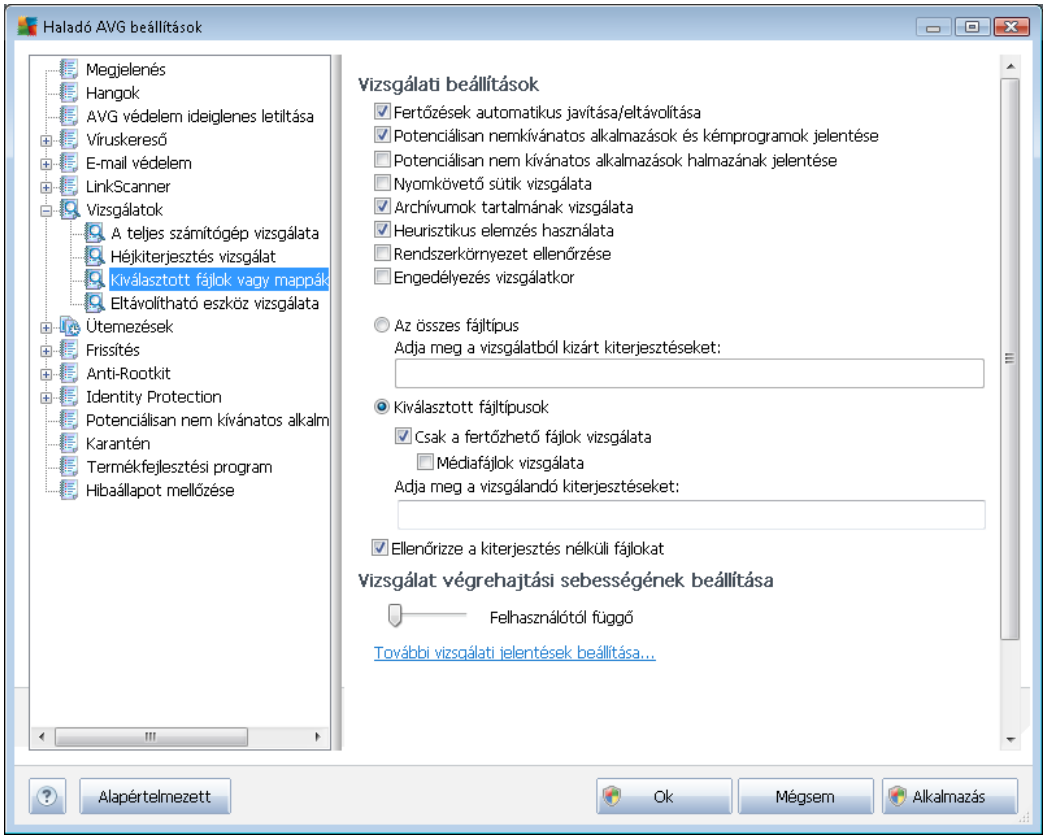
A paraméterek listája megegyezik a Teljes számítógép vizsgálata rész paramétereivel. Az alapértelmezett beállítások eltérnek (*például a Számítógép teljes vizsgálata szolgáltatás nem vizsgálja a tömörített fájlokat, de ellenőrzi a rendszerkörnyezetet, míg a héjkiterjesztési vizsgálat pont az ellenkezőjét teszi*).

Megjegyzés: *Az adott paraméterek leírásával kapcsolatban lásd az AVG Haladó beállítások / Vizsgálatok / Számítógép teljes vizsgálata fejezetet.*

A Számítógép teljes vizsgálata párbeszédpanelhez hasonlóan a ***Héjkiterjesztés vizsgálat*** párbeszédpanel is tartalmazza az ***AVG felhasználói felület egyéb beállításai*** részt, ahol meghatározhatja, hogy a vizsgálati folyamat és a vizsgálat eredménye elérhető legyen-e az AVG felhasználói felületéről. Meghatározhatja azt is, hogy a vizsgálati eredmények csak akkor jelenjenek meg, ha a rendszer fertőzést észlelt.

9.7.3. Kiválasztott fájlok vagy mappák ellenőrzése

A ***Kijelölt fájlok vagy mappák vizsgálata*** panel megegyezik a Számítógép teljes vizsgálata panellel. Minden beállítási lehetőség ugyanaz, azonban az alapértékek szigorúbbak a Teljes számítógép vizsgálata ablakban:

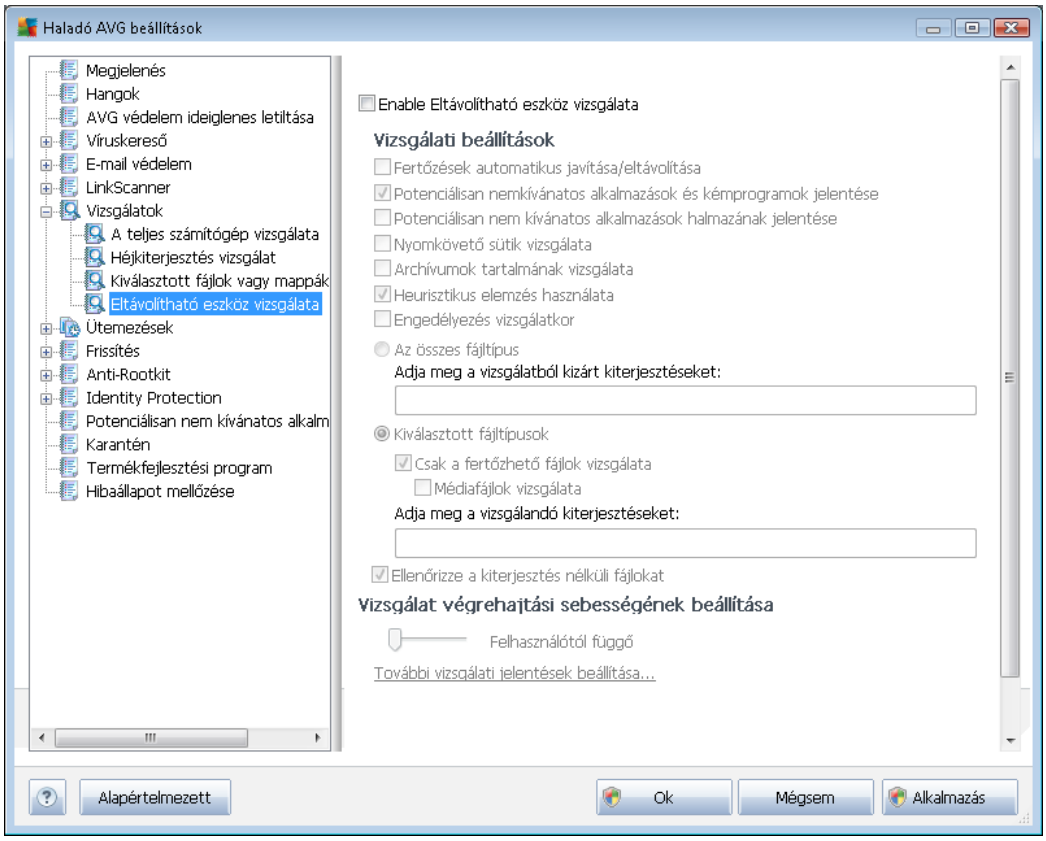


Az összes itt beállított paraméter csak a Bizonyos fájlok vagy mappák vizsgálata opcióra vonatkozik.

Megjegyzés: *Az adott paraméterek leírásával kapcsolatban lásd az AVG Haladó beállítások / Vizsgálatok / Számítógép teljes vizsgálata fejezetet.*

9.7.4. Cserélhető eszköz vizsgálata

A ***Cserélhető eszköz vizsgálata*** panel felülete hasonlít a Számítógép teljes vizsgálata panel felületéhez:



A ***Cserélhető eszközök vizsgálata*** automatikusan elindul, ha egy cserélhető eszközt csatlakoztat a számítógéphez. Alapállapotban ez a vizsgálat ki van kapcsolva. Azonban különösen fontos, hogy ellenőrizze a cserélhető eszközöket is, mivel azok potenciális veszélyforrást képviselnek. A vizsgálat beállításához és szükség esetén automatikus elindításához, jelölje be a ***Cserélhető eszközök vizsgálata*** opciót.

Megjegyzés: *Az adott paraméterek leírásával kapcsolatban lásd az AVG Haladó beállítások / Vizsgálatok / Számítógép teljes vizsgálata fejezetet.*

9.8. Ütemezések

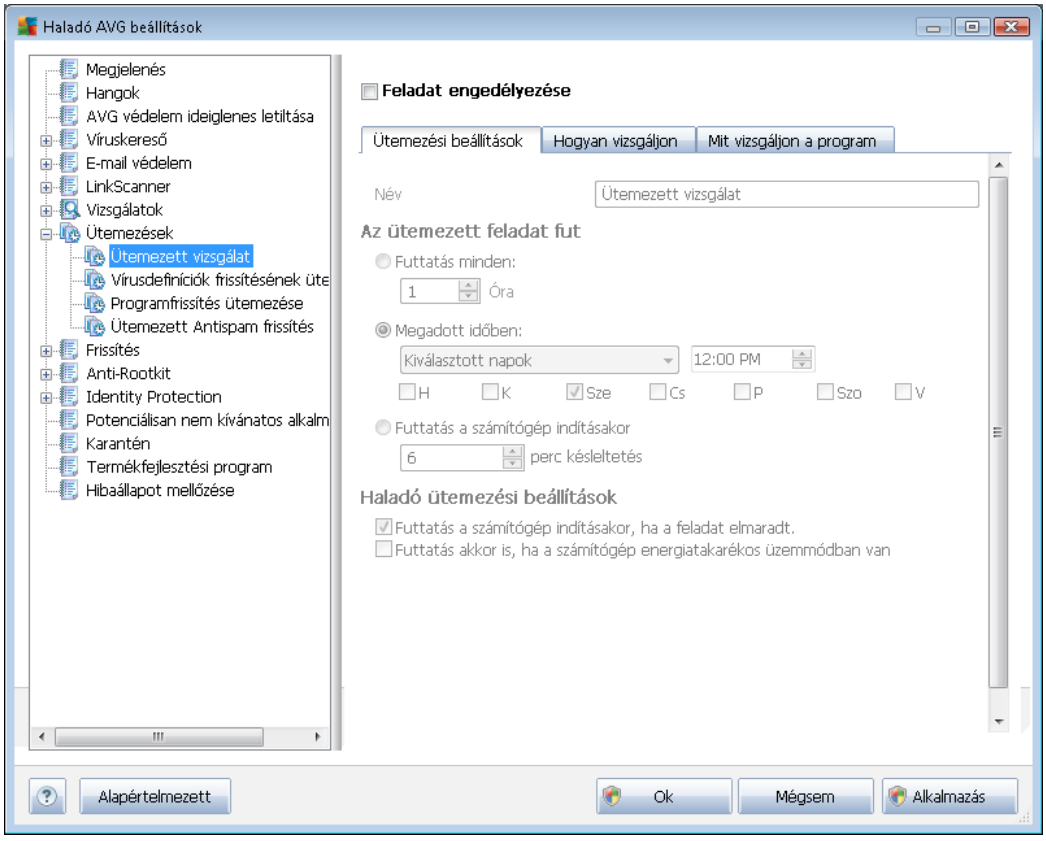
Az ***Ütemezések*** részben szerkesztheti a következők alapbeállításait:

- Ütemezett vizsgálat
- Vírusdefiníciók frissítésének ütemezése
- Programfrissítés ütemezése

- Levélszemétszűrő frissítés ütemezése

9.8.1. Ütemezett vizsgálat

Az ütemezett vizsgálat paramétereit három fülön szerkesztheti (*de akár új ütemezést is létrehozhat*). Az egyes füleken be- és kikapcsolhatja a ***Feladat engedélyezése*** opciót az ütemezett vizsgálat ideiglenes letiltásához. Szükség esetén újra bekapcsolhatja azt:



A ***Név*** (*mezőben kikapcsolva az alapértelmezett ütemezéseknél*) találhat egy nevet, amelyet a program gyártója hozott létre ezen ütemezéshez. Az újonnan létrehozott ütemezéseknél (*felvehet egy új ütemezést, ha az egér jobb gombjával az* ***Ütemezett vizsgálat*** *elemre kattint a bal oldali navigációs sávban*) felvehet egy saját nevet, ekkor a szöveges mező szerkesztésre megnyitható. Próbáljon mindig rövid, jellemző és megfelelő nevet adni a frissítési ütemezéseknek, így később könnyebben felismerheti majd azokat.

Például: *Nem javasolt, hogy a vizsgálatnak az "Új vizsgálat" vagy "Saját vizsgálat" nevet adja, mivel ez semmit nem mond arról, hogy a vizsgálat valójában mit ellenőriz. Ugyanakkor megfelelő leíró név például a "Rendszerterületek ellenőrzése" stb. Nem szükséges a névben megadni, hogy a számítógép teljes vagy részleges vizsgálatáról van szó, mivel a saját vizsgálatok minden esetben adott fájlok vagy mappák vizsgálatának minősülnek.*

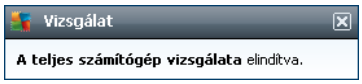
Ezen a panelen beállíthatja az adott keresés következő paramétereit:

Az ütemezett feladat fut

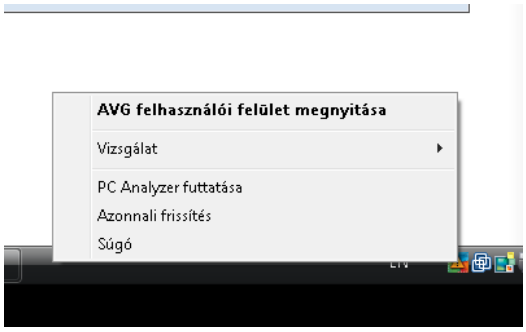
Itt megadhatja, hogy az ütemezett vizsgálatok milyen időközönként fussanak le. Az ütemezés megadható bizonyos időközönként indított ismételt vizsgálatok futtatásával (***Futtatás minden ...***), vagy egy pontos dátum és időpont megadásával (***Futtatás egy meghatározott időben ...***), illetve megadható egy adott eseményhez hozzárendelve is (***Futtatás a számítógép indításakor***).

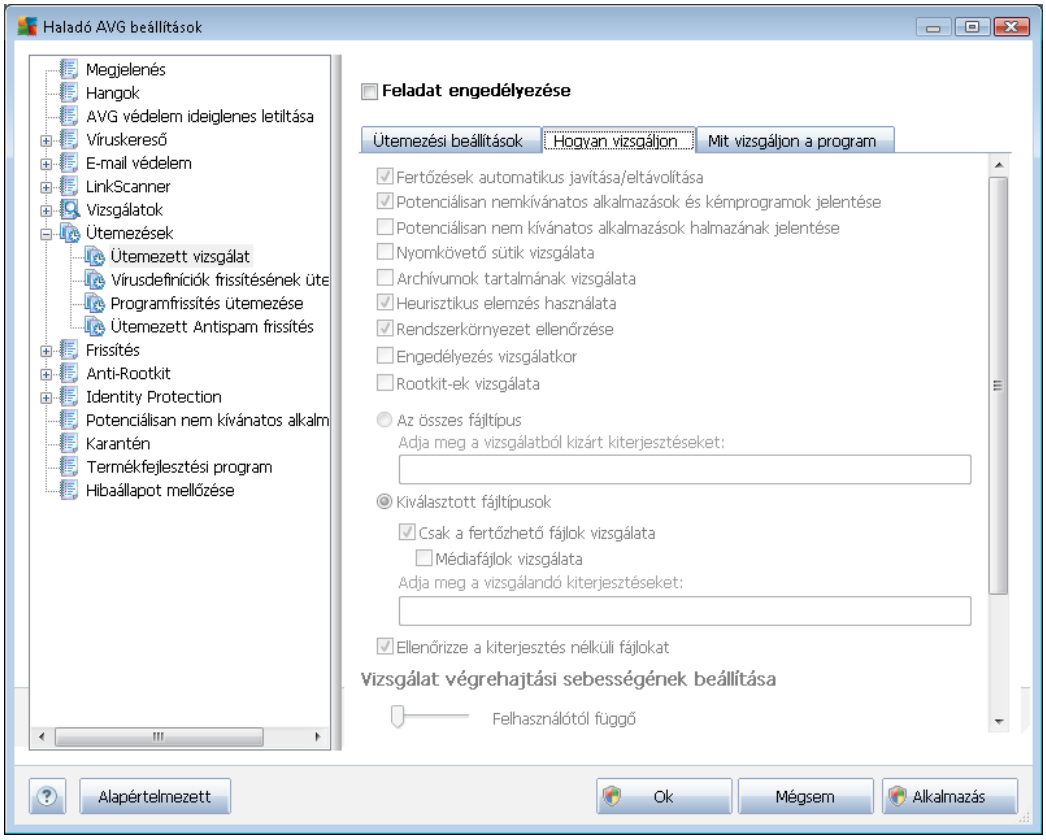
Haladó ütemezési beállítások

Ebben a részben meghatározhatja, hogy a vizsgálat mely körülmények között induljon/ne induljon, például ha a számítógép energiatakarékos módban van, vagy teljesen ki van kapcsolva. Miután az ütemezett vizsgálat elindult a megadott időben, erről értesítést kap egy felugró ablakban az AVG tálcaikonjánál:



Egy új AVG rendszerikon jelenik meg (*színes ikon*), és és tájékoztatja Önt az ütemezett vizsgálat futásáról. Kattintson az egér jobb gombjával az AVG ikonjára egy helyi menü megnyitásához, ahol szüneteltetheti vagy leállíthatja a futó vizsgálatot, illetve megváltoztathatja annak prioritását:





A ***Hogyan vizsgáljon***fülön a vizsgálati paraméterek listáját találhatja, melyeket tetszőlegesen be- és kikapcsolhat. Alapértelmezés szerint a legtöbb paraméter be van kapcsolva, és működni fog a vizsgálat során. ***Javasoljuk, hogy tartsa meg az alapértelmezett beállításokat, és csak akkor módosítson rajtuk, ha feltétlenül szükséges***:

- ***Fertőzés automatikus javítása/eltávolítása*** *(alapállapotban bekapcsolva):* ha vírust talál a vizsgálat során, akkor automatikusan javítja, amennyiben ez lehetséges.. Ha a fertőzött fájl nem javítható automatikusan, az objektum át lesz helyezve a Karanténba.

- ***Potenciálisan nemkívánatos programok és kémprogramok jelentése*** *(alapállapotban bekapcsolva):* jelölje be a Kémprogram-elhárító motor aktiválásához, illetve kémprogramok és vírusok kereséséhez. A kémprogramok külön kártevő kategóriát képviselnek: komoly biztonsági kockázatot jelentenek, mégis nagy részüket a felhasználók szándékosan telepítik. Javasoljuk, hogy tartsa bekapcsolva ezt az opciót, mivel így növelheti a számítógép biztonságát.

- ***Potenciálisan nem kívánatos alkalmazások jelentése*** (*alapállapotban kikapcsolva*): jelölje be ezt a jelölőnégyzetet a kémprogramok: speciális változatainak észleléséhez: olyan programok kereséséhez, amelyek ártalmatlanok, de később kártékony célokra használhatók. Ezzel tovább növelheti a számítógép biztonságát. A szolgáltatás legitim programokat is letilthat, ezért a funkció alapállapotban ki van kapcsolva.

- ***Nyomkövető sütik vizsgálata*** (*alapállapotban kikapcsolva*): ez az opció a Kémprogram-

elhárító összetevőben meghatározza, hogy a vizsgálat során felismert sütik észlelve legyenek-e (a *HTTP sütiket hitelesítéshez, nyomkövetéshez és bizonyos adatok gyűjtéséhez használják a felhasználókról, pl. honlap preferenciák vagy online vásárlás során a kosár tartalma*).

- ***Archívumok tartalmának vizsgálata*** (*alapállapotban bekapcsolva*): ez az opció meghatározza, hogy a vizsgálat minden fájlt - köztük archív fáljokat is, pl. ZIP, RAR ellenőrizzen-e.

- ***Heurisztika használata*** (*alapállapotban bekapcsolva*): a heurisztikus elemzés (*a vizsgált objektum utasításainak dinamikus emulációja egy virtuális környezetben*) lesz az egyik víruskeresési módszer a vizsgálat során.

- ***Rendszerkörnyezet ellenőrzése*** (*alapállapotban bekapcsolva*): a vizsgálat a számítógép rendszerterületeit is ellenőrzi.

- ***Átfogó vizsgálat engedélyezése*** (*alapállapotban kikapcsolva*) - bizonyos esetekben (*például, ha arra gyanakszik, hogy a számítógépét egy vírus megfertőzte*), akkor jelölje be ezt az opciót a legátfogóbb vizsgálati algoritmus bekapcsolásához, amely a számítógép nehezen fertőzhető részeit is ellenőrzi a biztonság kedvéért. Ne feledje, hogy ez a módszer meglehetősen időigényes.

- ***Rootkitek vizsgálata*** (*alapállapotban kikapcsolva*): jelölje be ezt az elemet, ha rootkiteket is keresni kíván a számítógép teljes vizsgálata során. A rootkit vizsgálat külön is indítható az Anti-Rootkit összetevőből;

Döntse el, hogy a programnak mely fájlokat kell vizsgálnia

- ***Összes fájltípus*** - lehetséges megadnia kivételeket, amelyek kimaradnak a vizsgálatból (*mentés után a vesszők pontosvesszőkre változnak*).

- ***Kiválasztott fájltípusok*** - megadhatja, hogy a program csak olyan fájlokat vizsgáljon, amelyek esetlegesen fertőzőek (*a nem fertőzhető fájlok, mint pl. a sima szöveges fájlok vagy egyéb nem futtatható fájlok, nem lesznek ellenőrizve*), pl. médiafájlok (*video-, audiofájlok - ha nem jelöli be ezt a négyzetet, akkor tovább csökken a vizsgálati idő, mivel ezen fájlok általában túl nagyok, és egyébként sem valószínű, hogy vírus fertőzné meg őket*). A kiterjesztések segítségével megadhatja, hogy mely fájlokat vizsgálja a program.

- Megadhatja azt is, hogy ***a program vizsgálja a kiterjesztés nélküli fájlokat*** - ez az opció alapállapotban be van kapcsolva és javasolt, hogy tartsa is így. A kiterjesztés nélküli fájlok különösen gyanúsak, ezért mindig ellenőrizni kell őket.

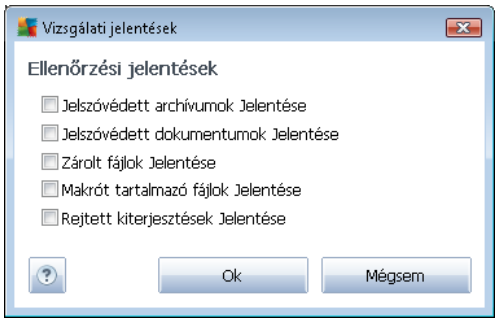
A vizsgálati sebesség beállítása

A ***Vizsgálati sebesség beállítása*** részben meghatározhatja a vizsgálat sebességét a rendszer erőforrásainak függvényében. Alapállapotban ez az érték *felhasználótól által függő* automatikus erőforráshasználatra van állítva. Ha azt szeretné, hogy a vizsgálat gyorsabban fusson, akkor kevesebb idő szükségeltetik, de a rendszererőforrások használata jelentősen megnő, és lelassíthatja a PC-n zajló egyéb tevékenységeket (*ezt az opciót csak akkor használhatja, ha a számítógép be van kapcsolva, és senki nem dolgozik rajta jelenleg*). Másrészt csökkentheti a

rendszererőforrások használatát, de ez a vizsgálathoz szükséges idő növekedésével jár.

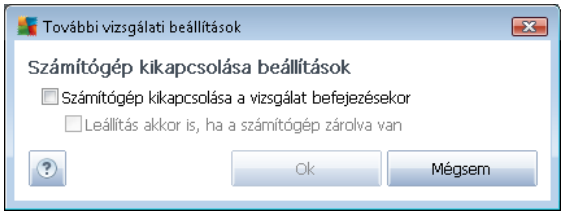
További vizsgálati jelentések beállítása

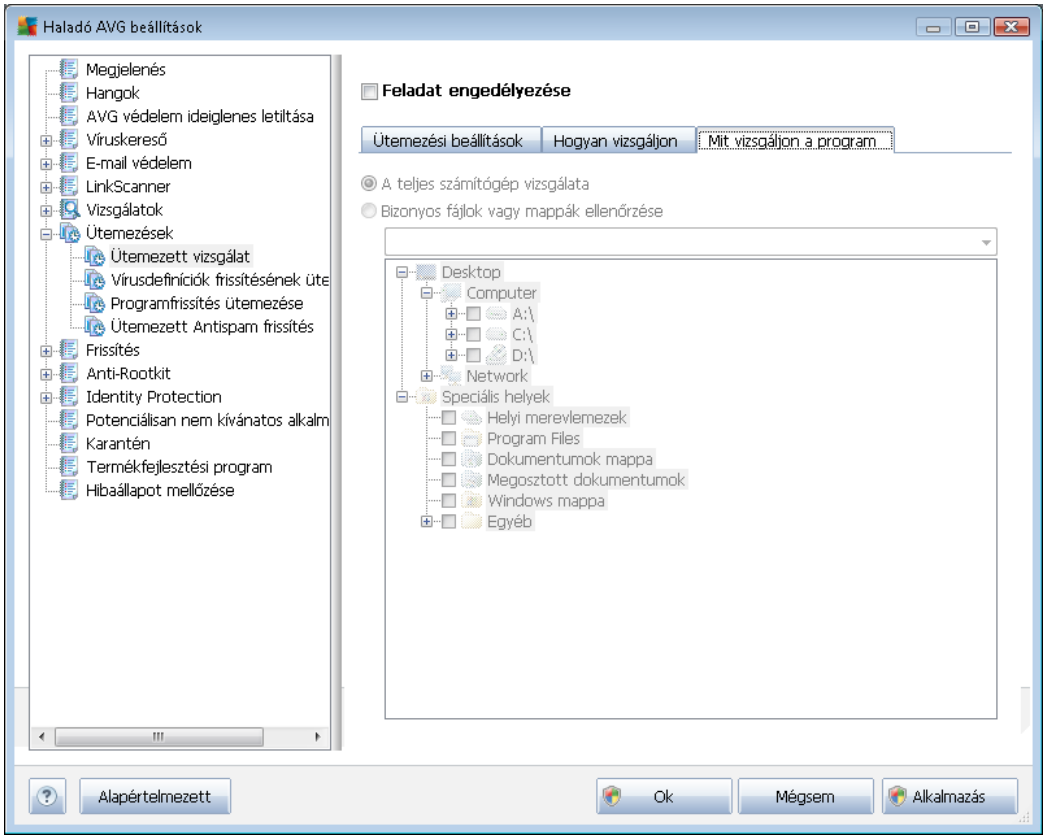
Kattintson a ***További vizsgálati jelentések...*** hivatkozásra a ***Vizsgálati jelentések*** panel megnyitásához, ahol számos opciót jelölhet be azzal kapcsolatban, hogy a programnak mit kell jelentenie:



További vizsgálati beállítások

Kattintson a ***További vizsgálati beállítások...*** részre a ***Számítógép kikapcsolása beállítások*** panel megnyitásához, ahol beállíthatja, hogy a számítógép automatikusan kikapcsoljon, ha a vizsgálat befejeződött. Miután megerősítette ezt a beállítást (***Számítógép leállítása a vizsgálat után***), egy új opció aktiválódik, mely lehetővé teszi, hogy akkor is leállítsa a számítógépet, ha az éppen zárolt (***Számítógép leállítása zárolás esetén is***).

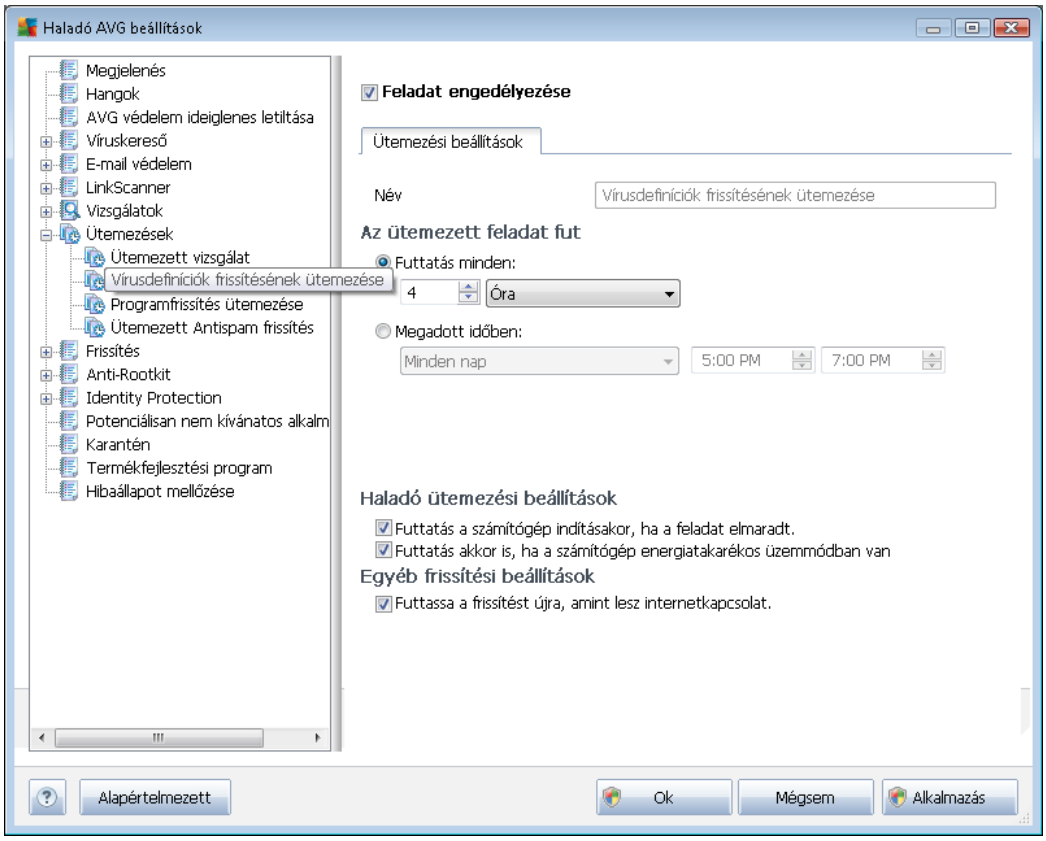




A ***Mit vizsgáljon a program*** fülön meghatározhatja, hogy a számítógép teljes vizsgálatát vagy csak bizonyos fájlok és mappák vizsgálatát szeretné ütemezni. Ha a bizonyos fájlok és mappák vizsgálatát választja, akkor a panel alsó részén a fastruktúra aktiválódik és bejelölheti az ellenőrzendő mappákat.

9.8.2. Vírusdefiníciók frissítésének ütemezése

Ha ***valóban szükséges***, kikapcsolhatja a ***Feladat engedélyezése*** elemet az ütemezett vírusdefiníció-frissítés ideiglenes letiltásához, majd később újra bekapcsolhatja azt:



Ebben az ablakban megadhatja a definíciófrissítés ütemezésének részletes paramétereit. A ***Név*** mezőben (*kikapcsolva az alapértelmezett ütemezéseknél*) találhat egy - a program gyártója által létrehozott - nevet ezen ütemezéshez.

Az ütemezett feladat fut

Ebben a részben adhatja meg, hogy az újonnan ütemezett vírusdefiníció-frissítés milyen gyakran induljon el. Az ütemezést meghatározhatja a rendszeresen történő futtatással (***Futattás minden ...***), dátummal és időponttal (***Futtatás meghatározott időben ...***).

Haladó ütemezési beállítások

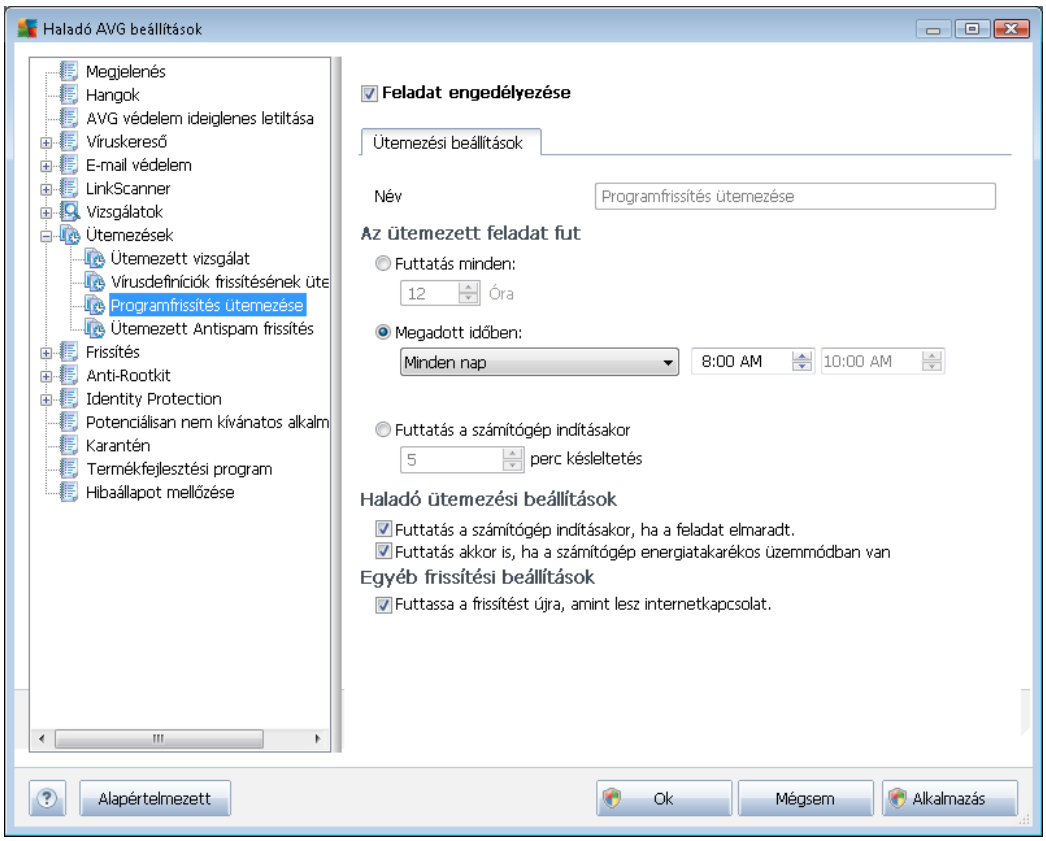
Ebben a részben meghatározhatja, hogy a vírusdefiníció-frissítés milyen körülmények között induljon el vagy ne induljon el, ha a számítógép energiatakarékos módban van, vagy teljesen ki van kapcsolva.

Egyéb frissítési beállítások

Jelölje be a ***Futtassa a frissítést újra, amint lesz internetkapcsolat*** lehetőséget, hogy ha az internetkapcsolat megszakad, és a frissítés sikertelen, akkor a folyamat újra lefusson, miután az internetkapcsolat helyreállt. Miután az ütemezett frissítés elindult a megadott időben, erről értesítést kap egy előugró ablakban az AVG tálcaikonjánál (*feltéve, hogy megtartotta a Haladó beállítások/ Megjelenés panel alapértelmezett beállításait).*

9.8.3. Programfrissítés ütemezése

Ha ***valóban szükséges***, kikapcsolhatja a ***Feladat engedélyezése*** elemet az ütemezett programfrissítés ideiglenes letiltásához. Később újra bekapcsolhatja azt:



A ***Név*** mezőben (*kikapcsolva az alapértelmezett ütemezéseknél*) találhat egy – a program gyártója által létrehozott – nevet ezen ütemezésnél.

Az ütemezett feladat fut

Adja meg, hogy az újonnan ütemezett programfrissítés milyen időközönként fusson le. Az ütemezést meghatározhatja a rendszeresen történő futtatással (***Futtatás minden ...***), dátummal és időponttal (***meghatározott időben ...***), vagy egy adott eseményhez kötheti (***Futtatás számítógép indításakor***).

Haladó ütemezési beállítások

Ebben a részben meghatározhatja, hogy a programfrissítés mely körülmények között induljon/ne induljon (például ha a számítógép energiatakarékos módban van, vagy teljesen ki van kapcsolva.

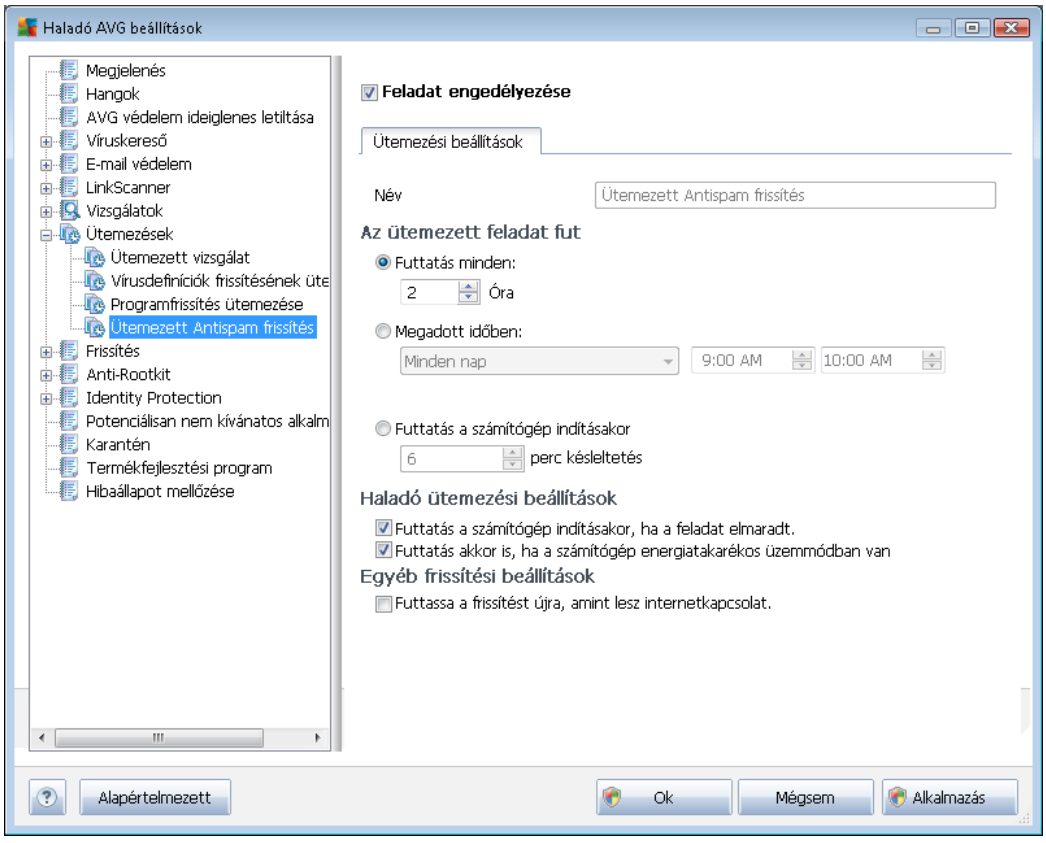
Egyéb frissítési beállítások

Jelölje be a ***Frissítés futtatása ismét, amint az internetkapcsolat elérhető*** opciót, hogyha az internetkapcsolat megszakad és a programfrissítés sikertelen, akkor az újra lefusson, miután az internetkapcsolat helyreállt. Miután az ütemezett frissítés elindult a megadott időben, erről értesítést kap egy felbukkanó ablak formájában az AVG ikonjánál (*feltéve, hogy megtartotta a Haladó beállítások/Megjelenés panel alapértelmezett beállításait).*

Megjegyzés: *Ha az ütemezett programfrissítés és az ütemezett vizsgálat időben ütközik, akkor a frissítési folyamatnak van elsődleges prioritása és a vizsgálat meg lesz szakítva.*

9.8.4. Levélszemétszűrő frissítési ütemezése

Ha valóban szükséges, kikapcsolhatja a ***Feladat engedélyezése*** elemet az ütemezett Levélszemétszűrés frissítésének ideiglenes letiltásához, majd később újra bekapcsolhatja azt:



Ebben az ablakban megadhatja a frissítési ütemezés részletes paramétereit. A ***Név*** mezőben (

kikapcsolva az alapértelmezett ütemezéseknél) találhat egy - a program gyártója által létrehozott - nevet ezen ütemezéshez.

Az ütemezett feladat fut

Itt az időközt adhatja meg az újonnan létrehozott Levélszemétszűrő frissítési ütemezésekhez. Az ütemezés megadható bizonyos időközönként indított ismételt Levélszemétszűrés frissítés futtatásával (***Futtatás minden ...***), vagy egy pontos dátum és időpont megadásával (***Futtatás egy meghatározott időben***), illetve megadható egy adott eseményhez hozzárendelve is (***A számítógép indításán alapuló művelet***).

Haladó ütemezési beállítások

Ebben a részben meghatározhatja, hogy a Levélszemétszűrés frissítése milyen körülmények között induljon el vagy ne induljon el, ha a számítógép energiatakarékos módban van, vagy teljesen ki van kapcsolva.

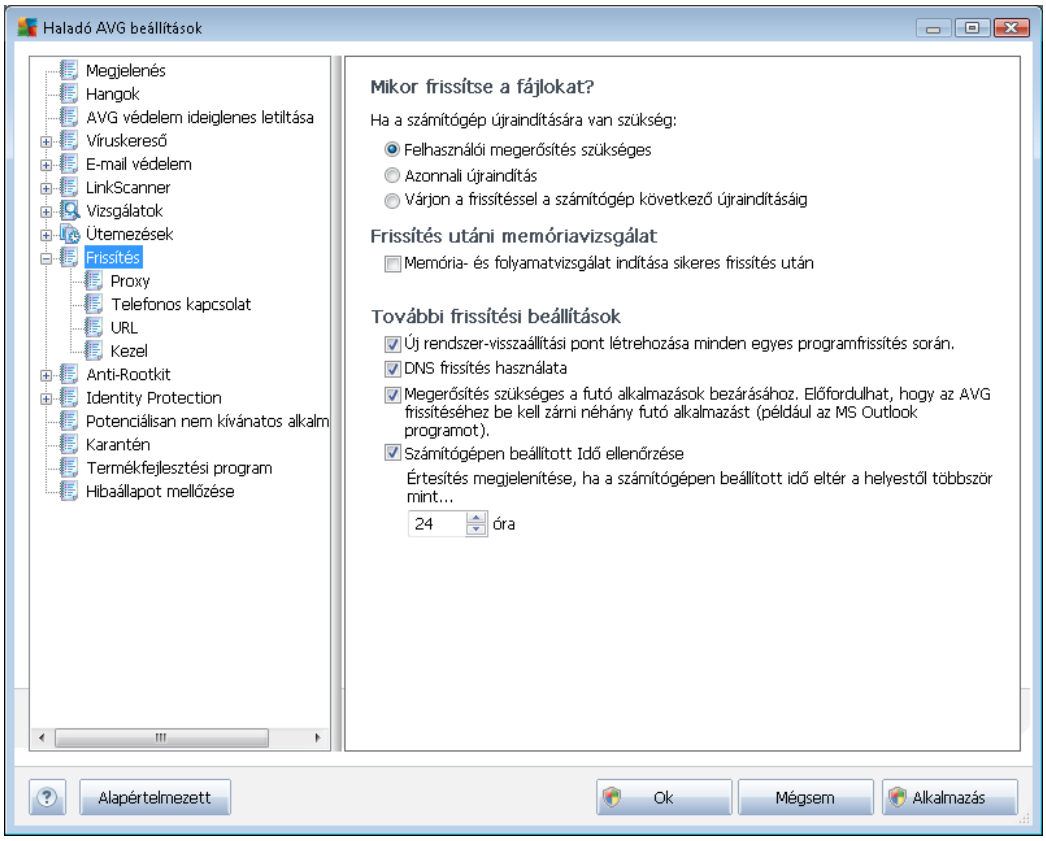
Egyéb frissítési beállítások

Jelölje be a ***Futtassa a frissítést újra, amint lesz internetkapcsolat*** lehetőséget, annak érdekében, hogy ha az internetkapcsolat megszakad és a Levélszemétszűrés frissítése sikertelen, a frissítés azonnal újrainduljon, miután az internetkapcsolat helyreállt.

Miután az ütemezett vizsgálat elindult a megadott időben, erről értesítést kap egy előugró ablakban az AVG tálcaikonjánál (*feltéve, hogy megtartotta a Haladó beállítások/Megjelenés panel alapértelmezett beállításait).*

9.9. Frissítés

A ***Frissítés*** navigációs elem egy új ablakot nyit meg, ahol általános paramétereket adhat meg az AVG frissítésekkelkapcsolatban:



Mikor frissítse a fájlokat?

Ezen a részen három különböző lehetőség közül választhat, ha a frissítési folyamathoz újra kell indítania a számítógépet. A frissítés befejezését ütemezheti a számítógép következő újraindítására, vagy akár azonnal is kezdeményezheti az újraindítást:

- ***Felhasználói megerősítés szükséges*** *(alapértelmezett)* – A program felszólítja a számítógép újraindítására a frissítési folyamat befejezéséhez
- ***Azonnali újraindítás*** – A program azonnal és automatikusan újraindítja a számítógépet, miután a frissítési folyamat befejeződött (nem szükséges az Ön hozzájárulása)
- ***Befejezés a számítógép következő újraindításakor*** – A frissítési folyamat befejezése a számítógép következő újraindításakor történik meg. Vegye figyelembe, hogy ez az opció csak akkor javasolt, ha a számítógépet rendszeresen újraindítja (naponta legalább egyszer).

Frissítés utáni memóriavizsgálat

Jelölje be ezt a négyzetet, ha új memóriavizsgálatot kíván elindítani minden egyes sikeresen befejezett frissítés után. A letöltött frissítés új vírusdefiníciókat tartalmaz és azonnal használható a vizsgálat során.

További frissítési opciók

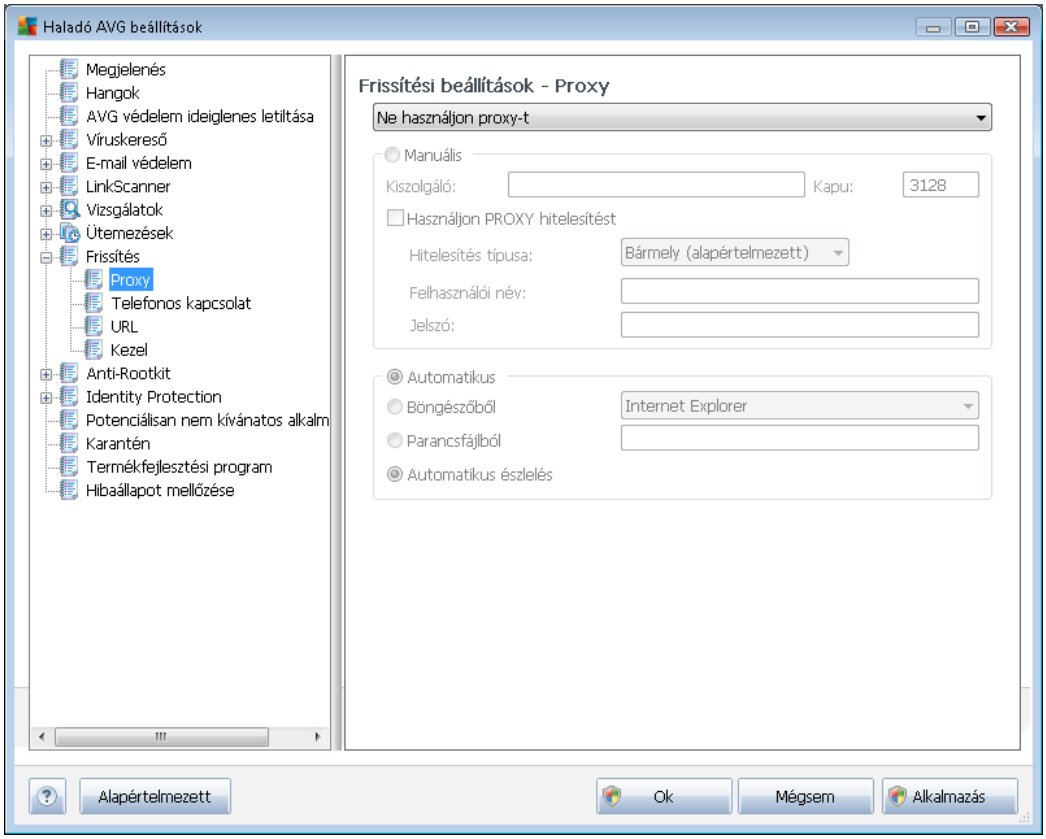
- ***Új rendszer-visszaállítási pont létrehozása programfrissítéskor*** - mielőtt az AVG programfrissítés lefutna, egy rendszer-visszaállítási pont lesz létrehozva. Ha a frissítési folyamat sikertelen, és az operációs rendszer összeomlik, akkor mindig visszaállíthatja a rendszert a korábbi állapotra. Az opció elérhető a Start / Minden program / Kellékek / Rendszereszközök / Rendszer-visszaállítás , menüből, de a módosítás csak tapasztalt felhasználóknak javasolt! Hagyja bejelölve ezt az elemet, ha használni akarja a funkciót.

- ***DNS frissítés használata*** (*alapállapotban bekapcsolva*) - ha bejelöli, akkor a frissítés indításakor az **AVG Internet Security 2012** megkeresi a legújabb vírusadatbázist és programverziót a DNS-kiszolgálón. Ekkor csak a legkisebb méretű, feltétlenül szükséges frissítőfájlok töltődnek le és települnek. Így a letöltendő teljes adatmennyiség minimalizálható, és a frissítési folyamat is gyorsabb lesz.

- ***A Megerősítés szükséges a futó alkalmazások bezárásához*** (*alapértelmezés szerint bekapcsolva*) elem bejelölésével biztosíthatja, hogy egyetlen futó alkalmazást se zárhasson be a program az Ön engedélye nélkül – ha ez szükséges a frissítési folyamat befejezéséhez.

- ***Számítógépen beállított idő ellenőrzése*** – Jelölje be ezt a lehetőséget, amennyiben szeretne értesítést kapni arról, ha a számítógépen beállított idő a megadottnál jobban eltér a tényleges időtől.

9.9.1. Proxy



A proxy kiszolgáló egy különálló kiszolgáló vagy egy számítógépen futó szolgáltatás, amely közvetett hozzáférést nyújt az internethez. A megadott hálózati szabályoknak megfelelően közvetlenül, vagy egy proxykiszolgálón keresztül csatlakozhat az Internethez; illetve a kétfajta csatlakozás egyidejűleg is történhet. A ***Frissítési beállítások - Proxy*** ablak fenti részében választania kell a következőkből:

- ***Használjon proxy-t***
- ***Ne használjon proxyt*** - alapértelmezett beállítások
- ***Próbáljon csatlakozni proxy használatával. Ha sikertelen, akkor csatlakozzon közvetlenül***

Ha proxy kiszolgálóval választja bármelyik opciót, akkor további adatokat kell megadnia. A kiszolgálóbeállításokat manuálisan vagy automatikusan is megadhatja.

Manuális beállítás

Ha a manuális beállítást választja (jelölje be a ***Manuális*** *opciót az adott elem aktiválásához*), akkor a következőket kell megadnia:

- ***Kiszolgáló***– a kiszolgáló IP-címe vagy neve

- ***Port***– az internetkapcsolatot szolgáltató port száma (*(alapértelmezés szerint ez a szám a 3128, de az értéket meg lehet változtatni – ha bizonytalan, forduljon a hálózat rendszergazdájához*)

A proxykiszolgálónál az egyes felhasználókra különböző szabályok vonatkozhatnak. Ha így állítja be a proxy kiszolgálót, akkor jelölje be a ***Használjon PROXY hitelesítést*** opciót, hogy ellenőrizhesse, a kiszolgálón keresztüli internetcsatlakozáshoz megadott felhasználónév és jelszó megfelelő.

Automatikus beállítás

Ha az automatikus beállítást választja (*jelölje be az **Automatikus** opciót az aktiválásához*), akkor válassza ki, hogy a proxybeállítások honnan legyenek átvéve:

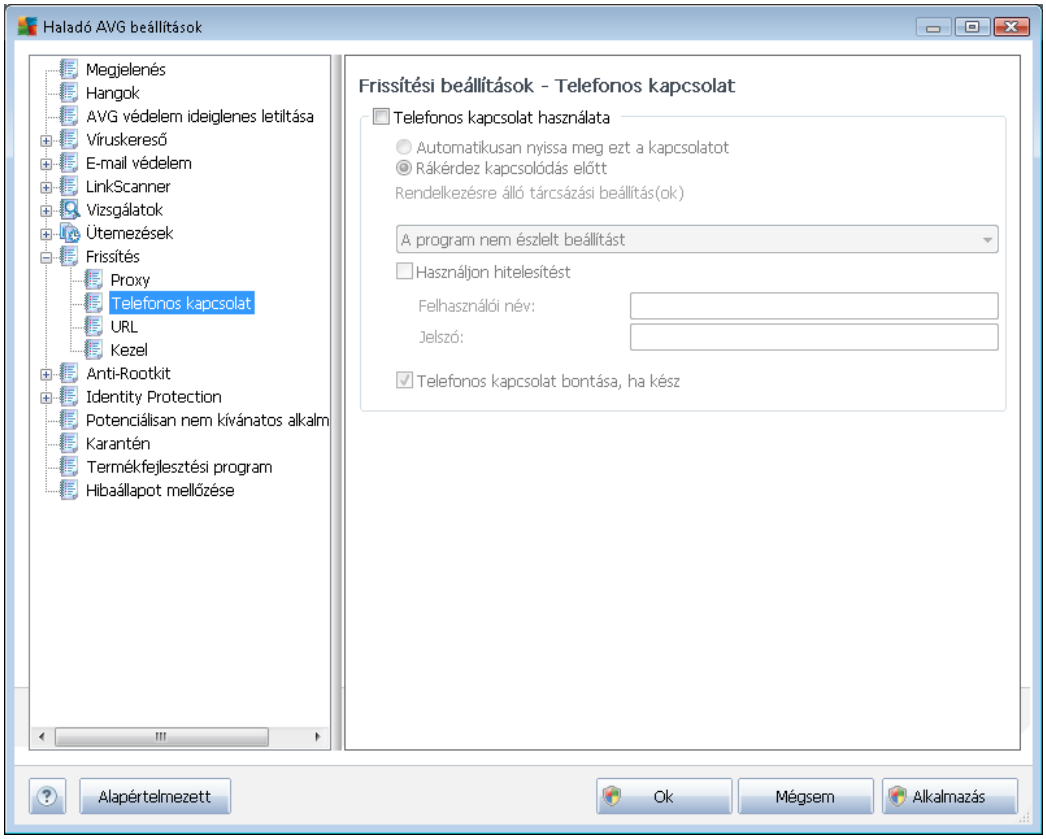
- ***Böngészőből*** - a programbeállításokat az alapértelmezett internetböngészőből olvassa be

- ***Parancsfájlból*** - a beállítások egy proxy címet adó, letöltött parancsfájlból lesznek beolvasva.

- ***Automatikus észlelés*** - beállítások automatikus felismerése a proxy kiszolgálóból

9.9.2. Telefonos kapcsolat

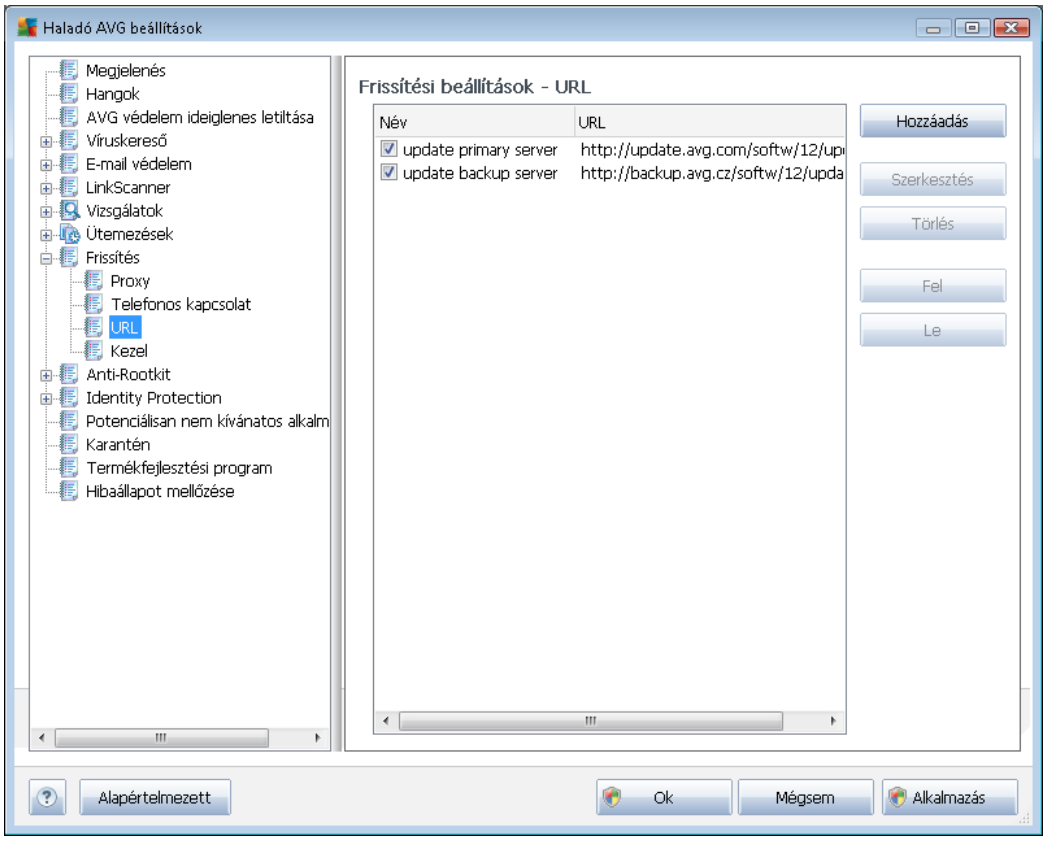
A tetszőlegesen meghatározható paraméterek a ***Frissítési beállítások - Telefonos kapcsolat*** panelen a betárcsázós internetkapcsolatra vonatkoznak. A panel mezői csak akkor válnak aktívvá, ha bejelöli a ***Telefonos kapcsolat használata*** elemet:



Adja meg, hogy az internethez automatikusan szeretne-e kapcsolódni (***Kapcsolat automatikus megnyitása***) vagy a kapcsolódást minden egyes alkalommal meg szeretné erősíteni (***Kérdés a kapcsolódás előtt***). Az automatikus kapcsolódáshoz azt is meg kell határoznia, hogy a kapcsolat lezáruljon-e a frissítés végeztével (***Kapcsolat bontása, ha kész***).

9.9.3. URL

Az ***URL*** párbeszédpanel azon internetes címek listáját tartalmazza, ahonnan a frissítési fájlok letölthetők:



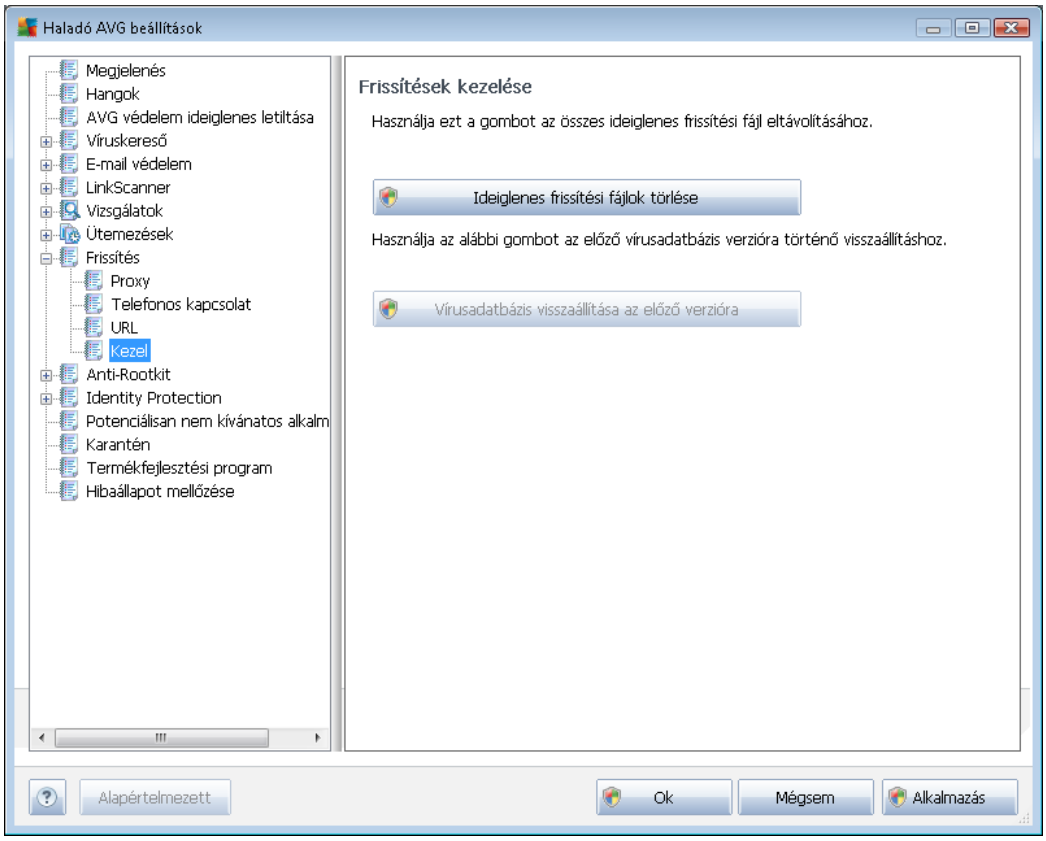
Vezérlőgombok

A lista és a lista elemeinek megváltoztatása a következő kezelőgombokkal történik:

- ***Hozzáadás*** – egy új párbeszédpanelt nyit meg, ahol új URL címeket adhat a listához
- ***Szerkesztés*** - egy párbeszédpanelt nyit meg, ahol módosíthatja a kijelölt URL paramétereit
- ***Törlés***– a kijelölt URL törlése a listából
- ***Fel*** – a kijelölt URL előrébb mozdítása a listában egy hellyel
- ***Le*** - a kijelölt URL hátrébb mozdítása a listában egy hellyel

9.9.4. Kezelés

A ***Frissítések kezelése*** párbeszédpanelről két lehetőség érhető el, mégpedig két gomb segítségével:

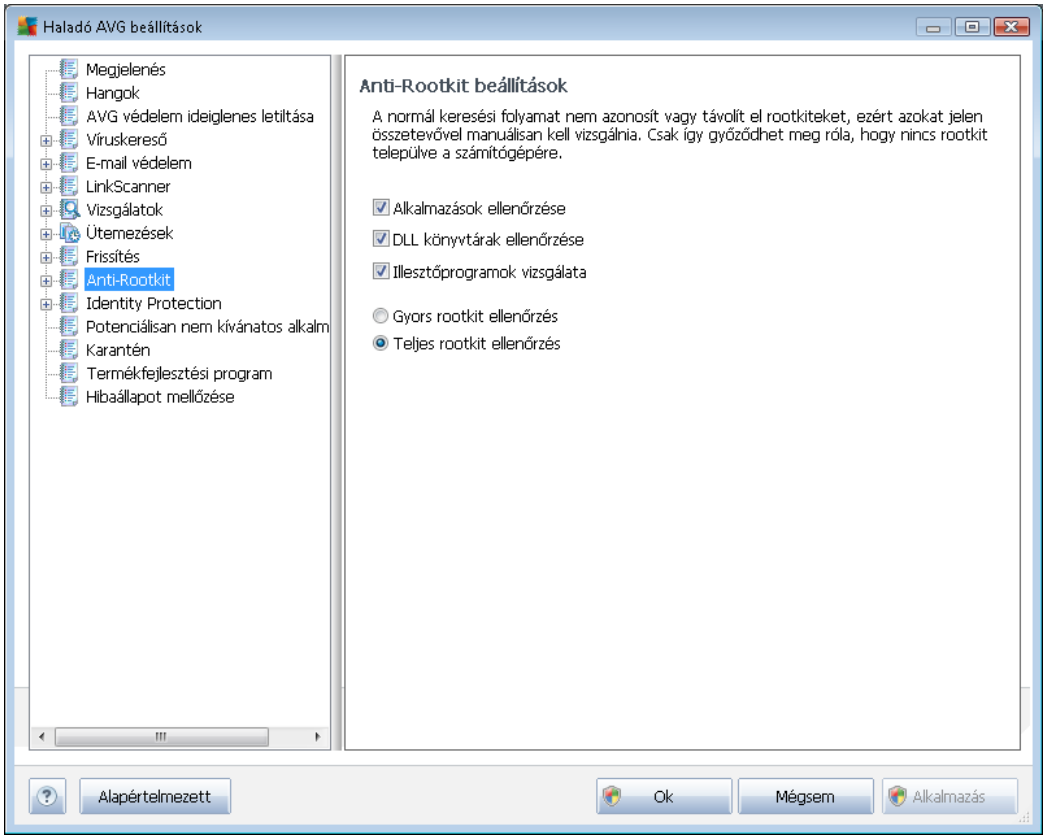


- ***Ideiglenes frissítési fájlok törlése*** - nyomja meg ezt a gombot az összes szükségtelen frissítési fájl törléséhez a merevlemezről (*alapállapotban ezek a fáljok 30 napig tárolódnak*)

- ***Vírusadatbázis visszaállítása az előző verzióra*** - nyomja meg ezt a gombot az aktuális vírusadatbázis törléséhez, és az előző mentett verzióhoz történő visszatéréshez (*az új adatbázis verzió a következő frissítéskor fog települni*)

9.10. Anti-Rootkit

Az ***Anti-rootkit beállítások*** területen szerkesztheti az Anti-Rootkit összetevő beállításait:



Az Anti-Rootkit összetevő ezen a párbeszédpanelen elérhető összes funkciójának szerkesztése közvetlenül az Anti-Rootkit összetevő felületről is lehetséges.

Jelölje be, hogy mely objektumokat kell ellenőrizni:

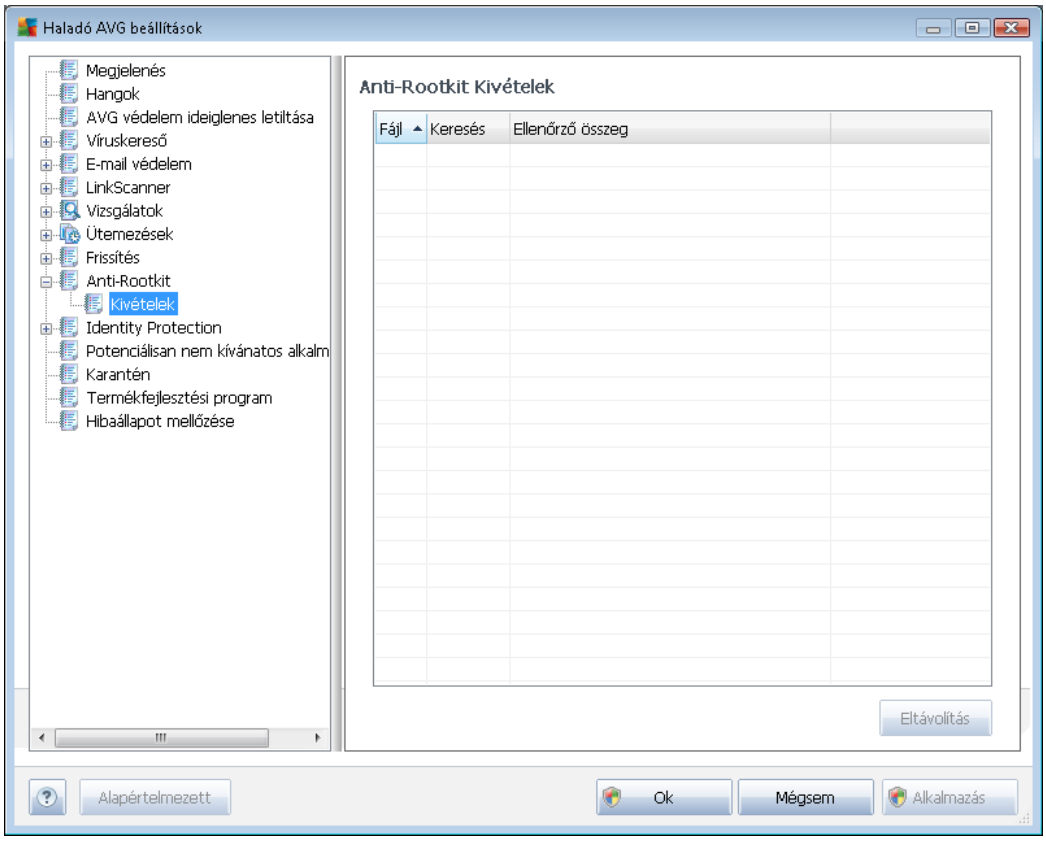
- ***Alkalmazások ellenőrzése***
- ***DLL könyvtárak ellenőrzése***
- ***Illesztőprogramok keresése***

Ezután kiválaszthatja a rootkit vizsgálati módot:

- ***Gyors rootkit vizsgálat*** - az összes futó folyamatot, a betöltött illesztőprogramokat és a rendszermappát (*általában c:\Windows*) ellenőrzi
- ***Teljes rootkit vizsgálat*** - a futó folyamatokat, a betöltött illesztőprogramokat, a rendszermappát (*általában c:\Windows*), valamint az összes helyi lemezt (*flash memóriával együtt, kivéve a floppy-/CD-meghajtókat*) ellenőrzi

9.10.1. Kivételek

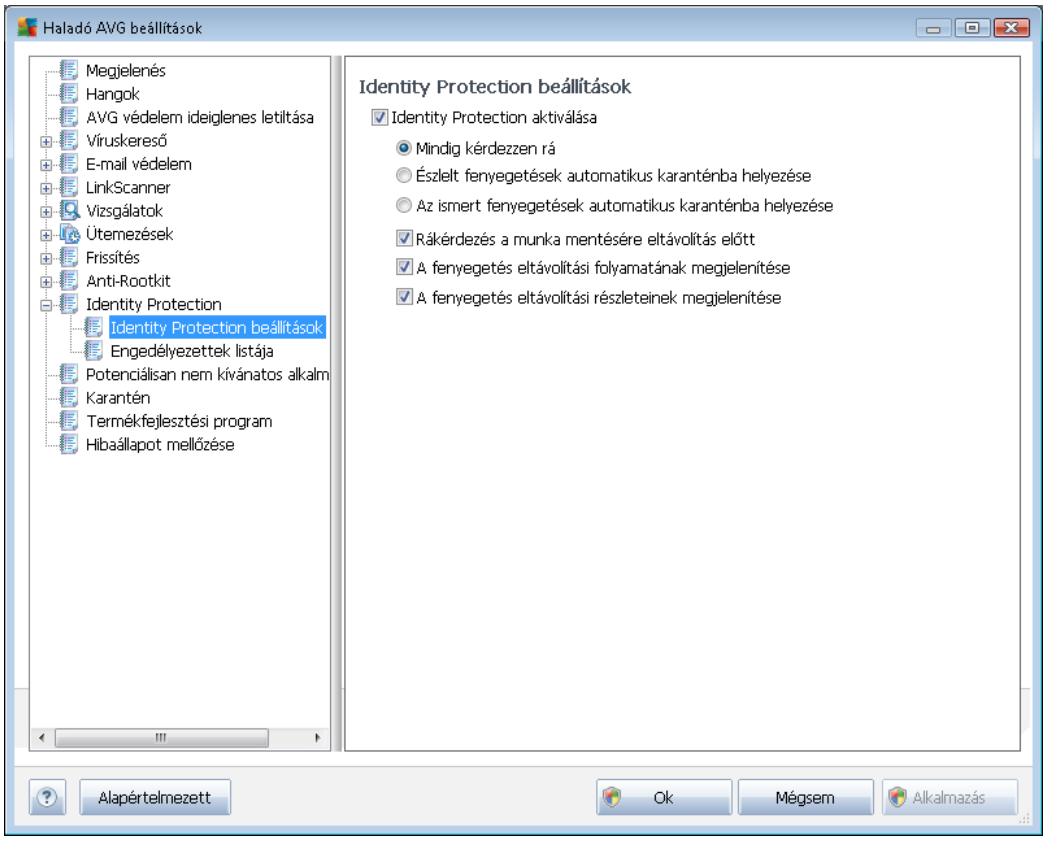
Az ***Anti-Rootkit kivételek*** párbeszédpanelen azon fájlokat adhatja meg, amelyeket ki kíván hagyni a vizsgálatból *(néhány illesztőprogramot például hibásan észlelhet a rootkit)*:



9.11. Identity Protection

9.11.1. Identity Protection beállítások

Az ***Identity Protection beállítások***panel lehetővé teszi, hogy ki és bekapcsolja az Identity Protection alapvető funkcióit:



Identity Protection aktiválása (*alapállapotban bekapcsolva*) – törölje a jelölőnégyzetet az Identity Protection összetevő kikapcsolásához.

Határozottan javasoljuk, hogy ezt az opciót ne kapcsolja ki, hacsak nem elkerülhetetlen!

Ha az Identity Protection be van kapcsolva, akkor meghatározhatja, hogy mi történjen egy fenyegetés észlelésekor:

- ***Mindig legyen kérdés*** (*alapállapotban bekapcsolva*) - ha a program fenyegetést észlel, akkor rákérdez, hogy áthelyezze-e azt a karanténba.
- ***Észlelt fenyegetések automatikus karanténba helyezése***- jelölje be ezt a jelölőnégyzetet az összes észlelt fenyegetés automatikus és azonnali áthelyezéséhez az víruskaranténjába. Az alapértelmezett beállítások szerint egy új fenyegetés észlelésekor a program rákérdez, hogy karanténba helyezze-e azt (így csak azon alkalmazásokat távolítja el, amelyeket Ön nem kíván futtatni).
- ***Ismert fenyegetések automatikus karanténba helyezése*** - jelölje be a kártevők automatikus és azonnali áthelyezéséhez az víruskaranténjába.

További opciókat is beállíthat az Identity Protection funkciójának kibővítéséhez:

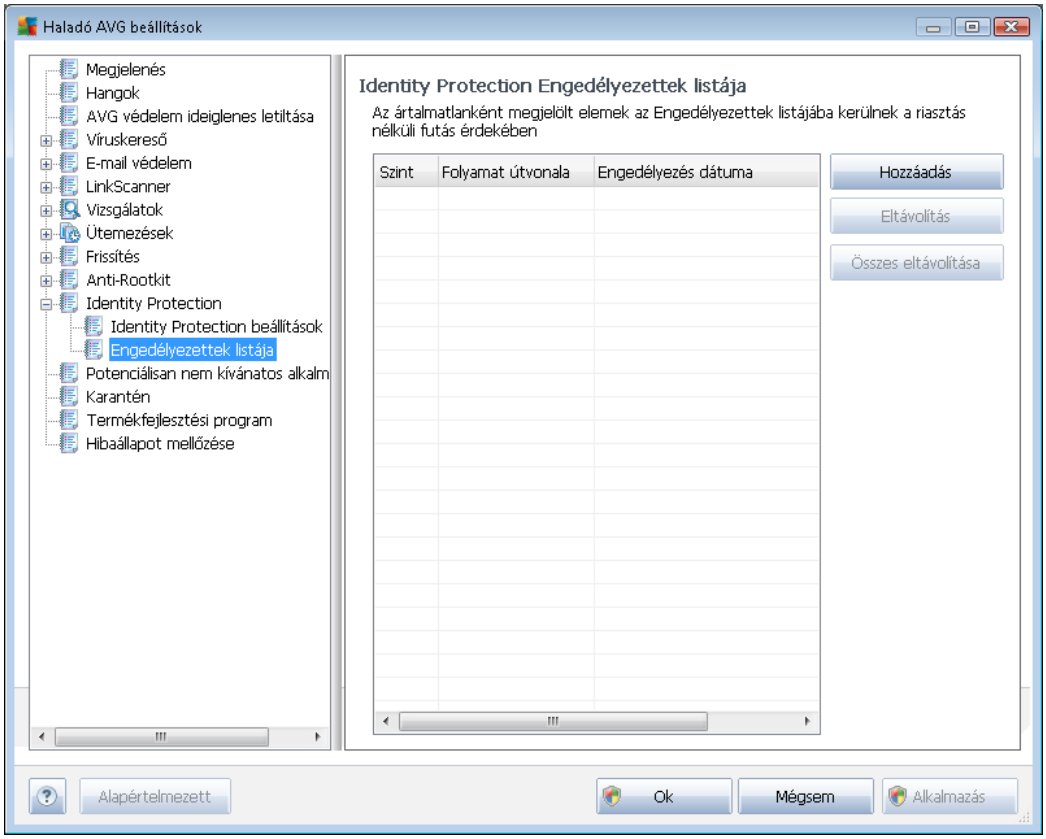
- ***Rákérdezés a munka mentésére eltávolítás előtt*** - (*alapállapotban bekapcsolva*) - jelölje be, ha azt szeretné, hogy a rendszer figyelmeztesse, mielőtt a potenciális kártevőként észlelt alkalmazást áthelyezi a karanténba. Ha az alkalmazással dolgozik, akkor a munkája elveszhet, ezért először mentse azt el. Alapállapotban ez az elem be van kapcsolva, és javasoljuk, hogy tartsa is így.

- ***Káros program eltávolítási folyamatának megjelenítése*** - (*alapállapotban bekapcsolva*) - ha bekapcsolja, akkor a kártevők észlelésekor egy új párbeszédpanel jelenik meg a kártevő eltávolítási folyamatának állapotával.

- ***Káros program eltávolításával kapcsolatos részletek megjelenítése*** - (*alapállapotban bekapcsolva*) - ha bekapcsolja, akkor az ***Identity Protection*** részletes információkat jelenít meg a karanténba helyezett objektumokról (*biztonsági szint, hely, stb.*).

9.11.2. Engedélyezettek listája

Ha az ***Identity Protection beállítások*** párbeszédpanelen nem jelölte be ***az észlelt fenyegetések automatikus karanténba helyezése*** elemet, akkor az esetleges veszélyes kártevők észlelésekor a program mindig rákérdez, hogy eltávolítsa-e azt. Ha a gyanús alkalmazást (*a viselkedése alapján*) biztonságosnak minősíti és megerősíti, hogy az maradhat a számítógépen, akkor az adott alkalmazás hozzá lesz adva az ***Identity Protection engedélyezettek listájához***, és a program nem fogja azt újra potenciális fenyegetésként észlelni:



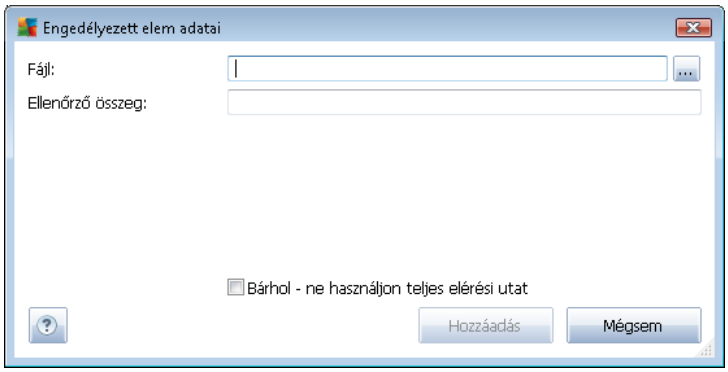
Az ***Identity Protection engedélyezettek listája*** a következő információkat tartalmazza az egyes alkalmazásokkal kapcsolatban:

- ***Súlyossági szint*** - az adott folyamat súlyossági szintjének grafikus megjelenítése egy négyszintű skálán a legkevésbé fontosabbtól (■□□□) a legfontosabbig (■■■■)
- ***A folyamat útvonala*** - útvonal az alkalmazás (*folyamat*) helyéhez
- ***Engedélyezés dátuma*** - a dátum, amikor az alkalmazást biztonságosként megjelölte

Vezérlőgombok

A vezérlőgombok az ***Identity Protection engedélyezettek listája*** felületen a következők:

- ***Hozzáadás*** - kattintson erre a gombra, ha új alkalmazást szeretne felvenni a listára. A következő panel jelenik meg:

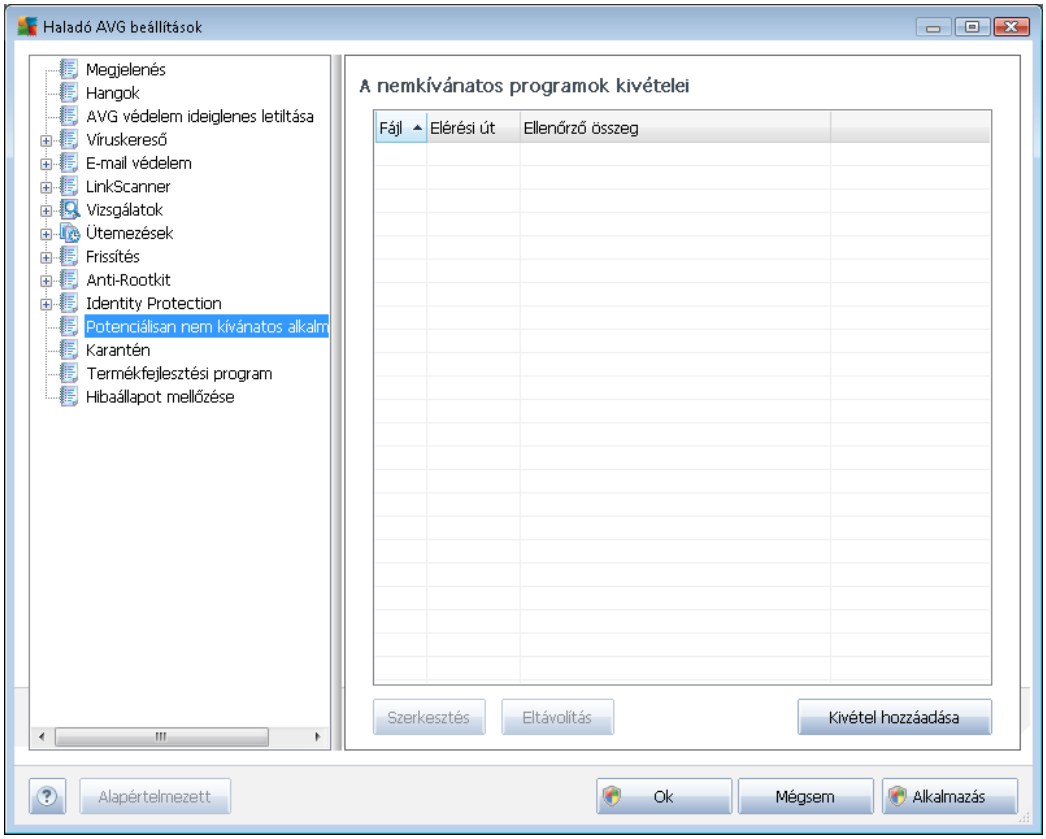


  - ***Fájl*** - írja be a teljes elérési útvonalat a fájlhoz (*alkalmazás*), amelyet kivételként kíván megadni
  - ***Ellenőrzőösszeg*** - megmutatja a fájl egyéni "aláírását". Az ellenőrző összeg egy automatikusan létrehozott karakterlánc, amellyel az AVG vírusirtó egyértelműen meg tudja különböztetni a fájlt a többi fájltól. Az ellenőrző összeg létrehozása és megjelenítése a fájl sikeres hozzáadása után történik.
  - ***Bárhol – ne használjon teljes elérési utat*** - ha az adott fájlt csak az adott helyen szeretné kivételként meghatározni, akkor ne jelölje be ezt az opciót
- ***Eltávolítás*** - nyomja meg ezt a gombot a kijelölt alkalmazás listából történő eltávolításához
- ***Összes eltávolítása*** - nyomja meg ezt a gombot az összes alkalmazás eltávolításához

9.12. Potenciálisan nemkívánatos programok

Az AVG Internet Security 2012 képes a rendszer nemkívánatos végrehajtható alkalmazásainak és DLL könyvtárainak elemzésére és azonosítására. Előfordulhat, hogy a felhasználó a számítógép bizonyos nemkívánatos programjait szeretné megtartani (mert ezeket szándékosan telepítette).

Egyes programok, főként az ingyenesek reklámprogramokat tartalmaznak. Az ilyen reklámprogramokat az **AVG Internet Security 2012** gyakran *potenciálisan nemkívánatos programként* azonosítja. Ha meg szeretné tartani ezeket a programokat, hozzáadhatja őket a Nemkívánatos programok kivételei listához:



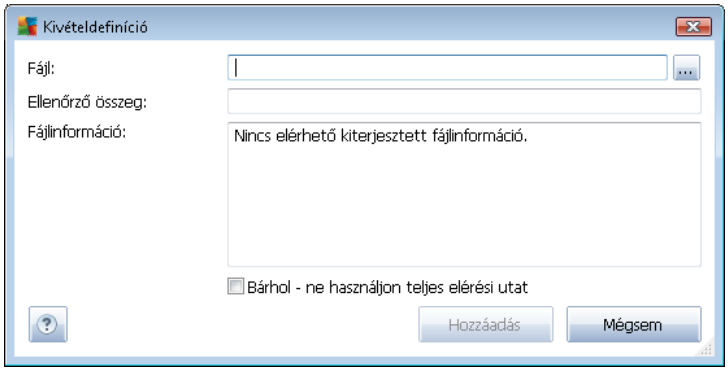
A ***A nemkívánatos programok kivételei*** panel megjeleníti a meghatározott és jelenleg érvényben lévő kivételeket a potenciálisan nemkívánatos programok szempontjából. A listát szerkesztheti, meglévő elemeket törölhet vagy új kivételeket vehet fel. A következő információk találhatók a listában az egyes kivételek esetében:

- ***Fájl*** – az adott alkalmazás pontos nevét adja meg
- ***Fájlútvonal*** - az adott alkalmazás helyét mutatja meg
- ***Ellenőrzőösszeg*** - megmutatja a fájl egyéni "aláírását". Az ellenőrző összeg egy automatikusan létrehozott karakterlánc, amellyel az AVG vírusirtó egyértelműen meg tudja különböztetni a fájlt a többi fájltól. Az ellenőrző összeg létrehozása és megjelenítése a fájl sikeres hozzáadása után történik.

Vezérlőgombok

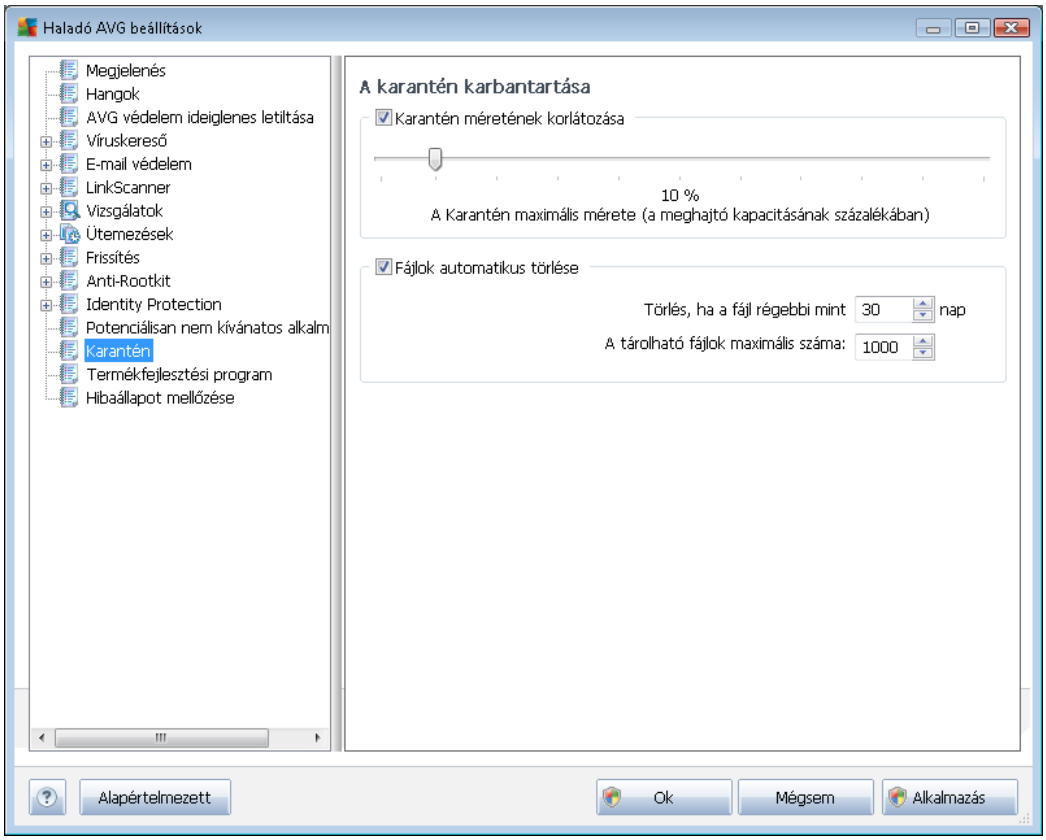
- ***Szerkesztés*** - megnyitja a szerkesztőpanelt (*megegyezik az új kivételek panellel, lásd lent*) a már létrehozott kivételekkel, ahol módosíthatja a kívánt paramétereket

- ***Eltávolítás*** - törli a kiválasztott elemeket a kivételek listájából
- ***Kivétel hozzáadása*** - megnyit egy szerkesztőpanelt, ahol meghatározhatja egy új kivétel paramétereit:



  - ***Fájl*** - írja be a kivételként megadni kívánt fájl teljes elérési útját
  - ***Ellenőrző összeg*** - megmutatja a a fájl egyéni "aláírását". Az ellenőrző összeg egy automatikusan létrehozott karakterlánc, amellyel az AVG vírusirtó egyértelműen meg tudja különböztetni a fájlt a többi fájltól. Az ellenőrző összeg létrehozása és megjelenítése a fájl sikeres hozzáadása után történik.
  - ***Fájlinformáció*** – megjeleníti a fájllal kapcsolatos további információkat *(licenc/verzióadatok stb.)*
  - ***Bárhol – ne használjon teljes elérési utat*** – ha az adott fájlt csak az adott helyen szeretné kivételként meghatározni, akkor ne jelölje be ezt a lehetőséget. Ha a jelölőnégyzet be van jelölve, akkor a megadott fájlt a helyétől függetlenül kivételként határozza meg *(adja meg a fájl teljes elérési útvonalát arra az esetre, ha a rendszer két ugyanilyen nevű fájlt talál a számítógépen)*.

9.13. Karantén



A ***Víruskarantén karbantartása*** ablak lehetővé teszi, hogy számos paramétert határozzon meg a Karanténban tárolt objektumok kezelésével kapcsolatban:

- ***Karantén méretének korlátozása*** – Használja a csúszkát a karantén maximális méretének meghatározásához. A karantén méretét a helyi lemez méretének megfelelően, annak arányában határozza meg a program.

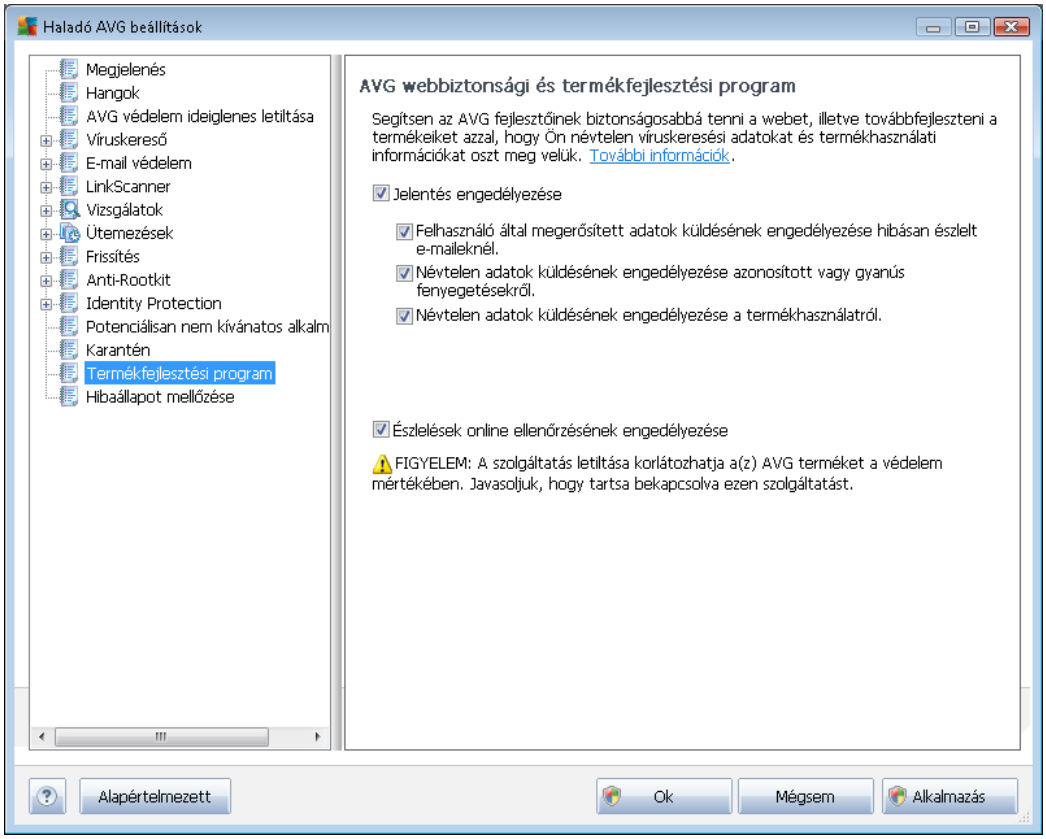
- ***Fájlok automatikus törlése*** – Ebben a részben meghatározhatja azt a maximális időtartamot, ameddig az objektum a karanténban marad (***Törlés, ha a fájl régebbi mint ... nap***), illetve a karanténban tárolható fájlok maximális számát (***A tárolható fájlok maximális száma***).

9.14. Termékfejlesztési program

Az ***AVG webbiztonsági és termékfejlesztési program*** panel meghívja Önt az AVG termékfejlesztésében való részvételre, így segíthet nekünk növelni az internet általános biztonsági szintjét. Hagyja bejelölve a ***Jelentés engedélyezése*** beállítást az észlelt fenyegetések az AVG laboratóriumai felé történő jelentésének engedélyezéséhez. Ez segít nekünk összegyűjteni a legfrissebb információkat a legújabb fenyegetésekről a világ számos pontján, és cserébe továbbfejlesztjük a védelmet mindenki számára.

A jelentés teljesen automatikus, ezért nem okoz kényelmetlenséget, és semmilyen személyes

azonosításra alkalmas adatot nem küld el. Az észlelt fenyegetések jelentése tetszőleges, de kérjük, hogy hagyja ezt a beállítást bekapcsolva, mivel így segít nekünk továbbfejleszteni a védelmet az Ön és más AVG felhasználók számára.



Manapság az egyszerű vírusoknál sokkal bonyolultabb fenyegetések is léteznek. A kártékony kódok és a veszélyes weboldalak szerzői rendkívül innovatívak, és rendszeresen tűnnek fel újfajta fenyegetések (jelentős részük az interneten). A következők a legelterjedtebbek:

- ***A vírus*** olyan rosszindulatú kód, amely sokszorosítja önmagát, szétterjed a számítógépen, és gyakran észrevétlen marad egészen addig, amíg kárt nem okoz. Egyes vírusok komoly fenyegetést jelentenek, mivel fájlokat törölnek a lemezről, szándékosan módosítják azokat, míg más vírusok nem okoznak kárt, csak zenét játszanak le például. Azonban alapvetően mégis minden vírus veszélyes a sokszorozódási képessége miatt - még egy egyszerű vírus is pillanatok alatt képes betelíteni a számítógép memóriáját, és teljesen lebéníthatja azt.

- ***A féreg*** a vírusok egyik olyan alkategóriájába tartozik, amely a vírustól eltérően semmilyen más „hordozóhoz” nem kapcsolódik, hanem egy az egyben küldi el saját magát más számítógépekre (általában e-mailben), és ennek eredményeképpen gyakran túlterheli az e-mail kiszolgálókat illetve a hálózati rendszereket.

- ***A kémprogram*** általában rosszindulatú kódként kategorizálható (*rosszindulatú kód = bármely rosszindulatú program, például vírusok*). Míg a rejtőzködő program jellemzően trójai faló, melynek célja, hogy személyes információkat (jelszavakat, hitelkártyaszámokat) szerezzen, illetve lehetővé tegye a számítógép feletti irányítás átvételét távolról egy külső

támadó számára. Természetesen mindezt a felhasználó tudta, illetve hozzájárulása nélkül.

- ***A potenciálisan nemkívánatos programok*** olyan kémprogramok, amelyek nem feltétlenül veszélyesek a számítógépre. A PUP-ra jó példa a reklámprogram, mely olyan kód, aminek célja reklámok terjesztése jellemzően felbukkanó ablakok formájában - bosszantó de nem feltétlenül káros módon.

- ***A nyomkövető sütik*** is egyfajta kémprogramnak minősülnek. Ezen apró fájlokat a rendszer a webböngészőben tárolódnak, és automatikusan elküldi a forrásoldalra a következő látogatáskor. A következő adatokat tartalmazhatják: böngészési előzmények vagy egyéb hasonló információk.

- ***Az exploit*** olyan kártékony kód, mely az operációs rendszer, az internetböngésző vagy egyéb fontos program hibáját illetve sérülékenységét használja ki

- ***Az adathalászat*** érzékeny és személyes adatok megszerzésére irányuló kísérlet, amelynek során a támadó egy megbízható és jól ismert szervezet álcája mögé bújik. A potenciális áldozatokat általában csoportos emailben keresik meg, és arra kérik őket, hogy például frissítsék bankszámlával kapcsolatos adataikat. Ehhez csak egy adott hivatkozást kell követniük, amely egy hamis banki weboldalra vezet.

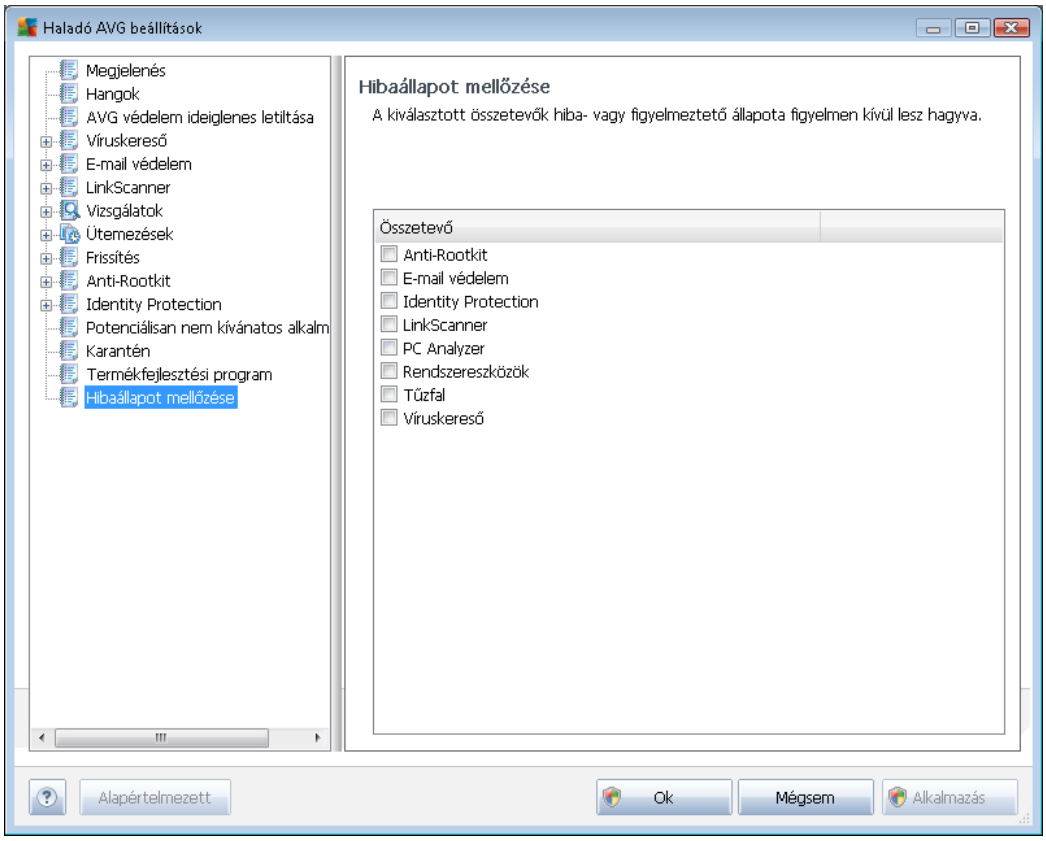
- ***A hoax*** olyan lánclevél, mely veszélyes, figyelmeztető vagy egyszerűen csak idegesítő és haszontalan információkat tartalmaz. Számos feljebb ismertetett fenyegetés hoax e-maileket használ a terjedéshez.

- ***A káros weboldalak*** szándékosan telepítenek kártékony kódot a felhasználó számítógépére. A feltört oldalak ugyanezt csinálják, azzal a különbséggel, hogy ezek legitim oldalak, melyeket a látogatók megfertőzésére használnak fel.

Az összes ilyen különböző típusú fenyegetés elleni védelem érdekében az AVG Internet Security 2012 a következő egyedi összetevőket tartalmazza. Ezek rövid leírásáért tekintse meg az Összetevők áttekintése című fejezetet.

9.15. Hibaállapot mellőzése

A ***Hibaállapot mellőzése*** párbeszédpanelen bejelölheti azon összetevőket, amelyekről nem akar értesítéseket kapni:



Alapállapotban egy összetevő sincs kiválasztva a listán. Ez azt jelenti, hogy ha valamelyik összetevő hibaállapotba lép, akkor Ön erről azonnal értesítést kap:

- ikon a tálcán - ha az AVG összes összetevője megfelelően működik, akkor az ikon négy színben jelenik meg. Viszont ha hiba történik, akkor az ikon sárga felkiáltójelre vált,
- a fennálló probléma szöveges leírása a Biztonsági állapot információk részen az AVG főablakán

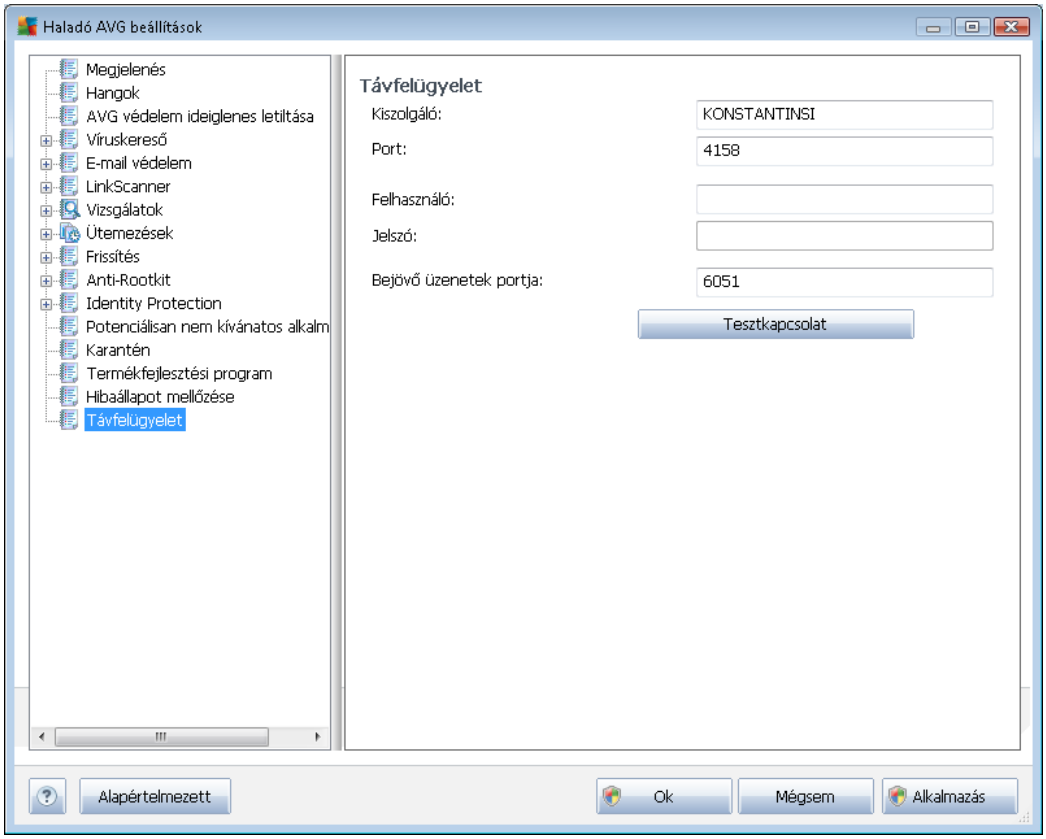
Elképzelhető olyan szituáció, hogy valamilyen okból átmenetileg ki kell kapcsolnia egy összetevőt (*ez nem javasolt, az összes összetevőt bekapcsolva kell tartania, de átmenetileg előfordulhat ilyen helyzet*). Ekkor a rendszerikon automatikusan jelzi az összetevő hibaállapotát. Ebben az esetben viszont nem beszélhetünk tényleges hibáról, mivel az összetevőt Ön szándékosan kapcsolta ki, és tudatában van a biztonsági kockázatoknak. Ugyanakkor, mivel az ikon már szürkére váltott, nem tud további esetleges hibákat jelezni.

Ezért a fenti panelen kiválaszthatja azokat az összetevőket, amelyek hibaállapotban vannak (*vagy ki vannak kapcsolva*), és nem kíván értesítést kapni róluk. Ugyanezen lehetőség *(Összetevő állapotának mellőzése)* közvetlenül is elérhető az AVG főablakának összetevők áttekintése

részében.

9.16. Távfelügyelet

A ***Távfelügyelet*** elem és ennek párbeszédpanelje csak akkor jelenik meg a navigációs fán, ha az **AVG Internet Security 2012** terméket egy AVG Business Edition licenc használatával telepítette, és a telepítési folyamat során megerősítette, hogy telepíteni kívánja a ***Távfelügyelet*** összetevőt. A távfelügyelet telepítéséről és konfigurációjáról szóló részletes leíráshoz tekintse meg a megfelelő AVG Network Edition dokumentációt, amely letölthető az AVG webhelyéről (http://www.avg.hu/),a Támogatóközpont / Letöltés résznél.



A ***Távfelügyelet*** beállítások az AVG ügyfélállomás távfelügyeleti rendszerhez történő csatlakozására vonatkoznak. Ha egy adott állomást a távfelügyelethez szeretne csatlakoztatni, akkor adja meg az alábbi paramétereket:

- ***Kiszolgáló*** - kiszolgáló neve (vagy IP-címe), amelyen az AVG Admin Server telepítve van
- ***Port*** - megmutatja azt a porszámot, amelyen keresztül az AVG ügyfél kommunikál az AVG Admin Server-rel (*az alapértelmezett portszám a 4158 - ha ezt használja, akkor nem kell megadni*)
- ***Bejelentkezés*** - ha az AVG ügyél és az AVG Admin Server közötti kommunikáció azonosítást igényel, akkor adja meg a felhasználónevet...

- ***Jelszó*** - ... és a jelszót
- ***Port a bejövő üzenetekhez*** - annak a portnak a száma, amelyen keresztül az AVG ügyfél a bejövő üzeneteket fogadja az AVG Admin Server-től

Vezérlőgombok

A ***Kapcsolat tesztelése*** gomb segít ellenőrizni, hogy a fenti adatok helyesek-e, és sikeresen lehet-e velük csatlakozni a DataCenter adatközponthoz.

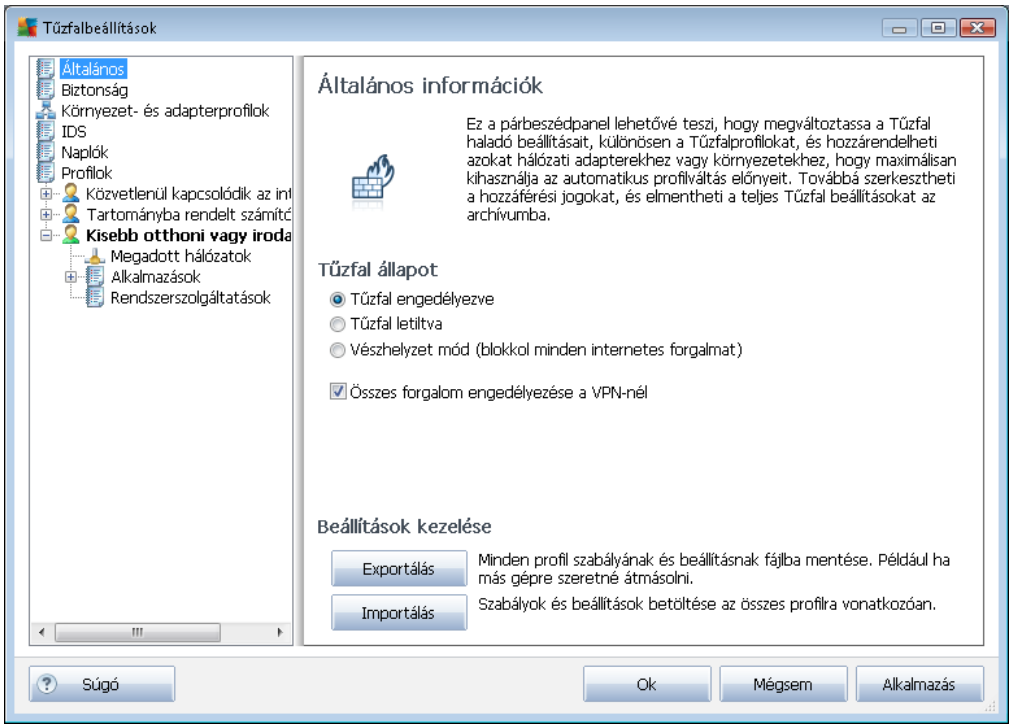
10. Tűzfalbeállítások

A Tűzfal beállítások új ablakban nyílnak meg, ahol megadhatja a haladó beállításokat.

A szoftver szállítója beállította az összes AVG Internet Security 2012 összetevőt, hogy azok optimális teljesítményt nyújtsanak. Javasoljuk, hogy ne változtassa meg az alapértelmezett beállításokat, hacsak nem feltétlenül szükséges. A beállítások módosítása kizárólag tapasztalt felhasználók számára javasolt.

10.1. Általános

Az ***Általános információk*** panel két részből áll:



Tűzfal állapota

A ***Tűzfal állapota*** részen módosíthatja a Tűzfal állapotát tetszés szerint:

- ***Tűzfal engedélyezve*** - válassza ezt az opciót azon alkalmazások kommunikációjának engedélyezéséhez , melyek "engedélyezett" minősítést kaptak a Tűzfal profilban.
- ***Tűzfal letiltva*** – Ez a lehetőség teljesen kikapcsolja a tűzfalat, és a rendszer minden hálózati forgalmat ellenőrzés nélkül engedélyez.
- ***Vészhelyzet mód (blokkol minden internetes adatforgalmat)*** – Válassza ezt a lehetőséget, ha minden adatforgalmat le kíván tiltani minden porton. A Tűzfal ekkor továbbra is működik, de minden adatforgalom megszakad.

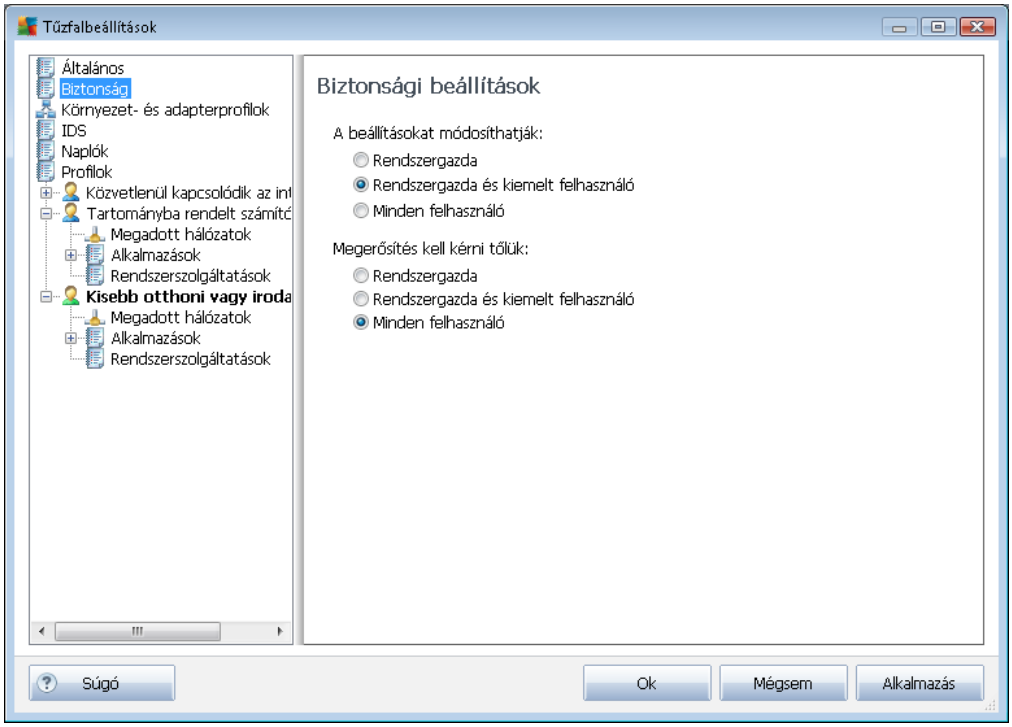
- ***Összes forgalom engedélyezése a VPN-nél*** *(alapértelmezés szerint bekapcsolva)* – Ha VPN kapcsolatot *(virtuális magánhálózatot)* használ (például az irodai hálózathoz csatlakozik otthonról), akkor javasoljuk, hogy jelölje be ezt a jelölőnégyzetet.***Az AVG Tűzfal*** automatikusan átnézi a hálózati adaptereket, és kiválasztja a VPN kapcsolathoz tartozókat, majd engedélyezi az összes alkalmazás kapcsolódását a célhálózathoz *(csak olyan alkalmazásoknál, amelyekhez nincs hozzárendelve külön Tűzfal szabály)*. Normál hálózati adapterekkel rendelkező rendszereken ez az egyszerű lépés időt takarít meg Önnek, mivel nem kell egyesével beállítania az összes alkalmazás kapcsolódását a VPN hálózatra.

Megjegyzés: *A VPN kapcsolat engedélyezéséhez engedélyezze a következő rendszerprotokollokat: GRE, ESP, L2TP, PPTP. Ezt a Rendszerszolgáltatások panelen végezheti el.*

Beállítások kezelése

A ***Beállítások kezelése*** területen ***exportálhat*** vagy ***importálhat*** tűzfal beállításokat. Például exportálhatja a meghatározott tűzfal szabályait és beállításait biztonsági másolatokba, vagy ellenkezőleg, importálhat egy ilyen beállításokat tartalmazó biztonsági másolatot.

10.2. Biztonság



A ***Biztonsági beállítások*** panelen meghatározhatja az általános szabályokat a Tűzfal viselkedéséhez, függetlenül a kiválasztott profiltól:

- ***A beállításokat módosíthatják*** – Itt adhatja meg, hogy ki változtathatja meg a Tűzfal

beállításait.

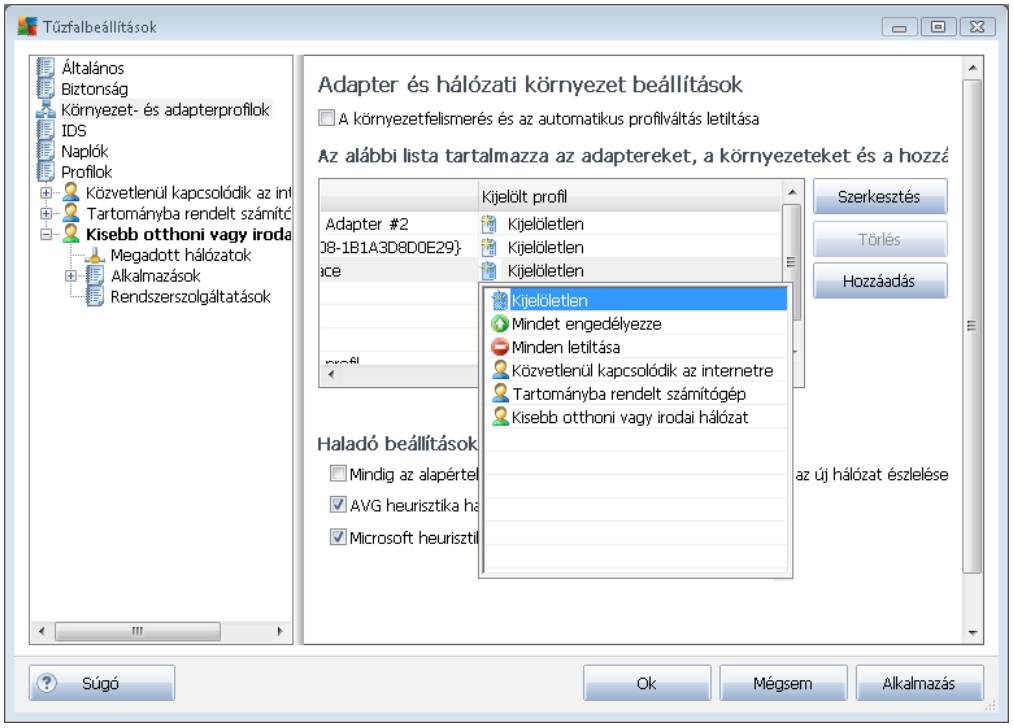
- ***Megerősítést kell kérni tőlük*** – Meghatározza, hogy kiknek jelenjenek meg megerősítő párbeszédpanelek *(olyan párbeszédpanelek, amelyek a megadott Tűzfal szabályban nem meghatározott helyzetekben kérdeznek rá, hogy mit kíván tenni)*.

Mindkét esetben a következő felhasználói csoportok valamelyikéhez rendelheti hozzá az adott jogokat:

- ***Rendszergazda*** – Teljes körű hozzáféréssel rendelkezik számítógéphez, és joga van az egyes felhasználókat külön definiált jogosultsággal rendelkező csoportokba sorolni.
- ***Rendszergazdák és kiemelt felhasználók*** – A rendszergazda bármely felhasználót egy adott csoportba (*Kiemelt felhasználók*) sorolhat, és meghatározhatja a csoporttagok jogait.
- ***Minden felhasználó*** – Egyéb felhasználók, akik nem tartoznak egyik külön definiált csoportba sem.

10.3. Terület- és adapterprofilok

Az ***Adapter és hálózati terület beállítások*** panelen szerkesztheti a beállításokat az adapterekhez és hálózatokhoz hozzárendelendő profilokhoz:



- ***A környezetfelismerés és az automatikus profilváltás letiltása*** *(alapértelmezés szerint ki van kapcsolva)* – A megadott profilok egyike hozzárendelhető minden egyes hálózati

csatolótípushoz, az egyes területeknek megfelelően. Ha nem kíván megadni meghatározott profilokat, akkor a rendszer egyetlen közös profilt használ. Ha úgy dönt, hogy külön profilokat határoz meg, és hozzárendeli őket bizonyos adapterekhez, illetve környezetekhez, továbbá később valamilyen okból váltani szeretne köztük, akkor jelölje be a ***Környezetfelismerés és az automatikus profilváltás letiltása*** opciót.

- ***Adapterek, területek és hozzárendelt profilok listája*** – Ebben a listában az észlelt adapterek és területek áttekintése található. Mindegyikhez hozzárendelhet egy adott profilt a meghatározott profilok menüjéből. A menü megnyitásához kattintson a bal gombbal a megfelelő elemre az adapterek listájában *(a Hozzárendelt profil oszlopban)*, és válassza ki a profilt a helyi menüből.

Haladó beállítások

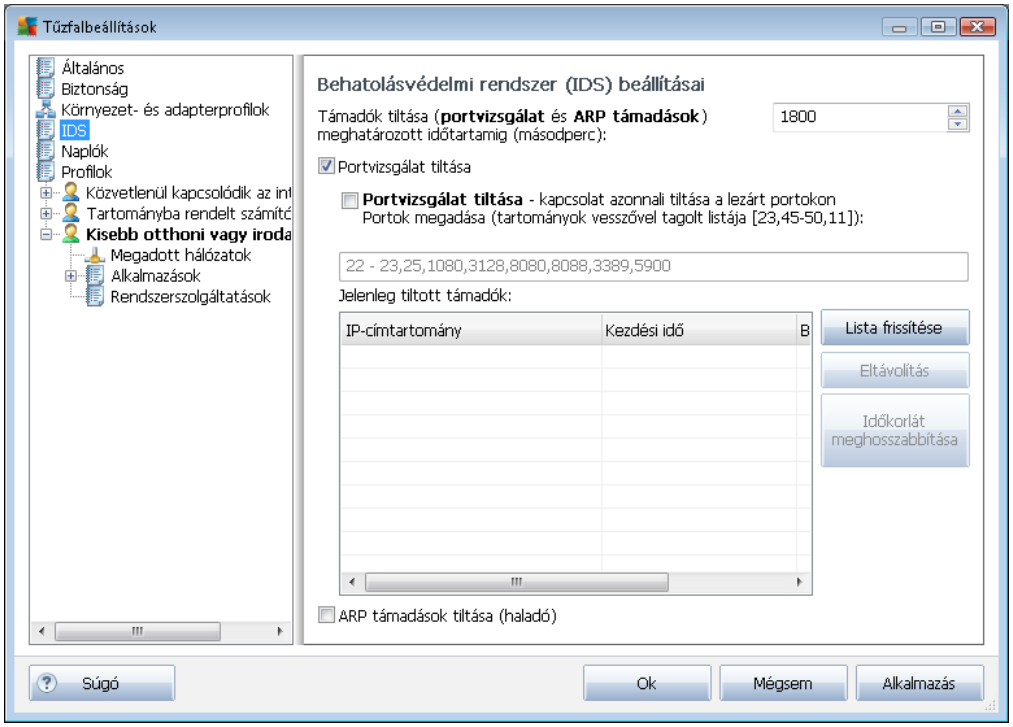
- ***Mindig az alapértelmezett profilt használja, és ne jelenítse meg az új hálózat észlelése párbeszédpanelt –*** Ha a számítógép új hálózatra csatlakozik, a Tűzfal értesíti Önt, és megjelenít egy párbeszédpanelt, ahol kiválaszthatja a hálózati kapcsolat típusát, és hozzárendelhet egy Tűzfal profilt. Ha nem szeretné megjeleníteni ezt a párbeszédpanelt, akkor jelölje be ezt a jelölőnégyzetet.

- ***AVG heurisztika használata új hálózatok észlelésekor –*** Lehetővé teszi az újonnan észlelt hálózattal kapcsolatos adatok összegyűjtését az AVG saját mechanizmusának segítségével (*ez a beállítás azonban csak Windows Vista vagy újabb operációs rendszerek esetén érhető el*).

- ***Microsoft heurisztika használata új hálózatok észlelésekor –*** Az újonnan észlelt hálózattal kapcsolatos adatokat a rendszer a Windows szolgáltatástól szerzi be (*ez a beállítás azonban csak Windows Vista vagy újabb operációs rendszerek esetén érhető el*).

10.4. IDS

A Behatolásvédelmi rendszer egy különleges viselkedéselemzési szolgáltatás, amely a számítógép bizonyos portjait használó gyanús kommunikációs kísérletek észlelésére és letiltására szolgál. Az IDS paraméterek a ***Behatolásvédelmi rendszer (IDS) beállításai*** párbeszédpanelen állíthatók be:



A ***Behatolásvédelmi rendszer (IDS) beállításai*** panel a következő konfigurációs lehetőségeket kínálja:

- ***Támadók (portvizsgálat és ARP támadások) letiltása adott időtartamig*** – Itt határozható meg, hogy a rendszer hány másodpercig tiltson le egy portot, ha gyanús adatforgalmat észlel rajta. Alapértelmezés szerint az időtartam 1800 másodperc (*30 perc*).

- ***Portvizsgálat tiltása*** *(alapértelmezés szerint bekapcsolva)* – Jelölje be a jelölőnégyzetet minden bejövő adatforgalom tiltásához az összes TCP és UDP porton. Az ilyen kapcsolatok esetén öt próbálkozás engedélyezett, a hatodikat blokkolja a rendszer. Alapértelmezés szerint a funkció be van kapcsolva, és javasoljuk, hogy hagyja így. Ha bekapcsolva hagyja a ***Portvizsgálat tiltása*** lehetőséget, további részletes beállításokat adhat meg *(máskülönben a következő elem nem aktív)*:

    - ***Portvizsgálat tiltása*** – A jelölőnégyzet bejelölésével azonnal letilthatja a kommunikációs kísérleteket az alábbi szövegmezőben meghatározott portokon. Az egyes portokat és porttartományokat vesszővel válassza el. Megtalálható itt az ajánlott portok listája, amennyiben használni kívánja ezt a szolgáltatást.

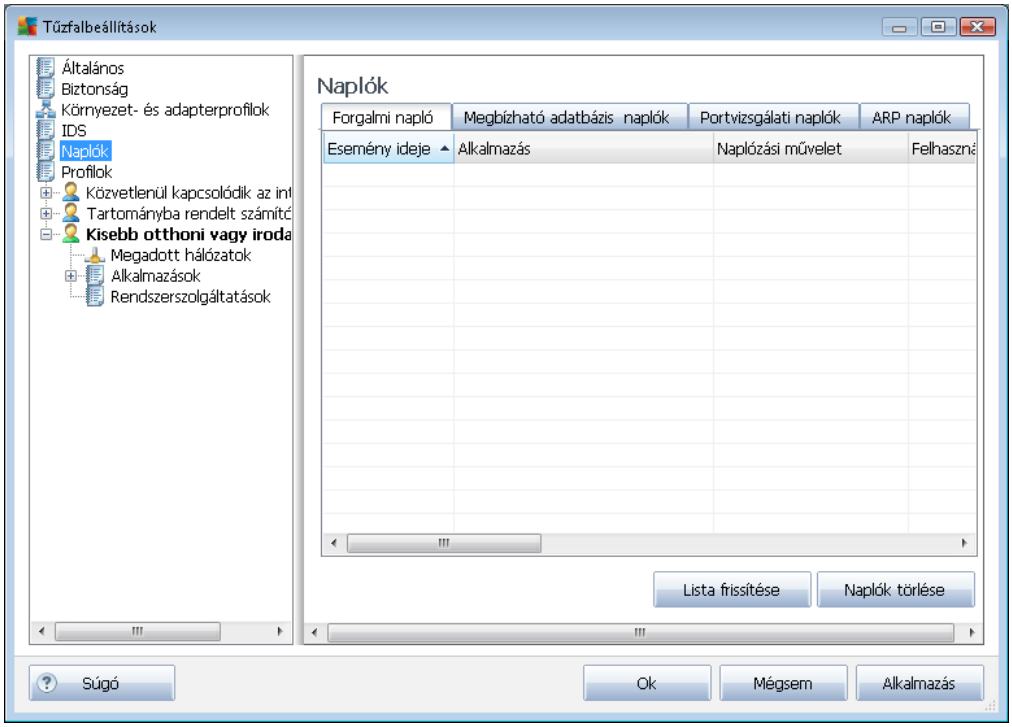
    - Jelenleg tiltott támadók – Listázza a Tűzfal által aktuálisan blokkolt összes kommunikációs kísérletet. A tiltott kísérletek teljes listája megtekinthető a *Portvizsgálati naplók lap* Naplók párbeszédpanelén .

- ***ARP támadások tiltása (haladó)*** *(alapértelmezés szerint kikapcsolva)* – Az ***IDS*** által potenciálisan veszélyesként észlelt, a helyi hálózaton észlelt kommunikációs kísérletek különleges fajtáinak tiltását aktiválja. A ***Támadók tiltása adott időtartamig*** részben megadott időtartam érvényes. Javasoljuk, hogy csak a helyi hálózat típusával és kockázati szintjével tisztában lévő tapasztalt felhasználók használják ezen szolgáltatást.

Vezérlőgombok

- ***Lista frissítése*** - nyomja meg ezt a gombot a lista frissítéséhez (*a legutóbb tiltott adatforgalmakkal együtt*)
- ***Eltávolítás*** - nyomja meg ezt a gombota kijelölt tiltás feloldásához
- ***Időtartam hosszabbítása*** - nyomja meg ezt a gombot a kijelölt adatforgalom tiltásának meghosszabbításához. Egy új párbeszédpanel jelenik meg részletes beállításokkal, ahol megadhatja az adott dátumot és időt, vagy a korlátlan időtartamot.

10.5. Naplók



A ***Naplók*** párbeszédpanel lehetővé teszi, hogy megtekintse a Tűzfal műveletek és események részletes naplóját (*esemény ideje, alkalmazás neve, kapcsolódó naplóművelet, felhasználó neve, PID, forgalom iránya, protokoll típus, a távoli és a helyi portok száma stb.*)négy fülön:

- ***Forgalmi napló*** - információk a hálózatot elérni kívánó összes alkalmazás tevékenységéről.
- ***A Megbízható adatbázis naplói*** - *A Megbízható adatbázis* egy olyan belső AVG adatbázis, amely információkat gyűjt a megbízható és tanúsított alkalmazásokról (amelyek mindig kommunikálhatnak az interneten). Ha egy új alkalmazás csatlakozni próbál a hálózatra (*és még nincs tűzfalszabály meghatározva az alkalmazáshoz*), akkor Önnek kell eldöntenie, hogy engedélyezi-e a hálózati kommunikációt az adott alkalmazás számára. Az AVG ellenőrzi a *Megbízható adatbázist*, és ha az alkalmazás megtalálható benne,

akkor azt automatikusan kiengedi a hálózatra. Ha a program nem talál semmilyen információt az alkalmazásról az adatbázisban, akkor Ön egy külön párbeszédpanelen engedélyezheti az alkalmazás számára a hálózati hozzáférést.

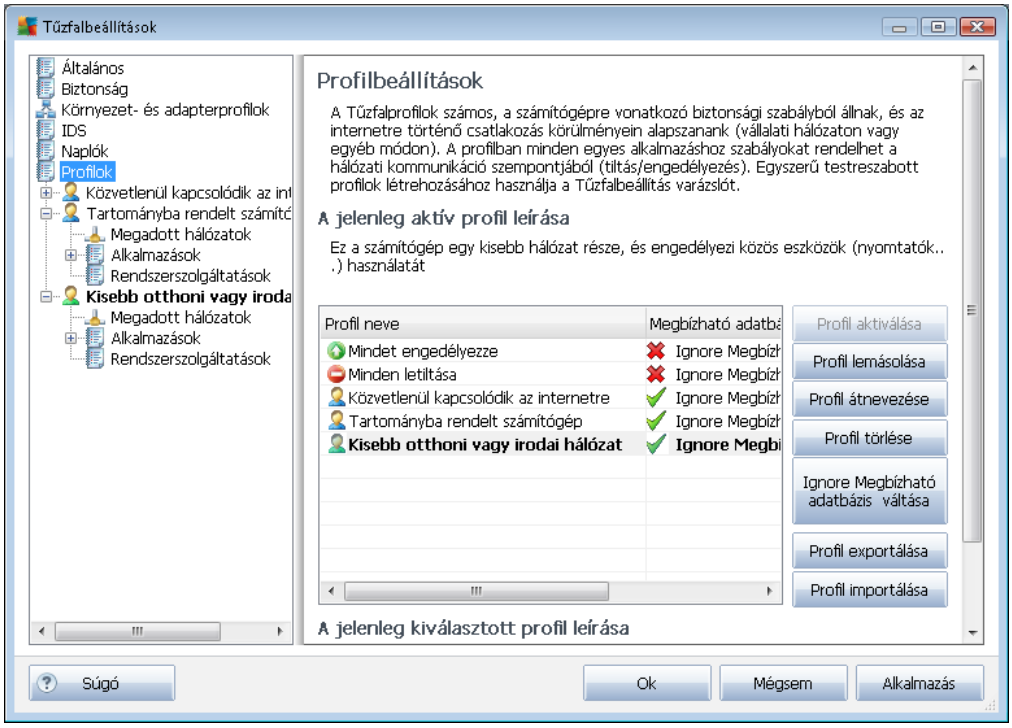
- ***Portvizsgálati naplók*** – í behatolásvédelmi rendszer minden tevékenységét naplózza.
- ***ARP napló*** - naplózza a helyi hálózatok azon különleges kommunikációs kísérleteit (*ARP támadások tiltása opció*), amelyeket a behatolásvédelmi rendszer esetlegesen veszélyesnek minősített.

Vezérlőgombok

- ***Lista frissítése*** – Az összes naplózott paraméter rendezhető a kiválasztott attribútum alapján időrendben (*dátum*) vagy betűrendben (*egyéb oszlopok*). Ehhez kattintson a megfelelő oszlopra. Használja a ***Lista frissítése*** gombot a megjelenített információk frissítéséhez.
- ***Naplók törlése*** – Kattintson ide a diagramon található összes bejegyzés törléséhez.

10.6. Profilok

A ***Profilbeállítások*** párbeszédpanelen megtalálja az összes elérhető profil listáját:



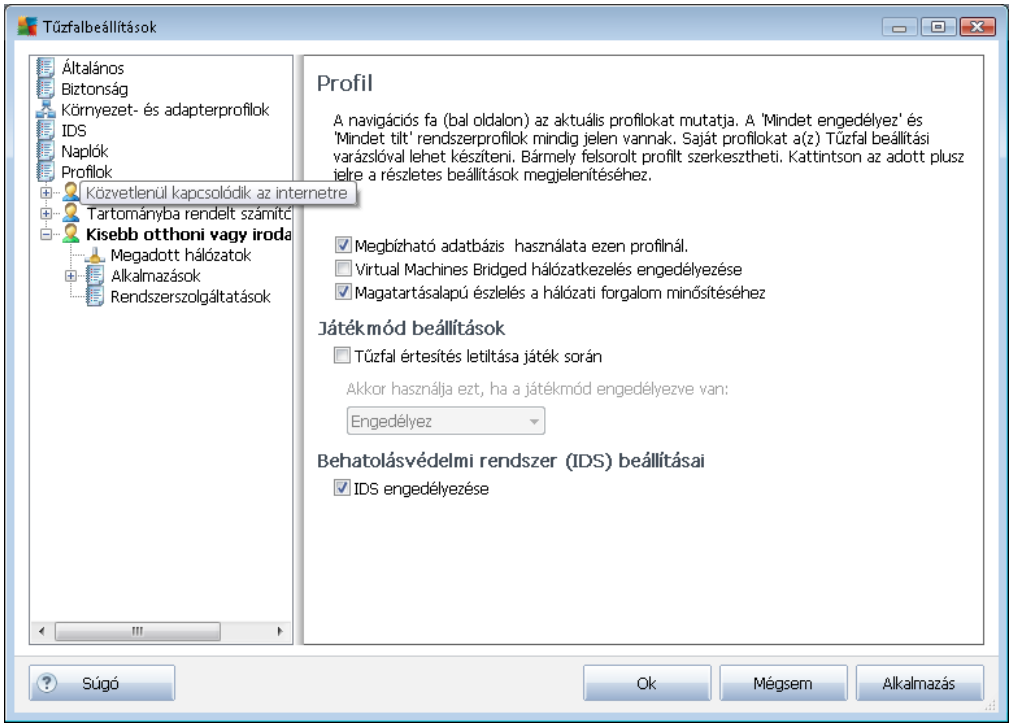
A Rendszerprofilok *(Minden engedélyezése, Minden letiltása)* nem szerkeszthetők. Azonban az összes saját profil *(Közvetlen csatlakozás az internetre , Tartományba rendelt számítógép, Kisebb otthoni vagy irodai hálózat)* szerkeszthető ezen a párbeszédpanelen a következő vezérlőgombokkal:

- ***Profil aktiválása*** – Ez a gomb aktiválja az adott profilt, azaz a Tűzfal ezt fogja használni a hálózati forgalom szabályozásához.
- ***Profil lemásolása*** – Pontos másolatot készít a kijelölt profilról. Ezt később szerkesztheti és átnevezheti, így egy új profilt hozhat létre az eredeti alapján.
- ***Profil átnevezése*** – Lehetővé teszi, hogy új nevet adjon a kijelölt profilnak.
- ***Profil törlése*** – Törli a kijelölt profilt a listából.
- ***Megbízható adatbázis bekapcsolása*** – A kiválasztott profilhoz bekapcsolhatja a *Megbízható adatbázis* információ használatát (*a Megbízható adatbázis olyan belső AVG adatbázis, amely adatokat gyűjt a hálózaton kommunikáló megbízható és tanúsított alkalmazásokról.*).
- ***Profil exportálása*** – A kijelölt profilbeállításokat egy fájlba menti későbbi használat céljából.
- ***Profil importálása*** – A profilbeállításokat egy korábban mentett konfigurációs fájlból tölti be.

A panel alsó részén megtalálhatja az aktuálisan kiválasztott profil leírását.

A listában lévő profilok alapján a ***Profil*** panelen a bal navigációs menü megfelelően változik. Mindegyik létrehozott profil külön ágat képvisel a ***Profil*** részben. Az adott profilokat a következő paneleken szerkesztheti (*ezek minden profilnál azonosak*):

10.6.1. Profilinformációk



A ***Profile information*** dialog is the first dialog of a section where you can edit configuration of each profile in separate dialogs referring to specific parameters of the profile.

- ***Megbízható adatbázis használata ezen profil esetén*** (*alapértelmezés szerint be van kapcsolva*) – Jelölje be ezt a lehetőséget a *Megbízható adatbázis* aktiválásához (*AVG adatbázis, amely információkat gyűjt az online kommunikációt folytató, megbízható és hitelesített alkalmazásokról. Ha nincs szabály megadva az adott alkalmazáshoz, akkor döntse el, hogy engedi-e kommunikálni az adott alkalmazást a hálózaton. Az AVG ellenőrzi a megbízható adatbázist, és ha az alkalmazás szerepel benne, akkor azt a program biztonságosnak tekinti, és kiengedi a hálózatra. Ellenkező esetben döntse el, hogy engedi-e kommunikálni az adott alkalmazást a hálózaton*)az adott profil esetében

- ***Virtual Machines Bridged hálózatkezelés engedélyezése*** (*alapértelmezés szerint kikapcsolva*) – Ezen elem bejelölésével a VMware részét képező virtuális gépek közvetlenül csatlakozhatnak a hálózathoz.

- ***Magatartásalapú észlelés a hálózati forgalom minősítéséhez*** (*alapértelmezés szerint bekapcsolva*) – Jelölje be ezt a lehetőséget, hogy engedélyezze a Tűzfal számára az Identity Protection funkció használatát egy alkalmazás értékelésekor – az Identity Protection meg tudja állapítani, hogy az alkalmazás gyanús vagy megbízható, és hogy engedélyezhető-e az online kommunikációja.

Játékmód beállításai

A ***Játékmód beállításai*** szakaszban a megfelelő elem bejelölésével megadhatja, hogy megjelenjenek-e a Tűzfal értesítő üzenetei, miközben teljes képernyős alkalmazás fut a számítógépen (*jellemzően játékok, de bármely teljes képernyős alkalmazásra vonatkozik a beállítás, például PPT-prezentációk*), mivel ezen üzenetek zavaróak lehetnek.

Ha bejelöli a ***Tűzfal értesítések letiltása játékok során*** elemet, akkor a legördülő menüből válassza ki a megfelelő műveletet a hálózattal kommunikálni próbálló új alkalmazásokhoz (*kérdés megjelenítése*). Majd engedélyezheti vagy letilthatja ezen alkalmazások kommunikációját.

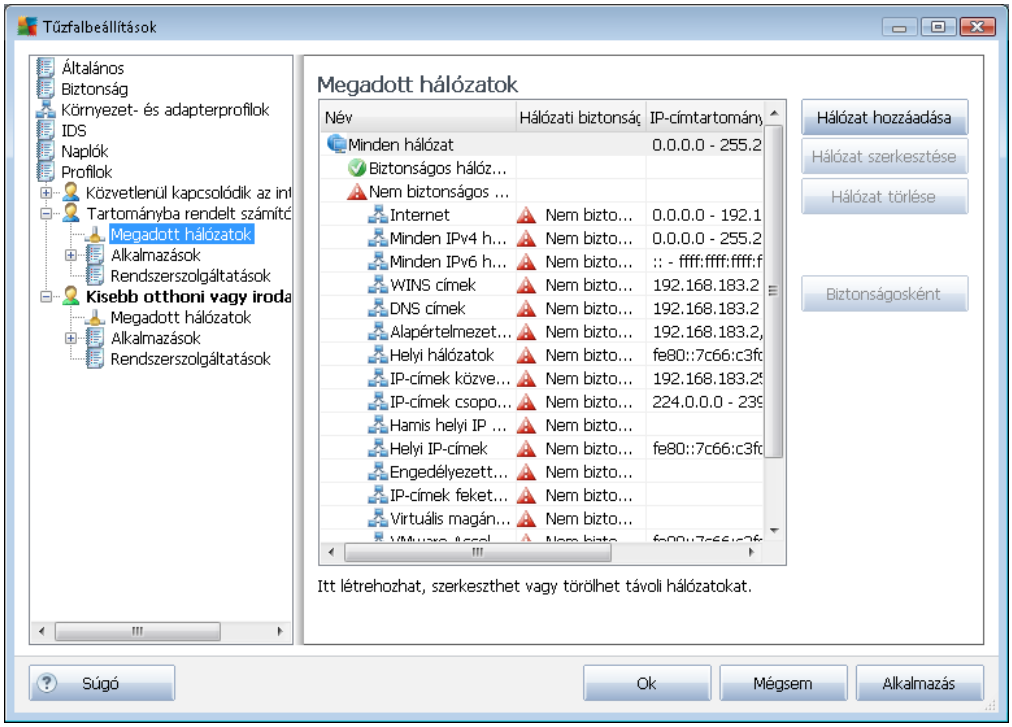
Ha a játékmód be van kapcsolva, akkor a rendszer az összes ütemezett feladatot (*vizsgálatot, frissítést*) elhalasztja az alkalmazás bezárásáig.

Behatolásvédelmi rendszer (IDS) beállításai

Jelölje be az ***IDS engedélyezése*** jelölőnégyzetet a számítógép meghatározott portjain keresztüli gyanús kommunikációs kísérleteket azonosító és blokkoló, különleges viselkedést elemző szolgáltatás *bekapcsolásához (a szolgáltatás beállításával kapcsolatos részletekért tekintse meg a dokumentáció IDS fejezetét).*

10.6.2. Megadott hálózatok

A ***Megadott hálózatok*** panel felsorolja az összes hálózatot, melyhez a számítógép csatlakozik.

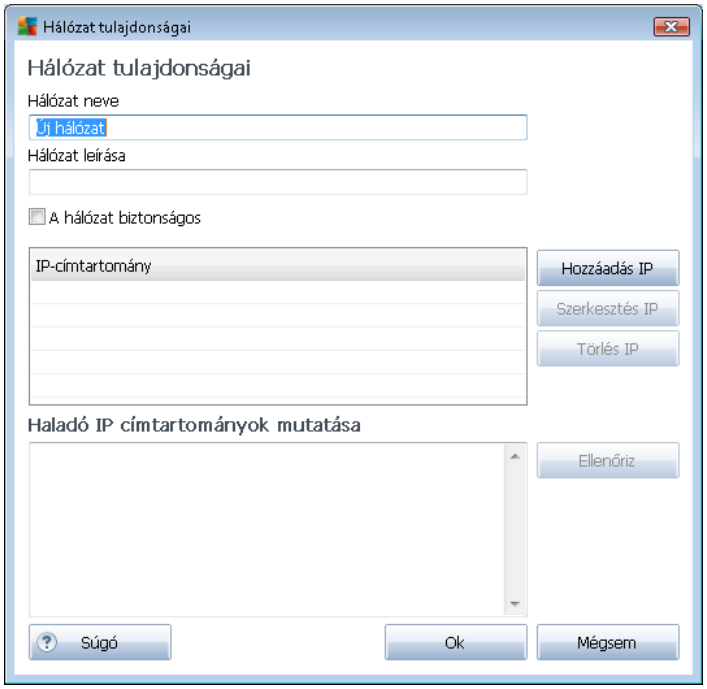


A lista a következő információkat tartalmazza minden egyes észlelt hálózattal kapcsolatban:

- ***Hálózatok*** – Felsorolja az összes hálózatot, amelyhez a számítógép csatlakozik.
- ***Hálózati biztonság*** – Alapértelmezés szerint egy hálózat sem biztonságos. Csak akkor használja ezt a funkciót, ha biztos benne, hogy a hálózat biztonságos (*kattintson a megfelelő hálózatra a listában, és válassza a Biztonságos lehetőséget a helyi menüből*) – ezután az alkalmazás az összes biztonságos hálózattal kommunikálhat a Biztonságos engedélyezése beállítású szabályoknak megfelelően.
- ***IP-címtartomány*** – Minden egyes hálózatot automatikusan észlel a rendszer, és IP-címtartományként határoz meg.

Vezérlőgombok

- ***Hálózat hozzáadása*** – Megnyitja a ***Hálózat tulajdonságai*** párbeszédpanelt, ahol szerkesztheti az újonnan meghatározott hálózat paramétereit:



Ezen a panelen meghatározhatja a ***Hálózat nevét***, a ***Hálózat leírását***, és beállíthatja a hálózatot biztonságosként. Az új hálózatot manuálisan is meghatározhatja egy külön ablakban az ***IP hozzáadása*** gomb segítségével (vagy ***IP szerkesztése*** / ***IP törlése***). Ezen a panelen meghatározhatja a hálózatot egy IP-tartomány vagy maszk megadásával. Nagy számú hálózat egyszerre történő hozzáadásakor használhatja a ***Haladó IP-cím tartományok mutatása***lehetőséget: adja meg a hálózatok listáját az adott szövegmezőben (*bármilyen szabványos formátum támogatott*), majd nyomja meg az ***Ellenőrzés*** gombot a megfelelő formátum ellenőrzéséhez. Ezután nyomja meg az ***OK*** gombot a megerősítéshez és az adatok mentéséhez.

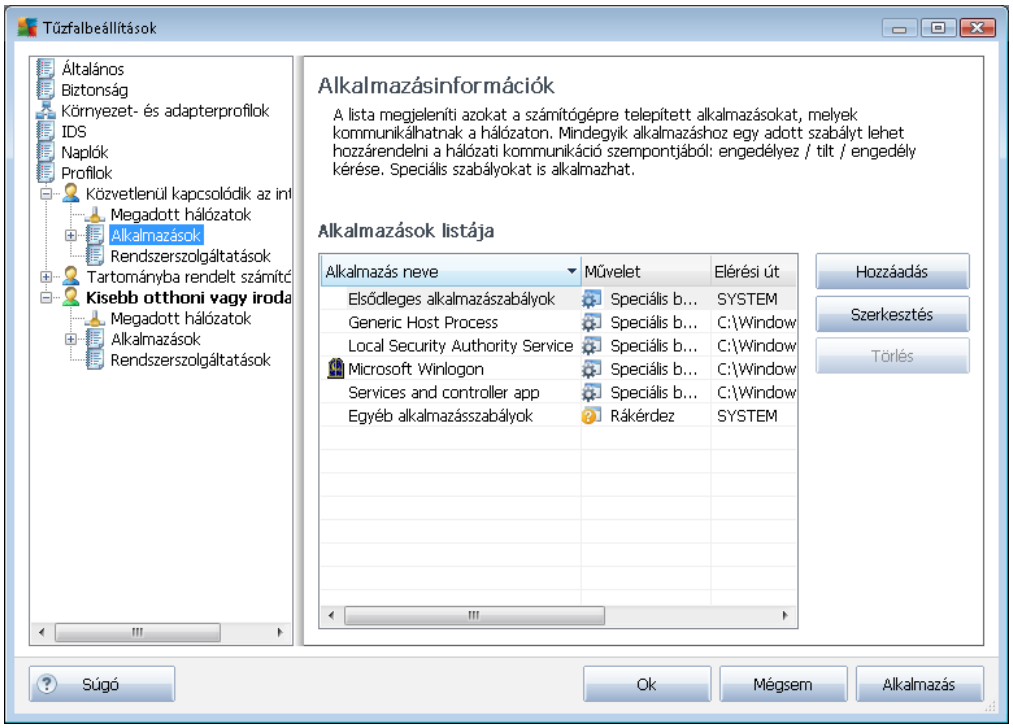
- ***Hálózat szerkesztése*** – Megnyitja a ***Hálózat tulajdonságai*** párbeszédpanelt (*lásd fent*), ahol egy már meghatározott hálózat paramétereit szerkesztheti (*a párbeszédpanel megegyezik az új hálózat hozzáadására szolgáló ablakkal, lásd az előző bekezdés leírását*).

- ***Hálózat törlése*** – Eltávolítja a kijelölt hálózatot a listából.

- ***Megjelölés biztonságosként*** – Alapértelmezés szerint egy hálózat sem biztonságos. Csak akkor használja ezt a gombot, ha teljesen biztos benne, hogy a hálózat biztonságos (*és fordítva, ha a hálózat biztonságosként van megjelölve, a gomb a „Megjelölés nem biztonságosként”* szövegre vált).

10.6.3. Alkalmazások

Az ***Alkalmazásadatok*** panel felsorolja az összes telepített alkalmazást, melynek szüksége van a hálózati kommunikációra, illetve megjeleníti a hozzájuk rendelt műveleteket:



Az ***Alkalmazások listája*** felületen a program által a számítógépen észlelt alkalmazások jelennek meg (*amelyekhez megfelelő műveleteket is rendelt a program*) . A következő művelettípusokat lehet használni:

- - Kommunikáció engedélyezése az összes hálózaton
- - Kommunikáció engedélyezése csak biztonságosnak minősített hálózatokon
- - Kommunikáció tiltása
- - Megjeleníti a megerősítő párbeszédpanelt (*a felhasználó eldöntheti, hogy engedélyezi vagy tiltja az alkalmazás kommunikációját a hálózaton*)
- - Megadott haladó beállítások

Vegye figyelembe, hogy csak már telepített alkalmazásokat ismer fel a program. Ezért új alkalmazás telepítése után meg kell hozzá határozni a megfelelő tűzfalszabályokat. Alapértelmezés szerint, ha egy új alkalmazás első alkalommal próbál csatlakozni a hálózatra, akkor a tűzfal automatikusan létrehoz egy szabályt a Megbízható adatbázis alapján, vagy Önnek kell eldöntenie, hogy engedélyezi-e vagy letiltja a kommunikációt. Az utóbbi esetben válaszát elmentheti állandó szabályként (amely megjelenik ezen a panelen).

Természetesen azonnal létrehozhat szabályokat az új alkalmazásoknak – nyomja meg ezen a

panelen a ***Hozzáadás*** gombot, és adja meg az alkalmazás részleteit.

Az alkalmazásokat leszámítva a lista két külön elemet tartalmaz:

- ***Az Elsődleges alkalmazásszabályok*** (*a lista tetején*) tetszőlegesek, és mindig az alkalmazásszabályok előtt kerülnek alkalmazásra.
- ***Az Egyéb alkalmazásszabályok*** (*a lista alján*) utolsóként kerülnek alkalmazásra, ha semmilyen más szabály nem lép érvénybe, pl. ismeretlen vagy nem meghatározott alkalmazások.

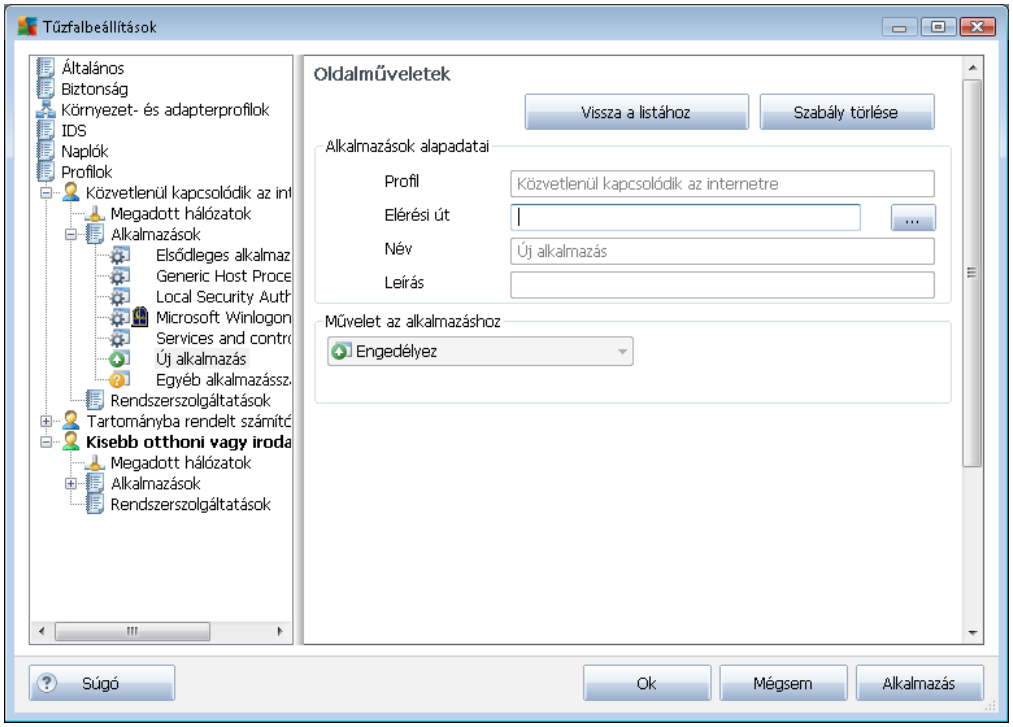
Ezen elemek más beállításokkal rendelkeznek mint a normál alkalmazások, és módosításukat csak tapasztalt felhasználóknak javasoljuk. Javasoljuk, hogy ne módosítsa a beállításokat.

Vezérlőgombok

A lista szerkesztése a következő kezelőgombokkal történik:

- ***Hozzáadás*** – Megnyit egy üres Oldalműveletek párbeszédpanelt új alkalmazásszabályok meghatározásához.
- ***Szerkesztés*** – Megnyitja ugyanezen Oldalműveletek párbeszédpanelt egy meglévő alkalmazás-szabálykészlet szerkesztéséhez.
- ***Törlés*** – Törli a kijelölt alkalmazást a listából.

Az ***Oldalműveletek*** párbeszédpanelen részletesen meghatározhatja a beállításokat az adott alkalmazáshoz:



Vezérlőgombok

Két vezérlőgomb áll rendelkezésre a párbeszédpanel tetején:

- ***Vissza a listához*** – Kattintson erre a gombra az összes alkalmazásszabály áttekintésének megjelenítéséhez.
- ***Szabály törlése*** – Kattintson erre a gombra az aktuálisan megjelenített alkalmazásszabály törléséhez. ***Vegye figyelembe, hogy ez a művelet nem vonható vissza.***

Alkalmazások alapadatai

Ebben a részben adja meg az alkalmazás ***nevét*** és tetszőlegesen a ***leírását*** (*saját információk röviden*). Az ***Elérési út*** mezőben adja meg az alkalmazás (*a futtatható fájl*) teljes elérési útját, vagy keresse meg a „***...***” gomb segítségével.

Alkalmazásművelet

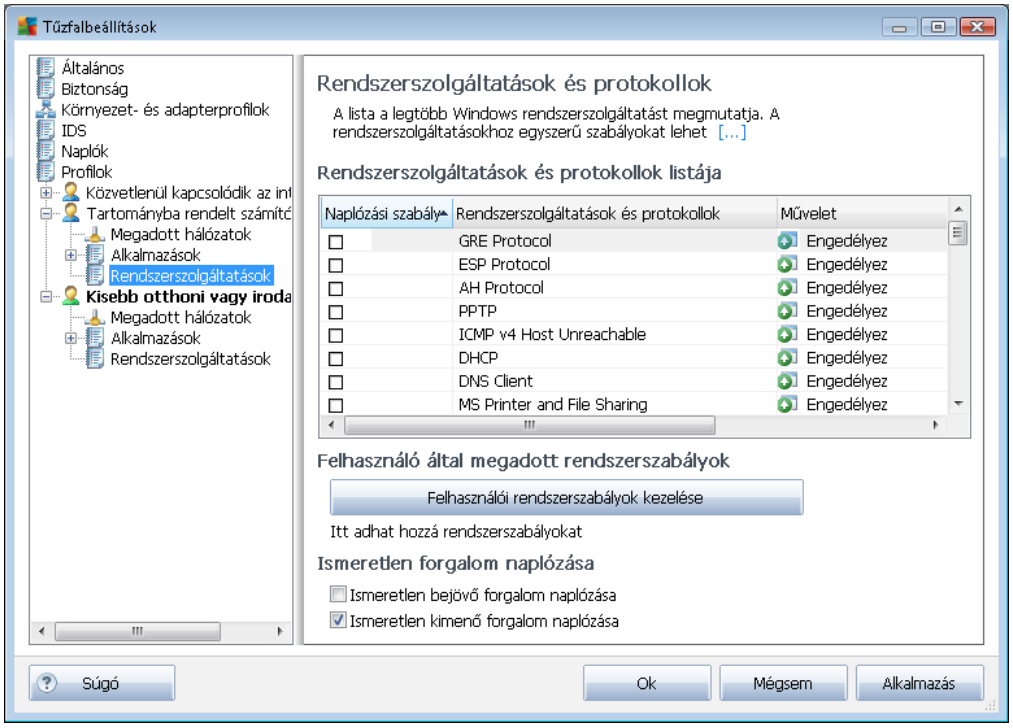
A legördülő menüből válassza ki a tűzfalszabályt az adott alkalmazáshoz, azaz a Tűzfalnak mit kell tennie, ha az alkalmazás kommunikálni próbál a hálózaton:

- ***Összes engedélyezése*** – Korlátozások nélkül engedi kommunikálni az alkalmazást az összes meghatározott hálózaton és adapteren.
- ***Biztonságos engedélyezése*** – Csak a biztonságosként *(megbízhatóként)* meghatározott hálózatokon engedi kommunikálni az alkalmazást.
- ***Tilt*** – Automatikusan letiltja a kommunikációt. Az alkalmazás nem csatlakozhat semmilyen hálózathoz.
- ***Rákérdez*** – Megjelenít egy párbeszédpanelt, amely rákérdez, hogy a kommunikációs próbálkozást az adott pillanatban engedélyezni vagy tiltani szeretné.
- ***Haladó beállítások*** – További részletes beállításokat jelenít meg a párbeszédpanel alsó részén, az ***Alkalmazás részletes szabályai*** részben. A részletek alkalmazása a lista sorrendjében történik, a ***Fel*** vagy ***Le*** gombokkal tetszés szerint módosíthatja a szabályok sorrendjét. Miután rákattint egy adott szabályra a listában, annak részletei megjelennek a párbeszédpanel alsó részén. Bármely kékkel aláhúzott értéket módosíthatja a megfelelő beállítási párbeszédpanelen. A kijelölt szabály törléséhez nyomja meg a ***Törlés*** gombot. Egy új szabály létrehozásakor használja a ***Hozzáadás*** gombot a ***Szabályok módosítása*** panel megnyitásához, ahol megadhatja a szükséges részleteket.

10.6.4. Rendszerszolgáltatások

Bármely beállítás módosítása a Rendszerszolgáltatások és protokollok panelen CSAK TAPASZTALT FELHASZNÁLÓK RÉSZÉRE javasolt.

A ***Rendszerszolgáltatások és protokollok*** panel felsorolja azon normál Windows rendszerszolgáltatásokat és protokollokat, amelyeknek szükségük van a hálózati kommunikációra:



Rendszerszolgáltatások és protokollok listája

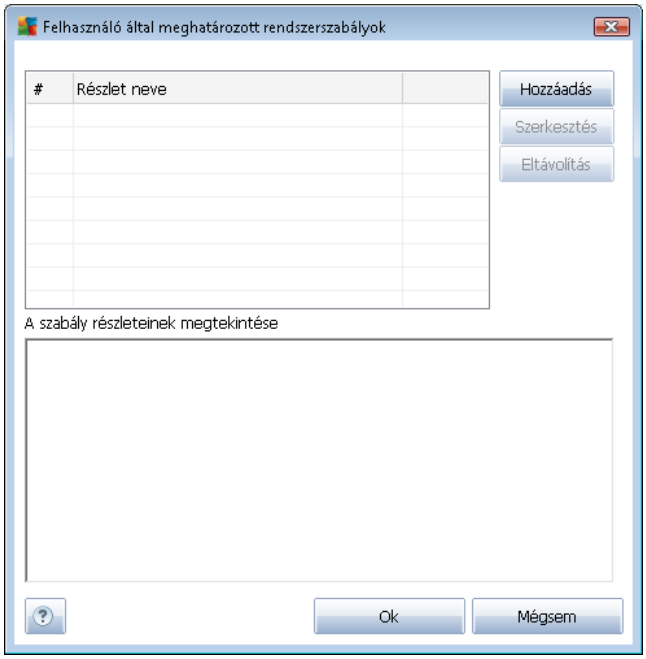
Ez a rész a következő oszlopokat tartalmazza:

- ***Szabályműveletek naplózása*** – Lehetővé teszi a szabályhasználat rögzítését a naplók részen.
- ***Rendszerszolgáltatás és protokollok*** – Ez az oszlop a kapcsolódó rendszerszolgáltatás nevét jeleníti meg.
- ***Művelet*** – Ez az oszlop a kapcsolódó művelet ikonját jeleníti meg:
  - Kommunikáció engedélyezése az összes hálózaton
  - Kommunikáció engedélyezése csak biztonságosnak minősített hálózatokon
  - Kommunikáció tiltása
- ***Hálózatok*** – Ez az oszlop megmutatja, hogy a rendszerszabály mely hálózaton lett alkalmazva.

A lista elemeinek (*és hozzárendelt műveleteinek*) szerkesztéséhez kattintson a jobb gombbal, majd válassza a ***Szerkesztés***lehetőséget. ***A rendszerszabályok módosítását kizárólag haladó felhasználók végezzék. A szabályok módosítását nem javasoljuk!***

Felhasználó által megadott rendszerszabályok

Egy új párbeszédpanel megnyitásához a rendszerszolgáltatási szabályok megadása érdekében (*lásd az alábbi képet*) nyomja meg a ***Felhasználói rendszerszabályok kezelése*** gombot. A ***Felhasználó által megadott rendszerszabályok*** panel felső részén a jelenleg szerkesztés alatt álló rendszerszabály részleteit láthatja, míg az alsó rész a kiválasztott szabályt mutatja. A felhasználó által megadott szabályokat szerkesztheti, felveheti vagy törölheti a megfelelő gombbal. A gyártó által megadott szabályok csak szerkeszthetők:



Vegye figyelembe, hogy a részletes szabálybeállítások összetettek, és elsősorban hálózati rendszergazdáknak szólnak, akiknek teljes felügyeletre van szükségük a tűzfal-konfiguráció felett. Ha nem ismeri a kommunikációs protokollokat, hálózati portszámokat, IP-címeket stb., akkor ne módosítsa ezen beállításokat! Ha mégis módosítania kell a konfigurációt, akkor további információkért forduljon a súgóhoz.

Ismeretlen forgalom naplózása

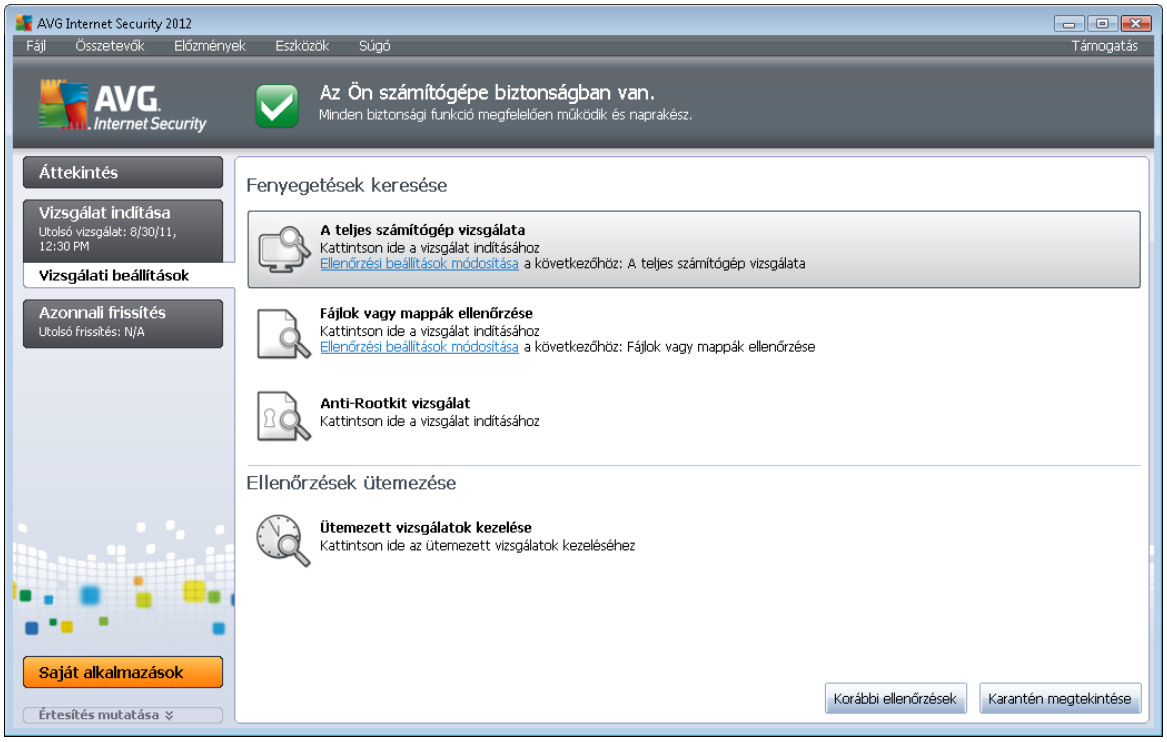
- ***Ismeretlen bejövő forgalom naplózása*** *(alapértelmezés szerint kikapcsolva)* – Jelölje be ezt a lehetőséget minden ismeretlen bejövő kommunikációs próbálkozás rögzítéséhez a naplókban.

- ***Ismeretlen kimenő forgalom naplózása*** *(alapértelmezés szerint bekapcsolva)* – Jelölje be ezt a lehetőséget minden ismeretlen kimenő kommunikációs próbálkozás rögzítéséhez a Naplókban.

11. AVG vizsgálat

Alapértelmezés szerint az **AVG Internet Security 2012** nem futtat semmilyen vizsgálatot, hiszen az első vizsgálat után Ön teljes védelemben részesül az **AVG Internet Security 2012** állandó összetevőinek köszönhetően, amelyek folyamatosan készenlétben állnak, és nem hagyják, hogy kártékony kódok férjenek hozzá a számítógépéhez. Természetesen rendszeres időközönként ütemezhet vizsgálatokat, vagy tetszés szerint manuálisan is elindíthat egy vizsgálatot.

11.1. Vizsgálati felület



Az AVG vizsgálati felület a ***Vizsgálati beállítások*** gyorsgombbal érhető el. Kattintson ide a ***Fenyegetések keresése*** panel megjelenítéséhez. Ezen a panelen a következőket találja:

- az előre meghatározott vizsgálatok áttekintése - háromféle vizsgálat (a gyártó által megadott) azonnal használható, akár manuálisan vagy ütemezve:
  - Vizsgálat a teljes számítógépen
  - Bizonyos fájlok vagy mappák ellenőrzése
  - Anti-Rootkit vizsgálat
- vizsgálat ütemezése rész - itt tetszőleges új vizsgálatokat és ütemezéseket (időzített vizsgálatok) hozhat létre.

Vezérlőgombok

A vizsgálati felületen elérhető vezérlőgombok a következők:

- ***Korábbi ellenőrzések*** - megjeleníti a Vizsgálat eredményének áttekintése panelt az összes korábbi vizsgálattal
- ***Víruskarantén megtekintése*** - megnyit egy új ablakot a Karanténnal - ahol az azonosított és karanténba helyezett fertőzések vannak tárolva.

11.2. Előre meghatározott vizsgálatok

Az **AVG Internet Security 2012** vírusirtó egyik legfontosabb funkciója az azonnali vizsgálat. Az azonnali keresés a számítógép különböző részeinek vizsgálatára szolgál, ha fertőzés gyanúja merül fel. Azt ajánljuk, hogy az ilyen teszteket rendszeresen végezze el, még akkor is, ha úgy gondolja, hogy a számítógépen nincs vírus.

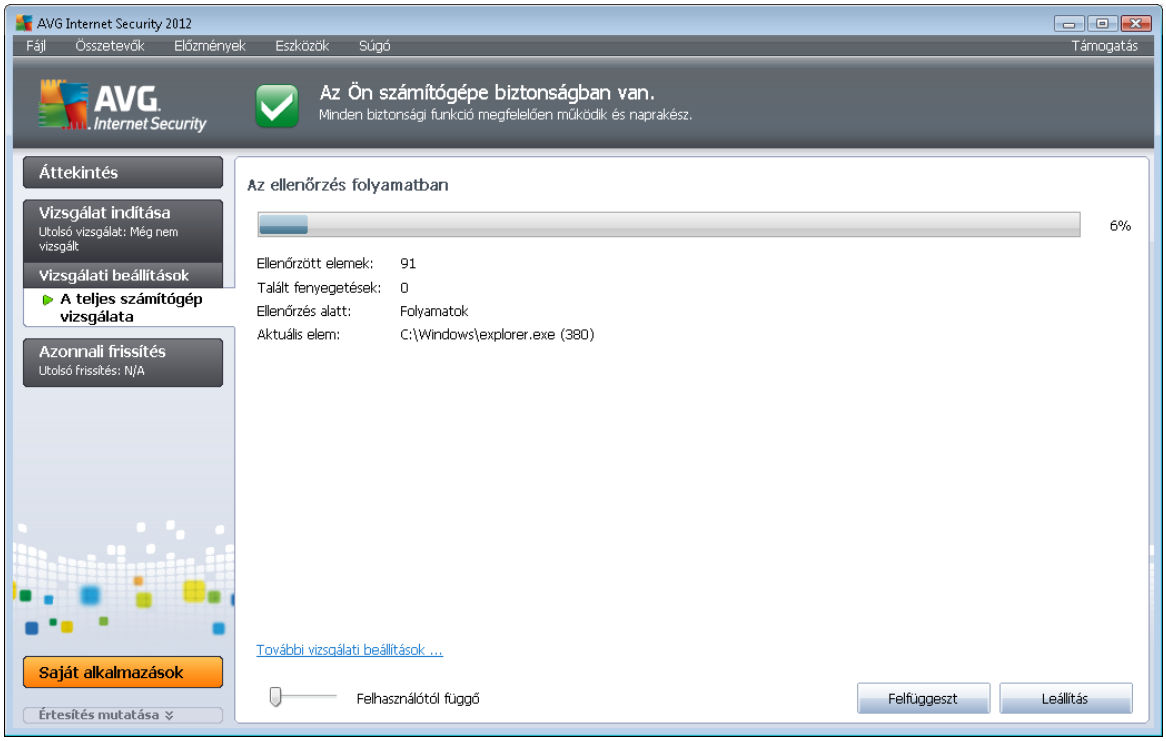
Az **AVG Internet Security 2012** programban a következő előre meghatározott vizsgálatokat találhatja, amelyeket a szoftver gyártója állított be:

11.2.1. Vizsgálat a teljes számítógépen

Számítógép teljes vizsgálata - megvizsgálja a teljes számítógépet esetleges fertőzések és/vagy potenciális nemkívánatos programok szempontjából. Ez a vizsgálat a számítógép összes merevlemezét ellenőrzi, azonosítja és javítja a talált vírusokat, és áthelyezi a fertőzéseket a Karanténba. A teljes számítógép vizsgálata funkciót javasolt beütemezni heti legalább egyszeri futtatásra.

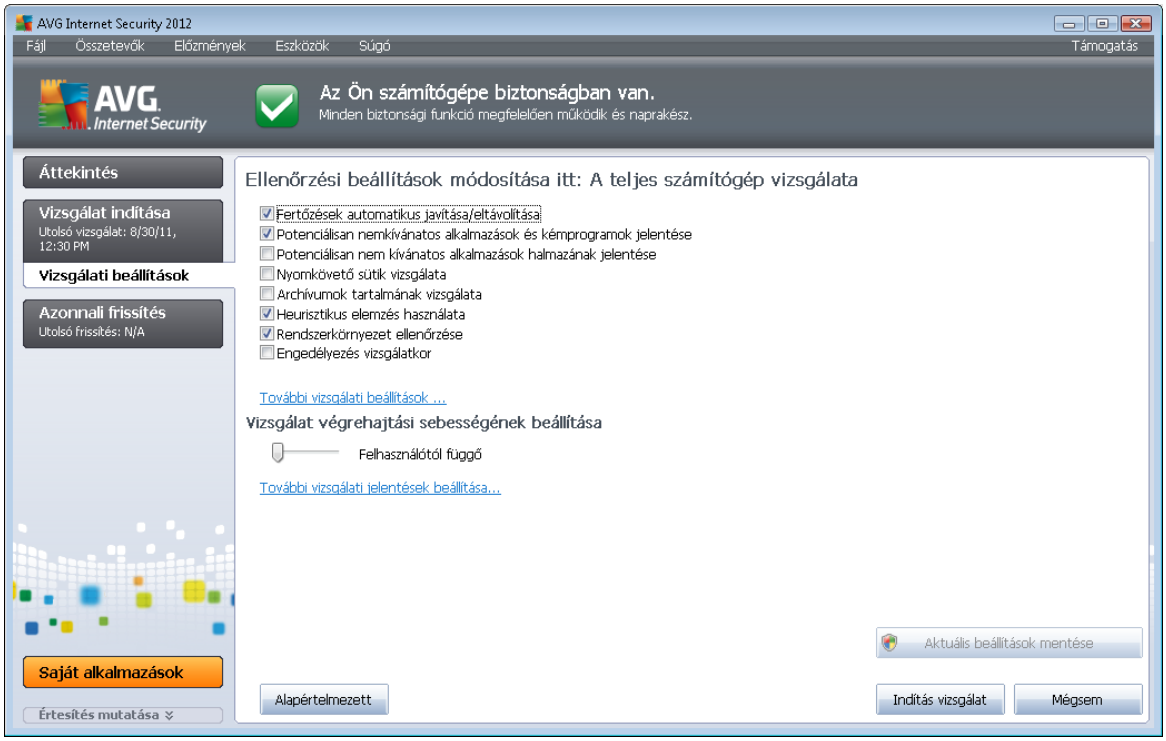
Vizsgálat indítása

Az ***Számítógép teljes vizsgálata*** közvetlenül a vizsgálati felületről indítható a vizsgálat ikonjára történő kattintással. Semmilyen egyéb beállítás nem szükséges ehhez a vizsgálathoz, a folyamat azonnal indul a ***Vizsgálat folyamatban*** panellel (*lásd a képet*). A vizsgálatot ideiglenesen szüneteltetheti (***Szünet***) vagy teljesen le is állíthatja (***Leállítás***), ha szükséges.



Vizsgálati beállítások szerkesztése

Lehetősége van az előre meghatározott alapértékek szerkesztésére a ***Számítógép teljes vizsgálata*** részen. Kattintson a ***Vizsgálati beállítások módosítása*** linkre a ***Vizsgálati beállítások módosítása a számítógép teljes vizsgálatánál*** panel megnyitásához *(elérhető a vizsgálati felületről a vizsgálati beállítások módosítása linken a Számítógép teljes vizsgálata részénél)*. ***Érdemes megtartani az alapbeállításokat, és csak akkor módosítsa azokat, ha feltétlenül szükséges!***



- ***Vizsgálati paraméterek*** - a listában tetszés szerint be- és kikapcsolhatja az adott vizsgálati paramétereket:

    - ***Fertőzés automatikus javítása/eltávolítása*** (*alapállapotban bekapcsolva*) - ha vírust talál a vizsgálat során, akkor automatikusan javítja, amennyiben ez lehetséges. Ha a fertőzött fájl nem javítható automatikusan, az objektum át lesz helyezve a Karanténba.

    - ***Potenciálisan nemkívánatos programok és kémprogramok jelentése*** - (*alapállapotban bekapcsolva*) - jelölje be a Kémprogram-elhárító motor aktiválásához, illetve kémprogramok és vírusok kereséséhez. A kémprogramok külön kártevő kategóriát képviselnek: komoly biztonsági kockázatot jelentenek, mégis nagy részüket a felhasználók szándékosan telepítik. Javasoljuk, hogy tartsa bekapcsolva ezt az opciót, mivel így növelheti a számítógép biztonságát.

    - ***Potenciálisan nem kívánatos alkalmazások halmazának jelentése*** (*alapértelmezés szerint kikapcsolva*) – jelölje be ezt a jelölőnégyzetet a kémprogramok speciális változatainak észleléséhez: olyan programok kereséséhez, amelyek ártalmatlanok, de később kártékony célokra használhatók. Ezzel tovább növelheti a számítógép biztonságát. A szolgáltatás legitim programokat is letilthat, ezért a funkció alapállapotban ki van kapcsolva.

    - ***Nyomkövető sütik vizsgálata*** (*alapállapotban kikapcsolva*) - ez az opció a Kémprogram-elhárító összetevőben meghatározza, hogy a vizsgálat során felismert sütik törölve legyenek-e (*a HTTP sütiket hitelesítéshez, nyomkövetéshez és bizonyos adatok gyűjtéséhez használják a felhasználókról, pl. honlap preferenciák vagy online vásárlás során a kosár tartalma*).

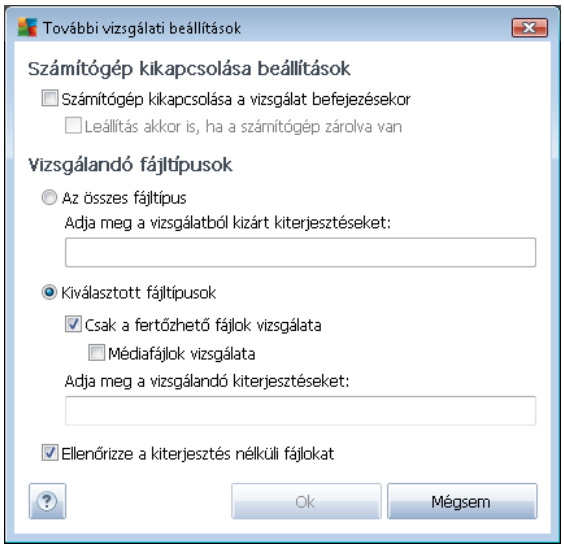
- ***Archívumok tartalmának vizsgálata*** (*alapállapotban kikapcsolva*) - ez a paraméter meghatározza, hogy a vizsgálat ellenőrizze-e az archívumban tárolt fájlokat, pl. ZIP, RAR.

- ***Heurisztika használata*** (*alapállapotban bekapcsolva*) - a heurisztikus elemzés (*a vizsgált objektum utasításainak dinamikus emulációja egy virtuális környezetben*) lesz az egyik víruskeresési módszer a vizsgálat során.

- ***Rendszerkörnyezet ellenőrzése*** (*alapállapotban bekapcsolva*) - a vizsgálat a számítógép rendszerterületeit is ellenőrzi.

- ***Átfogó vizsgálat engedélyezése*** (*alapállapotban kikapcsolva*) - bizonyos esetekben (*például, ha arra gyanakszik, hogy a számítógépét egy vírus megfertőzte*), akkor jelölje be ezt az opciót a legátfogóbb vizsgálati algoritmus bekapcsolásához, amely a számítógép nehezen fertőzhető részeit is ellenőrzi a biztonság kedvéért. Ne feledje, hogy ez a módszer meglehetősen időigényes.

- ***További vizsgálati beállítások*** - ez a link megnyit egy új ***További vizsgálati beállítások*** panelt, ahol a következő paramétereket adhatja meg:



  - ***A számítógép kikapcsolásának beállításai*** - döntse el, hogy a számítógép automatikusan kikapcsoljon-e, miután a vizsgálati folyamat véget ért. Miután megerősítette ezt a beállítást (***Számítógép leállítása a vizsgálat után***), egy új opció aktiválódik, mely lehetővé teszi, hogy akkor is leállítsa a számítógépet, ha az éppen zárolt (***Számítógép leállítása zárolás esetén is***).

  - ***Vizsgálandó fájltípusok*** – a továbbiakban döntse el, hogy a program mely fájlokat vizsgálja:

    - ***Összes fájltípus*** - lehetséges megadnia kivételeket, amelyek kimaradnak a vizsgálatból. Ezen fájlkiterjesztéseket vesszővel válassza el.

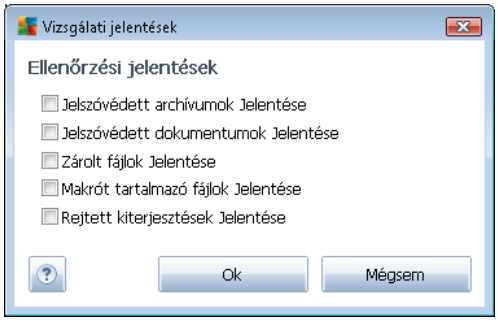
    - ***Kiválasztott fájltípusok*** - megadhatja, hogy a program csak olyan fájlokat

vizsgáljon, amelyek esetlegesen fertőzőek (*a nem fertőzhető fájlok, mint pl. a sima szöveges fájlok vagy egyéb nem futtatható fájlok, nem lesznek ellenőrizve*), pl. médiafájlok (*video-, audiofájlok - ha nem jelöli be ezt a négyzetet, akkor tovább csökken a vizsgálati idő, mivel ezen fájlok általában túl nagyok, és egyébként sem valószínű, hogy vírus fertőzné meg őket*). A kiterjesztések segítségével megadhatja, hogy mely fájlokat vizsgálja a program.

- Megadhatja azt is, hogy ***a program vizsgálja a kiterjesztés nélküli fájlokat*** - ez az opció alapállapotban be van kapcsolva és javasolt, hogy tartsa is így. A kiterjesztés nélküli fájlok különösen gyanúsak, ezért mindig ellenőrizni kell őket.

- ***Vizsgálat sebességének beállítása*** - használja a csúszkát a vizsgálati folyamat prioritásának módosításához. Alapállapotban ez az érték *felhasználótól függő* automatikus erőforráshasználatra van állítva. Alapállapotban a vizsgálati folyamatot lassabra állíthatja, ekkor a rendszer minimális erőforrást használ (*hasznos, ha a számítógépen kell dolgoznia, és nem számít a gyorsaság*); vagy gyorsabbra állíthatja, ekkor a rendszer több erőforrást használ (*a számítógépet ideiglenesen felügyelet nélkül hagyhatja*).

- ***További vizsgálati jelentések beállítása*** – a hivatkozás megnyit egy új ***Vizsgálati jelentések*** panelt, ahol kiválaszthatja, hogy milyen találati típusokat jelentsen a program:



Figyelmeztetés: *Ezek a beállítások megegyeznek az újonnan létrehozott vizsgálatok beállításaival - az AVG Vizsgálat / Vizsgálat ütemezése/ Hogyan vizsgáljon fejezetben leírtaknak megfelelően. Ha úgy dönt, hogy megváltoztatja az alapbeállításokat a* ***Teljes számítógép vizsgálata*** *részben, akkor elmentheti az új beállításokat alapértelmezettként, és azok lesznek használva a jövőben minden teljes vizsgálathoz.*

11.2.2. Kiválasztott fájlok vagy mappák ellenőrzése

Kijelölt fájlok vagy mappák ellenőrzése - csak azokat a rendszerterületeket ellenőrzi, amelyeket Ön előzőleg kiválasztott (*meghatározott mappák, merevlemezek, floppylemezek, CD-k stb.*). Vírustalálat és javítás során a folyamat megegyezik a teljes számítógép vizsgálati folyamatával: a program minden vírusfertőzést javít vagy Karanténba helyez. Az adott fájlokat vagy mappákat saját vizsgálatba is felveheti, és tetszőlegesen ütemezheti a kereséseket.

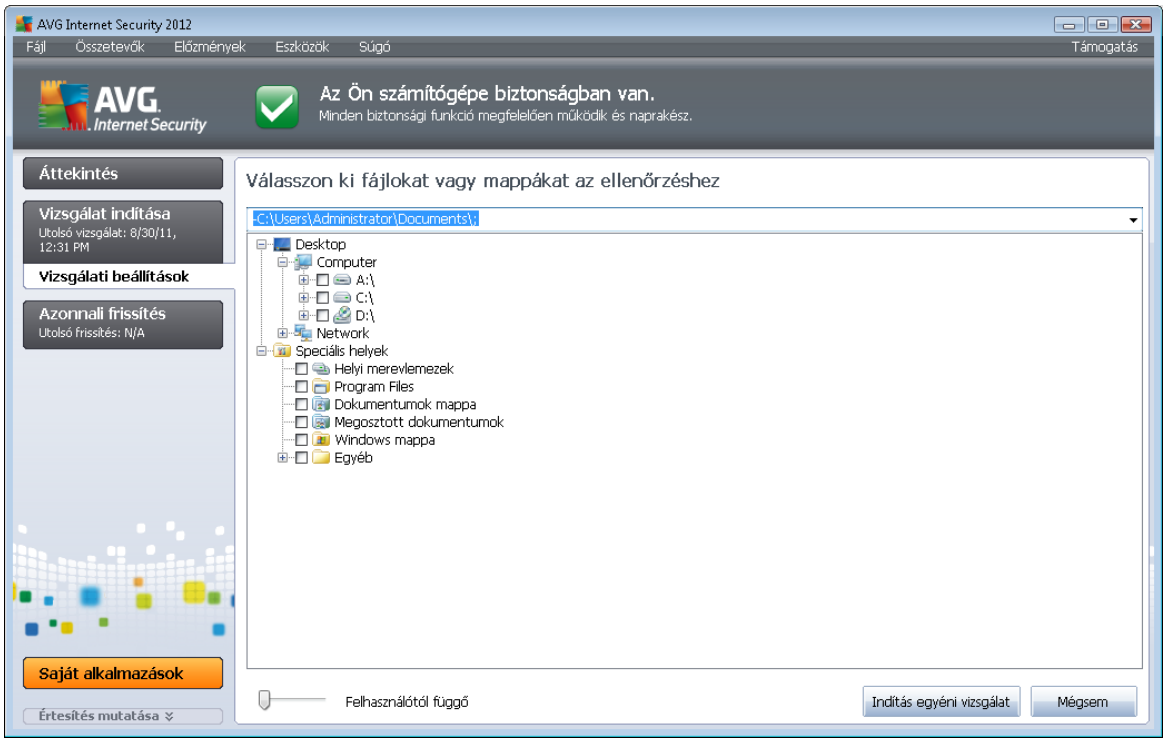
Vizsgálat indítása

A ***Bizonyos fájlok vagy mappák vizsgálatát*** közvetlenül a vizsgálati felületről indíthatja a vizsgálat ikonjára történő kattintással. A ***Válasszon ki bizonyos fájlokat vagy mappákat az ellenőrzéshez***

panel megjelenik. Válassza ki a vizsgálandó mappákat a számítógépen. A kiválasztott mappák elérési útvonala automatikusan megjelenik a panel felső részén látható szövegdobozban.

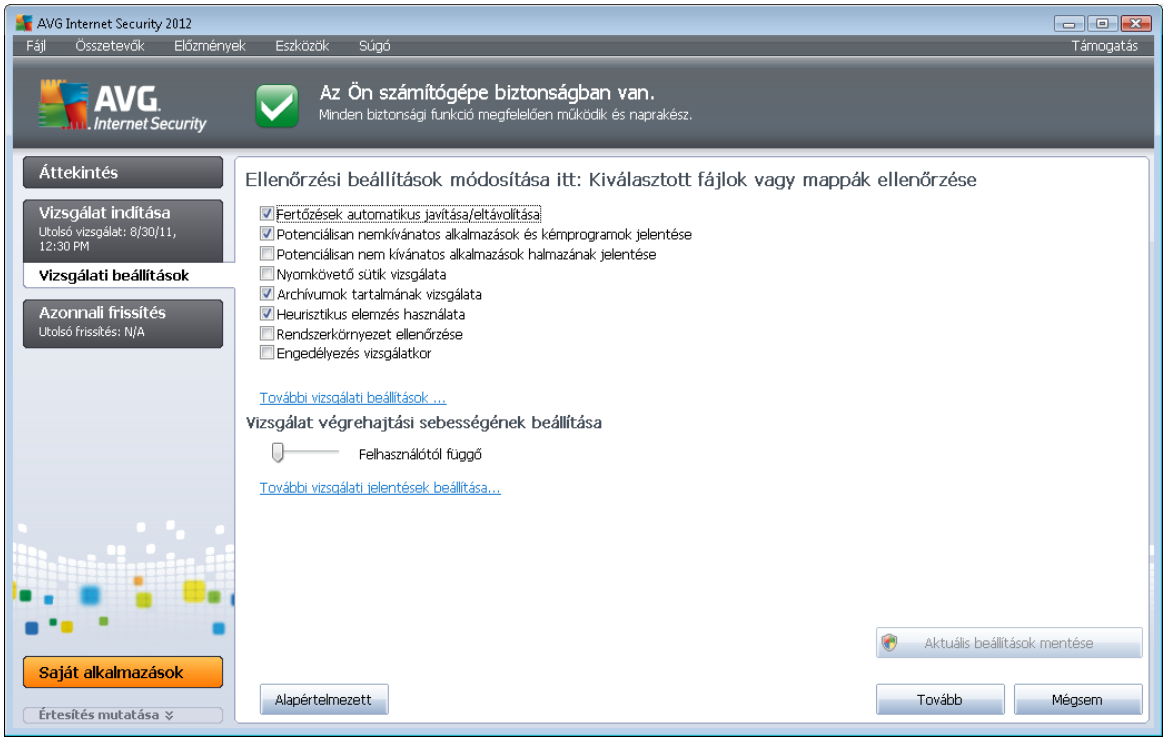
Lehetősége van arra is, hogy egy bizonyos mappát almappák nélkül ellenőrizzen. Ehhez adjon egy mínusz jelet "**-**" az automatikusan létrehozott elérési útvonal elé (*lásd a képet*). Egy teljes mappa vizsgálatból való kizárásához használja a "**!**" jelet paraméter.

Végül a vizsgálat indításához nyomja meg a ***Vizsgálat indítása*** gombot. A folyamat alapvetően megegyezik a Számítógép teljes vizsgálata funkcióval.



Vizsgálati beállítások szerkesztése

Lehetősége van az előre meghatározott alapértékek szerkesztésére a ***Meghatározott fájlok vagy mappák vizsgálata*** részben. Kattintson a ***Vizsgálati beállítások módosítása*** hivatkozásra a ***Vizsgálati beállítások módosítása bizonyos fájlok vagy mappák esetén*** panel megjelenítéséhez. ***Érdemes megtartani az alapbeállításokat, és csak akkor módosítsa azokat, ha feltétlenül szükséges!***



- ***Vizsgálati paraméterek*** - a listában tetszés szerint be- és kikapcsolhatja az adott vizsgálati paramétereket:

    - ***Fertőzés automatikus javítása/eltávolítása*** (*alapállapotban bekapcsolva*) - ha vírust talál a vizsgálat során, akkor automatikusan javítja, amennyiben ez lehetséges. Ha a fertőzött fájl nem javítható automatikusan, az objektum át lesz helyezve a Karanténba.

    - ***Potenciálisan nemkívánatos programok és kémprogramok jelentése*** - (*alapállapotban bekapcsolva*) - jelölje be a Kémprogram-elhárító motor aktiválásához, illetve kémprogramok és vírusok kereséséhez. A kémprogramok külön kártevő kategóriát képviselnek: komoly biztonsági kockázatot jelentenek, mégis nagy részüket a felhasználók szándékosan telepítik. Javasoljuk, hogy tartsa bekapcsolva ezt az opciót, mivel így növelheti a számítógép biztonságát.

    - ***Potenciálisan nem kívánatos alkalmazások halmazának jelentése*** (*alapértelmezés szerint kikapcsolva*) – jelölje be ezt a jelölőnégyzetet a kémprogramok speciális változatainak észleléséhez: olyan programok kereséséhez, amelyek ártalmatlanok, de később kártékony célokra használhatók. Ezzel tovább növelheti a számítógép biztonságát. A szolgáltatás legitim programokat is letilthat, ezért a funkció alapállapotban ki van kapcsolva.

    - ***Nyomkövető sütik vizsgálata*** (*alapállapotban kikapcsolva*) - ez az opció a Kémprogram-elhárító összetevőben meghatározza, hogy a vizsgálat során felismert sütik törölve legyenek-e (*a HTTP sütiket hitelesítéshez, nyomkövetéshez és bizonyos adatok gyűjtéséhez használják a felhasználókról, pl. honlap preferenciák vagy online vásárlás során a kosár tartalma*).

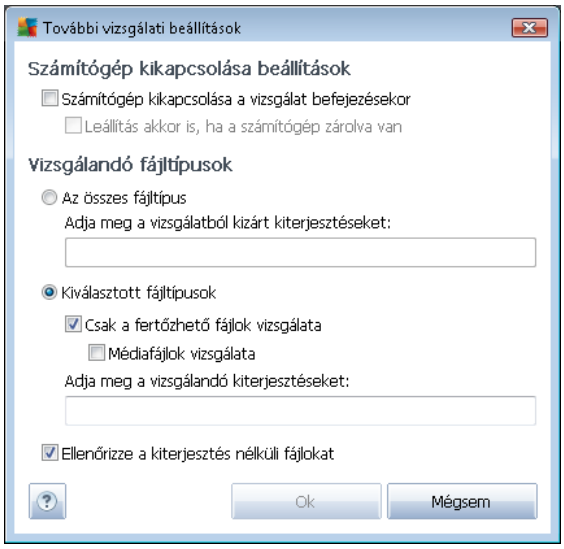
- ***Archívumok tartalmának vizsgálata*** (*alapállapotban bekapcsolva*) - ez a paraméter meghatározza, hogy a vizsgálat ellenőrizze-e az archívumban tárolt fájlokat, pl. ZIP, RAR.

- ***Heurisztika használata*** (*alapállapotban kikapcsolva*): a heurisztikus elemzés (*a vizsgált objektum utasításainak dinamikus emulációja egy virtuális környezetben*) lesz az egyik víruskeresési módszer a vizsgálat során.

- ***Rendszerkörnyezet ellenőrzése*** (*alapállapotban kikapcsolva*) - a vizsgálat a számítógép rendszerterületeit is ellenőrzi.

- ***Átfogó vizsgálat engedélyezése*** (*alapállapotban kikapcsolva*) - bizonyos esetekben (*például, ha arra gyanakszik, hogy a számítógépét egy vírus megfertőzte*), akkor jelölje be ezt az opciót a legátfogóbb vizsgálati algoritmus bekapcsolásához, amely a számítógép nehezen fertőzhető részeit is ellenőrzi a biztonság kedvéért. Ne feledje, hogy ez a módszer meglehetősen időigényes.

- ***További vizsgálati beállítások*** - ez a link megnyit egy új ***További vizsgálati beállítások*** panelt, ahol a következő paramétereket adhatja meg:



- ***A számítógép kikapcsolásának beállításai*** - döntse el, hogy a számítógép automatikusan kikapcsoljon-e, miután a vizsgálati folyamat véget ért. Miután megerősítette ezt a beállítást (***Számítógép leállítása a vizsgálat után***), egy új opció aktiválódik, mely lehetővé teszi, hogy akkor is leállítsa a számítógépet, ha az éppen zárolt (***Számítógép leállítása zárolás esetén is***).

- ***Vizsgálandó fájltípusok*** – a továbbiakban döntse el, hogy a program mely fájlokat vizsgálja:

  - ***Összes fájltípus*** - lehetséges megadnia kivételeket, amelyek kimaradnak a vizsgálatból. Ezen fájlkiterjesztéseket vesszővel válassza el.

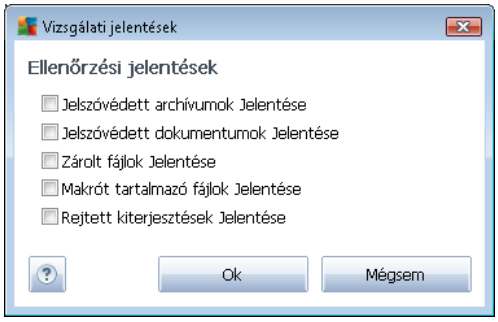
  - ***Kiválasztott fájltípusok*** - megadhatja, hogy a program csak olyan fájlokat

vizsgáljon, amelyek esetlegesen fertőzőek (*a nem fertőzhető fájlok, mint pl. a sima szöveges fájlok vagy egyéb nem futtatható fájlok, nem lesznek ellenőrizve*), pl. médiafájlok (*video-, audiofájlok - ha nem jelöli be ezt a négyzetet, akkor tovább csökken a vizsgálati idő, mivel ezen fájlok általában túl nagyok, és egyébként sem valószínű, hogy vírus fertőzné meg őket*). A kiterjesztések segítségével megadhatja, hogy mely fájlokat vizsgálja a program.

- Megadhatja azt is, hogy ***a program vizsgálja a kiterjesztés nélküli fájlokat*** - ez az opció alapállapotban be van kapcsolva és javasolt, hogy tartsa is így. A kiterjesztés nélküli fájlok különösen gyanúsak, ezért mindig ellenőrizni kell őket.

- ***Vizsgálati folyamat prioritása*** - használja a csúszkát a vizsgálati folyamat prioritásának módosításához. Alapállapotban ez az érték *felhasználótól függő* automatikus erőforráshasználatra van állítva. Alapállapotban a vizsgálati folyamatot lassabra állíthatja, ekkor a rendszer minimális erőforrást használ (*hasznos, ha a számítógépen kell dolgoznia, és nem számít a gyorsaság*); vagy gyorsabbra állíthatja, ekkor a rendszer több erőforrást használ (*a számítógépet ideiglenesen felügyelet nélkül hagyhatja*).

- ***További vizsgálati jelentések beállítása*** - a hivatkozás megnyit egy új ***Vizsgálati jelentések*** panelt, ahol kiválaszthatja, hogy milyen találati típusokat jelentsen a program:



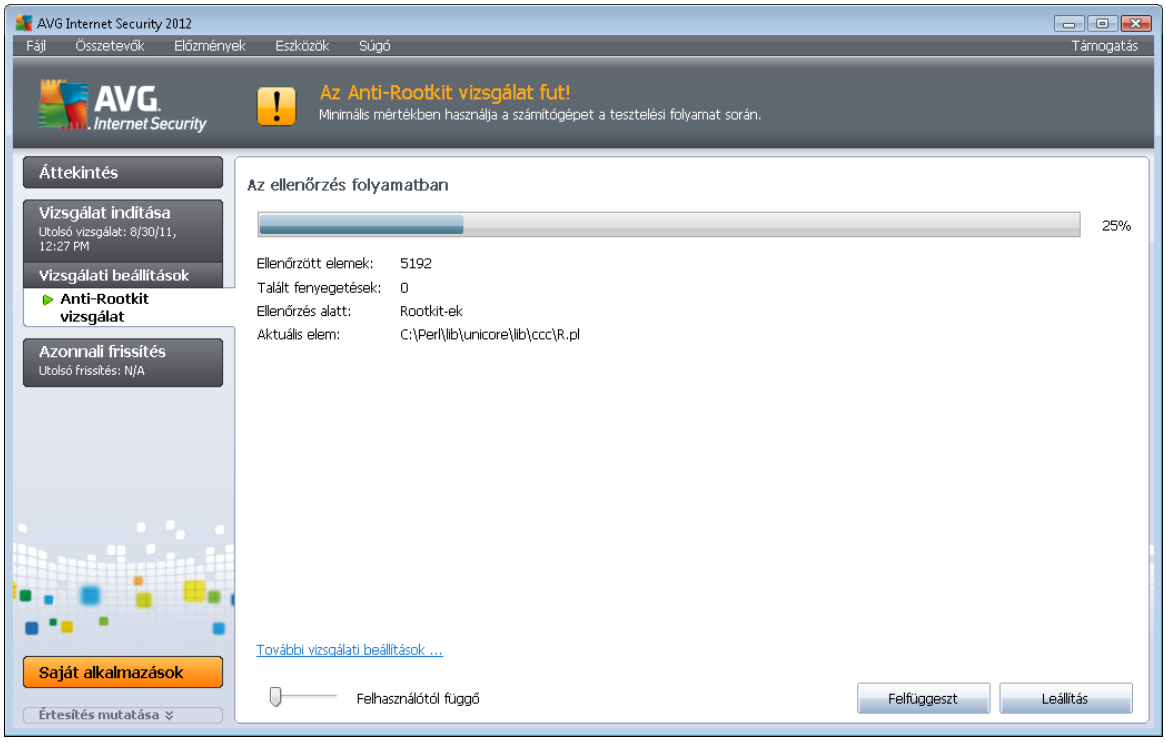
Figyelmeztetés: *Ezek a beállítások megegyeznek az újonnan létrehozott vizsgálatok beállításaival - az AVG Vizsgálat / Vizsgálat ütemezése/ Hogyan vizsgáljon fejezetben leírtaknak megfelelően. Ha úgy dönt, hogy megváltoztatja az alpbeállításokat a* ***Kijelölt fájlok vagy mappák ellenőrzése*** *részben, akkor elmentheti az új beállításokat alapértelmezettként, és azok lesznek használva a jövőben minden meghatározott fájl vagy mappa vizsgálatához. Továbbá ez a beállítás sablonként lesz használva minden újonnan létrehozott ütemezett vizsgálathoz (az egyéni keresések a Meghatározott fájlok vagy mappák vizsgálata rész aktuális beállításaitól függnek).*

11.2.3. Anti-Rootkit vizsgálat

Az Anti-Rootkit vizsgálat esetleges rootkiteket keres a számítógépen (*olyan programokat és technológiákat, amelyek kártékony tevékenységet lepleznek a számítógépen*). Ha a program rootkitet észlel, akkor az nem jelenti automatikusan azt, hogy a számítógép fertőzött. Bizonyos esetekben egyes eszközillesztők vagy legitim alkalmazások részeit a program tévesen rootkitként észleli.

Vizsgálat indítása

Az Anti-Rootkit vizsgálatot közvetlenül a vizsgálati felületről indíthatja a vizsgálat ikonjára történő kattintással. Semmilyen egyéb beállítás nem szükséges ehhez a vizsgálathoz, a folyamat azonnal indul a ***Vizsgálat folyamatban*** panellel (*lásd a képet*). A vizsgálatot ideiglenesen szüneteltetheti (***Szünet***) vagy teljesen le is állíthatja (***Leállítás***), ha szükséges.

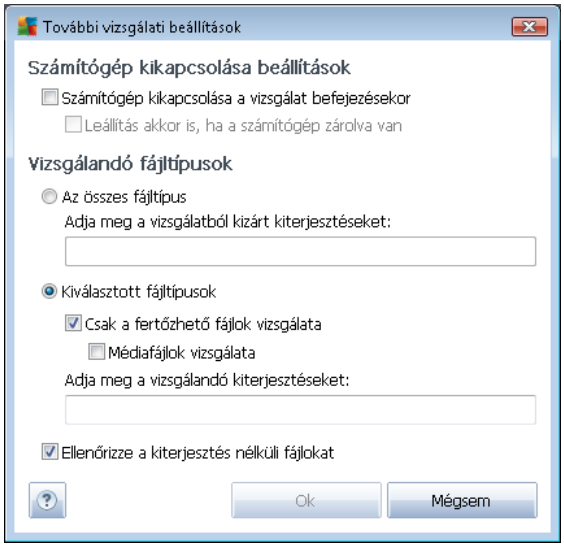


Vizsgálati beállítások szerkesztése

Az Anti-Rootkit vizsgálat mindig alapértelmezett beállításokkal indul, a vizsgálati paraméterek szerkesztése az AVG Haladó Beállítások / Anti-Rootkit panelen érhető el. A vizsgálati felületen a következő beállítási lehetőségek érhetők el, de csak akkor, ha a vizsgálat fut:

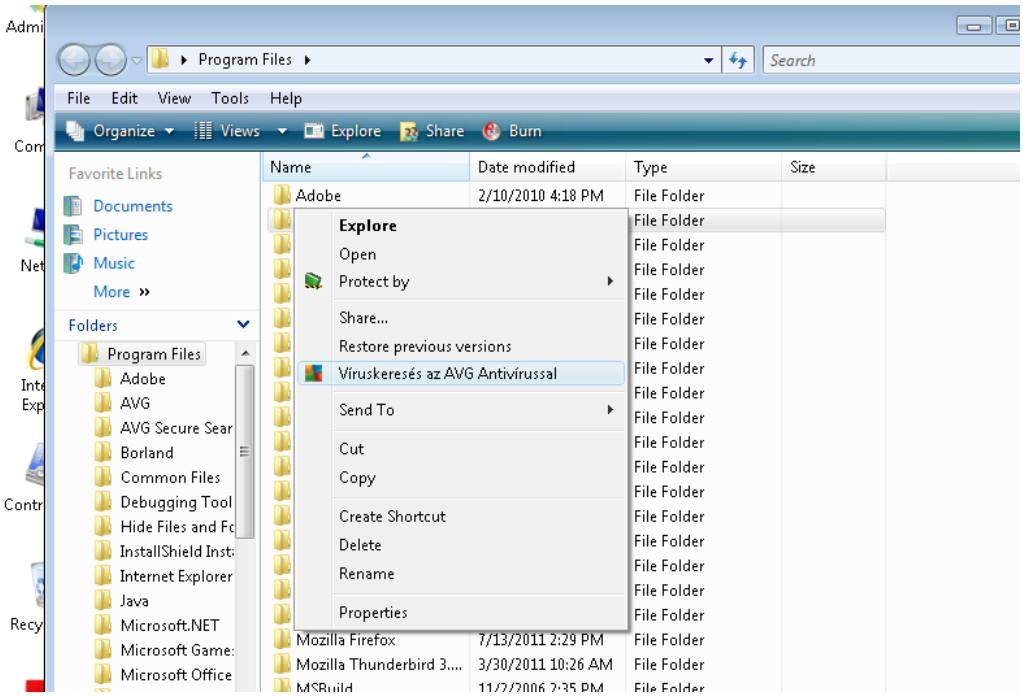
- ***Automatikus vizsgálat*** - használja a csúszkát a vizsgálati folyamat prioritásának módosításához. Alapállapotban ez az érték *felhasználótól függő* automatikus erőforráshasználatra van állítva. Alapállapotban a vizsgálati folyamatot lassabra állíthatja, ekkor a rendszer minimális erőforrást használ (*hasznos, ha a számítógépen kell dolgoznia, és nem számít a gyorsaság*); vagy gyorsabbra állíthatja, ekkor a rendszer több erőforrást használ (*a számítógépet ideiglenesen felügyelet nélkül hagyhatja*).

- ***További vizsgálati beállítások*** - megnyitja a ***További vizsgálati beállítások*** panelt, ahol megadhatja a számítógép esetleges leállítási feltételeit az ***Anti-Rootkit vizsgálathoz*** kapcsolódóan (***Számítógép leállítása a vizsgálat befejezésekor*** *vagy* ***Leállítás mindenképpen, ha a számítógép zárolt***):



11.3. Vizsgálat a Windows Intézőben

A számítógép teljes vagy részleges ellenőrzéséhez meghatározott vizsgálatokon kívül az **AVG Internet Security 2012** lehetővé teszi adott objektumok ellenőrzését közvetlenül a Windows Intézőből. Ha egy ismeretlen fájlt nyitna meg, de nem biztos a tartalmában, akkor elképzelhető, hogy előtte ellenőrizni szeretné. Kövesse az alábbi lépéseket:



- A Windows Intézőben jelölje ki a vizsgálni kívánt fájlt *(vagy mappát)*
- Kattintson a jobb gombbal az objektumra a helyi menü megnyitásához

- Válassza ki a ***Vizsgálat AVG-vel*** lehetőséget a fájl ellenőrzéséhez **AVG Internet Security 2012**

11.4. Parancssori vizsgálat

Az **AVG Internet Security 2012** terméken belül lehetőség van vizsgálat indítására parancssorból is. Ezt használhatja például kiszolgálókon, vagy a számítógép indításakor automatikusan lefutó kötegszkriptek létrehozásakor. A vizsgálatot az AVG grafikus felhasználói felületen elérhető legtöbb paraméterrel indíthatja a parancssorból.

Az AVG parancssorból történő indításához futtassa a következő parancsot abból a mappából, ahol az AVG telepítve van:

- ***avgscanx*** 32 bites operációs rendszerhez
- ***avgscana*** 64 bites operációs rendszerhez

A parancs formája

A parancs formája a következő:

- ***avgscanx /paraméter*** ... pl. ***avgscanx /comp*** a számítógép teljes vizsgálatához
- ***avgscanx /paraméter /paraméter*** .. több paraméter egy sorban legyen szóközzel és "/" jellel elválasztva
- ha a paraméter használatához egyedi érték megadására van szükség (pl. a ***/scan*** paraméter, melynél meg kell adni a számítógép vizsgálandó területeit pontos elérési útvonal formájában), akkor ezen értékek pontosvesszővel legyenek elválasztva, például: ***avgscanx /scan=C:\;D:***

Vizsgálati paraméterek

Az elérhető paraméterek teljes listájához gépelje be az adott parancsot a /? paraméterrel vagy /HELP (pl. ***avgscanx /?***). Az egyetlen kötelező paraméter a /SCAN, mely meghatározza, hogy a számítógép mely részeit kell vizsgálni. Az opciók részletesebb leírásához lásd a parancssori paraméterek áttekintését.

A vizsgálat indításához nyomja meg az ***Enter*** gombot. A vizsgálatot megszakíthatja a ***Ctrl+C*** vagy ***Ctrl+Pause***gomb megnyomásával.

A parancssori vizsgálat elindult a grafikus felületről

Ha a számítógépet Windows Biztonságos Módban futtatja, akkor elindíthatja a parancssori vizsgálatot a grafikus felületről. A vizsgálat a parancssorból fog futni. A ***Parancssori szerkesztő*** panel lehetővé teszi, hogy kényelmesen meghatározza a legtöbb vizsgálati paramétert a grafikus felhasználói felületen.

Mivel ez a panel csak a Windows Biztonságos Módból érhető el, a részletes leírásért forduljon a közvetlenül a panelből megnyitható súgóhoz.

11.4.1. Parancssori vizsgálat paraméterek

Az alábbiakban megtalálhatja a parancssori vizsgálathoz szükséges összes paramétert:

- ***/SCAN*** Bizonyos fájlok vagy mappák ellenőrzése /SCAN=útvonal;útvonal *(például /SCAN=C:\;D:\)*
- ***/COMP*** A számítógép teljes vizsgálata
- ***/HEUR*** Heurisztikus elemzés használata
- ***/EXCLUDE*** Elérési út vagy fájlok kihagyása a vizsgálatból
- ***/@*** Parancsfájl /fájlnév/
- ***/EXT*** Ezen kiterjesztések vizsgálata /például: EXT=EXE,DLL/
- ***/NOEXT*** Ne vizsgálja ezeket a kiterjesztéseket /például: NOEXT=JPG/
- ***/ARC*** Archívumok vizsgálata
- ***/CLEAN*** Automatikus javítás
- ***/TRASH*** Fertőzött fájlok karanténba helyezése
- ***/QT*** Gyorsvizsgálat
- ***/MACROW*** Makrók jelentése
- ***/PWDW*** Jelszóval védett fájlok jelentése
- ***/IGNLOCKED*** Zárolt fájlok mellőzése
- ***/REPORT*** Jelentéskészítés fájlba /fájlnév/
- ***/REPAPPEND*** Hozzáfűzés a jelentésfájlhoz
- ***/REPOK*** Nem fertőzött fájlok jelentése OK-ként
- ***/NOBREAK*** A CRTL+BREAK billentyű kombinációval való megszakítás tiltása
- ***/BOOT*** MBR/RENDSZERTÖLTŐ SZEKTOR ellenőrzés engedélyezése
- ***/PROC*** Aktív folyamatok vizsgálata
- ***/PUP*** "Potenciálisan nemkívánatos programok" jelentése
- ***/REG*** Rendszerleíró-adatbázis vizsgálata

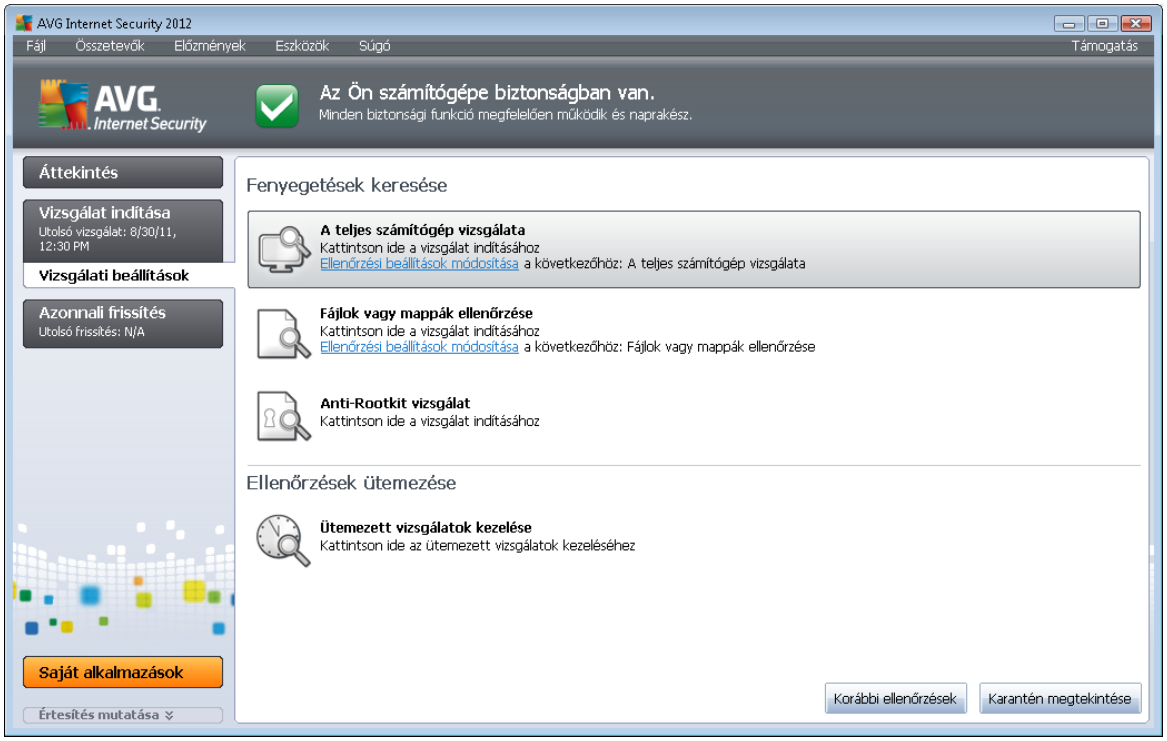
- ***/COO*** Sütik vizsgálata
- ***/?*** Súgó megjelenítése a témakörről
- ***/HELP*** Súgó megjelenítése a témakörről
- ***/PRIORITY*** Vizsgálati prioritás beállítása /Alacsony, Automatikus, Magas/ *(lásd: Haladó beállítások / Vizsgálatok)*
- ***/SHUTDOWN*** A számítógép leállítása a vizsgálat befejezésekor
- ***/FORCESHUTDOWN*** A számítógép kényszerített leállítása a vizsgálat befejezésekor
- ***/ADS*** Alternatív adatfolyamok vizsgálata *(csak NTFS)*
- ***/ARCBOMBSW*** Újratömörített archívumfájlok jelentése

11.5. Vizsgálatok ütemezése

A **AVG Internet Security 2012** segítségével bármikor elindíthat egy keresést (például ha gyanítja, hogy a számítógépen vírus található) vagy egy ütemezett vizsgálatot. Javasoljuk, hogy ütemezések alapján futtasson le vizsgálatokat: így biztosíthatja, hogy számítógép védve van mindenféle fertőzésveszélytől, és nem kell aggódnia, hogy mikor és hogyan indítson el egy keresést.

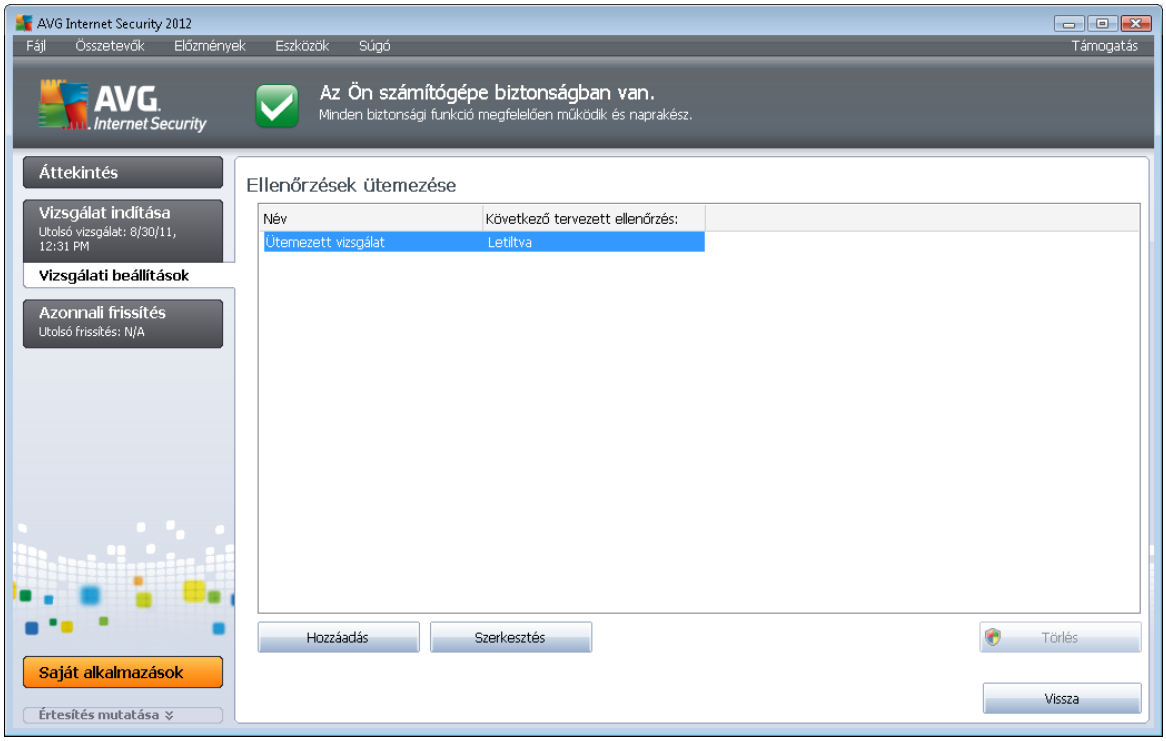
Rendszeresen, legalább hetente egyszer futtassa le a Számítógép teljes vizsgálata szolgáltatást. Azonban amennyiben lehetséges, a teljes számítógép vizsgálata napi szinten javasolt - az alapértelmezett vizsgálati ütemezésben is ez szerepel. Ha a számítógép mindig be van kapcsolva, akkor a munkaidő szerinti órákat kizárhatja a vizsgálati ütemezésből. Ha a számítógép néha ki van kapcsolva, akkor a vizsgálatot ütemezheti a számítógép indítási idejére, amennyiben a feladatot nem lehetett korábban végrehajtani, mivel az időzítés a kikapcsolt időszakra esett.

Új vizsgálati ütemezések létrehozásához nézze meg az AVG vizsgálati felületet, majd keresse meg az alsó ***Ellenőrzések ütemezése***részt:



Ellenőrzések ütemezése

Kattintson a grafikus ikonra a ***Vizsgálatok ütemezése*** részben egy új ***Vizsgálatok ütemezése*** párbeszédpanel megnyitásához, amelyen megtekintheti az összes jelenleg ütemezett vizsgálatot:



A vizsgálatokat szerkesztheti, illetve újakat vehet fel a következő vezérlőgombok segítségével:

- ***Vizsgálati ütemezés hozzáadása*** - a gomb megnyitja az ***Ütemezett vizsgálat beállításai*** ablakot, és a Ütemezési beállítások fület. Ebben az ablakban beállíthatja az újonnan létrehozott vizsgálat paramétereit.

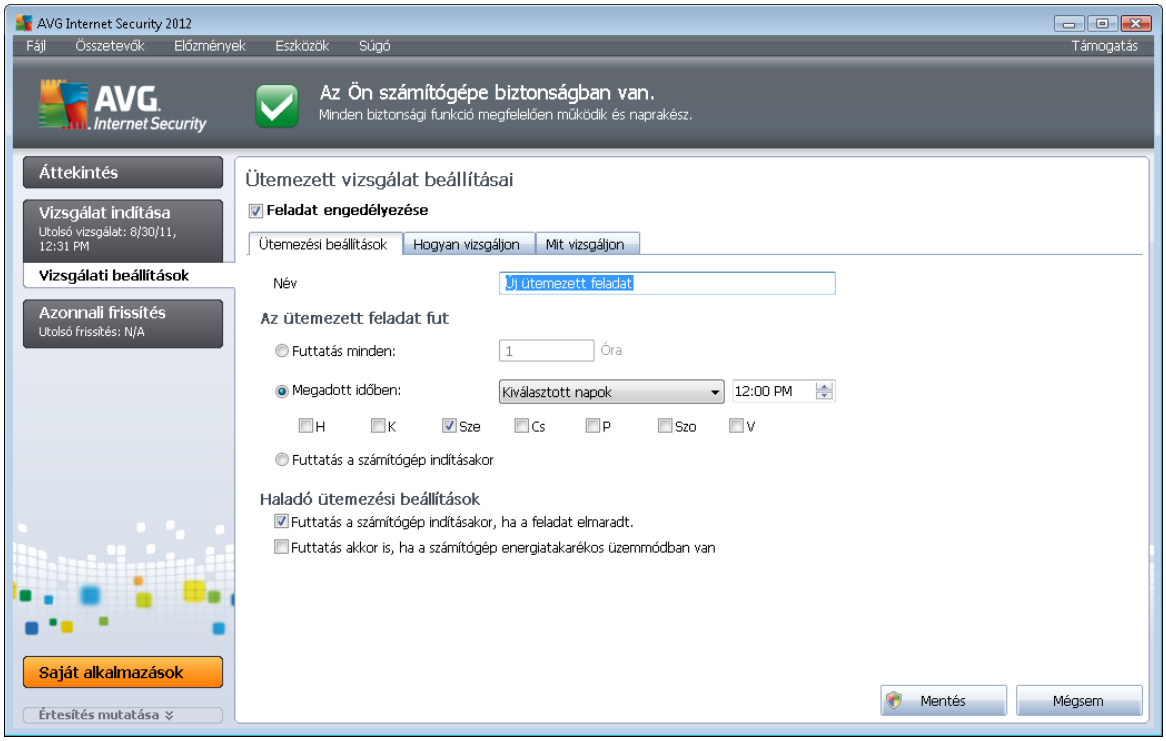
- ***Vizsgálati ütemezés szerkesztése*** - ezt a gombot csak akkor használhatja, ha előzőleg már kiválasztott egy adott ütemezett vizsgálatot a listából. Ebben az esetben a gomb aktív lesz, és ha rákattint, akkor megjelenik az ***Ütemezett vizsgálat beállításai*** ablak és az Ütemezési beállítások fül. A kiválasztott vizsgálat paraméterei itt vannak meghatározva és itt szerkesztheti őket.

- ***Vizsgálati ütemezés törlése*** - ez a gombot szintén aktív, ha előzőleg már kiválasztott egy adott ütemezett vizsgálatot a listából. A vizsgálatot törölheti a listából, ha rákattint erre a vezérlőgombra. A saját vizsgálatokat eltávolíthatja, de az alapértelmezett ***Vizsgálat ütemezése a teljes számítógépen*** beállítás nem törölhető.

- ***Vissza*** - visszatér az AVG vizsgálati felületre

11.5.1. Ütemezési beállítások

Ha új vizsgálatot szeretne ütemezni, akkor lépjen be az ***Ütemezett vizsgálat beállításai*** párbeszédpanelre (*kattintson az **Vizsgálati ütemezés hozzáadása** gombra az **Ellenőrzések ütemezése** panelen*). A párbeszédpanel három fülre van osztva: ***Beállítások ütemezése*** *(lásd az alábbi képet; az alapértelmezett fül, amelyre a rendszer automatikusan irányítja)*, Hogyan vizsgáljon és Mit vizsgáljon a program.



Az ***Ütemezési beállítások*** részben be- és kikapcsolhatja a ***Feladat engedélyezése*** opciót az ütemezett vizsgálat ideiglenes letiltásához. Szükség esetén újra bekapcsolhatja.

Adjon nevet a létrehozandó és ütemezendő vizsgálatnak. Gépelje be a nevet a szövegmezőbe a ***Név*** elem mellett. Próbáljon rövid, jellemző és megfelelő nevet adni a frissítési ütemezéseknek, így később könnyebben felismerheti majd őket.

Például: *Nem javasolt, hogy a vizsgálatnak az "Új vizsgálat" vagy "Saját vizsgálat" nevet adja, mivel ez semmit nem mond arról, hogy a vizsgálat valójában mit ellenőriz. Ugyanakkor megfelelő leíró név például a "Rendszerterületek ellenőrzése" stb. Nem szükséges a névben megadni, hogy a számítógép teljes vagy részleges vizsgálatáról van szó, mivel a saját vizsgálatok minden esetben adott fájlok vagy mappák vizsgálatának minősülnek.*

Ezen a panelen beállíthatja az adott keresés következő paramétereit:

- ***Ütemezés futtatása*** - adja meg, hogy az ütemezett vizsgálat milyen időközönként fusson le. Az ütemezést meghatározhatja a rendszeres időközönként történő futtatással (***Futtatás minden ...***), dátummal és időponttal (***meghatározott időben ...***), vagy egy adott eseményhez kötheti (***Futtatás számítógép indításakor***).

- ***Haladó ütemezési beállítások*** - ebben a részben meghatározhatja, hogy a vizsgálat mely körülmények között induljon / ne induljon (például ha a számítógép energiatakarékos módban van vagy teljesen ki van kapcsolva.

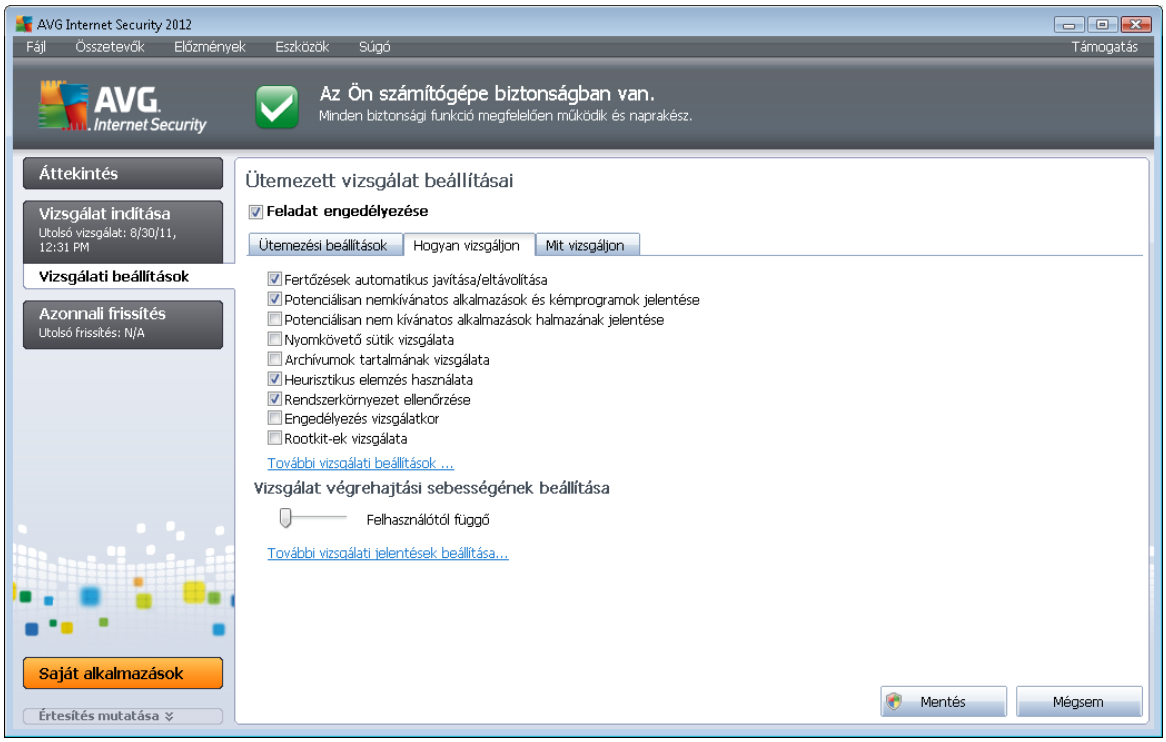
Vezérlőgombok az Ütemezett vizsgálat beállításai ablakban

Két vezérlőgomb található az ***Ütemezett vizsgálat beállításai*** párbeszédpanel mindhárom fülén *(Ütemezési beállítások, Hogyan vizsgáljon és Mit vizsgáljon a program)*, és ezek ugyanúgy működnek az adott fültől függetlenül:

- ***Mentés*** - elment minden változást az összes fülön, és visszatér az alapértelmezett AVG vizsgálati felület ablakhoz. Ezért ha be szeretné állítani a vizsgálati paramétereket az összes fülön, akkor csak abban az esetben nyomja meg ezt a gombot, ha végzett az összes beállítással.

- ***Mégsem*** - figyelmen kívül hagy minden változást az összes fülön, és visszatér az alapértelmezett AVG vizsgálati felület ablakhoz.

11.5.2. Hogyan keressen a program



A ***Hogyan vizsgáljon*** fülön a vizsgálati paraméterek listáját találhatja, melyeket tetszőlegesen be- és kikapcsolhat. Alapértelmezés szerint a legtöbb paraméter be van kapcsolva, és működni fog a vizsgálat során. Javasoljuk, hogy tartsa meg az alapértelmezett beállításokat, és csak akkor módosítson rajtuk, ha feltétlenül szükséges:

- ***Fertőzés automatikus javítása/eltávolítása*** (*alapértelmezés szerint bekapcsolva*): ha vírust talál a vizsgálat során, akkor automatikusan javítja, amennyiben ez lehetséges. Ha a fertőzött fájlt nem lehet automatikusan javítani, vagy kikapcsolja ezt az opciót, akkor értesítést fog kapni a vírus azonosításáról, és eldöntheti, hogy mi legyen a fertőzött fájllal. A javasolt megoldás a fertőzött fájl Karanténba helyezése.

- ***Potenciálisan nemkívánatos programok és kémprogramok jelentése*** (*alapértelmezés szerint bekapcsolva*): jelölje be a Kémprogram-elhárító motor aktiválásához, illetve kémprogramok és vírusok kereséséhez. A kémprogramok külön kártevő kategóriát

képviselnek: komoly biztonsági kockázatot jelentenek, mégis nagy részüket a felhasználók szándékosan telepítik. Javasoljuk, hogy tartsa bekapcsolva ezt az opciót, mivel így növelheti a számítógép biztonságát.

- ***Potenciálisan nem kívánatos alkalmazások halmazának jelentése*** (*alapértelmezés szerint kikapcsolva*): jelölje be ezt a jelölőnégyzetet a kémprogramok speciális változatainak észleléséhez: olyan programok kereséséhez, amelyek ártalmatlanok, de később kártékony célokra használhatók. Ezzel tovább növelheti a számítógép biztonságát. A szolgáltatás legitim programokat is letilthat, ezért a funkció alapállapotban ki van kapcsolva.

- ***Nyomkövető sütik vizsgálata*** (*alapállapotban kikapcsolva*): ez az opció a Kémprogram-elhárító összetevőben meghatározza, hogy a vizsgálat során felismert sütik törölve legyenek-e (*a HTTP sütiket hitelesítéshez, nyomkövetéshez és bizonyos adatok gyűjtéséhez használják a felhasználókról, pl. honlap preferenciák vagy online vásárlás során a kosár tartalma*).

- ***Archívumok tartalmának vizsgálata*** (*alapállapotban kikapcsolva*): ez az opció meghatározza, hogy a vizsgálat minden fájlt - köztük archív fáljokat is, pl. ZIP, RAR - ellenőrizzen-e

- ***Heurisztika használata*** (*alapállapotban bekapcsolva*): a heurisztikus elemzés (*a vizsgált objektum utasításainak dinamikus emulációja egy virtuális környezetben*) lesz az egyik víruskeresési módszer a vizsgálat során.

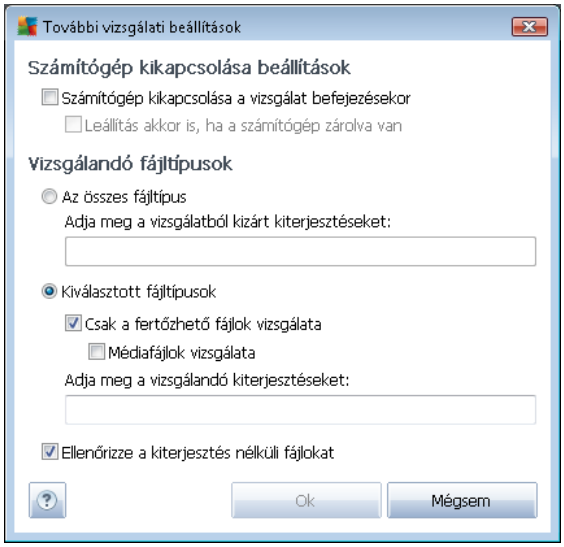
- ***Rendszerkörnyezet ellenőrzése*** (*alapállapotban bekapcsolva*): a vizsgálat a számítógép rendszerterületeit is ellenőrzi.

- ***Átfogó vizsgálat engedélyezése*** (*alapállapotban kikapcsolva*) - bizonyos esetekben (*például, ha arra gyanakszik, hogy a számítógépét egy vírus megfertőzte*), akkor jelölje be ezt az opciót a legátfogóbb vizsgálati algoritmus bekapcsolásához, amely a számítógép nehezen fertőzhető részeit is ellenőrzi a biztonság kedvéért. Ne feledje, hogy ez a módszer meglehetősen időigényes.

- ***Rootkitek vizsgálata*** (*alapállapotban kikapcsolva*): jelölje be ezt az elemet, ha rootkiteket is keresni kíván a számítógép teljes vizsgálata során. A rootkit vizsgálat külön is indítható az Anti-Rootkit összetevőből.

A vizsgálati beállításokat a következőképpen módosíthatja:

- ***További vizsgálati beállítások*** - ez a link megnyit egy új ***További vizsgálati beállítások*** panelt, ahol a következő paramétereket adhatja meg:



- ***A számítógép kikapcsolásának beállításai*** - döntse el, hogy a számítógép automatikusan kikapcsoljon-e, miután a vizsgálati folyamat véget ért. Miután megerősítette ezt a beállítást (***Számítógép leállítása a vizsgálat után***), egy új opció aktiválódik, mely lehetővé teszi, hogy akkor is leállítsa a számítógépet, ha az éppen zárolt (***Számítógép leállítása zárolás esetén is***).

- ***Vizsgálandó fájltípusok*** – a továbbiakban döntse el, hogy a program mely fájlokat vizsgálja:

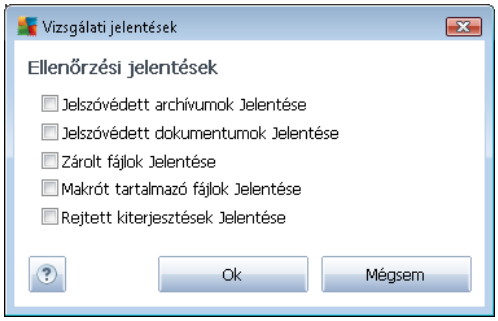
  - ***Összes fájltípus*** - lehetséges megadnia kivételeket, amelyek kimaradnak a vizsgálatból. Ezen fájlkiterjesztéseket vesszővel válassza el.

  - ***Kiválasztott fájltípusok*** - megadhatja, hogy a program csak olyan fájlokat vizsgáljon, amelyek esetlegesen fertőzőek (*a nem fertőzhető fájlok, mint pl. a sima szöveges fájlok vagy egyéb nem futtatható fájlok, nem lesznek ellenőrizve*), pl. médiafájlok (*video-, audiofájlok - ha nem jelöli be ezt a négyzetet, akkor tovább csökken a vizsgálati idő, mivel ezen fájlok általában túl nagyok, és egyébként sem valószínű, hogy vírus fertőzné meg őket*). A kiterjesztések segítségével megadhatja, hogy mely fájlokat vizsgálja a program.

  - Megadhatja azt is, hogy ***a program vizsgálja a kiterjesztés nélküli fájlokat*** - ez az opció alapállapotban be van kapcsolva és javasolt, hogy tartsa is így. A kiterjesztés nélküli fájlok különösen gyanúsak, ezért mindig ellenőrizni kell őket.

- ***Vizsgálat sebességének beállítása*** - használja a csúszkát a vizsgálati folyamat prioritásának módosításához. Alapállapotban ez az érték *felhasználótól függő* automatikus erőforráshasználatra van állítva. Alapállapotban a vizsgálati folyamatot lassabra állíthatja, ekkor a rendszer minimális erőforrást használ (*hasznos, ha a számítógépen kell dolgoznia, és nem számít a gyorsaság*); vagy gyorsabbra állíthatja, ekkor a rendszer több erőforrást használ (*a számítógépet ideiglenesen felügyelet nélkül hagyhatja*).

- ***További vizsgálati jelentések beállítása*** – a hivatkozás megnyit egy új ***Vizsgálati jelentések*** panelt, ahol kiválaszthatja, hogy milyen találati típusokat jelentsen a program:

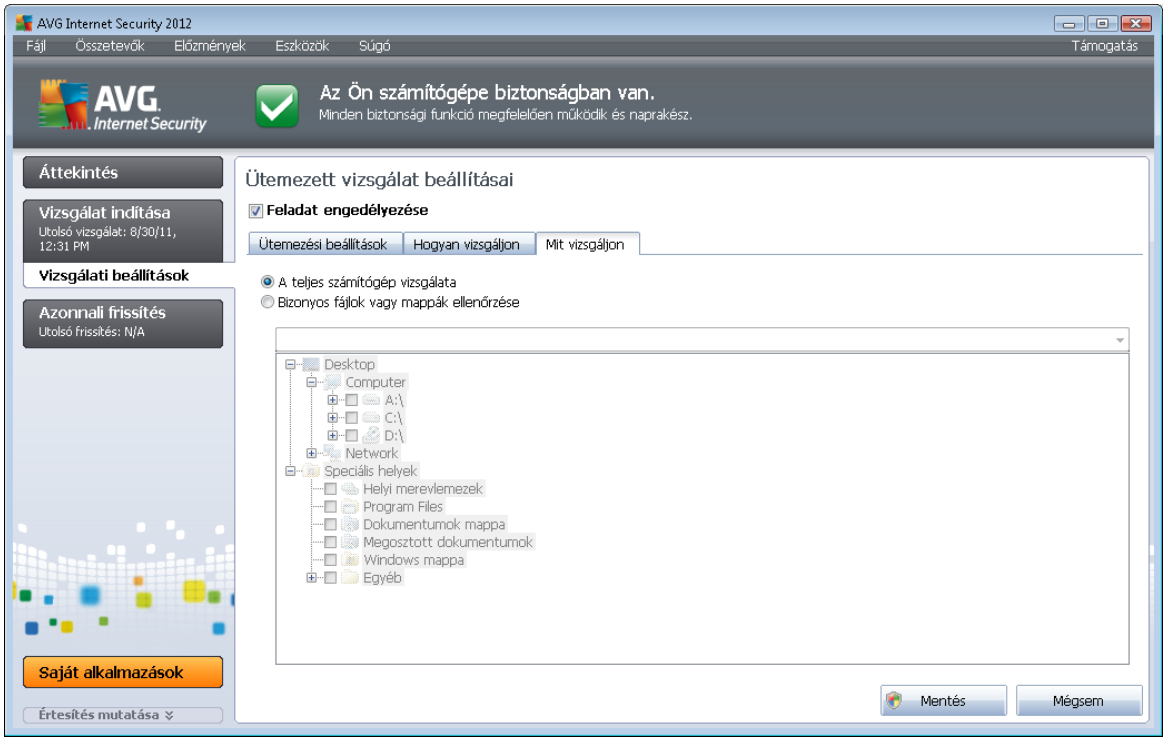


Vezérlőgombok

Két vezérlőgomb található az ***Ütemezett vizsgálat beállításai*** párbeszédpanel mindhárom fülén *(Ütemezési beállítások, Hogyan vizsgáljon és Mit vizsgáljon a program)*, és ezek ugyanúgy működnek az adott fültől függetlenül:

- ***Mentés*** - elment minden változást az összes fülön, és visszatér az alapértelmezett AVG vizsgálati felület ablakhoz. Ezért ha be szeretné állítani a vizsgálati paramétereket az összes fülön, akkor csak abban az esetben nyomja meg ezt a gombot, ha végzett az összes beállítással.
- ***Mégsem*** - figyelmen kívül hagy minden változást az összes fülön, és visszatér az alapértelmezett AVG vizsgálati felület ablakhoz.

11.5.3. Mit vizsgáljon a program



A ***Mit vizsgáljon a program*** fülön meghatározhatja, hogy a számítógép teljes vizsgálatát vagy csak bizonyos fájlok és mappák vizsgálatát szeretné ütemezni.

Ha bizonyos fájlok és mappák vizsgálatát választja, akkor a panel alsó részén a fastruktúra aktiválódik és bejelölheti az ellenőrzendő mappákat (*kattintson a plusz jelre a kívánt mappa kiválasztásához*). Több mappát is kiválaszthat egyszerre az adott dobozok bejelölésével A kiválasztott mappák megjelennek a szövegmezőben a panel tetején, míg a legördülő menü eltárolja a vizsgálati előzményeket későbbi használatra. Akár manuálisan is megadhatja a kívánt mappa teljes elérési útvonalát (*ha több útvonalat ír be, akkor pontosvesszővel válassza el őket, szóköz nélkül*).

A fastruktúrában láthat egy ***Különleges helyek*** ágat. Az alábbiakban láthatja azon helyeket, amelyek ellenőrizve lesznek, ha az adott jelölőnégyzetet bejelöli:

- ***Helyi merevlemezek*** – A számítógép összes merevlemeze
- ***Program Fájlok***
  - C:\Program Files\
  - *a 64-bit verziónál:* C:\Program Files (x86)
- ***Dokumentumok mappa***
  - *Windows XP-nél:* C:\Documents and Settings\Default User\My Documents\
  - *Windows Vista/7 rendszereknél*: C:\Users\user\Documents\
- ***Megosztott dokumentumok***
  - *Windows XP-nél*: C:\Documents and Settings\All Users\Documents\
  - *Windows Vista/7 rendszereknél*: C:\Users\Public\Documents\
- ***Windows mappa*** - C:\Windows\
- ***Egyéb***
  - *Rendszermeghajtó* - az a merevlemez, amelyen az operációs rendszer telepítva van (általában C:)
  - *Rendszermappa* - C:\Windows\System32\
  - *Ideiglenes fájlok mappa* - C:\Documents and Settings\User\Local\ (*Windows XP*); vagy C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
  - *Ideiglenes internetes fájlok* - C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*); vagy C: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows*

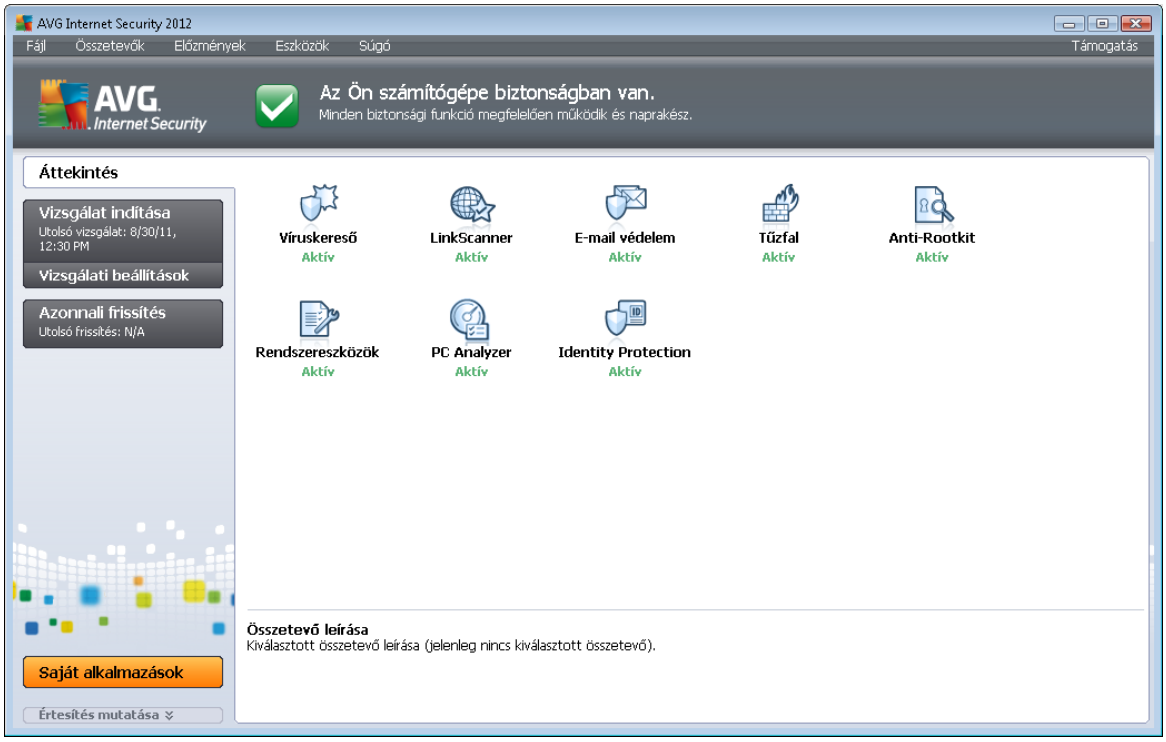
Vista/7)

Vezérlőgombok

A két ugyanolyan vezérlőgomb mindhárom lapon rendelkezésre áll az ***Ütemezett vizsgálat beállításai*** párbeszédpanelen *(Ütemezési beállítások, Hogyan keressen a program és Mit vizsgáljon a program)*:

- ***Mentés*** - elment minden változást az összes fülön, és visszatér az alapértelmezett AVG vizsgálati felület ablakhoz. Ezért ha be szeretné állítani a vizsgálati paramétereket az összes fülön, akkor csak abban az esetben nyomja meg ezt a gombot, ha végzett az összes beállítással.
- ***Mégsem*** - figyelmen kívül hagy minden változást az összes fülön, és visszatér az alapértelmezett AVG vizsgálati felület ablakhoz.

11.6. Vizsgálati eredményének áttekintése



A ***Vizsgálat eredményének áttekintése*** ablak elérhető az AVG vizsgálati felületről a ***Korábbi ellenőrzések*** gombbal. Az ablak megmutatja az összes korábban indított vizsgálatot és azok eredményeit:

- ***Név*** - vizsgálattól függ; lehet valamelyik alapértelmezett vizsgálat neve, vagy olyan név, melyet Ön adott egy saját ütemezett vizsgálatnak. Minden név tartalmaz egy ikont a vizsgálat eredményére vonatkozólag:

 - a zöld ikon azt jelenti, hogy a program nem talált fertőzést a vizsgálat során

 - a kék ikon azt jelenti, hogy a program talált fertőzést a vizsgálat során, de azt automatikusan eltávolította

 - a piros ikon azt jelenti, hogy a program talált fertőzést a vizsgálat során, de nem tudta azt eltávolítani!

Mindegyik ikon teljes vagy félbevágott alakú lehet - a teljes azt jelenti, hogy a vizsgálat rendben befejeződött; míg a félbevágott ikon azt jelenti, hogy a vizsgálat megszakadt vagy leállították.

***Megjegyzés**: Mindegyik vizsgálattal kapcsolatos további információkért nézze meg a Vizsgálat eredménye ablakot a Részletek megtekintése gombbal (az ablak alján).*

- ***Kezdési idő*** - a dátum és idő a vizsgálat indításakor
- ***Befejezés ideje*** - a dátum és idő a vizsgálat befejezésekor
- ***Vizsgált objektumok*** - a vizsgálat során ellenőrzött objektumok száma
- ***Fertőzések*** - a felismert / eltávolított vírusfertőzések száma
- ***Kémprogramok*** - a felismert / eltávolított kémprogramok száma
- ***Figyelmeztetések*** - észlelt gyanús objektumok
- ***Rootkitek*** - észlelt rootkitek
- ***Vizsgálati napló információk*** - információk a vizsgálat folyamatához és eredményéhez kapcsolódóan (jellemzően befejezéskor vagy megszakításkor)

Vezérlőgombok

A vezérlőgombok a ***Vizsgálat eredményének áttekintése*** ablakban a következők:

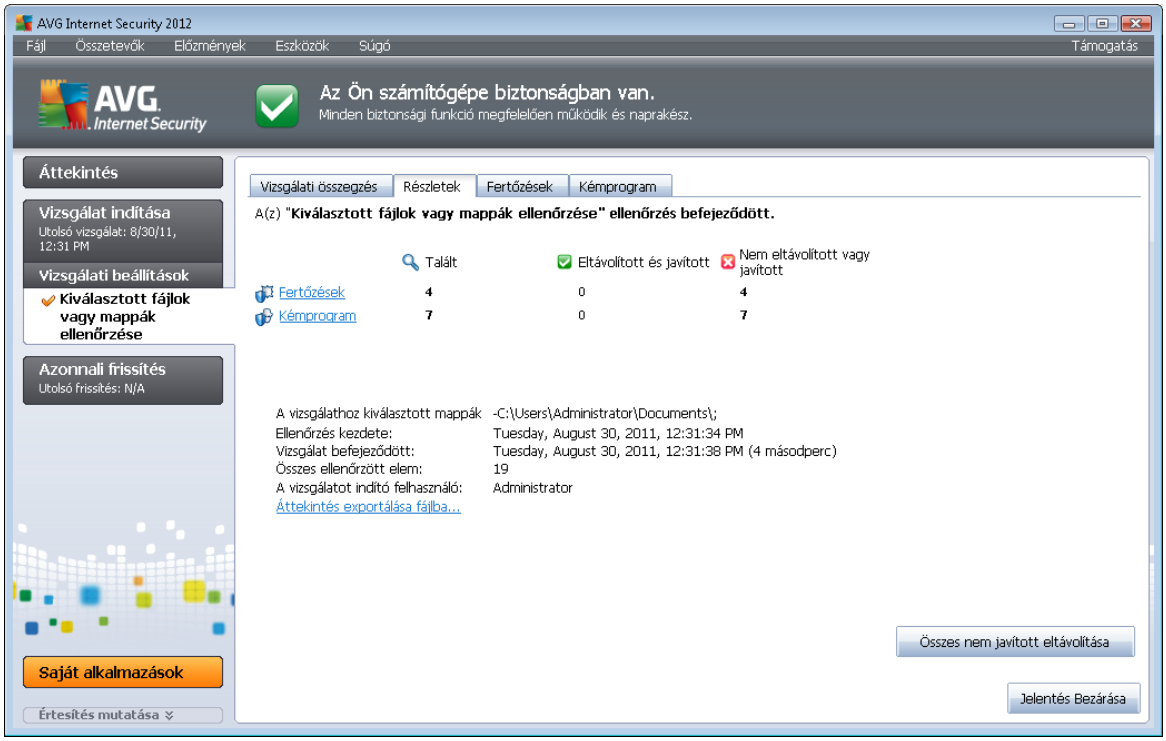
- ***Részletek megtekintése*** - nyomja meg ezt a gombot a Vizsgálati eredmények párbeszédpanel megjelenítéséhez és a kijelölt vizsgálat részletes adatainak megtekintéséhez
- ***Eredmény törlése*** - nyomja meg ezt a gombot a kijelölt elem vizsgálati eredményekből történő eltávolításához
- ***Vissza*** - visszatér az alapértelmezett AVG vizsgálati felülethez

11.7. Vizsgálati eredmények részletei

Ha A vizsgálat eredményének áttekintése panelen egy adott vizsgálat ki van jelölve, akkor kattintson a ***Részletek megtekintése*** gombra a ***Vizsgálati eredmények*** ablak megnyitásához, amely részletes adatokat közöl a vizsgálat folyamatáról és eredményéről. Az ablak több lapra van osztva:

- Eredmények áttekintése – Ez a fül mindig megjelenik, és statisztikai adatokat nyújt a vizsgálati folyamatról
- Fertőzések – Ez a fül csak akkor jelenik meg, ha a program vírusfertőzést azonosított a vizsgálat során
- Kémprogramok – Ez a fül csak akkor jelenik meg, ha a program kémprogramokat azonosított a vizsgálat során
- Figyelmeztetések – Ez a fül csak akkor jelenik meg, ha a program például cookie-kat azonosított a vizsgálat során
- Rootkitek – Ez a fül csak akkor jelenik meg, ha a program rootkiteket azonosított a vizsgálat során
- Információk – Ez a fül csak akkor jelenik meg, ha a program potenciális fenyegetést azonosított, de az nem sorolható be a fenti kategóriákba. Ezért a program figyelmeztető üzenetet jelenít meg a találattal kapcsolatban. Továbbá itt információkat találhat olyan objektumokról, amelyek nem vizsgálhatók *(például jelszóval védett archívumok)*.

11.7.1. Eredmények áttekintése fül



A ***A vizsgálat eredménye*** fülön részletes statisztikákat találhat a következő információkkal:

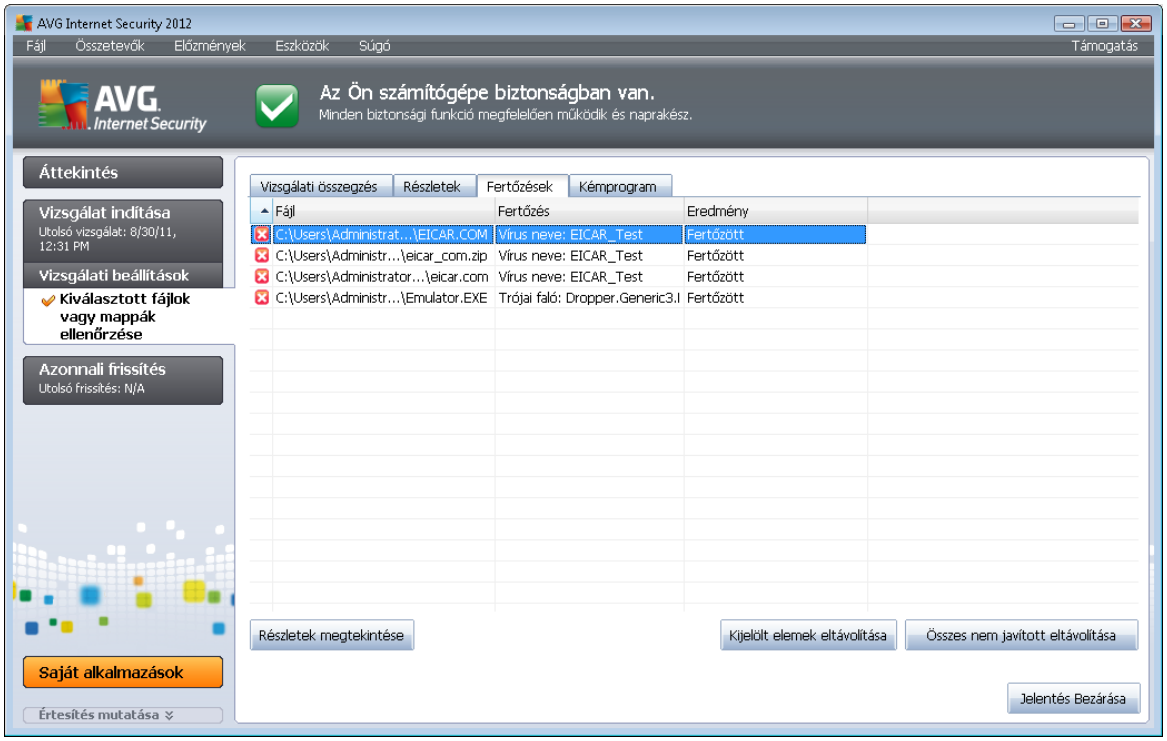
- észlelt vírusfertőzés/kémprogram
- eltávolított vírusfertőzés/kémprogram
- a nem javítható vagy eltávolítható vírusfertőzések/kémprogramok száma

Ezenkívül információkat találhat a vizsgálat indításának pontos dátumával és idejével, a vizsgált objektumok teljes számával, a vizsgálat időtartamával és az esetlegesen felmerült hibákkal kapcsolatban is.

Vezérlőgombok

Csak egy vezérlőgomb érhető el ezen a panelen. ***Az Eredmények bezárása*** gombbal visszatérhet a Vizsgálat eredményének áttekintése panelre.

11.7.2. Fertőzések fül



A ***Fertőzések*** fül csak akkor jelenik meg a ***Vizsgálat eredménye*** ablakban, ha a program vírusfertőzést talált a vizsgálat során. A fül három részre van osztva a következő információkal:

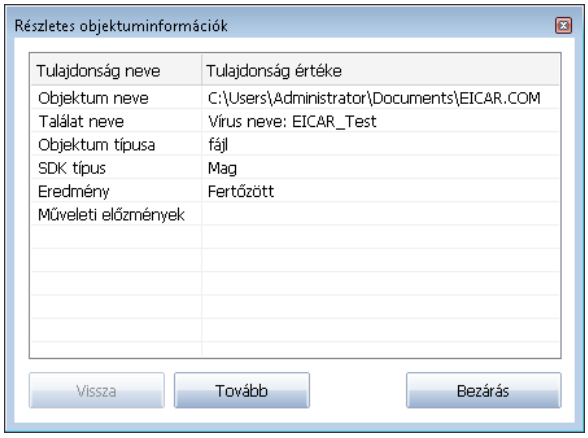
- ***Fájl*** - teljes elérési útvonal a fertőzött objektum eredeti helyéhez
- ***Fertőzések*** - a felismert vírus neve (*adott vírussal kapcsolatos részletes információkért nézze meg a Vírusenciklopédiát online*)

- ***Eredmény*** - megmutatja a fertőzött objektum vizsgálat során meghatározott állapotát:
  - ***Fertőzött*** - a felismert és eredeti helyükön hagyott fertőzött objektumok (*például ha az automatikus javítás opció ki van kapcsolva a vizsgálati beállításokban*)
  - ***Javítva*** - az automatikusan javított és eredeti helyükön hagyott fertőzött objektumok
  - ***Karanténba áthelyezve*** - a Karanténba áthelyezett fertőzött objektumok
  - ***Törölve*** - a törölt fertőzött objektumok
  - ***Hozzáadva a PUP kivételekhez*** - kivételként értelmezett találat, mely hozzá lett adva a PUP kivételek listájához *(meghatározva a PUP kivételekben a haladó beállításokban)*
  - ***Zárolt fájl - nem vizsgált*** - az adott objektum zárolva van, ezért az AVG nem tudja megvizsgálni
  - ***Potenciálisan veszélyes elem*** - az objektum potenciálisan veszélyes de nem fertőzött (*lehet például makró*). Az információ csak figyelmeztetésnek számít
  - ***Újraindítás szükséges a művelet befejezéséhez*** - a fertőzött objektumot nem lehet eltávolítani, a teljes eltávolításhoz újra kell indítania a számítógépet

Vezérlőgombok

Három vezérlőgomb található az ablakban:

- ***Részletek megtekintése*** - ez a gomb egy újabb ablakot nyit meg ***Részletes objektumadatok*** néven:

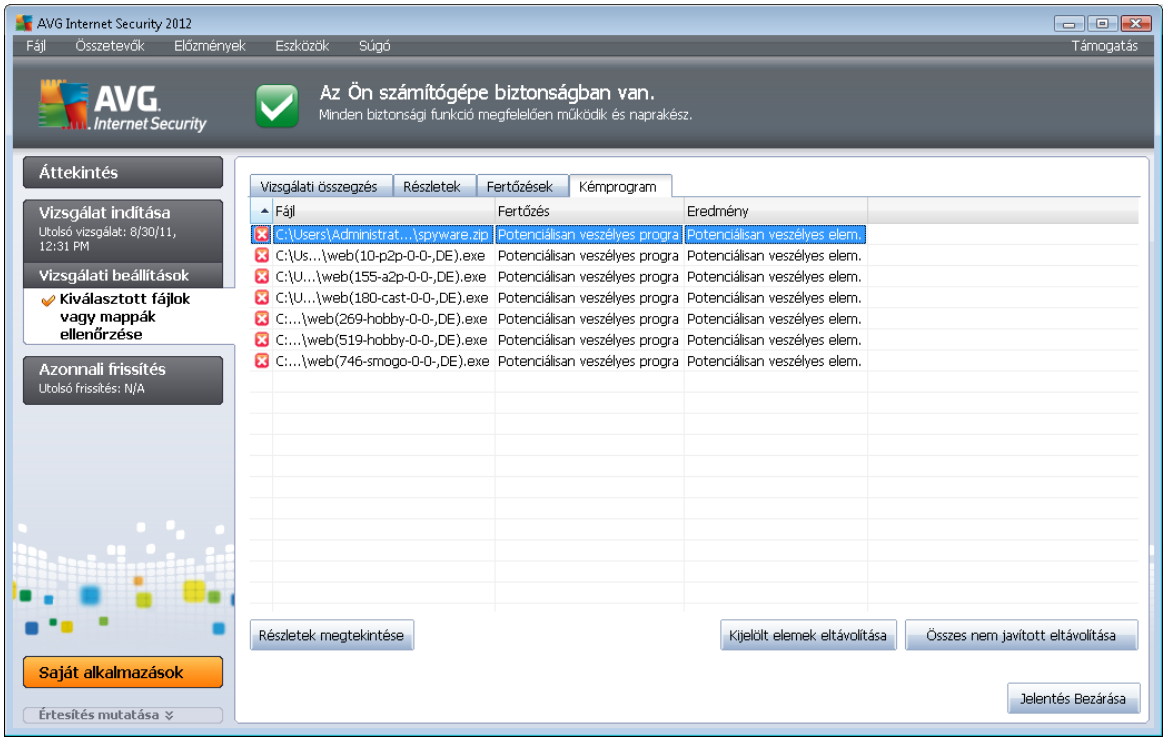


Ezen a panelen részletes információkat találhat a fertőzött objektumról (*pl. fertőzött objektum neve és helye, objektum típusa, SDK típusa, észlelési eredmény és a fertőzött objektumhoz tartozó műveletek előzményei*). A ***Vissza*** / ***Tovább*** gombokkal további információkat tekinthet meg. Használja a ***Bezárás*** gombot az ablak

bezárásához.

- ***Kijelölt eltávolítása*** - használja ezt a gombot a kiválasztott objektum Karanténba helyezéséhez
- ***Összes nem javított eltávolítása*** - ezzel a gombbal törölheti az olyan objektumokat, amelyeket nem lehet javítani vagy a Karanténba áthelyezni
- ***Eredmények bezárása*** - kilép a részletes információk áttekintéséből és visszatér a Vizsgálat eredményének áttekintése ablakba

11.7.3. Kémprogram fül



A ***Kémprogram*** fül a ***Vizsgálat eredménye*** párbeszédpanelen csak akkor jelenik meg, ha a program kémprogramokat talált a vizsgálat során. A fül három részre van osztva a következő információkal:

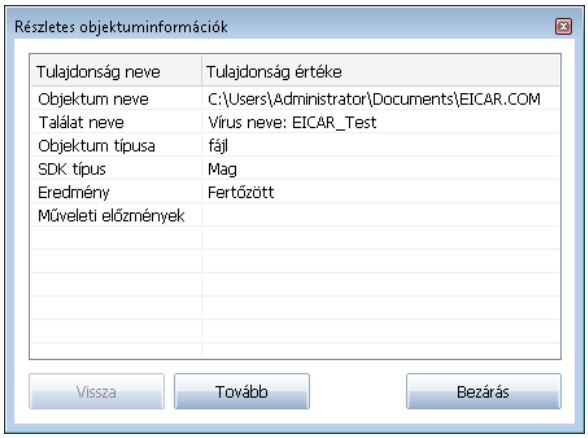
- ***Fájl*** - teljes elérési útvonal a fertőzött objektum eredeti helyéhez
- ***Fertőzések*** – A felismert kémprogramok neve *(egy adott vírussal kapcsolatos részletes információkért nézze meg a Vírusenciklopédiát az interneten)*
- ***Eredmény*** – Megjeleníti a vizsgálat során észlelt objektum aktuális állapotát:
  - ***Fertőzött*** – A program felismerte és eredeti helyén hagyta a fertőzött objektumot *(például ha az automatikus javítás lehetőség ki van kapcsolva a vizsgálati beállításokban)*

- ***Javítva*** – A program automatikusan javította és eredeti helyén hagyta a fertőzött objektumot
- ***Karanténba áthelyezve*** – A program áthelyezte a karanténba a fertőzött objektumot
- ***Törölve*** – A program törölte a fertőzött objektumot
- ***Hozzáadva a PUP kivételekhez*** – A program kivételként értelmezte a találatot, amelyet hozzáadott a PUP kivételek listájához *(ez a haladó beállítások PUP kivételek párbeszédpanelén adható meg)*
- ***Zárolt fájl - nem vizsgált*** - az adott objektum zárolva van, ezért az AVG nem tudja megvizsgálni
- ***Potenciálisan veszélyes elem*** - az objektum potenciálisan veszélyes de nem fertőzött (lehet makró például). Az információ csak figyelmeztetésnek számít
- ***Újraindítás szükséges a művelet befejezéséhez*** - a fertőzött objektumot nem lehet eltávolítani, a teljes eltávolításhoz újra kell indítania a számítógépet

Vezérlőgombok

Három vezérlőgomb található az ablakban:

- ***Részletek megtekintése*** - ez a gomb egy újabb ablakot nyit meg ***Részletes objektumadatok*** néven:



Ezen a panelen részletes információkat találhat a fertőzött objektumról (*pl. fertőzött objektum neve és helye, objektum típusa, SDK típusa, észlelési eredmény és a fertőzött objektumhoz tartozó műveletek előzményei*). ***A Vissza*** / ***Tovább*** gombokkal további információkat tekinthet meg. Használja a ***Bezárás*** gombot az ablakból történő kilépéshez.

- ***Kijelölt eltávolítása*** - használja ezt a gombot a kiválasztott objektum Karanténba helyezéséhez

- ***Összes nem javított eltávolítása*** - ezzel a gombbal törölheti az olyan objektumokat, amelyeket nem lehet javítani vagy a Karanténba áthelyezni

- ***Eredmények bezárása*** – Kilép a részletes információk áttekintéséből, és visszatér A Vizsgálat eredményének áttekintése párbeszédpanelre

11.7.4. Figyelmeztetések fül

A ***Figyelmeztetések*** fül információkat nyújt a "gyanús" objektumokról (*jellemzően fájlok*), melyek a vizsgálat során lettek azonosítva. Ezen fájlok hozzáférése blokkolva lesz, miután az Állandó védelem azonosította őket. Jellemző példák ezen találatokra: rejtett fájlok, sütik, gyanús regisztrációs adatbázis-bejegyzések, jelszóvédett dokumentumok vagy archívumok stb. Az ilyen fájlok nem jelentenek közvetlen veszélyt a számítógépre vagy a rendszer biztonságára. Az információk ezen fájlokról általában akkor hasznosak, ha a program valamilyen reklámprogramot vagy kémprogramot észlelt a számítógépen. Ha az **AVG Internet Security 2012** teszteredményei között csak figyelmeztetések szerepelnek, akkor nem szükséges további művelet.

Az alábbiakban egy rövid leírást talál az ezen eredmények leggyakoribb előfordulásával kapcsolatban:

- ***Rejtett fájlok*** - A rejtett fájlok alapértelmezés szerint nem láhatóak a Windows-ban, és néhány vírus vagy egyéb fenyegetés úgy próbálja elkerülni az észlelést, hogy ezt a jellemzőt veszi fel. Ha az **AVG Internet Security 2012** olyan rejtett fájlt talál, amelyet Ön is kártékonynak talál, akkor azt áthelyezheti a Karanténba.

- ***Sütik*** - A sütik egyszerű szöveges fájlok, amelyeket egyes weboldalak használnak a felhasználók információinak tárolására, hogy azok segítségével később egyedi tartalmakat jelenítsenek meg (pl. nevek megjegyzése stb).

- ***Gyanús regisztrációs adatbázis kulcsok*** - Néhány kártevő a Windows regisztrációs adatbázisában tárolja az adatait, hogy minden egyes rendszerindításkor betöltődhessen, és hatással legyen a teljes operációs rendszerre.

11.7.5. Rootkit-ek fül

A ***Rootkitek*** fül információkat jelenít meg a vizsgálat során észlelt rootkitekről, ha futtatott korábban egy rootkit vizsgálatot.

A rootkit olyan program, amelyet arra terveztek, hogy átvegye az irányítást a számítógép felett annak tulajdonosának vagy jogos használójának hozzájárulása nélkül. Hardverhez való hozzáférés ritkán szükséges, mivel a rootkit az azon futó operációs rendszer feletti irányítást veszi át. A rootkitek jellemzően leplezik jelenlétüket a rendszeren az operációs rendszer normál biztonsági mechanizmusának kijátszásával vagy megkerülésével. Gyakran egyúttal trójaiak is, és elhitetik a felhasználóval, hogy biztonságosan futtathatók a számítógépen. Az ehhez használt módszerek a következők lehetnek: futó folyamatok elrejtése a figyelőprogramoktól, fájlok vagy rendszeradatok elrejtése az operációs rendszeren.

Ezen lap felépítése gyakorlatilag ugyanaz mint a Fertőzések vagy a Kémprogramok lapé.

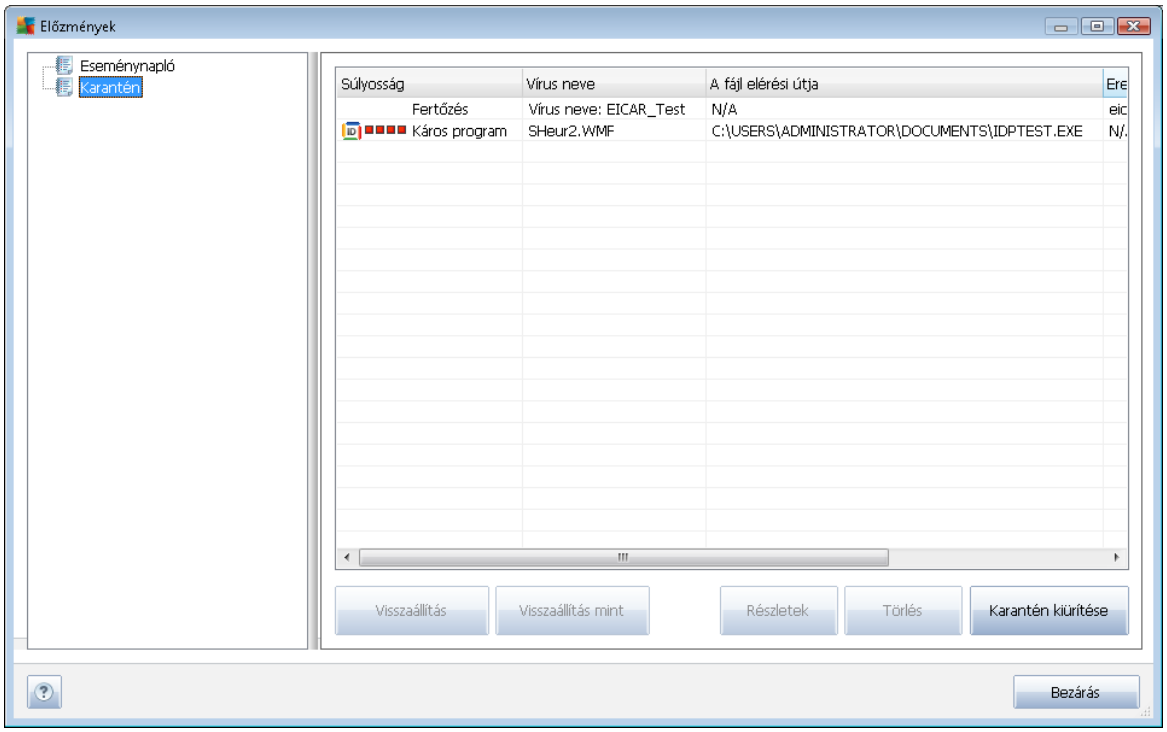
11.7.6. Információk fül

Az ***Információk*** fül adatokat tartalmaz olyan találatokkal kapcsolatban, melyeket nem lehet a fertőzések, kémprogramok, stb közé sorolni. Nem egyértelműen veszélyesek, de határozottan figyelmet kívánnak. **Az AVG Internet Security 2012** olyan fájlokat is képes észlelni, amelyek lehet, hogy nem fertőzöttek, de gyanúsak. Ezeket a fájlokat a program Figyelmeztetés vagy Információ megjegyzéssel jelenti.

A ***tájékoztató*** megjegyzés a következő esetekben fordul elő:

- ***Futtatás közbeni tömörítők*** - A fájlt egy kevésbé ismert futtatás közbeni tömörítő csomagolta, amely az ilyen fájlok vizsgálatának megakadályozására utalhat. Azonban nem minden ilyen megjegyzés utal vírusra.
- ***Futtatás közbeni rekurzív tömörítők*** - Hasonló a fentihez, bár kevésbé gyakori. Az ilyen fájlok gyanúsak, és törölni kell vagy el kell küldeni azokat elemzésre.
- ***Jelszóval védett archívum vagy dokumentum*** – A jelszóval védett fájlokat az **AVG Internet Security 2012** nem tudja ellenőrizni (*de más, káros programok elleni védelmet szolgáló programok sem*).
- ***Dokumentum makrókkal*** - A dokumentum olyan makrókat tartalmaz, amelyek veszélyesek lehetnek.
- ***Rejtett kiterjesztés*** - A rejtett kiterjesztéssel rendelkező fájlok képeknek tűnhetnek, de valójában futtatható fájlok (*pl. kép.jpg.exe*). A második kiterjesztés a Windows számára alapértelmezés szerint nem látható, ezért az **AVG Internet Security 2012** jelenti ezeket a fájlokat, hogy véletlenül ne nyissa meg azokat.
- ***Nem megfelelő fájlútvonal*** – Ha bizonyos fontos rendszerfájlok nem az alapértelmezett helyükről futnak (*például a winlogon.exe nem a Windows mappából*), akkor az **AVG Internet Security 2012** jelenti a normálistól eltérő viselkedést. Bizonyos esetekben a vírusok normál rendszerfolyamatok neveit használják, hogy jelenlétük a rendszerben kevésbé legyen nyilvánvaló.
- ***Zárolt fájl*** – A fájl zárolt, ezért az **AVG Internet Security 2012** nem tudja azt ellenőrizni. Ez azt jelenti, hogy bizonyos fájlokat (*például lapozófájlokat*) folyamatosan használ a rendszer.

11.8. Karantén



A Karantén biztonságos környezetet nyújt az AVG tesztjei során azonosított gyanús/fertőzött fájlok kezeléséhez. Ha a vizsgálat során az AVG vírusirtó fertőzött objektumot talál, és nem tudja automatikusan megjavítani, a program megkérdezi, hogy mihez kezdjen a gyanús objektumokkal. Azt ajánljuk, hogy helyezze át az objektumot a ***Karanténba*** a további műveletekhez. A ***Karantén*** lényege, hogy bármely törölt fájlt megőrizzen egy bizonyos ideig, így meggyőződhet róla, hogy a fájlra nincs szüksége az eredeti helyen. Amennyiben a fájl hiánya problémákat okozna, akkor küldje el a fájlt elemzésre, vagy állítsa vissza azt az eredeti helyére.

A ***Karantén*** felület külön ablakban nyílik meg, és áttekintést nyújt az elkülönített fertőzött objektumokról:

- ***Kockázati szint*** - ha telepítette az Identity Protection összetevőt, akkor **AVG Internet Security 2012** a kockázati szint grafikus formában jelenik meg egy négyszintű skálán a gyanústól (■□□□) a rendkívül veszélyesig (■■■■). A fertőzés típusa szintén megjelenik (*a fertőzöttségi szint alapján az objektumok határozottan vagy potenciálisan fertőzöttek lehetnek*)

- ***Vírus neve*** - a felismert fertőzés nevét mutatja a Vírusenciklopédia *szerint (online)*

- ***Fájl elérési útja*** - teljes elérési útvonal az azonosított és fertőzött fájl eredeti helyéhez

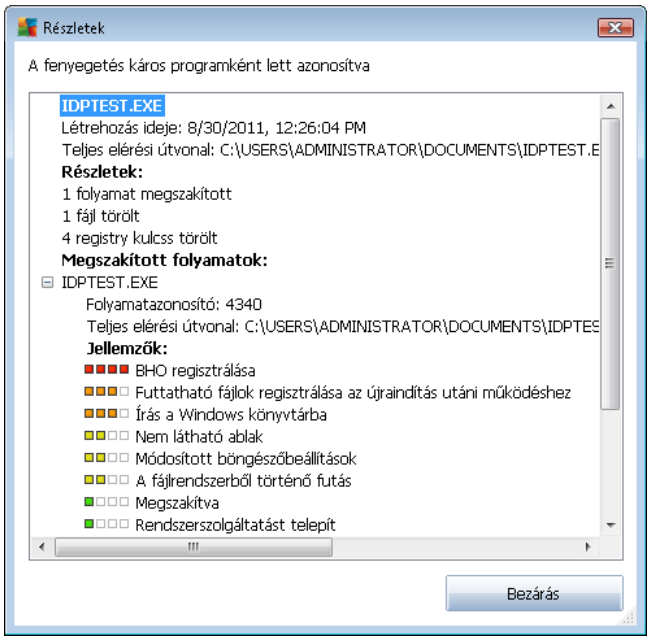
- ***Eredeti objektumnév*** - Az összes észlelt objektum fel van sorolva a listában, és meg van jelenítve a vizsgálat során az AVG által kiosztott név is. Ha az objektum egy adott ismert eredeti névvel rendelkezik (*pl. egy e-mail csatolmány neve, mely azonban nem jeleníti meg a melléklet tényleges tartalmát*), akkor az ebben az oszlopban jelenik meg.

- ***Tárolás dátuma*** - dátum és idő, amikor a gyanús fájlt a program azonosította és áthelyezte a Karanténba

Vezérlőgombok

A következő vezérlőgombok érhetők el a ***Karantén*** felületről:

- ***Visszaállítás*** - visszahelyezi a fertőzött fájlt az eredeti helyére a lemezen
- ***Visszaállítás másként*** – áthelyezi a fertőzött fájlt egy kiválasztott mappába
- ***Részletek*** - ez a gomb kizárólag az Identity Protection által észlelt fenyegetésekre vonatkozik. Ha rákattint, akkor a program megjeleníti a fenyegetésekkel kapcsolatos részletek összefoglalását (*érintett fájlok/folyamatok, folyamat jellemzői stb.*). Vegye figyelembe, hogy a nem IDP által észlelt fenyegetéseknél ez a gomb szürke és inaktív!



- ***Törlés*** - véglegesen és visszavonhatatlanul törli a fertőzött fájlt a ***Karanténból***
- ***Karantén kiürítése*** - törli a ***Karantén*** tartalmát . A fájlok ***Karanténból*** történő eltávolításával a fájlok véglegesen törlődnek a lemezről (*nem a Lomtárba kerülnek át*).

12. AVG frissítések

Semmilyen biztonsági szoftver nem garantálhat védelmet a különböző típusú fenyegetések ellen, ha az nincs rendszeresen frissítve. A vírusok készítői mindig újabb és újabb kihasználható hibákat keresnek az egyes szoftverekben és operációs rendszerekben. Új vírusok, rosszindulatú kódok és hackelési stratégiák jelennek meg minden egyes nap. Ezért a szoftvergyártók folyamatosan adnak ki frissítéseket és biztonsági javításokat újonnan felfedezett biztonsági rések betöméséhez.

Tekintettel az újonnan megjelenő számítógépes fenyegetések természetére és elterjedésük gyorsaságára, alapvető fontosságú az **AVG Internet Security 2012** rendszeres frissítése. A legjobb megoldás, ha megtartja az alapértelmezett beállításokat, amelyek szabályozzák az automatikus frissítést is. Felhívjuk figyelmét, hogy amennyiben az **AVG Internet Security 2012** vírusadatbázisa nem naprakész, a program nem képes felismerni a legújabb veszélyforrásokat.

Kulcsfontosságú, hogy rendszeresen frissítse az AVG programot. A vírusdefiníciós adatbázisokat lehetőleg naponta frissítse. A kevésbé fontos programfrissítéseket elég hetente elvégezni.

12.1. Frissítés indítása

A lehető legnagyobb biztonság elérése érdekében az **AVG Internet Security 2012** alapértelmezés szerint négy óránként ellenőrzi a frissítéseket. Mivel az AVG frissítések nem előre meghatározott ütemezés szerint jelennek meg, hanem az új fenyegetések mértéke és súlyossága alapján, ezért az ellenőrzés nagyon fontos az AVG vírusadatbázisának naprakészen tartásához.

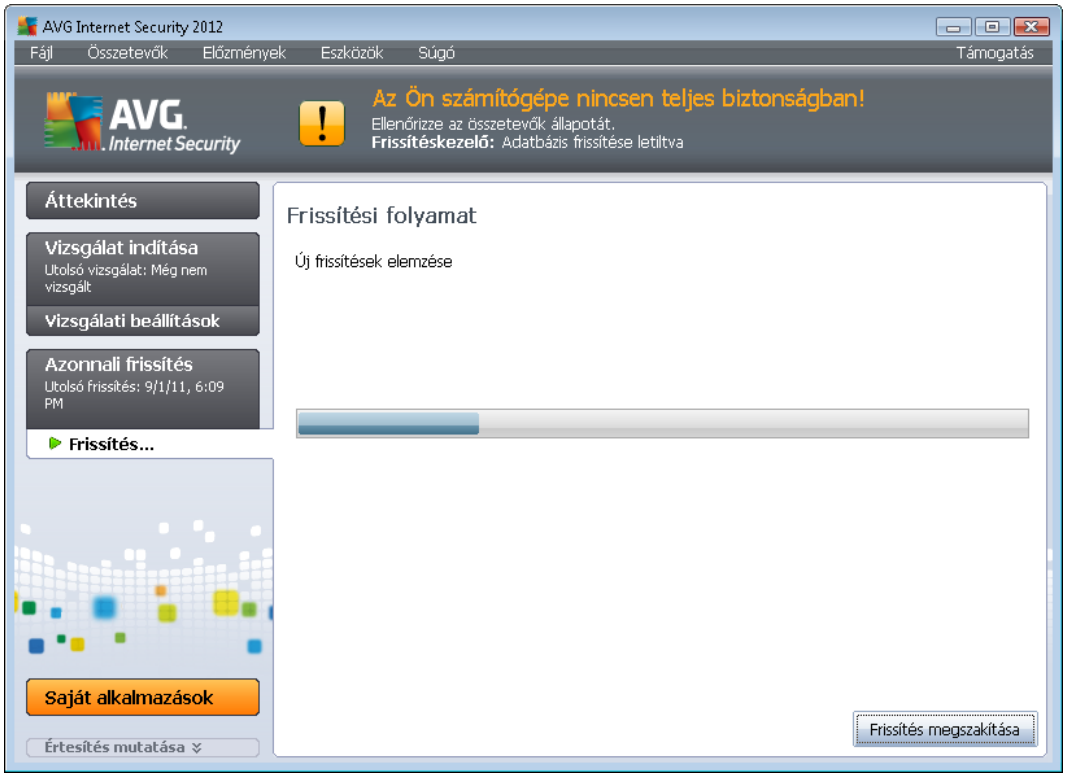
Ha csökkenteni kívánja a frissítéskeresések indításának számát, beállíthatja a saját indítási paramétereit. Azonban határozottan ajánlott a frissítést naponta legalább egyszer elindítani. A beállítást a Haladó beállítások/Ütemezés szakaszban lehet elvégezni, a következő párbeszédpaneleken:

- Vírusdefiníciók frissítésének ütemezése
- Programfrissítés ütemezése
- Levélszemétszűrő frissítés ütemezése

Ha azonnal ellenőrizni kívánja a frissítéseket, használja a fő felhasználói felületen található Azonnali frissítés gyorshivatkozást. A hivatkozás mindig, az összes felhasználói felület ablakból elérhető.

12.2. Frissítési folyamat

Amikor elindítja a frissítést, az AVG először ellenőrzi, hogy rendelkezésre állnak-e frissítési fájlok. Ha igen, akkor az **AVG Internet Security 2012** elindítja a letöltést és a frissítési folyamatot. A frissítési folyamat során a ***Frissítés*** felületre kerül, ahol ellenőrizheti a folyamat állapotát egy grafikus ábra, illetve a legfontosabb statisztikai paraméterek formájában (*a frissítési fájl mérete, fogadott adatok, letöltési sebesség, eltelt idő stb.*):



***Megjegyzés**: Mielőtt az AVG programfrissítés elindul, egy rendszer-visszaállítási pontot hoz létre a program. Ha a frissítési folyamat sikertelen és az operációs rendszer összeomlik, akkor visszaállíthatja az operációs rendszert egy korábbi állapotra. Ez a beállítás elérhető a Windows menüből: Start menü / Minden program / Kellékek / Rendszereszközök / Rendszer-visszaállítás. A beállítás használatát csak tapasztalt felhasználóknak javasoljuk.*

12.3. Frissítési szintek

Az AVG Internet Security 2012 kétféle frissítési szintet kínál:

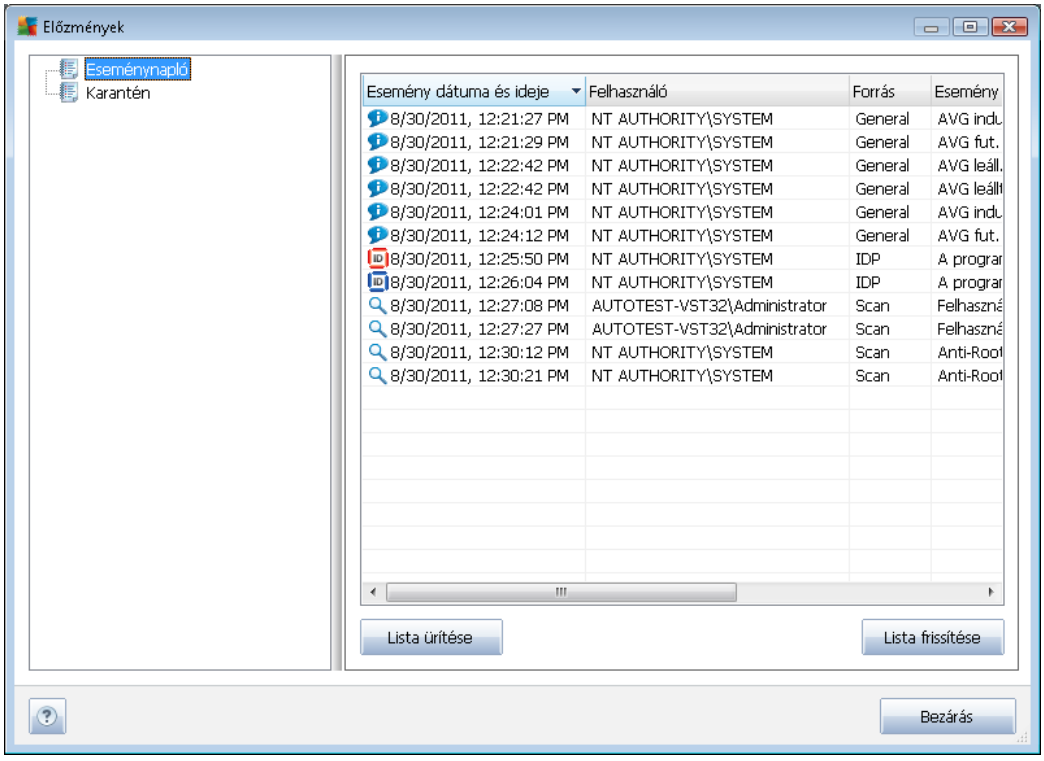
- ***Az adatbázisfrissítés*** a vírusok, levélszemetek és rosszindulatú programok elleni megbízható védelemhez szükséges módosításokat tartalmazza. A kód módosítását általában nem foglalja magában, csak a vírusadatbázis frissítésére szolgál. A frissítést rögtön alkalmazni kell, amint elérhető.
- ***A Programfrissítés*** a program különböző módosításait, javításait és fejlesztéseit tartalmazza.

A frissítés ütemezésekor mindkét frissítési szint paraméterei megadhatók:

- Vírusdefiníciók frissítésének ütemezése
- Programfrissítés ütemezése

***Megjegyzés:** Ha az ütemezett programfrissítés és az ütemezett vizsgálat időben ütközik, akkor a frissítési folyamatnak van elsődleges prioritása, és a vizsgálat meg lesz szakítva.*

13. Eseménynapló



Az ***Előzmények*** panel elérhető a rendszermenüből az ***Előzmények/Eseménynapló*** elemen keresztül. Ezen a panelen az **AVG Internet Security 2012** működése közben fellépett fontosabb események összegzését tekintheti át. ***Az Esemény*** rész a következő típusú események rögzítésére szolgál:

- Az AVG alkalmazás frissítésével kapcsolatos információk.
- A vizsgálat kezdetével, befejezésével és megszakításával kapcsolatos információk (*beleértve az automatikusan végrehajtott teszteket*)
- A vírusészleléshez kapcsolódó eseményekről szóló információk (*Állandó védelem vagy keresés* segítségével) az előfordulás helyével együtt
- Egyéb jelentős események.

Az egyes eseményeknél a következő adatok találhatók:

- ***Az Esemény dátuma és ideje*** az esemény bekövetkezésének pontos dátumát és idejét adja meg
- ***A Felhasználó*** az esemény bekövetkezésekor aktuálisan bejelentkezett felhasználó nevét mutatja
- ***A Forrás*** a forrás összetevőjének adatait vagy az AVG rendszer más, az eseményt kiváltó részét mutatja

- ***Az Esemény leírása*** röviden leírja, hogy mit történt

Vezérlőgombok

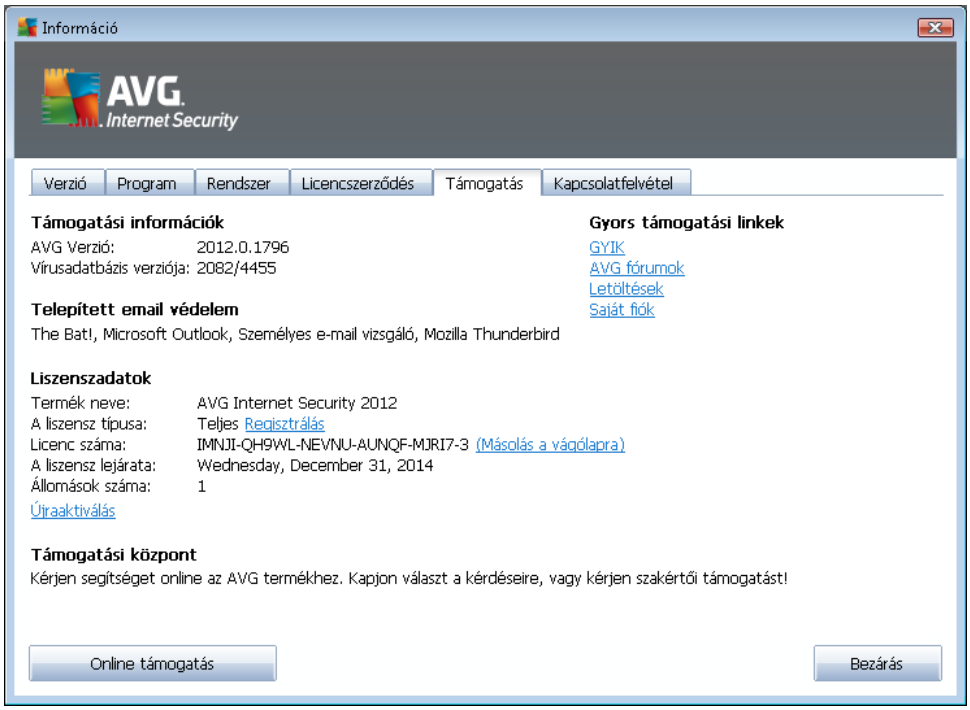
- ***Lista ürítése –*** a gomb megnyomásával az összes bejegyzést törölheti az események listájából
- ***Lista frissítése –*** a gomb megnyomásával az összes bejegyzést frissítheti az események listájában

14. Gyakori kérdések és műszaki támogatás

Ha az **AVG Internet Security 2012** termékkel kapcsolatban bármilyen értékesítési vagy technikai problémája van, több módon is segítséghez juthat. Kérjük, válasszon a következő lehetőségek közül:

- ***Kapcsolatfelvétel az ügyfélszolgálattal***: Közvetlenül az AVG alkalmazásból léphet kapcsolatba szakértő ügyfélszolgálatunkkal. Használja a ***Súgó / Online súgó*** főmenü elemet, amely átirányítja az AVG éjjel-nappal működő ügyfélszolgálatának online kapcsolatfelvételi űrlapjához. A licencszámát automatikusan kitölti a program. A folytatáshoz kövesse a weboldalon megjelenő utasításokat.

- ***Támogatás (főmenü hivatkozás)***: Az AVG alkalmazás menüben (*a fő felhasználói felület tetején*) megtalálható a ***Támogatás*** hivatkozás, amely egy új párbeszédpanelt nyit meg. Ezen az összes szükséges információ megtalálható a segítségkéréshez. A párbeszédpanel a telepített AVG program alapvető adatait (*program / adatbázis-verzió*), a licencadatokat, és a gyorstámogatási hivatkozások listáját tartalmazza:



- ***Problémamegoldás súgófájlban***: Az **AVG Internet Security 2012** súgófájljának részeként közvetlenül elérhető egy új ***Hibaelhárítás*** nevű szakasz. Ez a szakasz a leggyakrabban előforduló olyan helyzetek listáját tartalmazza, amikor egy felhasználónak szakértői segítségre van szüksége egy technikai problémával kapcsolatban. Válassza ki azt a szituációt, amely a legjobban leírja a problémáját, és kattintson rá a probléma megoldását részletesen leíró útmutatás megnyitásához.

- ***AVG webhely támogatási központ***: Az AVG webhelyén (http://www.avg.hu/) is kereshet megoldást a problémájára. ***A Támogatási központ*** szakaszban tematikus csoportok strukturált áttekintését találja, amelyek mind értékesítési, mind technikai problémákkal foglalkoznak.

- ***Gyakori kérdések***: Az AVG webhelyén (http://www.avg.hu/) egy, a gyakori kérdésekkel foglalkozó, különálló és részletesen kidolgozott szakaszt is talál. Ez a szakasz a ***Támogatási központ / GYIK*** menüponton keresztül érhető el. A kérdések itt is jól rendszerezve, értékesítés, technikai problémák illetve vírus kategóriákba vannak sorolva.

- ***Vírusokról és fenyegetésekről***: Az AVG webhely (http://www.avg.hu/) egy külön fejezete foglalkozik a vírusokkal kapcsolatos problémákkal. Az online fenyegetésekkel kapcsolatos strukturált információkat tartalmazó oldalra történő belépéshez a menüben válassza a ***Támogatási központ / Vírusokról és fenyegetésekről*** lehetőséget. Itt a vírusok és kémprogramok eltávolításához talál útmutatásokat, valamint tanácsokat azzal kapcsolatban, hogyan tudhatja számítógépét mindig biztonságban.

- ***Vitafórum***: Használhatja az AVG felhasználók a http://forums.avg.com webhelyen található vitafórumát is.