



AVG Internet Security 2011

Felhasználói kézikönyv

Dokumentumverzió 2011.21 (16.5.2011)

Copyright AVG Technologies CZ, s.r.o. Minden jog fenntartva.
Minden egyéb márkanév a tulajdonosok tulajdonát képezi.

A termék hasznosítja az RSA Data Security, Inc. MD5 üzenetfeldolgozó algoritmusát. Copyright (C) 1991-2, RSA Data Security, Inc. Készítési dátum: 1991.

Ez a termék a C-SaCzech függvénytar kódját használja, Copyright (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).

A termék használja a zlib tömörítési függvénytarat. Copyright (c) 1995-2002 Jean-loup Gailly és Mark Adler.
A termék hasznosítja a libzip2 tömörítési függvénytarat. Copyright (c) 1996-2002 Julian R Seward.

Tartalom

1. Bevezetés	8
2. AVG telepítési követelmények	9
2.1 Támogatott operációs rendszerek	9
2.2 Minimum és ajánlott hardverkövetelmények	9
3. AVG telepítési lehetőségek	10
4. AVG telepítési folyamat	11
4.1 Üdvözlöképernyő	11
4.2 AVG liszensz aktiválása	11
4.3 Telepítés típusának kiválasztása	12
4.4 Egyéni opciók	13
4.5 Az AVG Biztonság eszköztár telepítése	14
4.6 Telepítési folyamat	15
4.7 A telepítés sikerült	15
5. A telepítés utáni teendők	17
5.1 Termék regisztrálása	17
5.2 Hozzáférés a felhasználói felülethez	17
5.3 A teljes számítógép vizsgálata	17
5.4 Eicar teszt	17
5.5 AVG alapértelmezett konfiguráció	18
6. AVG felhasználói felület	19
6.1 System (Rendszer) menü	20
6.1.1 Fájl	20
6.1.2 Összetevok	20
6.1.3 Elozmények	20
6.1.4 Eszközök	20
6.1.5 Súly	20
6.2 Biztonsági állapot információk	23
6.3 Gyors linkek	24
6.4 Összetevok áttekintése	24
6.5 Statisztikák	26
6.6 Tálcaikon	26
6.7 AVG minialkalmazás	27

7. AVG összetevők	30
7.1 Víruskereso	30
7.1.1 Víruskeresési alapelvek	30
7.1.2 Víruskereso felület	30
7.2 Kémprogram-elhárító	31
7.2.1 Kémprogram-elhárító alapelvek	31
7.2.2 Kémprogram-elhárító felület	31
7.3 Levélszemétszuro	33
7.3.1 Levélszemétszuro alapelvek	33
7.3.2 Levélszemétszuro felület	33
7.4 Tuzfal	34
7.4.1 Tuzfal alapelvek	34
7.4.2 Tuzfal profilok	34
7.4.3 Tuzfal felület	34
7.5 Linkvizsgáló	38
7.5.1 LinkScanner alapelvek	38
7.5.2 LinkScanner felület	38
7.5.3 Kereso védelem	38
7.5.4 Böngészés védelem	38
7.6 Állandó védelem	42
7.6.1 Állandó védelem alapelvek	42
7.6.2 Állandó védelem felület	42
7.6.3 Állandó védelem észlelés	42
7.7 Family Safety	47
7.8 AVG LiveKive	47
7.9 E-mail vizsgáló	47
7.9.1 E-mail vizsgáló alapelvek	47
7.9.2 E-mail vizsgáló felület	47
7.9.3 E-mail vizsgáló észlelés	47
7.10 Frissítéskezelő	51
7.10.1 Frissítéskezelő alapelvek	51
7.10.2 Frissítéskezelő felület	51
7.11 Licenc	53
7.12 Távfelügyelet	54
7.13 Online szuro	55
7.13.1 Online szuro alapelvek	55
7.13.2 Online szuro felület	55

7.13.3 Online szuro észlelés	55
7.14 Anti-Rootkit	58
7.14.1 Anti-Rootkit alapelvek	58
7.14.2 Anti-Rootkit felület	58
7.15 Rendszereszközök	59
7.15.1 Folyamatok	59
7.15.2 Hálózati kapcsolatok	59
7.15.3 Automatikus indítás	59
7.15.4 Böngésző kiterjesztések	59
7.15.5 LSP megjelenítő	59
7.16 PC Analyzer	65
7.17 ID Protection	67
7.17.1 ID Protection alapelvek	67
7.17.2 ID Protection felület	67
7.18 Biztonság eszköztár	69
8. AVG Biztonság eszköztár	71
8.1 AVG Biztonság eszköztár felület	71
8.1.1 AVG logó gomb	71
8.1.2 AVG Secure Search (powered by Google) keresotechnológia	71
8.1.3 Oldalállapot	71
8.1.4 AVG hírek	71
8.1.5 Hírek	71
8.1.6 Elozmények törlése	71
8.1.7 E-mail értesítő	71
8.1.8 Időjárési adatok	71
8.1.9 Facebook	71
8.2 AVG Biztonság eszköztár beállítások	78
8.2.1 Általános fül	78
8.2.2 Hasznos gombok fül	78
8.2.3 Biztonság fül	78
8.2.4 Haladó beállítások fül	78
9. AVG Haladó beállítások	82
9.1 Megjelenés	82
9.2 Hangok	84
9.3 Hibaállapot mellozése	86
9.4 Azonosság védelem	87
9.4.1 Identity Protection beállítások	87

9.4.2 Engedélyezett listája	87
9.5 Karantén	91
9.6 Nemkívánatos programok kivételei	91
9.7 Levélszemét-szűrő	93
9.7.1 Beállítások	93
9.7.2 Teljesítmény	93
9.7.3 RBL	93
9.7.4 Engedélyezett listája	93
9.7.5 Feketelista	93
9.7.6 Haladó beállítások	93
9.8 Online szűrő	105
9.8.1 Web védelem	105
9.8.2 Azonnali üzenetküldés	105
9.9 Linkvizsgáló	109
9.10 Vizsgálatok	110
9.10.1 A teljes számítógép vizsgálata	110
9.10.2 Héjkiterjesztés vizsgálat	110
9.10.3 Kiválasztott fájlok vagy mappák ellenőrzése	110
9.10.4 Cserélhető eszköz vizsgálata	110
9.11 Ütemezések	115
9.11.1 Ütemezett vizsgálat	115
9.11.2 Vírusadatbázis frissítésének ütemezése	115
9.11.3 Programfrissítés ütemezése	115
9.11.4 Levélszemétszűrő frissítés ütemezése	115
9.12 E-mail vizsgáló	126
9.12.1 Tanúsítás	126
9.12.2 Levélszűrő	126
9.12.3 Kiszolgálók	126
9.13 Állandó védelem	135
9.13.1 Haladó beállítások	135
9.13.2 Kizárt elemek	135
9.14 Gyorsítótár kiszolgálója	139
9.15 Anti-Rootkit	140
9.16 Frissítés	141
9.16.1 Proxy	141
9.16.2 Telefonos kapcsolat	141
9.16.3 URL	141
9.16.4 Kezel	141

9.17 Az AVG védelem ideiglenes letiltása	148
9.18 Termékfejlesztési program	148
10. Tuzfalbeállítások	151
10.1 Általános	151
10.2 Biztonság	152
10.3 Terület- és adapterprofilok	153
10.4 IDS	154
10.5 Naplók	156
10.6 Profilok	157
11. AVG vizsgálat	159
11.1 Vizsgálati felület	159
11.2 Elore meghatározott vizsgálatok	160
11.2.1 Vizsgálat a teljes számítógépen	160
11.2.2 Kiválasztott fájlok vagy mappák ellenorzése	160
11.2.3 Anti-Rootkit vizsgálat	160
11.3 Vizsgálat a Windows Intézőben	170
11.4 Parancssori vizsgálat	171
11.4.1 Parancssori vizsgálat paraméterek	171
11.5 Vizsgálatok ütemezése	173
11.5.1 Ütemezési beállítások	173
11.5.2 Hogyan keressen a program	173
11.5.3 Mit vizsgáljon a program	173
11.6 Vizsgálati eredményének áttekintése	183
11.7 Vizsgálati eredmények részletei	184
11.7.1 Eredmények áttekintése föl	184
11.7.2 Fertozések föl	184
11.7.3 Kémprogramok föl	184
11.7.4 Figyelmeztetések föl	184
11.7.5 Rootkit-ek föl	184
11.7.6 Információk föl	184
11.8 Karantén	191
12. AVG frissítések	194
12.1 Frissítési szintek	194
12.2 A frissítés típusai	194
12.3 Frissítési folyamat	194



13. Esemény elozmények	196
14. Gyakori kérdések és technikai támogatás	198



1. Bevezetés

A felhasználói kézikönyv átfogó dokumentációt kínál az **AVG Internet Security 2011** termékhez.

Gratulálunk az AVG Internet Security 2011 termék megvásárlásához!

Az **AVG Internet Security 2011** egyike a díjnyertes AVG termékeknek, melyeket úgy terveztünk, hogy nyugalmat és teljes biztonságot nyújtsanak Önnek és számítógépének. Mint minden terméket, az **AVG Internet Security 2011** szoftvert is teljesen - az alapoktól kezdve - újraterveztük, hogy biztosíthassa az AVG jól ismert és neves biztonsági megoldásait egy új, még inkább felhasználóbarát és hatékonyabb módon. Az Ön új **AVG Internet Security 2011** terméke letisztult felülettel és még pontosabb, illetve gyorsabb keresési képességgel rendelkezik. Több biztonsági funkció automatikussá vált az Ön kényelmének érdekében, illetve intelligens felhasználói opciókkal testreszabhatja biztonsági megoldásainkat. Nem kell többé feláldoznia a használhatóságot a biztonság kárára!

Az AVG-t úgy terveztük és fejlesztettük, hogy megvédje számítógépét és hálózatát. Élvezze a teljes védelem élményét az AVG-tól!

Összes AVG termékajánlat

- Védelem, amely azon alapul, ahogy Ön a számítógépet és az internetet használja: bankolás és vásárlás, böngészés és keresés, csevegés és e-mailezés, fájlok letöltése és közösségi hálózatok - az AVG személyre szabott védelmet kínál
- Problémamentes védelem, amelyet több mint 110 millió felhasználó használ szerte a világon, és amelyet rendkívül tapasztalt kutatók globális hálózata támogat
- Védelem, amely mögött állandó szakértői támogatás áll



2. AVG telepítési követelmények

2.1. Támogatott operációs rendszerek

Az **AVG Internet Security 2011a** 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 szervízcsoomagok bizonyos operációs rendszerekhez)

Megjegyzés: Az [ID Protection](#) összetevő nem támogatott Windows XP x64 rendszerek alatt. Erre az operációs rendszerre kizárólag az AVG Internet Security 2011 terméket telepítheti, az IDP összetevő nélkül.

2.2. Minimum és ajánlott hardverkövetelmények

Minimális hardverkövetelmények a **AVG Internet Security 2011** termékhez:

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

Ajánlott hardverkövetelmények a **AVG Internet Security 2011** termékhez:

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM memória
- 1400 MB szabad merevlemez-terület ((telepítési célokra)



3. AVG telepítési lehetőségek

Az AVG telepítése történhet a telepítési lemezen lévő telepítési fájlokkal, illetve a legfrissebb telepítőkészlettel, amelyet az AVG weboldaláról tölthet le (<http://www.avg.hu/>).

Az AVG telepítésének megkezdése előtt érdemes felkeresnie az AVG honlapját (<http://www.avg.hu/>) a legújabb telepítési fájlok letöltéséhez. Ilyen módon biztosíthatja, hogy az AVG Internet Security 2011 legfrissebb verziója kerüljön a számítógépre.

A telepítés során a program kérni fogja a licenc-/eladási számot. Készítse elő ezeket a telepítés megkezdése előtt. Az értékesítési számot az AVG szoftver CD csomagolásán találhatja. Ha az AVG terméket az interneten keresztül vásárolta meg, a licencet/értékesítési számot e-mailben kapja meg.



4. AVG telepítési folyamat

Az **AVG Internet Security 2011** telepítéséhez szüksége van a legújabb telepítőfájltra. Használhatja a csomagban lévő CD-n található telepítőfájlt is, de az lehet, hogy már elavult. Ezért javasoljuk, hogy mindig töltsse le az internetről a legújabb telepítőfájlt. A fájlt letöltheti az AVG webhelyéről (<http://www.avg.hu/>), a **Támogatási központ / Letöltés** részről.

A telepítés párbeszédpanel-ablakok sorozata, rövid ismertetovel az egyes lépésekről. A következőkben bemutatjuk az összes párbeszédpanel-ablakot:

4.1. Üdvözlőképernyő

A telepítési folyamat az **üdvözlőképernyővel** kezdődik. Itt válassza ki a telepítéshez használt nyelvet és az AVG felhasználói felület alapértelmezett nyelvét. Az ablak felső részén található a választható nyelvek legördülő listáját:



Figyelem: Az itt kiválasztott nyelv csak a telepítési folyamatra vonatkozik. A kiválasztott nyelv az AVG felhasználói felület alapértelmezett nyelveként teljesül (az automatikusan települő angol nyelv mellett). Ha más nyelveket is telepítene a felhasználói felülethez, akkor azokat az [Egyéni beállítások](#) részen adja meg.

Ez a panel az AVG liszensz megállapodás 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.

4.2. AVG liszensz aktiválása

Az **Liszensz aktiválása** panelen írja be a liszenszkódot a megfelelő szövegmezőbe.

Az értékesítési számot az **AVG Internet Security 2011** szoftver CD lemezének csomagolásán



találhatja meg. A licenckód az **AVG Internet Security 2011** 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.

Nyomja meg a **Tovább** gombot a telepítés folytatásához.

4.3. Telepítés típusának kiválasztása

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



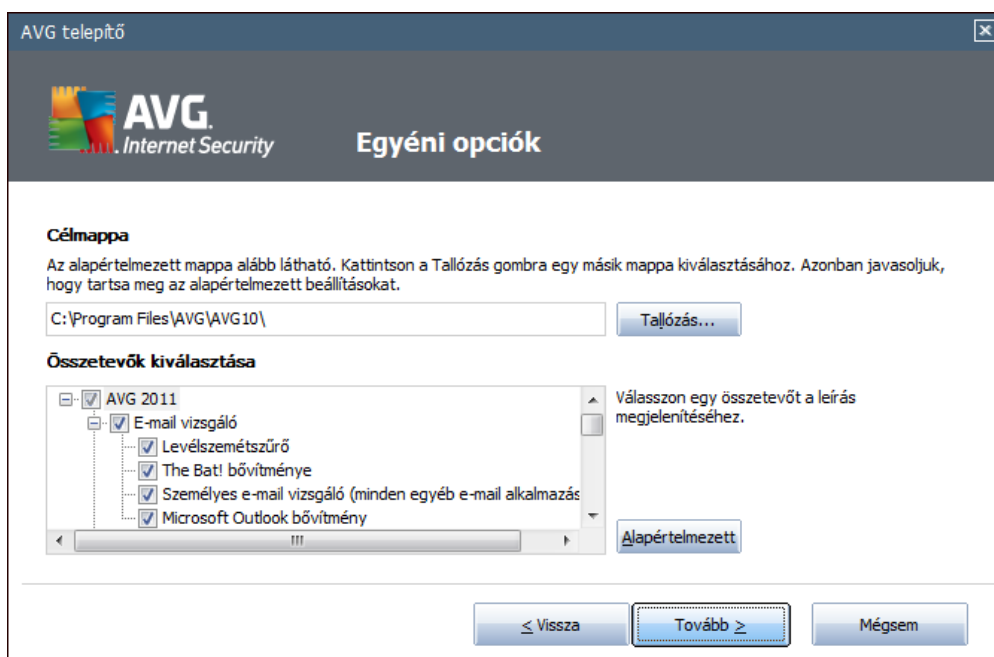
A legtöbb felhasználó számára a szokásos **Gyors telepítést** ajánljuk, mivel az teljesen automatikusan telepíti az AVG programot a gyártó által előre megadott beállításokkal. Ez a konfiguráció maximális biztonságot nyújt optimális rendszererőforrás használattal. Ha a későbbiekben meg szeretné változtatni a konfigurációt, akkor ezt közvetlenül megteheti az AVG alkalmazáson belül. Ha a **Gyors telepítés** opciót választotta, akkor nyomja meg a **Tovább** gombot a következő [Az AVG Biztonság eszköztár telepítése](#) panelre történő ugráshoz.

Az **Egyéni telepítést** csak azon tapasztalt felhasználók válasszák, akik mindenképpen egyéni beállításokkal szeretnék telepíteni az AVG programot, például megadott rendszerkövetelményeknek megfelelően. Ha ezt az opciót választotta, akkor nyomja meg a **Tovább** gombot a [Egyéni beállítások](#) panelre történő ugráshoz.

A panel jobb oldali részén található 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 2011** legfontosabb szolgáltatásaihoz, pl. [vizsgálat](#) és [frissítés](#).

4.4. Egyéni opciók

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



Célmappa

A **Célmappa** részen megadhatja az **AVG Internet Security 2011** telepítési helyét. Alapbeállítás szerint az AVG a C: meghajtón a Program Files mappába lesz telepítve. Ha módosítani szeretné ezt a helyet, akkor használja a **Böngészés** gombot a meghajtó tartalmának megjelenítéséhez, majd válassza ki a kívánt mappát.



Összetevők kiválasztása

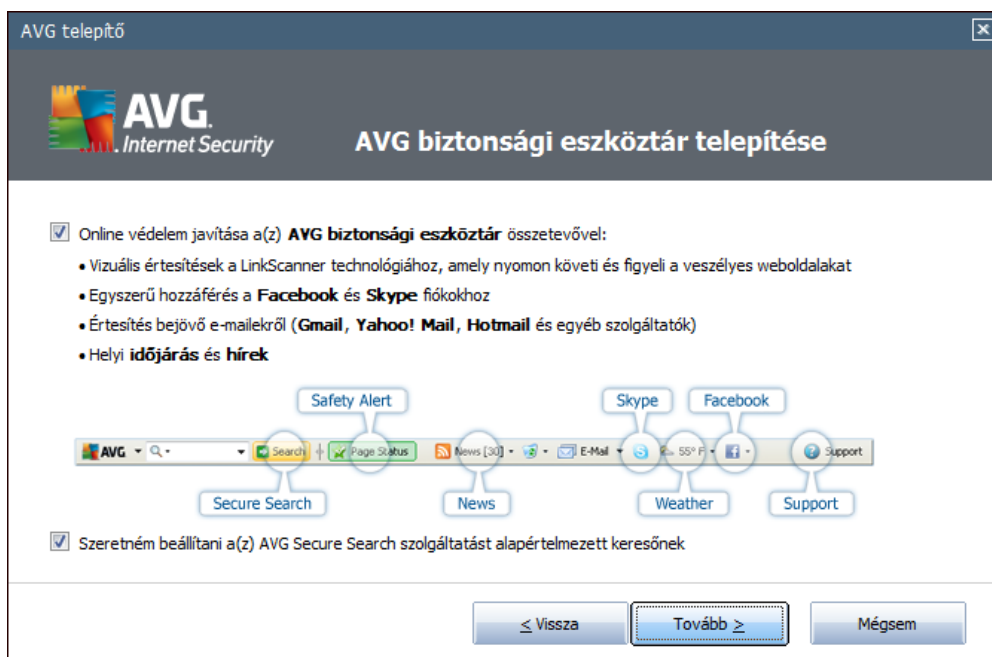
Az **Összetevő kiválasztása** rész az összes telepíthető **AVG Internet Security 2011** összetevőt mutatja. Ha az alapbeállítások nem felelnek meg Önnek, akkor eltávolíthat/hozzáadhat összetevőket.

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.

Nyomja meg a **Tovább** gombot a folytatáshoz.

4.5. Az AVG Biztonság eszköztár telepítése



Az **AVG Biztonság eszköztár telepítése** panelen eldöntheti, hogy akarja-e telepíteni az [AVG Biztonság eszköztár](#). 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* szükséges) és átfogó online védelmet nyújt az internet böngészése során.

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



4.6. Telepítési folyamat

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



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

4.7. A telepítés sikerült





A **Sikeres telepítés** panel megerősíti, hogy az **AVG Internet Security 2011** terméket a rendszer sikeresen telepítette és konfigurálta.

Ezen a részen adja meg a kapcsolati adatait, hogy a termékekkel kapcsolatos információkat és híreket tudjunk Önnek küldeni. Az alábbi regisztrációs urlapon a következő két lehetőséget találja:

- **Igen, értesítéseket kérek vírusbiztonsági hírekről és AVG 2011 különleges ajánlatokról e-mailben** - jelölje be a jelölőnégyzetet, ha információkat szeretne kapni arról, hogy milyen újdonságok történnek az internetbiztonság területén, illetve ha tájékoztatást kér különleges AVG termékajánlatokról, termékfejlesztésekről és frissítésekről stb.
- **Szeretnék résztvenni az AVG 2011 webbiztonsági és termékfejlesztési programjában...** - jelölje be ezt a jelölőnégyzetet, ha részt kíván venni azon termékfejlesztési programban, amely névtelen információkat gyűjt az észlelt fenyegetésekről az online biztonság növelése érdekében (további részletekért lásd az [AVG Haladó beállítás / Termékfejlesztési program](#)) fejezetet).

A telepítési folyamat befejezéséhez indítsa újra a számítógépet: válassza ki az **Újraindítás most** gombot, vagy ha elhalasztaná a műveletet, akkor az **Újraindítás később** gombot.

Megjegyzés: Ha Ön AVG üzleti liszenszet használ és ha korábban telepítette a Távfelügyelet szolgáltatást (lásd [Egyéni opciók](#)), akkor a Sikeres telepítés 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 állítsa be később a **Haladó beállítások / Távfelügyelet** panelen. Az AVG Távfelügyelettel kapcsolatos információkért forduljon az AVG Business Edition felhasználói kézikönyvéhez. Ezt az AVG honlapjáról töltheti le (<http://www.avg.hu/>).



5. A telepítés utáni teendők

5.1. Termék regisztrálása

Miután befejezte az **AVG Internet Security 2011** telepítését, regisztrálja a terméket online az AVG weboldalán (<http://www.avg.hu/>), a **Regisztráció** oldalon (kövesse az oldalon található utasításokat). A regisztráció után teljes hozzáférést kap az Ön saját AVG felhasználói fiókjához, az AVG frissítés hírlevélhez és számos egyéb kizárólag regisztrált felhasználóknak szóló szolgáltatásokhoz.

5.2. Hozzáférés a felhasználói felülethez

Az [AVG felhasználói felület](#) 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)
- használja a **Start/Programok/AVG 2011/AVG felhasználói felület parancsot**
- Az [AVG Biztonság eszköztárról](#) az **AVG indítása**

5.3. A teljes számítógép vizsgálata

Fennáll a veszély, hogy az **AVG Internet Security 2011** telepítése előtt vírus került a számítógépre. Ezért futtassa le a [Teljes számítógép vizsgálata](#) funkciót, hogy meggyőződhessen róla, hogy számítógépe vírusmentes.

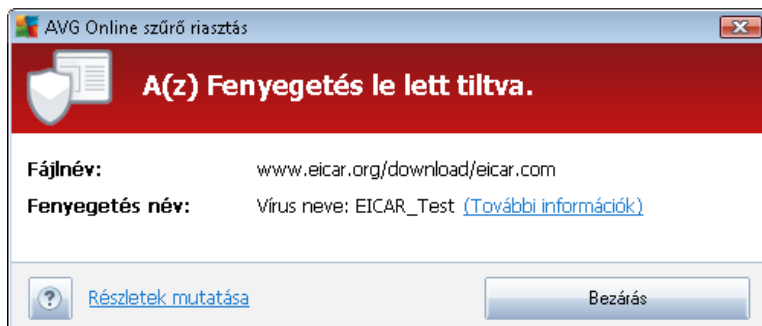
A [Teljes számítógép vizsgálata](#) funkció futtatásával kapcsolatos információkért forduljon az [AVG vizsgálat](#) fejezethez.

5.4. Eicar teszt

Az **AVG Internet Security 2011** 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 víruskereso 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](http://www.eicar.com) fájlt, és mentse a helyi lemezre. A tesztfájl letöltésének megerősítése után az [Online szuro](#) 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](#) észleli a 'vírust' a kicsomagolás során. **Ha az AVG nem azonosítja vírusként az EICAR tesztfájlt, akkor ismételtelen ellenőriznie kell a program beállításait!**

5.5. AVG alapértelmezett konfiguráció

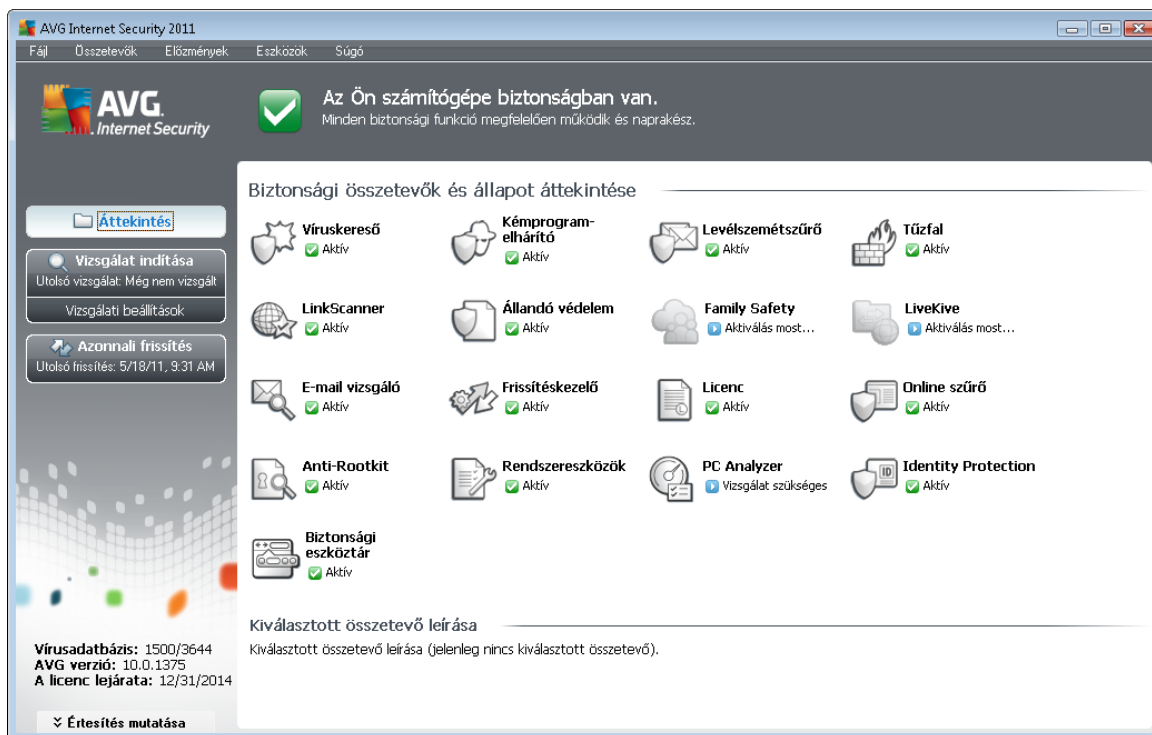
Az alapbeállításokat (vagyis a program telepítés utáni viselkedését) a **AVG Internet Security 2011** szoftvergyártó előre meghatározta az összes funkció és összetevő optimális teljesítményének érdekében.

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.

6. AVG felhasználói felület

Az **AVG Internet Security 2011** megnyílik a foablakkal együtt:



A foablak több részből áll:

- **A Rendszermenü** (az ablakban a felső sor) a normál kiindulópont, ahonnan az összes AVG összetevőt, szolgáltatást és funkciót elérheti - [részletek >>](#)
- **A Biztonsági állapot információk** (az ablak felső részén) részletekkel szolgálnak az AVG program aktuális állapotával kapcsolatban - [részletek >>](#)
- **A Gyorsgombok** (az ablak bal oldalán) lehetővé teszik, hogy Ön azonnal hozzáférjen a legfontosabb és leggyakrabban használt AVG feladatokhoz - [részletek >>](#)
- **Az Összetevők áttekintése** (az ablak középső részén) megmutatja az összes telepített AVG összetevőt - [részletek >>](#)
- **A Statisztika** (az ablak bal alsó részén) statisztikai adatokat közöl a program működésével kapcsolatban - [részletek >>](#)
- **A Tálcaikon** (a képernyő jobb alsó részén, az értesítő területen) az AVG aktuális állapotát mutatja - [részletek >>](#)
- **Az AVG minialkalmazás** (Windows oldalsáv, támogatott rendszerek: Windows Vista/7) gyors hozzáférést biztosít az AVG vizsgálathoz és a frissítésekhez - [részletek >>](#)



6.1. System (Rendszer) menü

The **Rendszer menü** a Windows alkalmazásokban található normál navigációs menü. Vízszintesen helyezkedik el az **AVG Internet Security 2011** foablak legfelso részén. Használja a Rendszer menüt adott AVG összetevők, funkciók és szolgáltatások eléréséhez.

A Rendszer menü öt fő részre van osztva:

6.1.1. Fájl

- **Kilépés** - bezárja az **AVG Internet Security 2011** felhasználói felületet . Az AVG továbbra is fut a háttérben, és az Ön számítógépe továbbra is tökéletesen védve van!

6.1.2. 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 Víruskereso** biztosítja, hogy a számítógépe védve legyen a vírustámadások ellen - [részletek >>](#)
- A **Kémprogramelhárító** biztosítja, hogy az Ön számítógépe védve van a kém- és reklámprogramoktól - [részletek >>](#)
- **A Levélszemétszuro** minden bejövő emailt ellenőriz, és a kéréslen üzeneteket LEVÉLSZEMÉTKÉNT azonosítja - [részletek >>](#)
- **A Tuzfal** szabályozza, hogy a számítógép hogyan cseréljen adatokat a helyi hálózaton vagy az interneten található más számítógépekkel - [részletek >>](#)
- **A LinkScanner** ellenőrzi az internetböngészőben megjelenő keresési eredményeket - [részletek >>](#)
- **Az E-mail vizsgáló** ellenőrzi minden bejövő és kimenő emailt vírusok szempontjából - [részletek >>](#)
- **A Family Safety** összetevő figyeli a gyermekei online tevékenységét, és védi őket a nem megfelelő tartalmaktól – [részletek >>](#)
- **A LiveKive** összetevő automatikus online adatmentést biztosít – [részletek >>](#)
- **Az Állandó védelem** a háttérben fut és ellenőrzi a másolandó, megnyitandó vagy mentendo fájlokat - [részletek >>](#)
- **A Frissítéskezelő** szabályozza az összes AVG frissítést - [részletek >>](#)
- **A Licenc** megjeleníti a licenckódot, a típust és a lejárat dátumát - [részletek >>](#)



- A **Online szuro** ellenorzi a böngésző által letöltött összes adatot - [részletek >>](#)
- A **Anti-Rootkit** felismeri azon programokat és technológiákat, melyek rosszindulatú kódokat lepleznek - [részletek >>](#)
- A **Rendszerezszközök** részletes áttekintést nyújt az AVG környezettel és az operációs rendszerrel kapcsolatban - [részletek >>](#)
- A **PC Analyzer** információkat nyújt a számítógép állapotáról - [részletek >>](#)
- **Identity Protection** – kártevők elleni összetevő, amely megakadályozza, hogy illetéktelenek ellopják az Ön személyes digitális adatait – [részletek >>](#)
- A **Biztonság eszköztár** összetevővel közvetlenül a webböngészőből érhet el bizonyos AVG szolgáltatásokat – [részletek >>](#)
- A **Távoli adminisztráció** összetevő kizárólag az AVG üzleti verziókban érhető el, ha [engedélyezi azt](#) a telepítés során

6.1.3. Elozmények

- [A vizsgálat eredménye](#) - megjeleníti az AVG vizsgálati felületet, illetve a [Vizsgálat eredményének áttekintése](#) panelt
- [Állandó védelem észlelés](#) - megnyit egy panelt a fenyegetések áttekintésével, amelyeket az [Állandó védelem](#)
- [E-mail vizsgáló észlelés](#) - megnyit egy panelt azon mellékletek áttekintésével, amelyeket az [E-mail vizsgáló](#) összetevő veszélyesnek talált
- [Online szuro találatok](#) - megnyit egy panelt a fenyegetések áttekintésével, melyeket az [Online szuro](#)
- [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 2011** eseménnyel
- [Tuzfal](#) - megnyitja a Tuzfalbeállítások ablakot a [Naplók](#) fülön a Tuzfal muveletek részletes áttekintésével

6.1.4. Eszközök

- [Számítógép vizsgálata](#) – átvált az [AVG vizsgálati felületre](#), és elindítja a számítógép teljes vizsgálatát.
- [Kijelölt mappa vizsgálata](#) – átvált az [AVG vizsgálati felületre](#), és lehetővé teszi a vizsgálandó mappák és fájlok kiválasztását.



- **Fájl vizsgálata** – egyetlen fájl manuális vizsgálatát teszi lehetővé.
- **Frissítés** – automatikusan elindítja az **AVG Internet Security 2011** frissítési folyamatot.
- **Frissítés könyvtárból** - elindítja a frissítési folyamatot az adott 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 az **AVG haladó beállítások** panelt, ahol szerkesztheti az **AVG Internet Security 2011** konfigurációt. Általában javasolt, hogy megtartsa a szoftvergyártó által megadott alapbeállításokat az alkalmazásban.
- **Tuzfalbeállítások** – megnyitja a **Tuzfal** összetevő haladó beállítások paneljét.

6.1.5. Súly

- **Tartalomjegyzék** - megnyitja az AVG súgófájlokat
- **Online súgó** - megnyitja az AVG weboldalát (<http://www.avg.hu/>) az ügyféltámogatási központ oldalon
- **Az Ön AVG honlapja** - megnyitja az AVG honlapját (<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 adatokkal, 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 weboldalának regisztrációs oldalához (<http://www.avg.hu/>). Töltse ki a regisztrációs adatokat! Csak regisztrált ügyfelek jogosultak ingyenes AVG muszaki terméktámogatásra.

Megjegyzés: Ha az **AVG Internet Security 2011** próbaverzióját használja, akkor az utolsó két lépés a **Vásárlás most** és az **Aktiválás**, melyek segítségével azonnal megvásárolhatja a program teljes verzióját. Az értékesítési számmal telepített **AVG Internet Security 2011** esetében ezen lépések a következők: **Regisztrálás** és **Aktiválás**. További információkért forduljon a dokumentáció **Licenc** részéhez.

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

6.2. Biztonsági állapot információk

Az **Biztonsági állapot információk** rész az AVG foablakának felső részén helyezkedik el. Itt mindig információkat találhat az **AVG Internet Security 2011** aktuális biztonsági állapotáról. Tekintse át az ebben a részben esetlegesen megjelenő ikonok listáját és jelentésüket:



- A zöld ikon azt jelenti, hogy az AVG teljesen működőképes. A számítógép védelme teljes körű, a rendszer naprakész és a telepített összetevők megfelelően működnek.



- A narancsszínű ikon figyelmeztet, hogy egy vagy több összetevő beállítása nem megfelelő, így ellenőrizni kell ezek beállításait. Nincs súlyos hiba az AVG működésében, elképzelhető, hogy csak valamely okból kikapcsolta az egyik összetevőt. Önt továbbra is védi az AVG. Azonban fordítson figyelmet a problémás összetevő beállításaira! A név a **Biztonsági állapot információk** részen fog megjelenni.

Ez az ikon akkor is megjelenik, ha valamilyen okból úgy döntött, hogy [mellozi az összetevő hibaállapotát](#) (az "Összetevő állapotának mellozése" opció elérhető a helyi menüből, ha jobb kattintással megnyitja azt az adott összetevő áttekintésénél az AVG foablakában). Lehet, hogy bizonyos helyzetekben használnia kell, de javasoljuk, hogy amint lehetséges, minél hamarabb kapcsolja ki az "**Összetevő állapotának mellozése**" opciót.



- A piros ikon azt jelenti, hogy az AVG működésében súlyos hiba van! Egy vagy több összetevő nem megfelelően működik, és az AVG nem tudja megvédeni számítógépét. Fordítson figyelmet az észlelt probléma azonnali kijavítására. Ha nem tudja egyedül kijavítani a hibát, akkor vegye fel a kapcsolatot az [AVG műszaki támogatás](#) csapattal.

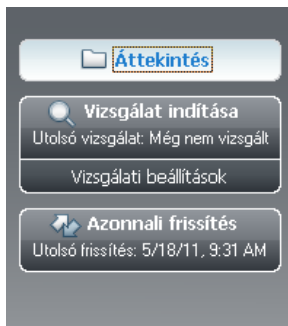
Ha az AVG nincs optimális teljesítményre állítva, akkor egy új javítás (vagy összes javítása, ha több problémáról van szó) gomb jelenik meg a biztonsági állapot mellett. Kattintson erre a gombra az automatikus végrehajtáshoz és konfigurációhoz. Ez egy egyszerű mód az AVG optimális teljesítményre állításához és a maximális biztonsági szint eléréséhez.

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 állapotinformáció bármikor látható a [rendszerterületen megjelenő ikon formájában](#).

6.3. Gyors linkek

A **Gyorsgombok** (az [AVG felhasználói felület](#) bal oldalán) lehetővé teszik, hogy Ön azonnal hozzáférjen a legfontosabb és leggyakrabban használt AVG szolgáltatásokhoz:



- **Áttekintés** - használja ezt a gombot bármely jelenleg nyitott AVG felület átváltásához az alapértelmezett összes telepített összetevő felületre - lásd az [Összetevők áttekintése fejezetet >>](#)
- **Vizsgálat** - alapállapotban ezzel a gombbal információkat kaphat az utoljára futtatott vizsgálatról (*vizsgálat típusa, dátuma*). Használhatja a **Vizsgálat** parancsot ugyanezen vizsgálat ismételt futtatásához, vagy kattintson a **Vizsgálati beállítások** linkre az AVG vizsgálati felület megnyitásához, ahol vizsgálatokat futtathat, ütemezhet vagy szerkesztheti azok paramétereit - lásd az [AVG vizsgálat fejezetet >>](#)
- **Frissítés** - ez a link megjeleníti a legutóbbi frissítési folyamat dátumát. Kattintson erre a gombra a frissítési felület megnyitásához, majd indítson el egy azonnali AVG frissítést - lásd az [AVG frissítések fejezetet >>](#)

Ezen gyorsgombok bármikor elérhetők a felhasználói felületről. Ha használ egy gyorsgombot egy adott folyamat futtatásához, a felhasználói felület az új panelre vált, de a gyorsgombok továbbra is elérhetőek maradnak. A futó folyamat is meg lesz jelenítve grafikus formában

6.4. Összetevők áttekintése

Az **Összetevők áttekintése** rész az [AVG felhasználói felület](#) központi részén helyezkedik el. A felület két részből áll:

- Az összes telepített összetevő áttekintése ikonokkal és információkkal, hogy az összetevő aktív-e vagy sem
- Egy kiválasztott összetevő leírása

Az **AVG Internet Security 2011** termékben az **Összetevők áttekintése** rész a következő összetevőkről nyújt információkat:

- **A Víruskereso** biztosítja, hogy a számítógépe védve legyen a vírusáadások ellen - [részletek >>](#)



- A **Kémprogramelhárító** biztosítja, hogy az Ön számítógépe védve van a kém- és reklámprogramoktól - [részletek >>](#)
- A **Levélszemétszuro** minden bejövő emailt ellenőriz, és a kóros üzeneteket LEVÉLSZEMÉTKÉNT azonosítja - [részletek >>](#)
- A **Tuzfal** szabályozza, hogy a számítógép hogyan cseréljen adatokat a helyi hálózaton vagy az interneten található más számítógépekkel- [részletek >>](#)
- A **LinkScanner** ellenőrizi az internetböngészőben megjelenő keresési eredményeket - [részletek >>](#)
- Az **E-mail vizsgáló** ellenőriz minden bejövő és kimenő emailt vírusok szempontjából - [részletek >>](#)
- Az **Állandó védelem**a háttérben fut és ellenőrizi a másolandó, megnyitandó vagy mentendo fájlokat - [részletek >>](#)
- A **Family Safety** összetevő figyeli a gyermekei online tevékenységét, és védi őket a nem megfelelő tartalmaktól – [részletek >>](#)
- A **LiveKive** összetevő automatikus online adatmentést biztosít – [részletek >>](#)
- A **Frissítéskezelő** szabályozza az összes AVG frissítést - [részletek >>](#)
- A **Licenc** megjeleníti a licenckódot, a típust és a lejárat dátumát - [részletek >>](#)
- A **Online szuro** ellenőrizi a böngésző által letöltött összes adatot - [részletek >>](#)
- Az **Anti-Rootkit** felismeri azon programokat és technológiákat, melyek rosszindulatú kódokat lepleznek - [részletek >>](#)
- A **Rendszereszközök** részletes áttekintést nyújt az AVG környezettel és az operációs rendszerrel kapcsolatban - [részletek >>](#)
- A **PC Analyzer** információkat nyújt a számítógép állapotáról - [részletek >>](#)
- **Identity Protection** – kártevők elleni összetevő, amely megakadályozza, hogy illetéktelenek ellopiák az Ön személyes digitális adatait – [részletek >>](#)
- A **Biztonság eszköztárral** közvetlenül a webböngészőből érhető el bizonyos AVG szolgáltatásokat – [részletek >>](#)
- A **Távoli adminisztráció** összetevő kizárólag az AVG üzleti verziókban érhető el, ha [engedélyezi azt](#) a telepítés során

Kattintson egyszer bármelyik összetevőre az áttekintésben történő kijelöléshez. Ekkor az összetevő alapvető funkciójának leírása megjelenik a felhasználói felület alsó részén. Kattintson kétszer az ikonra az összetevő saját felületének megnyitásához alapvető statisztikai adatokkal.



Kattintson jobb gombbal az összetevo ikonjára a helyi menü megjelenítéséhez: az összetevo grafikus felületének megnyitásán kívül választhatja az **Összetevo állapotának mellozése** opciót is. Válassza ezt az opciót az [összetevo állapotának](#) megerősítéséhez, hogy az AVG mellozze a hibaállapotot, és egy ikon jelenjen meg az [értesítési területen](#).

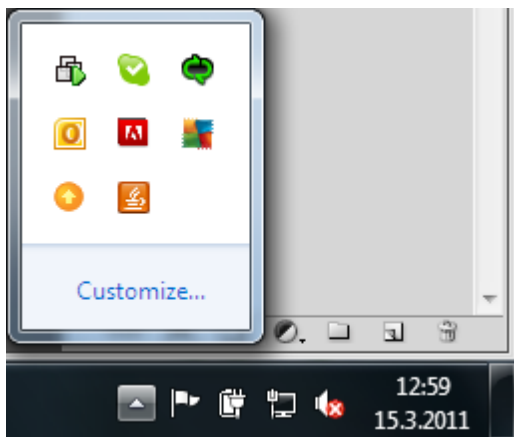
6.5. Statisztikák

A **Statisztikák** rész az [AVG felhasználói felület](#) bal alsó részén helyezkedik el. Számos információt nyújt a program működésével kapcsolatban:

- **Vírus adatbázis** - tájékoztat a jelenleg telepített vírusadatbázis verziójáról
- **AVG verzió** - megmutatja a telepített AVG program verzióját (a szám 10.0.xxxx formátumban van, ahol a 10.0 a termékvonallal verziója, míg az xxxx az alverzió számát mutatja)
- **Licenc lejárata** - megmutatja az AVG licenc lejárata dátumát

6.6. Tálcáikon

A **Tálcáikon** (a Windows tálcán) az **AVG Internet Security 2011** aktuális állapotát mutatja. Folyamatosan látható a tálcán, függetlenül attól, hogy az AVG foablaka nyitva vagy zárva van:



Ha teljes színű , akkor a **Tálcáikon** azt jelzi, hogy az AVG összetevők aktívak és tökéletesen működőképesek. Az AVG rendszerikon lehet teljesen színes, ha az AVG hibaállapotban van, de Ön ezzel tisztában van, és szándékosan [mellozte az összetevo hibaállapotát](#). Ikon felkiáltójellel  problémára utal (inaktív összetevo, hibaállapot, stb.). Kattintson kétszer a **Tálcáikonra** a foablak megnyitásához és az összetevo beállításainak módosításához.

A tálcáikon további információkat nyújt az aktuális AVG műveletekről és a program esetleges állapotváltozásairól (ütemezett vizsgálat vagy frissítés automatikus indítása, Tuzfalprofil váltása, összetevo állapotváltozása, hibaállapot, ...) felbukkanó ablak segítségével az AVG tálcáikonján áll:





A **Tálcaikon** gyorsgombként is szolgál az AVG foablakának bármikor történő azonnali eléréséhez - kattintson kétszer az ikonra. Kattintson jobb gombbal a **Tálcaikonra** a helyi menü megnyitásához a következő lehetőségekkel:

- **AVG felhasználói felület megnyitása** - kattintson rá az [AVG felhasználói felület megnyitásához](#)
- **Vizsgálatok** - kattintson ide a(z)
- **Tuzfal** - kattintson ide a [Tuzfal](#) beállítások helyi menüjének megnyitásához, ahol módosítja a főbb paramétereket: [Tuzfal állapota](#) (*Tuzfal engedélyezve/Tuzfal kikapcsolva/Vészhelyzet mód*), [Játék módra váltás](#) és [Tuzfal profilok](#)
- **PC Analyzer** futtatása - kattintson ide a [PC Analyzer](#) összetevő indításához
- **Aktív vizsgálatok** - ez az elem csak akkor jelenik meg, ha egy vizsgálat jelenleg 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 súgó fájlt a kezdolapon

6.7. 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 2011** szolgáltatásokhoz, pl. [vizsgálat](#) és [frissítés](#):



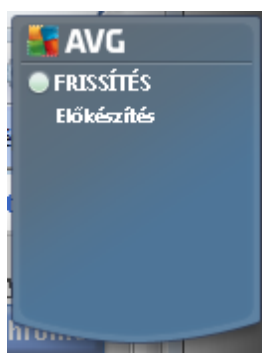
Az **AVG minialkalmazás** a következő gyors hozzáférési lehetőségeket biztosítja:

- **Vizsgálat most** - kattintson a **Vizsgálat most** linkre a [teljes számítógép](#) közvetlen vizsgálatához. 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 [Vizsgálati eredmények áttekintése](#) panelt,

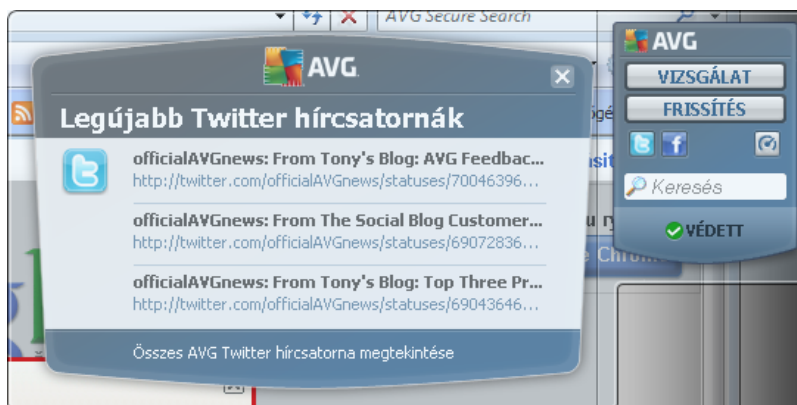
amely a közvetlenül a minialkalmazásból nyitható meg a **Részletek megjelenítése** opcióval (az eredmények a **Vizsgálati minialkalmazásnál** láthatók).



- **Frissítés most** - kattintson a **Frissítés most** linkre az AVG minialkalmazásból történő közvetlen frissítéséhez:



- **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 az opció csak hálózati telepítés esetén érhető el (például ha Ön az AVG valamelyik üzleti kiadását telepítette). A rendszer megnyitja a böngészőt az **AVG SMB Community** weboldalán a LinkedIn közösségi oldalon.
- **PC Analyzer**  – megnyitja a [PC Analyzer](#) összetevő felhasználói felületét
- **Keresődoboz** – írjon be egy kulcsszót, és kapjon találatokat azonnal az alapértelmezett böngésző egy újonnan megnyíló ablakában



7. AVG összetevők

7.1. Víruskereso

7.1.1. Víruskeresési alapelvek

Az antivírus szoftver keresomotorja minden fájlt illetve műveletet megvizsgál (fájlok megnyitása/ bezárása stb.) az ismert vírusok szempontjából. A felismert vírusok el lesznek zárva minden fájlmuvelettől, ezután a program megjavítja vagy karanténba helyezi őket. A legtöbb antivírus szoftver heurisztikus keresést is alkalmaz, ahol a program vírusra utaló tulajdonságokat, ún. víruskarakteristikákat keres az egyes fájlokban. Ez azt jelenti, hogy az antivírus program felismerhet egy teljesen új, idáig ismeretlen vírusokat is, ha az tartalmaz bizonyos - már létező vírusokra jellemző - tulajdonságokat.

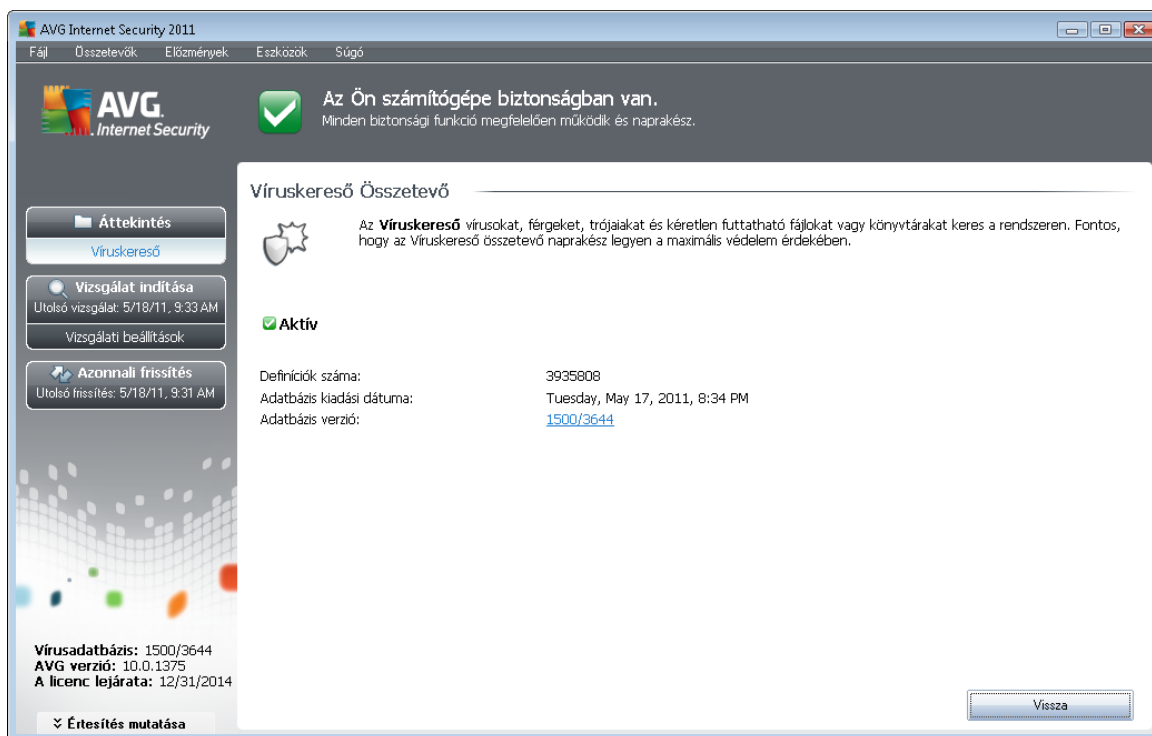
Az antivírus védelem lényege, hogy semmilyen ismert vírus nem futhat a számítógépen!

Mivel egyetlen technológia nem feltétlenül elegendő a vírus azonosításához, az **antivírus** program többféle technológiát ötvöz a számítógép védelmének érdekében:

- Keresés – egy adott vírusra jellemző minta keresése.
- Heurisztikus elemzés – a vizsgált objektum utasításainak dinamikus emulálása biztonságos módon virtuális számítógépes környezetben
- Általános azonosítás – az adott vírusra/víruscsoportra jellemző utasítások azonosítása.

Az AVG vírusirtó képes a rendszer nemkívánatos végrehajtható alkalmazásainak és DLL könyvtárainak elemzésére és azonosítására. Az ilyen fenyegetéseket nemkívánatos alkalmazásoknak nevezzük (többféle kémprogram, reklámprogram, stb.). Az AVG víruskereso megvizsgálja a rendszerleíró adatbázist is, ahol gyanús bejegyzéseket, ideiglenes internetes fájlokat és nyomkövető cookie-kat keres, és lehetőséget nyújt a kártékony elemek fertőzőként történő kezelésére.

7.1.2. Víruskereso felület



A **Víruskereso** felhasználói felülete alapvető információkat nyújt az összetevő működéséről illetve az aktuális állapotról (a **Víruskereso** összetevő **aktív**.), rövid áttekintés a **Víruskereso** statisztikákról:

- **Fertőzésminták száma** - megmutatja, hogy hány vírusminta található a legfrissebb vírusadatbázisban
- **Adatbázis kiadási dátuma** - megmutatja, hogy a vírusadatbázis mikor lett legutóbb frissítve
- **Adatbázis verziója** - a jelenleg telepített vírusadatbázis verziószámát mutatja. Ez a szám minden egyes adatbázis-frissítéssel tovább nő

Egyetlen működő gomb van az összetevő felhasználói felületén (**Vissza**) - nyomja meg ezt a gombot az alapértelmezett [AVG felhasználói felületre](#) (történo visszatéréshez összetevők áttekintése).

7.2. Kémprogram-elhárító

7.2.1. Kémprogram-elhárító alapelvek

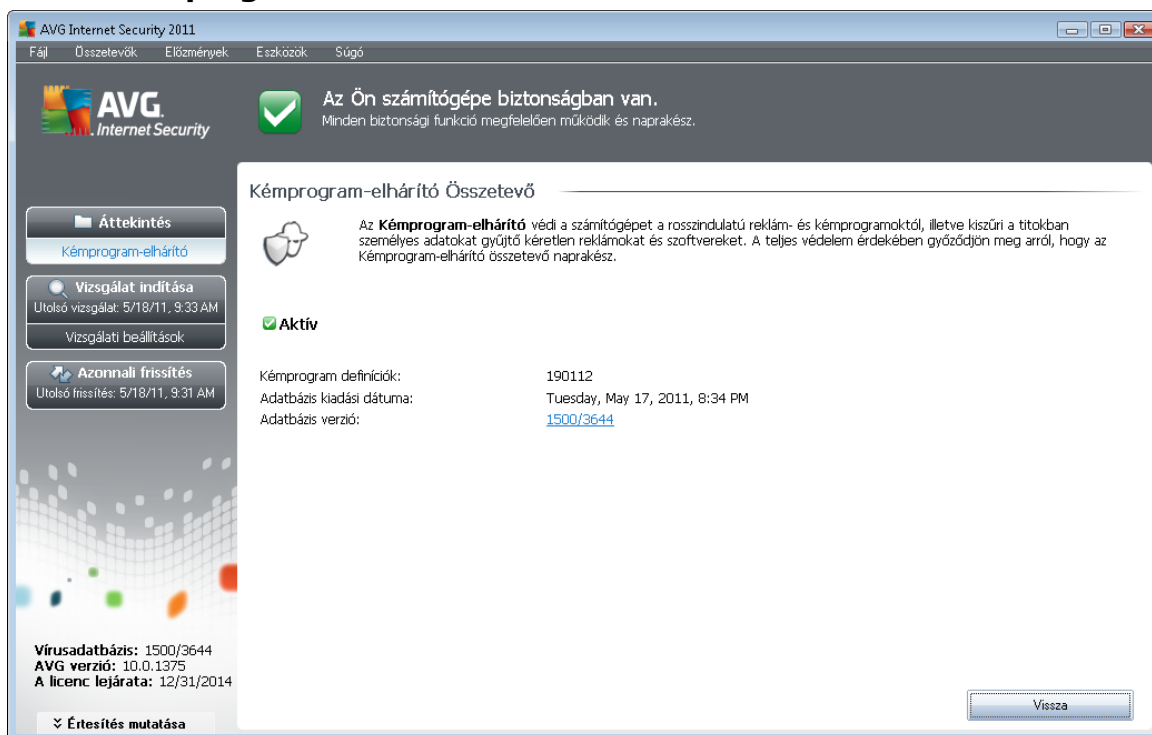
A kémprogramok a rosszindulatú programok olyan típusaként azonosíthatók, melyek a felhasználó tudta vagy beleegyezése nélkül adatokat gyűjtenek össze a felhasználó számítógépéről. Bizonyos kémprogramok telepítése szándékosan is történhet. Ezek gyakran hirdetéseket, felugró ablakokat és más kellemetlen 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-kereso**, amely az alkalmazásokat futásuk közben a háttérben ellenőrzi.

Fennáll a veszélye annak, hogy még a vírusirtó telepítését megelőzően, vagy az **AVG Internet Security 2011** vírusirtó adatbázis- és programfrissítéseinek megelőzése következtében [rosszindulatú program került a számítógépre](#). Ilyen esetekben jól használható az AVG vírusirtó keresési funkciója, amely a számítógép kém- és rosszindulatú programjainak azonosítására szolgál. A vizsgálat során a program a még „szunnyadó és inaktív”, azaz a letöltött, de még nem működő rosszindulatú programokat is azonosítja.

7.2.2. Kémprogram-elhárító felület



A **Kémprogram-elhárító** felhasználói felülete rövid áttekintést nyújt az összetevő működéséről, az aktuális állapotáról és a **Kémprogram-elhárító** statisztikáiról:

- **Kémprogram minták** - megmutatja, hogy mennyi kémprogram minta található a legújabb verziójú kémprogram adatbázisban
- **Adatbázis kiadási dátuma** - megmutatja, hogy a kémprogram adatbázis mikor lett frissítve
- **Adatbázis verzió** - a legújabb kémprogram adatbázis verziószámát mutatja. Ez a szám minden egyes adatbázis frissítéssel tovább nő.

Egyetlen működő gomb van az összetevő felhasználói felületén (**Vissza**) - nyomja meg ezt a gombot az alapértelmezett [AVG felhasználói felületre](#) (történo visszatéréshez összetevők áttekintése).

7.3. Levélszemétszuro

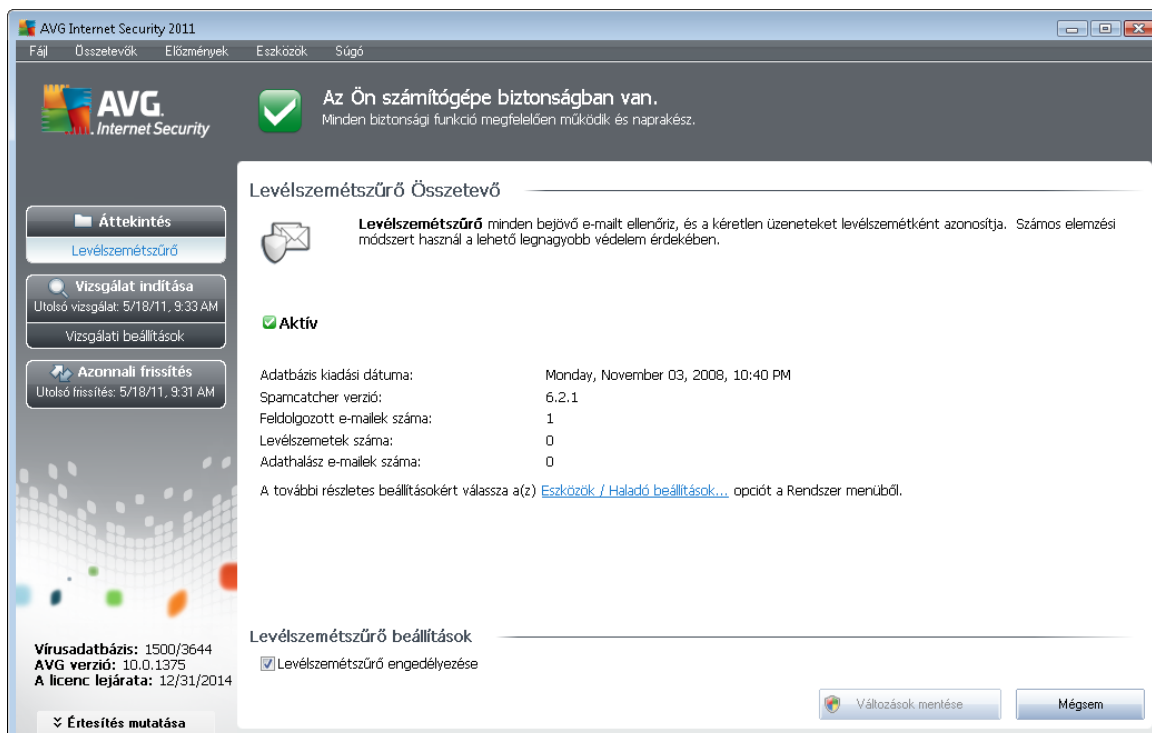
A levélszemét általában azokat a kérietlen leveleket jelenti, melyek valamilyen terméket vagy szolgáltatást reklámoznak. Ezeket nagy tömegben, egyszerre sok e-mail címre küldik el, megtöltve ezzel a postaládákat. A levélszemét nem vonatkozik a jogszerűen küldött kereskedelmi e-mailekre, amelyeket a felhasználó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

7.3.1. Levélszemétszuro alapelvek

Az **AVG Levélszemétszuro** minden bejövő e-mailt ellenőriz, és a kérietlen üzeneteket levélszemétként azonosítja. Az **AVG Levélszemétszuro** módosíthatja az e-mail tárgyát (amely levélszemétként lett azonosítva) úgy, hogy egy különleges szöveges karakterláncot fűz hozzá. Ezután könnyen szűrheti e-mailjeit a levelezőprogramban.

Az **AVG Levélszemétszuro** összetevő többféle elemzési módszerrel dolgozza fel az egyes e-maileket, így maximális védelmet nyújt a kérietlen üzenetek ellen. Az **AVG Levélszemétszuro** rendszeresen frissített adatbázist használ a levélszemetek észleléséhez. Használhat [RBL-kiszolgálót](#) (ismert levélszemétküldők e-mail címeinek nyilvános adatbázisa), és kézzel is hozzáadhatja az e-mail címeket az [Engedélyezett listájához](#) (soha nem levélszemét) és a [Feketelistához](#) (mindig levélszemét).

7.3.2. Levélszemétszuro felület



A **Levélszemétszuro** ablakban rövid leírást találhat az összetevő működéséről, aktuális állapotáról és a következő statisztikákról:

- **Adatbázis kiadás** - megmutatja, hogy a levélszemét adatbázis mikor lett frissítve és kiadva



- **Spamcatcher verzió** - megmutatja a levélszemétszuro motor legutóbbi verziószámát
- **Feldolgozott e-mailek száma** - megjeleníti, hogy a rendszer hány e-mail üzenetet ellenőrzött a levélszemétszuro motor utolsó indítása óta
- **Levélszemetek száma** - megjeleníti, hogy a rendszer hány üzenetet jelölt meg levélszemétként az összes vizsgált e-mailbol
- **Adathalász e-mailek száma** - megjeleníti, hogy a rendszer hány üzenetet jelölt meg adathalász kísérletként az összes vizsgált e-mailbol

A **Levélszemétszuro** párbeszédpanel tartalmazza az [Eszközők/Haladó beállítások](#) linket. Használja ezt a hivatkozást az **AVG Internet Security 2011** összetevők haladó beállításainak eléréséhez.

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

Egyetlen működő gomb van az összetevő felhasználói felületén (**Vissza**) - nyomja meg ezt a gombot az alapértelmezett [AVG felhasználói felületre](#) (történo visszatéréshez összetevők áttekintése).

7.4. Tuzfal

A tuzfal olyan rendszer, amely a hálózati adatforgalom blokkolásával, illetve engedélyezésével érvényt szerez a beállított hozzáférési szabályoknak. A tuzfalban általában szabályok határozhatók meg, amelyek védik a belső hálózatot a kívülről (jellemzően az internetről) érkező támadásokkal szemben, és a tuzfal minden egyes hálózati porton figyeli a kommunikációt. Miután a tuzfal összevetette a kommunikációt a megadott szabályokkal, vagy engedélyezi, vagy blokkolja azt. Ha a tuzfal behatolási kísérletet észlel, akkor „blokkolja” a kísérletet, és nem engedi meg a behatolónak, hogy hozzáférjen a számítógéphez.

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

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

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



7.4.1. Tuzfal alapelvek

Az AVG-ben a **Tuzfal** összetevő a teljes adatforgalmat szabályozza a számítógép minden hálózati portján. A **Tuzfal** a megadott szabályok alapján felméri azokat az alkalmazásokat, amelyek a számítógépen futnak (és amelyek kapcsolódni szeretnének az internethez vagy a helyi hálózathoz), továbbá azokat az alkalmazásokat, amelyek kívülről próbálnak kapcsolódni a számítógéphez. A **Tuzfal** ezután engedélyezi vagy megtiltja az egyes alkalmazásoknak a hálózati portokon való kommunikációt. Alapállapotban, ha az alkalmazás ismeretlen (vagyis meghatározott **Tuzfal** szabállyal nem rendelkezik), akkor a **Tuzfal** megkérdezi, hogy engedélyezze-e vagy tiltsa a kommunikációs próbálkozást.

Megjegyzés: az AVG Tuzfal használata nem javasolt szerver platformokon!

Mi a feladata az AVG tuzfalnak:

- 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

7.4.2. Tuzfal profilok

A **Tuzfal** 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 **Tuzfal profil** a **Tuzfal** összetevő egy bizonyos konfigurációja, ahol számos előre meghatározott beállítást használhat.

Elérhető profilok

- **Mindent engedélyezze** - olyan **Tuzfal** 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 mintha a **Tuzfal** védelem ki lenne kapcsolva (*minden alkalmazás engedélyezett, de az adatcsomagok továbbra is ellenőrizve lesznek - a szűrés teljes kikapcsolásához tiltsa le a Tuzfalat*). Ezt a rendszerprofilot nem lehet másolni, törölni vagy a beállításait módosítani.
- **Mind tiltása** - olyan **Tuzfal** rendszerprofil, melyet a gyártó előre beállított és mindig elérhető. Ha ez a profil aktivált, akkor minden hálózati kommunikáció blokkolva lesz, a számítógép nem lesz elérhető külső hálózatok számára, és nem is tud majd kifelé kommunikálni. Ezt a rendszerprofilot nem lehet másolni, törölni vagy a beállításait módosítani.
- **Saját profilok:**
 - o **Közvetlenül csatlakozik az internetre** – általános otthoni asztali számítógépekhez

javasolt, amelyek közvetlenül csatlakoznak az internetre, vagy olyan notebook esetében, amely a biztonságos vállalati hálózaton kívül csatlakozik az internetre. Válassza ezt az opciót, ha otthonról csatlakozik az internetre, vagy olyan kisebb vállalati hálózatot használ, amely nem rendelkezik központi felügyelettel. Akkor is válassza ezt az opciót, ha utazik és ismeretlen vagy esetlegesen veszélyes helyeken kapcsolódik az internetre notebookjával (*internet kávézó, hotelszoba stb.*). Szigorúbb szabályok lesznek létrehozva, mivel feltételezhető, hogy ezen számítógépek nem rendelkeznek további védelemmel, ezért maximális védelemre van szükség.

- o **Tartományba rendelt számítógép** - helyi hálózatban lévő számítógépekhez javasolt, pl. iskola vagy vállalati hálózat. Feltételezük, hogy a hálózat valamennyire védve van, ezért itt a biztonsági szint alacsonyabb lehet mint a különálló számítógépeknél.
- o **Kisebb otthoni vagy irodai hálózat** – kisebb hálózatban (pl. otthon vagy kisvállalkozás) lévő számítógépekhez javasolt, ahol jellemzően néhány számítógép van összekapcsolva központi rendszergazda alkalmazása nélkül.

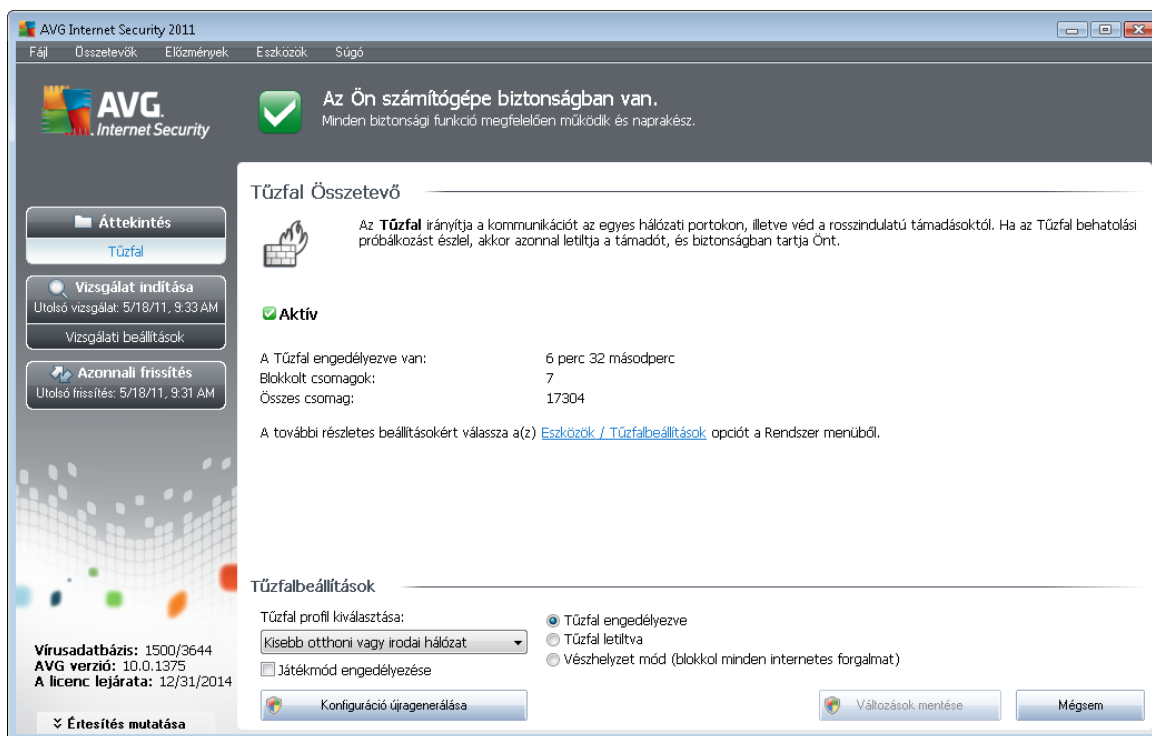
Profilváltás

A Profilváltás funkció lehetővé teszi a [Tuzfal](#) 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 [Tuzfal](#) egy párbeszédpanelen megkérdezi, hogy kíván-e hozzárendelni egy profilt.

Profilokat rendelhet hozzá minden helyi hálózati felülethez vagy területhez, és meghatározhat beállításokat a [Környezet- és adapterprofilok](#) panelen, ahol le is tilthatja az adott funkciót, ha nincs rá szüksége (*akkor minden kapcsolatnál az alapértelmezett profil lesz használva*).

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.

7.4.3. Tuzfal felület



A **Tűzfal** felület alapvető információkat nyújt az összetevő működéséről, állapotáról, illetve a **Tűzfal** statisztikákról:

- **A Tűzfal működik ... óta** - a Tűzfal utolsó indítása óta eltelt idő
- **Blokkolt csomagok** - a blokkolt csomagok az összes ellenőrzött adatcsomagból
- **Összes csomag** - a Tűzfal futása alatt ellenőrzött összes adatcsomag száma

Tűzfal beállítások

- **Tűzfal profil kiválasztása** - a legördülő menüből válassza ki az egyik profilt - két profil mindig elérhető (ezek az *alapértelmezett profilok*: **Összes engedélyezése** és **Összes tiltása**), egyéb profilok a Tűzfalbeállítás varázsló segítségével lettek hozzáadva, vagy szerkesztve lettek a [Profilok](#) panelen a [Tűzfal beállításai](#)ban.
- **Játék mód engedélyezése** - Jelölje be ezt az opciót annak biztosításához, hogy ha teljes képernyős alkalmazásokat (*játékokat, prezentációkat, filmeket, stb.*) futtat, akkor a **Tűzfal** nem kérdez rá arra, hogy Ön engedélyezi-e vagy tiltja az ismeretlen alkalmazások kommunikációját. Ha egy ismeretlen alkalmazás megpróbál kommunikálni a hálózaton, a **Tűzfal** automatikusan engedélyezi vagy tiltja 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.



- **Tuzfal állapota:**

- o **Tuzfal engedélyezve** – válassza ezt az opciót azon alkalmazások kommunikációjának engedélyezéséhez, amelyek "engedélyezett" minősítést kaptak a [Tuzfal](#) profilban
- o **Tuzfal letiltva** – ez az opció teljesen kikapcsolja a [Tuzfalat](#) . A rendszer minden hálózati forgalmat engedélyez, ellenőrzés nincs.
- o **Vészhelyzet mód (teljes internetes forgalom tiltása)** – használja ezt az opciót az összes forgalom tiltásához minden porton. A [Tuzfal](#) fut, de a hálózati forgalom tiltva van.

Megjegyzés: A szoftver gyártója minden AVG összetevőt az az optimális teljesítménynek megfelelően állított be. Ne változtassa meg az AVG beállításokat, hacsak nem feltétlenül szükséges. Bármely változtatást hozzáférő felhasználónak kell végeznie. Ha meg kell változtatnia a Tuzfal beállításait, akkor válassza az **Eszközök / Tuzfal beállítások** menüt, majd módosítsa az opciókat a megnyíló [Tuzfal beállítások](#) ablakban.

Vezérlogombok

- **Konfiguráció újragenerálása** - nyomja meg ezt a gombot az aktuális **Tuzfal** konfiguráció felülírásához, illetve az alapállapotra történő visszaállításhoz az automatikus észlelés szerint.
- **Változások mentése** - nyomja meg ezt a gombot a mentéshez és a változtatások alkalmazásához
- **Mégsem**- nyomja meg ezt a gombot az alapértelmezett [AVG felhasználói felületre](#) történő visszatéréshez (összetevők áttekintése)

7.5. Linkvizsgáló

7.5.1. LinkScanner alapelvek

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 márkákig, 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** technológia két funkciót tartalmaz: [Kereső védelem](#) és [Böngészés védelem](#):

- A [Kereső védelem](#) olyan weboldalak listáját tartalmazza (**URL-címek**), amelyek veszélyesnek minősülnek. Ha a Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg vagy SlashDot keresomotorokkal keres, akkor a rendszer ellenőrzi a keresési találatokat, és egy ikont jelenít meg mellettük (a Yahoo esetében csak a "káros weboldal" ikonok jelennek meg).

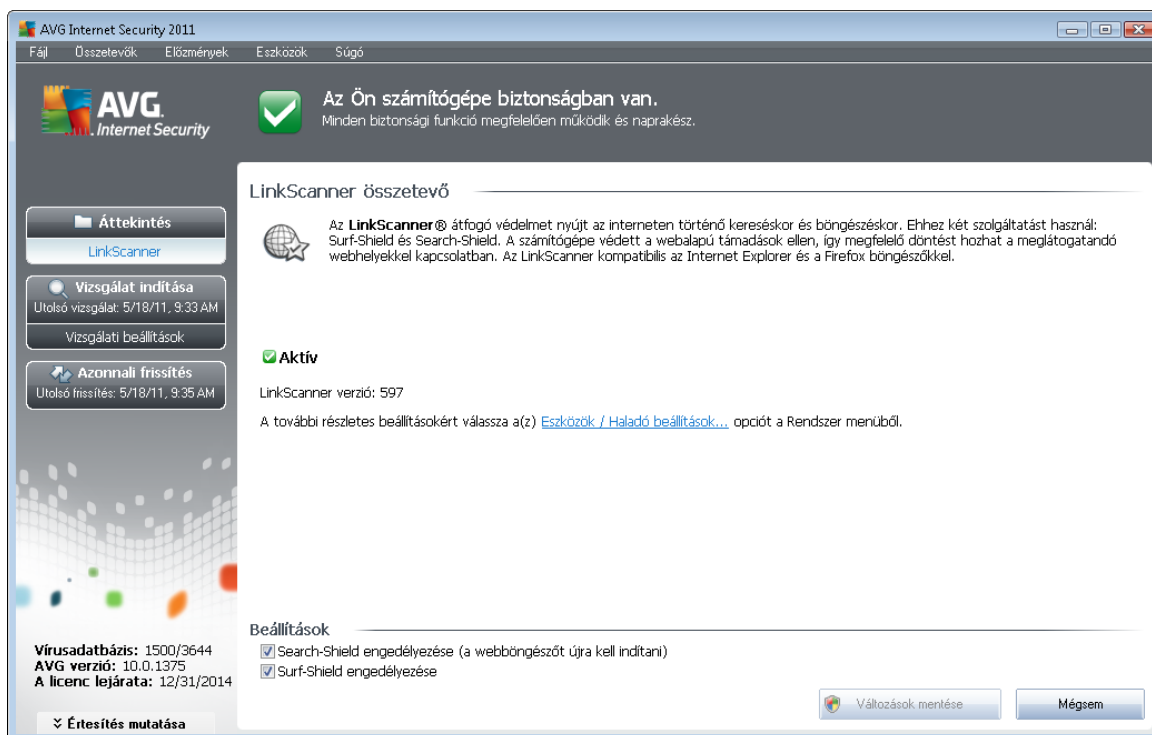


- A **Böngészés védelem** a meglátogatandó weboldalak tartalmát azok címétől függetlenül ellenorzi. Ha egyes oldalakat az **Keresés védelem** nem észlel (pl. amikor új veszélyes weboldal jön létre, vagy amikor egy korábban jóindulatú weboldal megfertőződik), akkor az **Böngészés védelem** észleli és letiltja a meglátogatandó gyanús tartalmakat.

Megjegyzés: a LinkScanner használata nem javasolt szerverplatformokon!

7.5.2. LinkScanner felület

A **LinkScanner** rövid leírást nyújt az összetevő működéséről, és értesít annak aktuális állapotáról. A program megjeleníti a **LinkScanner** adatbázisverziójának számát (**LinkScanner verziója**).



LinkScanner beállítások

A párbeszédpanel alsó részén számos beállítást adhat meg:

- **Keresés védelem** engedélyezése – (alapállapotban bekapcsolva): értesítések a következő keresomotorok használatakor: Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg vagy SlashDot. A rendszer elozetesen ellenorzi az adott webhelyek tartalmát.
- **Böngészés védelem** engedélyezése -(alapállapotban bekapcsolva): aktív (valós idejű) 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.

7.5.3. Kereso védelem

Ha a **Kereso védelemmel** keres az interneten, akkor a rendszer az összes népszerű keresomotorból (*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 az [AVG Link Scanner](#) figyelmezteti Önt még mielőtt egy veszélyes vagy gyanús hivatkozásra kattintana. Így biztos lehet benne, hogy mindig csak biztonságos weboldalakat 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.

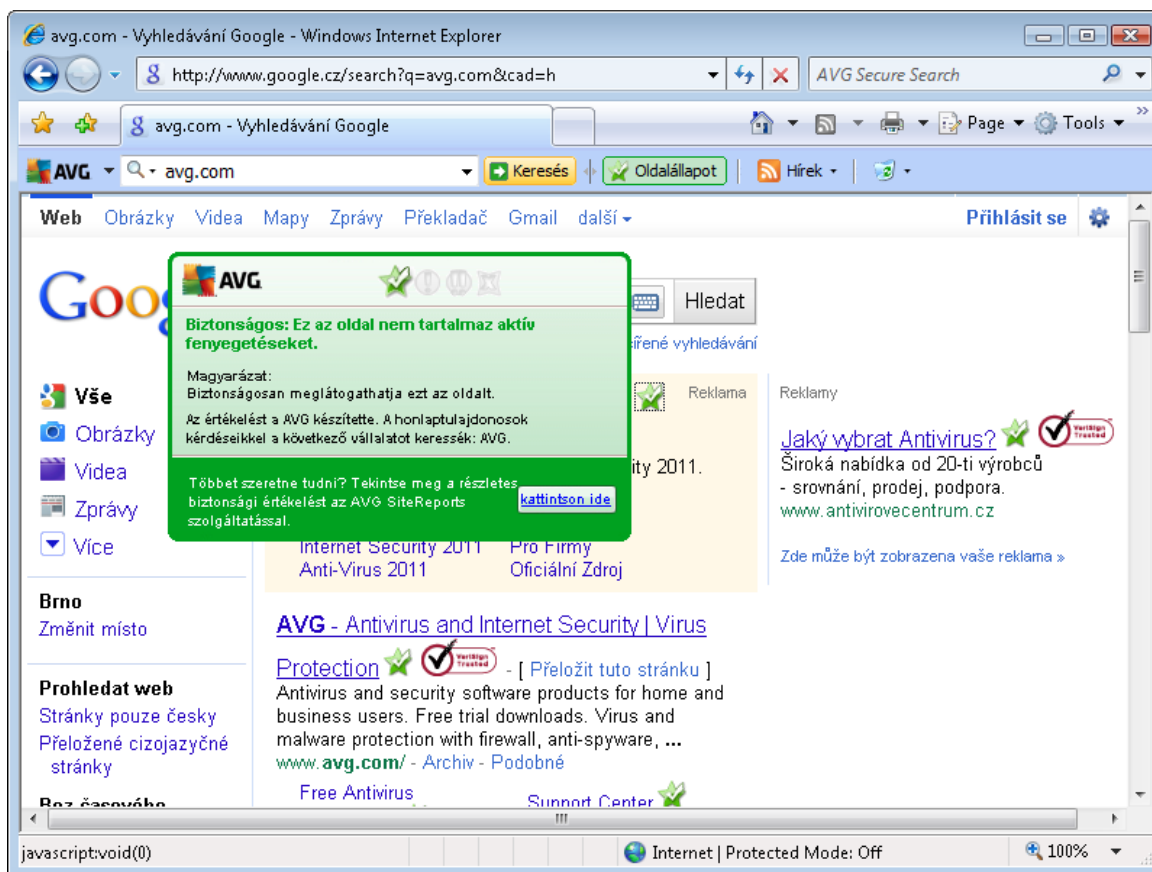


A linkelt oldal aktív fenyegetést jelent! Saját biztonsága érdekében nem engedélyezett az oldal meglátogatása.



A linkelt oldal nem elérhető, ezért nem lehet ellenőrizni.

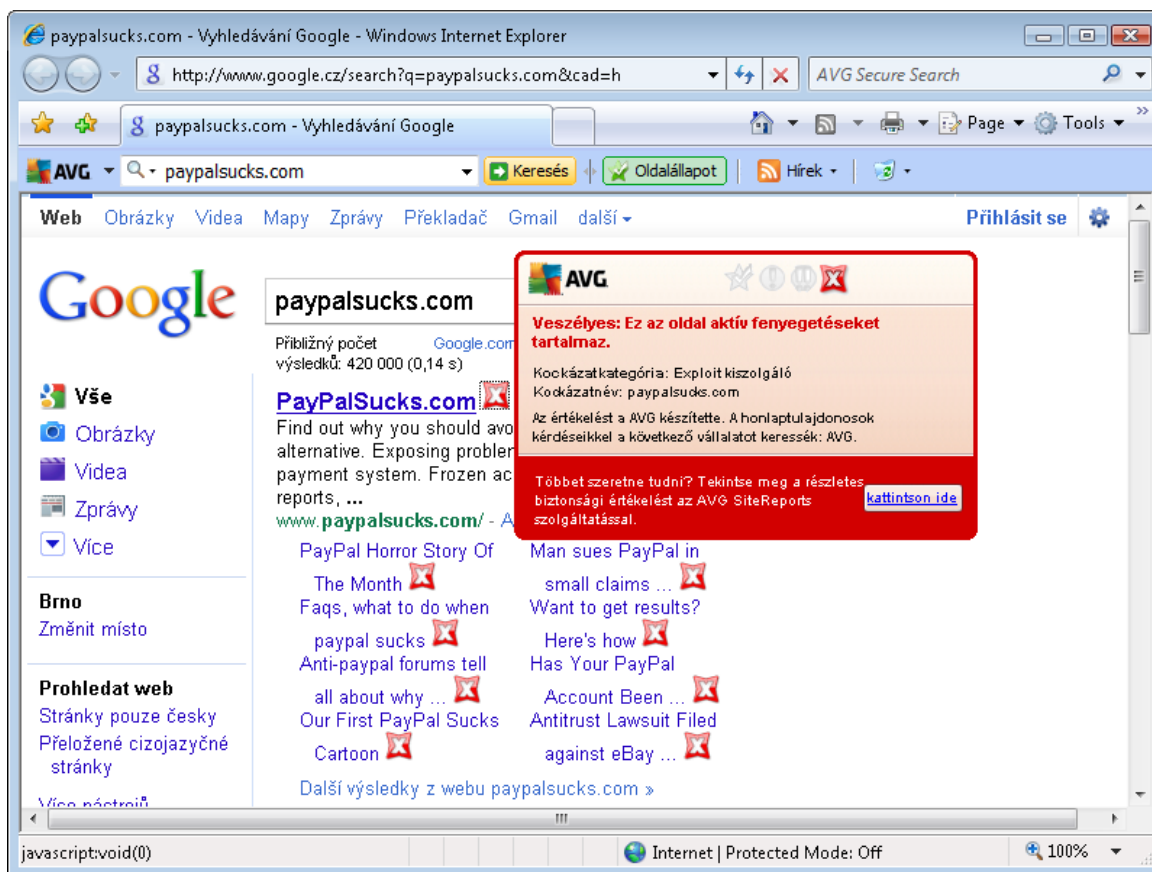
Ha ráviszi az egérmutatót egy adott információs ikonra, akkor részletek jelennek meg a kérdéses hivatkozással kapcsolatban. A fenyegetésről további részletek is rendelkezésre állnak (ha vannak):



7.5.4. Böngészés védelem

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 Ön olyan veszélyes weboldalt látogatna meg, mely exploitokat vagy egyéb komoly fenyegetést tartalmaz, akkor az **AVG Link Scanner** nem engedélyezi annak megjelenítését a böngészőben.

Ha káros weboldalt látogat meg, akkor az **AVG Linkvizsgáló** egy hasonló figyelmeztetést jelenít meg a böngészőben:



Az ilyen weboldalakra történő belépés rendkívül kockázatos és nem javasolt!

7.6. Állandó védelem

7.6.1. Állandó védelem alapelvek

Az **Állandó védelem** összetevő folyamatos védelmet biztosít számítógépének. Minden fájlt ellenőriz, amelyet Ön megnyit, ment vagy másol, és védi a számítógép rendszerterületeit. Ha a **Állandó védelem** vírus észlel a fájllal végzett műveletek során, akkor megszakítja az éppen végrehajtott műveletet, és meggátolja a vírus működésbe lépését. Jellemzően láthatatlan folyamat, amely a háttérben fut, és csak akkor értesít, ha valamilyen fenyegetést talál. Ugyanakkor a **Állandó védelem** megakadályozza a fenyegetések aktiválódását, illetve eltávolítja azokat. A **Állandó védelem** rendszerindítás során töltődik be a számítógép memóriájába.

Mi a feladata az Állandó védelemnek:

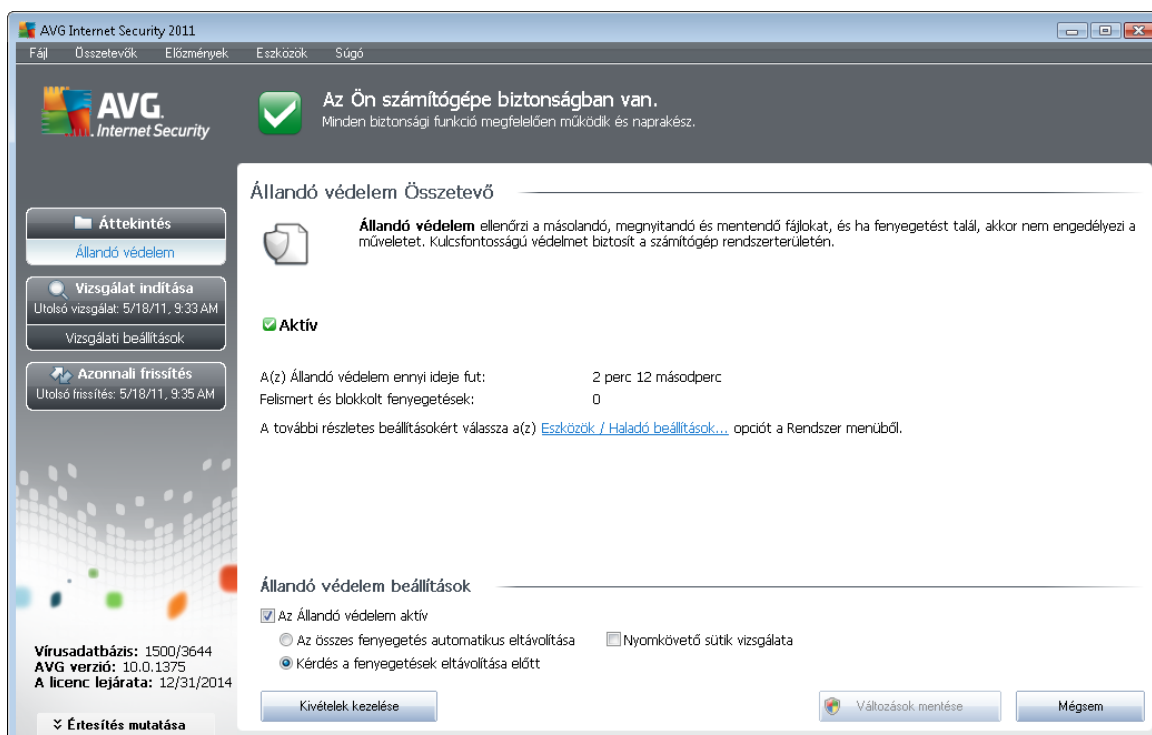
- Bizonyos típusú potenciális fenyegetések vizsgálata
- Cserélhető eszközök vizsgálata (*flash memória stb.*)
- Megadott kiterjesztésű vagy kiterjesztés nélküli fájlok vizsgálata



- Kivételek engedélyezése a vizsgálatnál - bizonyos fájlok vagy mappák, melyeket soha nem kell ellenőrizni

Figyelem: Az **Állandó védelem** a rendszer indulásakor töltődik be a számítógép memóriájába, és különösen fontos, hogy ott is maradjon, illetve folyamatosan működjön!

7.6.2. Állandó védelem felület



Az **Állandó védelem** szolgáltatás áttekintésén és az összetevő állapotán kívül az **Állandó védelem** felülete néhány statisztikai adatot is megjelenít:

- **Az Állandó védelem aktív ... óta**- megmutatja az összetevő utolsó indítása óta eltelt időt
- **Észlelt és blokkolt fenyegetések**- olyan észlelt fertőzések, melyek futtatása/megnyitása le lett tiltva (ha szükséges az érték visszaállítható statisztikai célból - **Érték** visszaállítása)

Állandó védelem beállítások

A panel alsó részén található az **Állandó védelem beállítások**, ahol az összetevő néhány alapbeállítását szerkesztheti (a *részletes konfiguráció* - a többi összetevővel együtt - a *Fájl/Haladó beállítások* menüből érhető el).

Az **Állandó védelem aktív** opció lehetővé teszi, hogy könnyen ki-/és bekapcsolja a rezidens védelmet. Alapállapotban a funkció be van kapcsolva. A bekapcsolt állandó védelemnél eldöntheti, hogy az esetleges észlelt fertőzések hogyan legyenek kezelve (eltávolítva):



- o automatikusan (**Az összes fenyegetés automatikus eltávolítása**)
- o vagy a felhasználó megerősítésével (**Kérdés a fenyegetések eltávolítása előtt**)

Ez a beállítás nincsen hatással a biztonsági szintre, és csak az Ön személyes preferenciáit tükrözi.

Mindkét esetben beállíthatja a **Nyomkövető sütik vizsgálatát**. Bizonyos esetekben bekapcsolhatja ezt a funkciót a maximális biztonsági szint eléréséhez, azonban alapállapotban ki van kapcsolva. (*sütik = olyan szöveges adatcsomagok, melyeket a kiszolgáló küld a webböngészőnek illetve melyeket a webböngésző küld vissza a kiszolgálónak, ha újra csatlakozik a szerverhez. a HTTP sütiket hitelesítéshez, nyomkövetéshez és bizonyos adatok gyűjtéséhez használják a felhasználókról, pl. honlap preferenciák vagy online vásárlás során a kosár tartalma).*

Megjegyzés: A szoftver gyártója minden AVG összetevőt beállított az optimális teljesítmény érdekében. 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 opciókat a megnyíló [AVG Haladó beállítások](#) ablakban.

Vezérlogombok

A vezérlogombok az **Állandó védelem** felületen a következők:

- **Kivételek kezelése**- megnyitja az [Állandó védelem - Kizárt elemek](#) panelt, amely lehetővé teszi, hogy meghatározza az [Állandó védelem](#) vizsgálatból kizárandó mappák és fájlok listáját
- **Változások mentése** - nyomja meg ezt a gombot a mentéshez és a változtatások alkalmazásához
- **Mégsem**- nyomja meg ezt a gombot az alapértelmezett [AVG felhasználói felületre](#) történő visszatéréshez (összetevők áttekintése)

7.6.3. Állandó védelem észlelés

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



Ezzen a panelen adatokat találhat azon fájlokról, amelyek fertőzöttnek lettek minősítve (*Fájlnév*), továbbá itt jelenik meg a fertőzés neve (*Fenyegetés neve*), illetve a [Vírusenciklopédia](#) címe, ahol részletes adatokat talál a fertőzésről (*További információk*).

Döntsön a következő lépésről - a következő lehetőségek állnak rendelkezésre:

Vegye figyelembe, hogy bizonyos esetekben (fertőzött fájl típusa és helye) nem minden opció érhető el!

- **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** - az AVG 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!

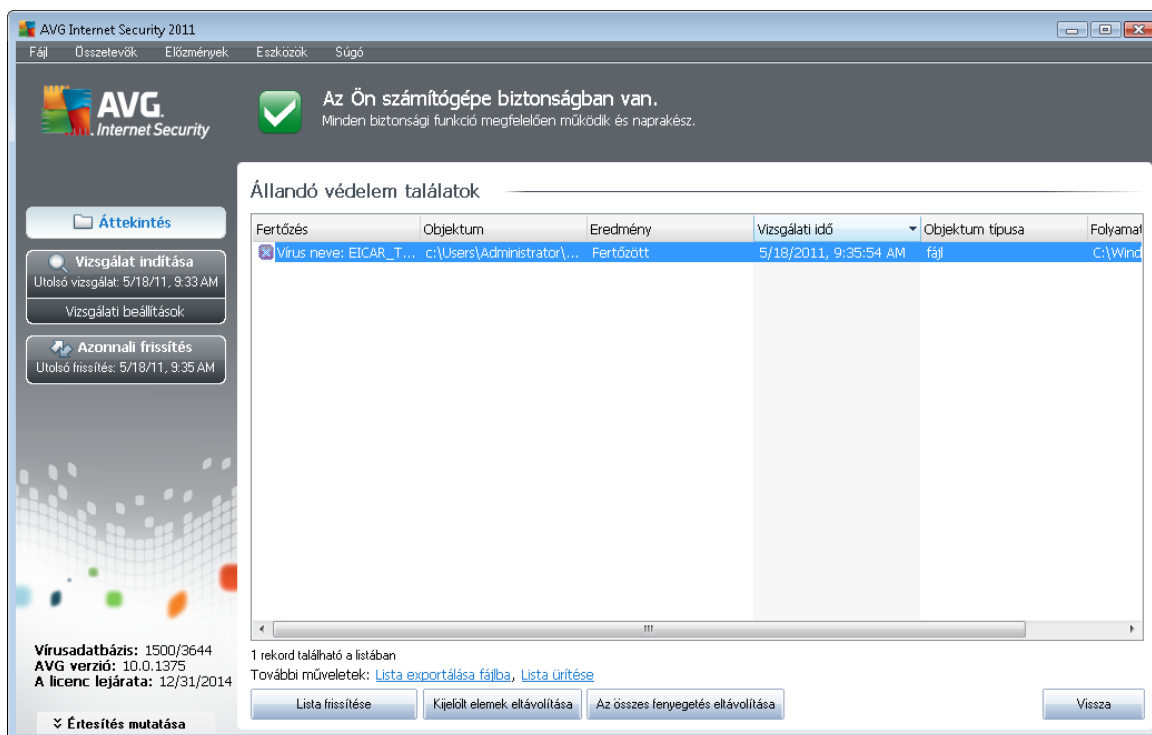
Megjegyzés: Eloffordulhat, hogy az észlelt objektum mérete túllépi a karantén szabad helyének méretét. Ebben az esetben egy figyelmeztető üzenet jelenik meg, ha Ön fertőzött objektumot



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** linket - kattintson rá, ekkor részletes adatok jelennek meg a fertőzés észlelésekor futó folyamatról, illetve a folyamat azonosításáról.

Az [Állandó védelem](#) által észlelt fenyegetés összes áttekintése megtalálható az **Állandó védelem észlelés** panelen, amely a rendszerben [Elozmények/ Állandó védelem találatok](#) részen 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** gomb visszaviszi Önt a alapértelmezett [AVG felhasználói felületre](#) (összetevok áttekintése).

7.7. Family Safety

Az **AVG Családi biztonság** segít megvédeni az Ön gyermekeit a nem megfelelő weboldaltól, médiatartalmaktól és online keresésektől, illetve jelentésekkel szolgál az online tevékenységekről. Minden egyes felhasználó esetében megadhatja a kívánt védelmi szintet, és külön-külön figyelheti a felhasználók tevékenységét az egyedi bejelentkezéseken keresztül.

Az összetevő csak akkor aktív, ha az **AVG Családi biztonság** termék telepítve van a számítógépre. Ha nem telepítette az **AVG Családi biztonság** terméket, akkor kattintson a megfelelő ikonra a(z) **AVG Internet Security 2011** felhasználói felületén. A rendszer ekkor átirányítja Önt a termék weboldalára, ahol megtalálhatja a szükséges információkat.

7.8. AVG LiveKive

Az **AVG LiveKive** automatikusan menti az összes fájlt, képet és zenét egyetlen biztonságos helyre, és lehetővé teszi, hogy Ön megossza azokat a családjával és barátaival, illetve hozzáférjen azokhoz bármilyen internetezésre alkalmas eszközzel, például iPhone és Androidos készülékekkel.

Az összetevő csak akkor aktív, ha az **AVG LiveKive** termék telepítve van a számítógépre. Ha nem telepítette az **AVG LiveKive** terméket, akkor kattintson a megfelelő ikonra az **AVG Internet Security 2011** felhasználói felületén. A rendszer ekkor átirányítja Önt a termék weboldalára, ahol megtalálhatja a szükséges információkat.

7.9. E-mail vizsgáló

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.

7.9.1. E-mail vizsgáló alapelvek

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 automatikus szerverek lesznek beállítva az e-mailek ellenőrzése



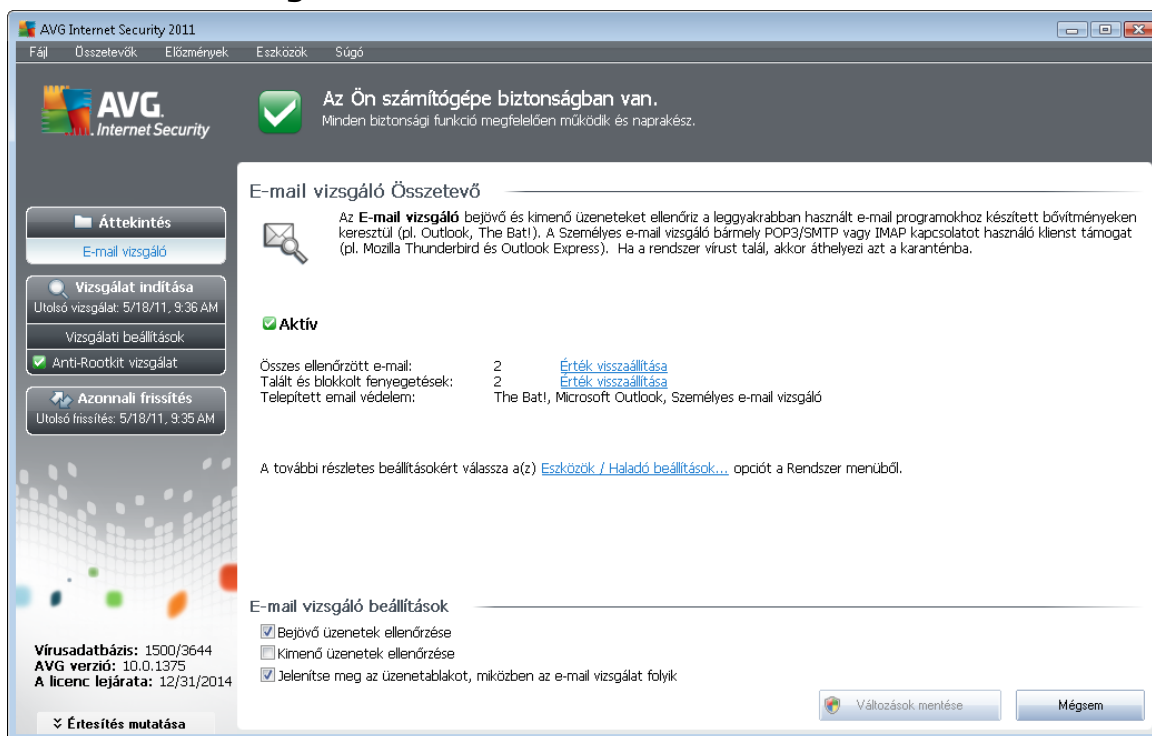
érdekében: egy a bejövő e-mailek ellenőrzéséhez és egy a kimenő e-mailek ellenőrzéséhez. Ezen két szerver használatával az e-mailek automatikusan ellenőrizve lesznek a 110-es és a 25-ös porton (a bejövő/kimenő e-mailek szabványos portjai).

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. Észleléskor a vírusok azonnal a **Víruskaranténba** kerülnek. Az üzenet ezután átkerül az e-mail kliensbe.
- **Kimenő levél:** Az üzenet az e-mail klinesből az E-mail vizsgálóhoz kerül, amely ellenőrzi azt, majd továbbküldi az üzenetet az SMTP kiszolgálóra (a kimenő e-mailek vizsgálata alapállapotban le van tiltva, ezt külön kapcsolhatja be).

Megjegyzés: az AVG E-mail Scanner használata nem javasolt szerver platformokon!

7.9.2. E-mail vizsgáló felület



Az **E-mail vizsgáló** panelen rövid leírást találhat az összetevő működéséről, aktuális állapotáról és a következő statisztikákról:

- **Összes vizsgált e-mail** - hány e-mail lett ellenőrizve az **E-mail vizsgáló** utolsó indítása óta (ha szükséges, az érték visszaállítható, pl. statisztikai célból - Érték visszaállítása)
- **Talált és blokkolt fenyegetések** - megmutatja az emailekben talált azonosított fertőzések számát az **E-mail vizsgáló** utolsó indítása óta
- **Telepített e-mail védelem** - információk egy adott e-mail védelem bővítményről, mely az



alapértelmezett telepített e-mail klienshez kapcsolódik

E-mail vizsgáló beállítások

Az ablak alsó részén megtalálhatja az **Email vizsgáló beállításokat**, ahol megadhatja az összetevő alapszintű beállításait:

- **Bejövő üzenetek ellenőrzése** - jelölje be ezt az elemet, annak meghatározásához, hogy az e-mail fiókba érkező összes üzenet ellenőrizve legyen. Alapállapotban ez az elem legyen bekapcsolva, és javasoljuk, hogy ne is módosítsa ezt a beállítást.
- **Kimenő üzenetek ellenőrzése** - jelölje be a postafiókból elküldött összes e-mail vírusellenőrzéséhez. Alapállapotban kikapcsolva.
- **Értesítő ablak megjelenítése e-mailek ellenőrzésekor** - jelölje be, ha értesítést kér a rendszerterületen, miközben az AVG [E-mail vizsgáló](#) összetevője az e-maileket ellenőrzi. Alapállapotban ez az elem legyen bekapcsolva, és javasoljuk, hogy ne is módosítsa ezt a beállítást.

Az **E-mail vizsgáló** összetevő haladó beállításai elérhetőek a **Eszközök/Haladó beállítások** részben a rendszermenüben. Azonban ezek módosítását csak gyakorlott felhasználóknak ajánljuk!

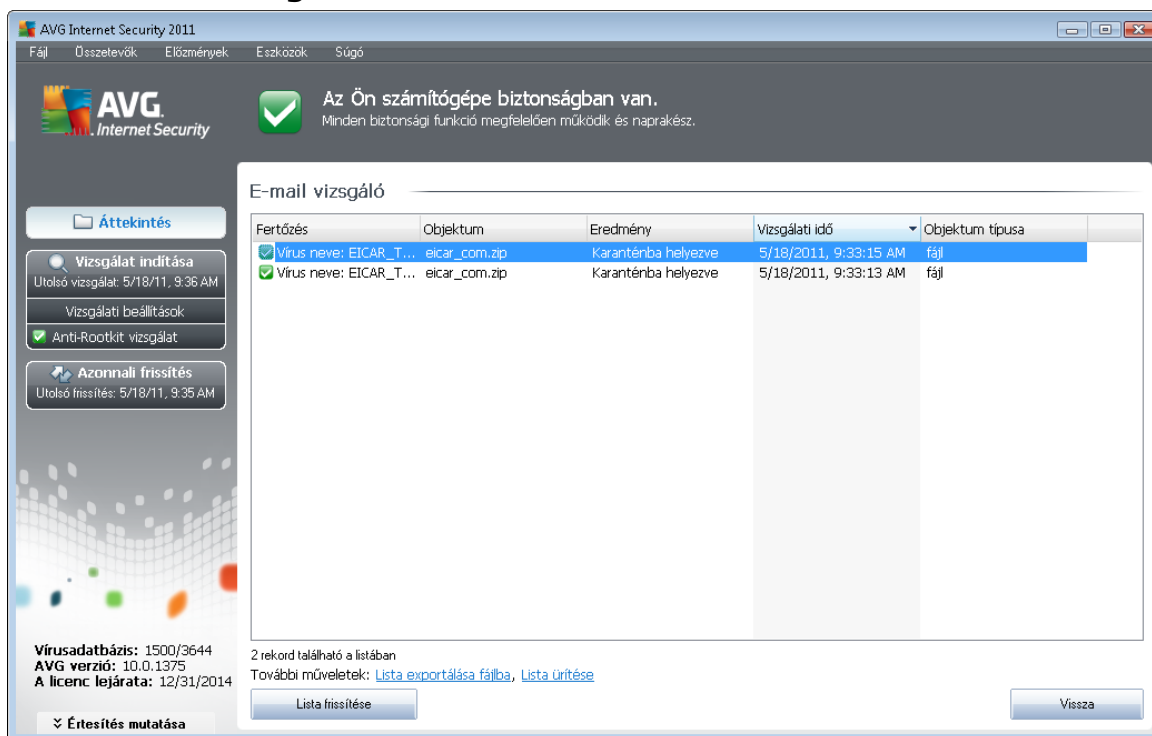
Megjegyzés: A szoftver gyártója minden AVG összetevőt az az optimális teljesítménynek megfelelően állított be. Ne változtassa meg az AVG beállításokat, hacsak nem feltétlenül szükséges. Bármely változtatást gyakorlott felhasználónak kell végeznie. Ha meg kell változtatnia az AVG beállításait, akkor válassza az **Eszközök / Haladó beállítások** menüt, majd módosítsa az opciókat a megnyíló [AVG Haladó beállítások](#) ablakban.

Vezérlogombok

A vezérlogombok az **Email vizsgáló** felületen a következők:

- **Változások mentése** - nyomja meg ezt a gombot a mentéshez és a változtatások alkalmazásához
- **Mégsem** - nyomja meg ezt a gombot az alapértelmezett [AVG felhasználói felületre](#) történő visszatéréshez (összetevők áttekintése)

7.9.3. E-mail vizsgáló észlelés



Az **E-mail vizsgáló észleléspanel**en (elérhető itt: [Elozmények / E-mail vizsgáló észlelés](#)) az összes találatot láthatja, melyet az **E-mail vizsgáló** összetevő azonosított. 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**).

Vezérlogombok

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

- **Lista frissítése** - frissíti az észlelt fenyegetések listáját
- **Vissza** - visszatérés az előző párbeszédpanelhez

7.10. Frissítéskezelő

7.10.1. Frissítéskezelő alapelvek

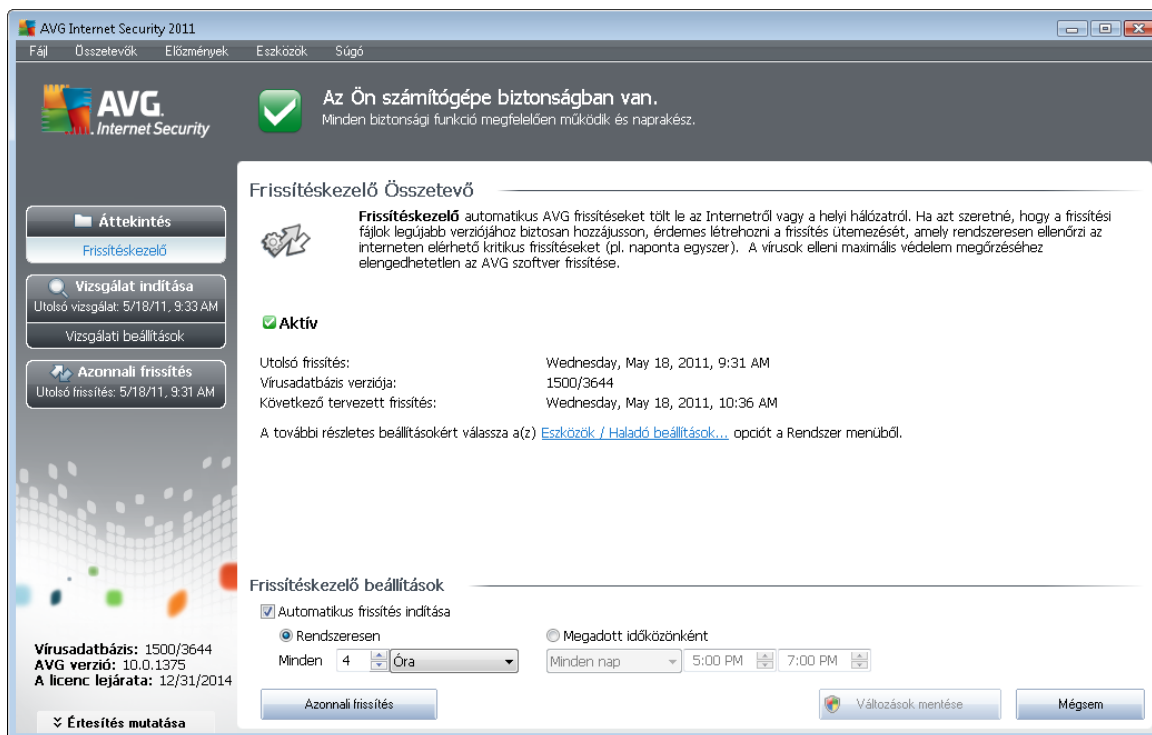
Semmilyen biztonsági szoftver nem garantálhat védelmet a különböző típusú fenyegetések ellen, ha az nincs rendszeresen frissítve! A vírusok készítői mindig újabb és újabb kihasználható hibákat keresnek az egyes szoftverekben és operációs rendszerekben. Új vírusok, rosszindulatú kódok és hackelési stratégiák jelennek meg minden egyes nap. Ezért a szoftvergyártók folyamatosan adnak ki frissítéseket és biztonsági javításokat újonnan felfedezett biztonsági rések betöméséhez.

Kulcsfontosságú, hogy rendszeresen frissítse az AVG programot!

A **Frissítéskezelő** segíti Önt a frissítési feladatok rendszeres elvégzésében. Az összetevőn belül a frissítési fájlok internetről vagy helyi hálózatról történő automatikus letöltését ütemezheti. A vírusvédelem elengedhetetlen része a napi szintű frissítése. A kevésbé fontos programfrissítések hetente is történhetnek.

Megjegyzés: Kérjük, nézze át az [AVG frissítések](#) fejezetet a frissítések típusaival és szintjeivel kapcsolatos további információkért!

7.10.2. Frissítéskezelő felület



A **Frissítéskezelő** felülete információkat jelenít meg az összetevő működéséről, állapotáról, illetve kapcsolódó statisztikai adatokat jelenít meg:



- **Legújabb frissítés** - megmutatja a legújabb adatbázis-frissítés dátumát és időpontját
- **Vírusadatbázis verziója** - megjeleníti a jelenleg telepített vírusadatbázis verziójának számát. Ez a szám minden egyes adatbázis-frissítéssel növekszik
- **Következő ütemezett frissítés** - megmutatja a következő adatbázis-frissítés dátumát és időpontját

Frissítéskezelő beállítások

Az ablak alsó részén megtalálhatja a **Frissítéskezelő beállítások** részt, ahol módosíthatja a frissítési szabályokkal kapcsolatos beállításokat. Meghatározhatja, hogy automatikusan (**Automatikus frissítések indítása**) vagy manuálisan szeretné-e letölteni a frissítési fájlokat. Alapállapotban az **Automatikus frissítések indítása** opció van bekapcsolva, és javasoljuk, hogy tartsa is így! A legújabb frissítési fájlok rendszeres letöltése kulcsfontosságú bármely biztonsági szoftver megfelelő működéséhez!

Továbbá meghatározhatja, hogy a frissítést mikor kell lefuttatni.

- o **Folyamatosan** - határozza meg az időközöket
- o **Bizonyos időközönként** - adja meg azt a napot, amikor a rendszer a frissítést lefuttatja

Alapállapotban a frissítés 4 óránként fut. Érdemes megtartani ezt a beállítást, és csak akkor módosítsa, ha feltétlenül szükséges!

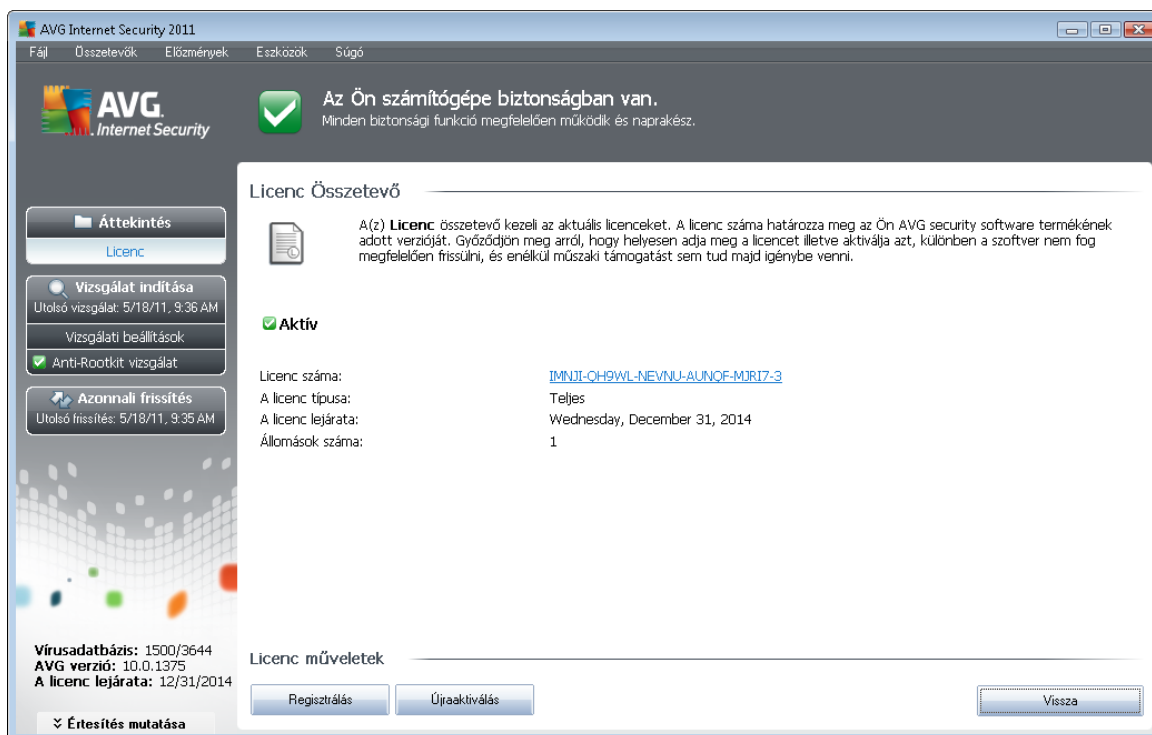
Megjegyzés: A szoftver gyártója minden AVG összetevőt beállított az optimális teljesítmény érdekében. Ne változtassa meg az AVG beállításokat, hacsak nem feltétlenül szükséges. Bármely változtatást gyakorlott felhasználónak kell végeznie. Ha meg kell változtatnia az AVG beállításait, akkor válassza az **Eszközök / Haladó beállítások** menüt, majd módosítsa az opciókat a megnyíló [AVG Haladó beállítások](#) ablakban.

Vezérlogombok

A vezérlogombok a **Frissítéskezelő** felületen a következők:

- **Frissítés most** - elindítja az [azonnali frissítést](#) manuálisan
- **Változások mentése** - nyomja meg ezt a gombot a mentéshez és a változtatások alkalmazásához
- **Mégsem** - nyomja meg ezt a gombot az alapértelmezett [AVG felhasználói felületre](#) történő visszatéréshez (összetevők áttekintése)

7.11. Licenc



A **Licensz** ablakban rövid leírást találhat az (összefügg működéséről, aktuális állapotáról és a következő információkról:

- **Licenszkód** - megjeleníti a licenszkódot rövidített formában (*biztonsági okokból az utolsó négy karakter hiányzik*). Amikor megadja a licenckódot, akkor különösen ügyeljen a pontosságra, és ugyanúgy gépelje be, ahogy az megjelenik. Különösen javasoljuk, hogy a másolás és beillesztés módszert használja a licenckód megadásakor.
- **Licenc típusa** - a telepített termék típusát mutatja.
- **Licenc lejárata** - megmutatja a licenc érvényességének végét. Ha ezen dátum után is használni szeretné az **AVG Internet Security 2011** programot, akkor meg kell újítania a licencet. A licensz megújítását online kezdeményezheti az [AVG weboldalon](#).
- **Állomások száma** - megmutatja, hogy hány munkaállomáson jogosult telepíteni az szoftvert **AVG Internet Security 2011**.

Vezérlogombok

- **Regisztrálás** - csatlakozik az AVG weblapjának regisztrációs oldalához (<http://www.avg.hu/>). Töltse ki a regisztrációs adatokat! Csak regisztrált ügyfelek jogosultak ingyenes AVG műszaki terméktámogatásra.
- **Újraaktiválás** - megnyitja az **AVG aktiválása** panelt azokkal az adatokkal, amiket megadott az [AVG teszteszt](#) panelen a [telepítési folyamat során](#). Ezen a panelen

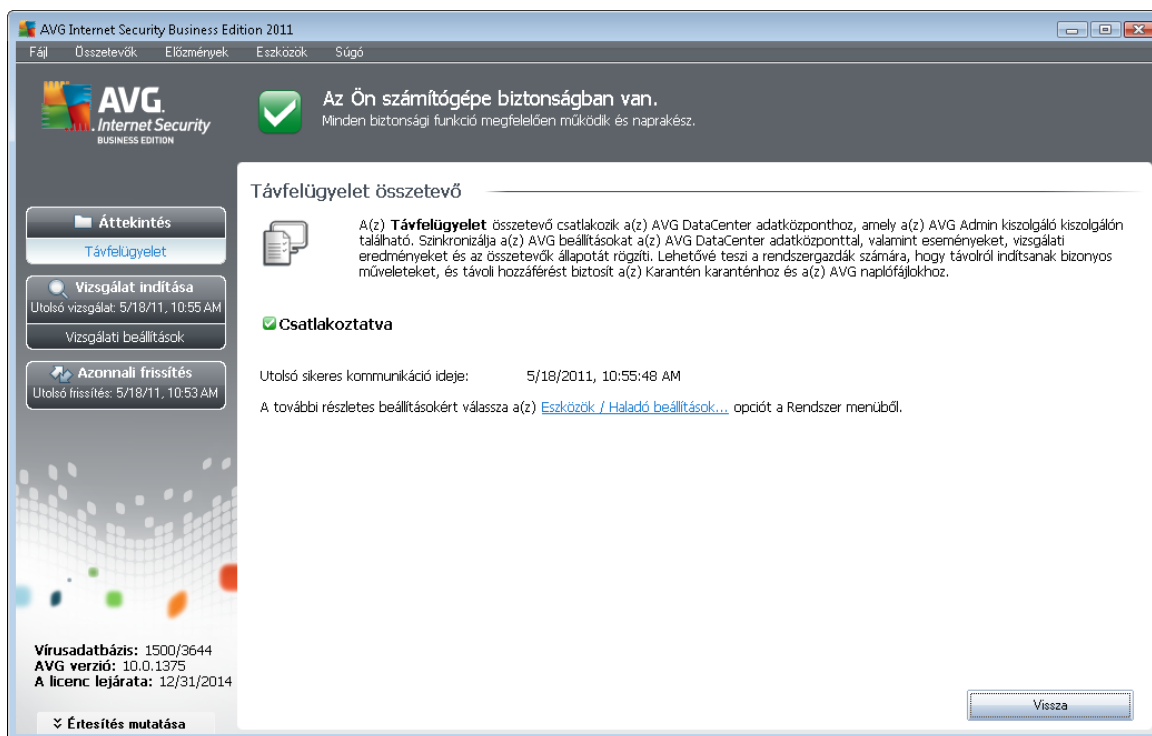


megadhatja a licenckódot, hogy lecserélje az értékesítési számot (az a szám, amivel telepítette az AVG-t), vagy hogy lecserélje a régi licenckódot (pl. mikor frissíti az új AVG terméket).

Megjegyzés: Ha az **AVG Internet Security 2011** próbaverzióját használja, akkor a **Vásárlás most** és **Aktiválás** gombok jelennek meg, amelyekkel azonnal megvásárolhatja a program teljes verzióját. Az értékesítési számmal telepített **AVG Internet Security 2011** esetében ezen lépések a következők: **Regisztrálás** és **Aktiválás**.

- **Vissza** - nyomja meg ezt a gombot az alapértelmezett [AVG felhasználói felületre](#) történő visszatéréshez (összetevők áttekintése).

7.12. Távfelügyelet



A **Távfelügyelet** összetevő kizárólag az **AVG Internet Security 2011** felhasználói felületén jelenik meg, ha telepítette a termék üzleti változatát (lásd a [Liszensz](#) összetevőt). A **Távfelügyelet** panelen láthatja, hogy az összetevő aktív-e, illetve kapcsolódott-e a kiszolgálóhoz. A **Távfelügyelet** összetevő összes beállítását a **Haladó beállítások / Távfelügyelet** részen végezheti el.

Az AVG Távfelügyelet összetevő beállításával és szolgáltatásaival kapcsolatos részletes leírásért forduljon az összetevőről szóló dokumentációhoz. A dokumentációt letöltheti az [AVG weboldaláról](#) (www.avg.com) a **Támogatás / Letöltés / Dokumentációk** részen.

Vezérlogombok

- **Vissza** - nyomja meg ezt a gombot az alapértelmezett [AVG felhasználói felületre](#) történő



visszatéréshez (összetevők áttekintése).

7.13. Online szuro

7.13.1. Online szuro alapelvek

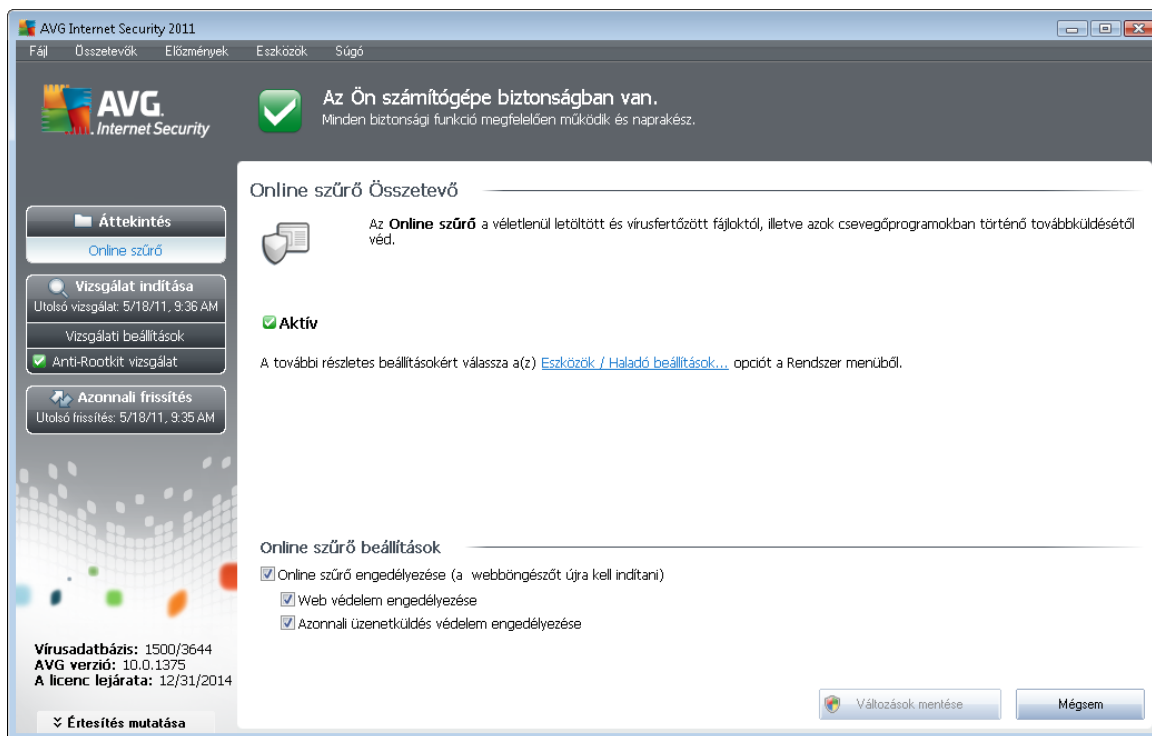
Az **Online szuro**valós idejű állandó védelmet nyújt. Ellenorzi a meglátogatandó weboldalakat (és az esetlegesen beágyazott dokumentumokat), mielőtt azok megjelenének a webböngészőben vagy letöltnének a számítógépre.

Az **Online szuro** felismeri, ha a meglátogatandó oldal veszélyes java szkriptet tartalmaz, és megakadályozza annak betöltődését. Természetesen azonosítja a beágyazott rosszindulatú kódokat is, és megakadályozza azok letöltődését is a számítógépre.

Megjegyzés: az AVG Online szuro használata nem javasolt szerver platformokon.

7.13.2. Online szuro felület

Az **Online szuro** összetevő felülete leírja ezen védelmi típus viselkedését. Itt megtalálhatja az információkat az összetevő aktuális állapotáról. A panel alsó részén alapvető beállítási lehetőségeket találhat az összetevő működésével kapcsolatban:



Online szuro beállításai



Mindenekelőtt azonnal be- és kikapcsolhatja az **Online szuro** funkciót az **Online szuro engedélyezése** elem bejelölésével. Ez az opció alapállapotban be van kapcsolva, és az **Online szuro** összetevő aktív. Csak akkor kapcsolja ki az aktív összetevőt, ha feltétlenül szükséges. Ha az elem be van jelölve és az **Online szuro** fut, akkor további két beállítási lehetőség érhető el:

- **Web védelem engedélyezése** - ez az opció biztosítja, hogy az **Online szuro** ellenőrizze a honlapok tartalmát.
- **Azonnali üzenetküldés védelem engedélyezése** - jelölje be ezt az elemet, ha azt szeretné, hogy az **Online szuro** ellenőrizze az azonnali üzenetküldés kommunikációjának (pl. ICQ, MSN Messenger,) vírusmentességét.

Megjegyzés: A szoftver gyártója minden AVG összetevőt beállított az optimális teljesítmény érdekében. 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 opciókat a megnyíló [AVG Haladó beállítások](#) ablakban.

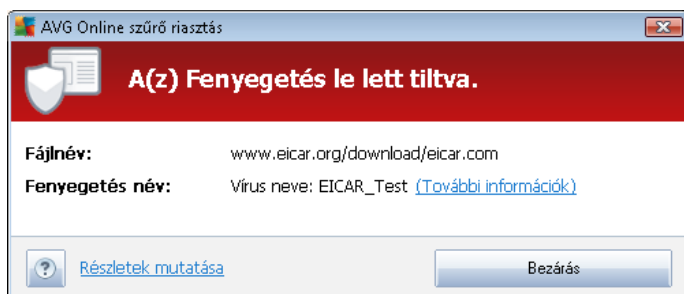
Vezérlogombok

A vezérlogombok az **Online szuro** felületen a következők:

- **Változások mentése** - nyomja meg ezt a gombot a mentéshez és a változtatások alkalmazásához
- **Mégsem** - nyomja meg ezt a gombot az alapértelmezett [AVG felhasználói felületre](#) történő visszatéréshez (összetevők áttekintése)

7.13.3. Online szuro észlelés

Az **Online szuro** 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 azon fájlokról, amelyek fertőzöttnek lettek minősítve (*Fájlnev*), továbbá itt jelenik meg a fertőzés neve (*Fenyegetés neve*), illetve a [Vírusenciklopédia](#) címe, ahol részletes adatokat talál a fertőzésről (*ha van ilyen*). A párbeszédpanel a következő gombokat tartalmazza:

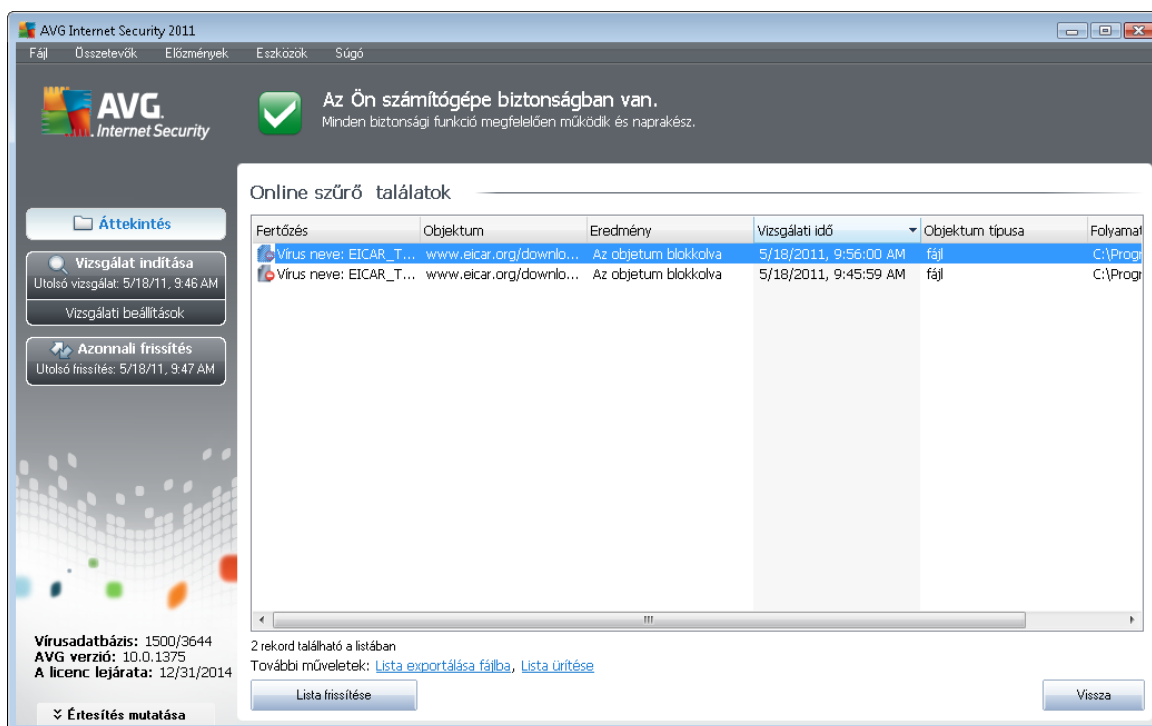
- **Részletek megjelenítése** - kattintson a **Részletek megjelenítése** gombra egy új felbukkanó



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 szuro találatokban** - az észlelt fenyegetések áttekintése a rendszerenü [Elozmények / Online szuro 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 letiltotta 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**). A **Lista frissítése** gomb frissíti az **Online szuro** által észlelt fenyegetések listáját. A **Vissza** gomb visszaviszi Önt a alapértelmezett [AVG](#)

[felhasználói felületre](#) (összetevők áttekintése).

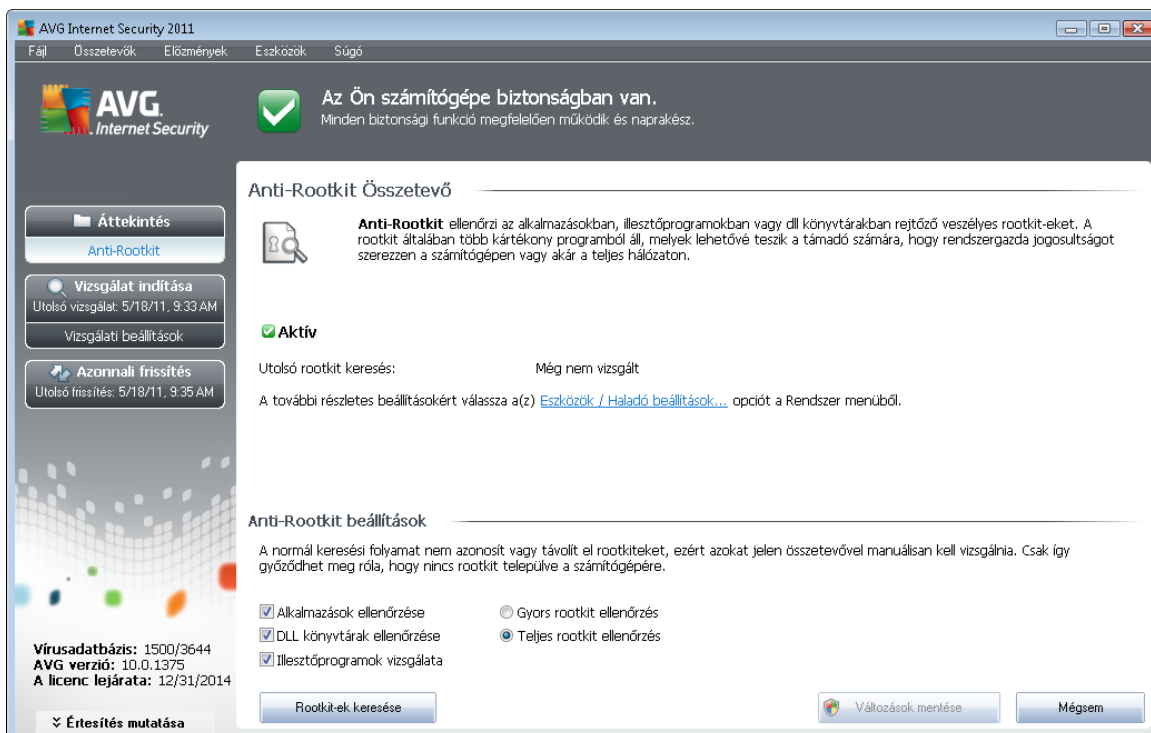
7.14. Anti-Rootkit

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 elhítetik 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.

7.14.1. Anti-Rootkit alapelvek

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

7.14.2. Anti-Rootkit felület



Az **Anti-Rootkit** felhasználói felülete rövid leírást tartalmaz az összetevő működéséről, tájékoztat az összetevő aktuális állapotáról, illetve megjeleníti az **Anti-Rootkit** vizsgálat futtatásának legutóbbi



idopontját (**Legutóbbi rootkit keresés**). Az **Anti-Rootkit** párbeszédpanel tartalmazza az [Eszközök/Haladó beállítások](#) linket. Használja ezt a hivatkozást az **Anti-Rootkit** összetevő haladó beállításainak eléréséhez.

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

Anti-Rootkit beállítások

Az ablak alsó részén megtalálhatja az **Anti-Rootkit beállításokat**, ahol megadhatja az összetevő alapszintű beállításait. Eloszor 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** - 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

Vezérlogombok

- **Rootkit-ek keresése** - mivel a rootkit vizsgálat nem része a [Számítógép teljes vizsgálata](#) funkciónak, ezért azt az **Anti-Rootkit** felületről indíthatja ezzel a gombbal.
- **Változások mentése** - nyomja meg ezt a gombot az összes változás mentéséhez, és az alapértelmezett [AVG felhasználói felületre](#) (összetevők áttekintése) történő visszatéréshez
- **Mégsem** - nyomja meg ezt a gombot az alapértelmezett [AVG felhasználói felületre](#) (összetevők áttekintése) történő visszatéréshez a változások mentése nélkül

7.15. Rendszereszközök

A **Rendszereszközök** rész a **AVG Internet Security 2011** környezet és az operációs rendszer részletes összefoglaló információit jeleníti meg. Az összetevő a következő elemek áttekintését jeleníti meg:

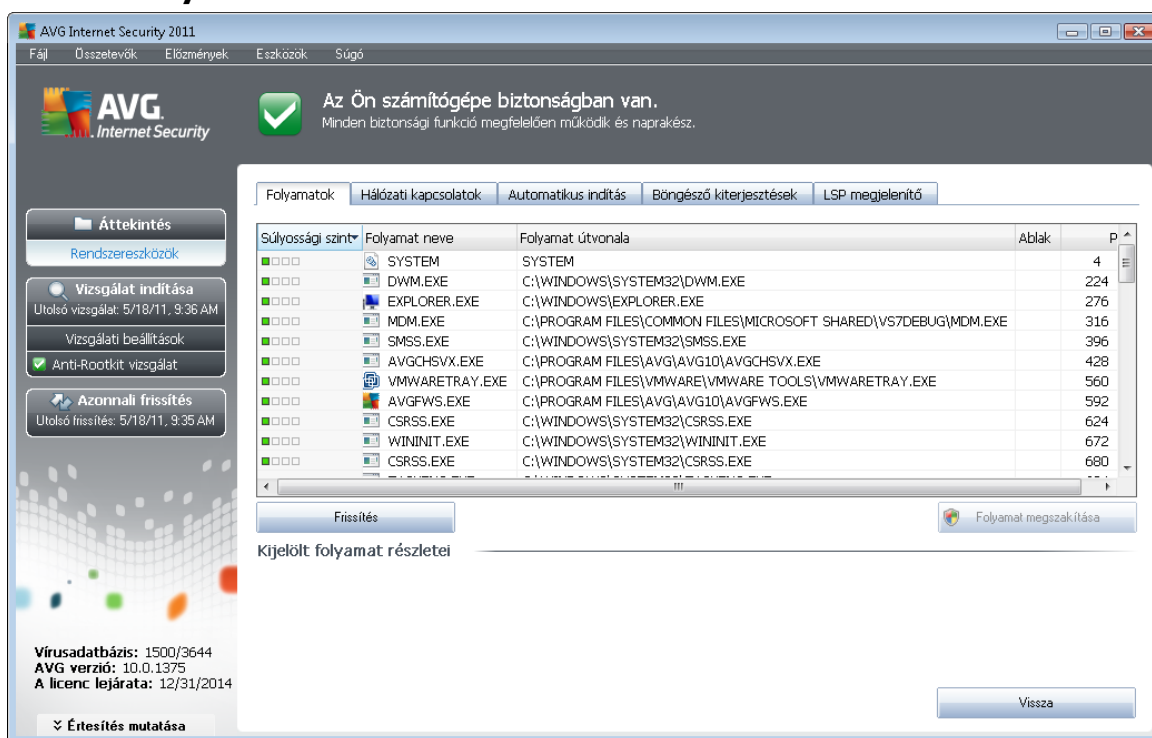
- [Folyamatok](#) - a számítógépen jelenleg aktív (pl. futó alkalmazások) folyamatok listája



- [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!

7.15.1. Folyamatok



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

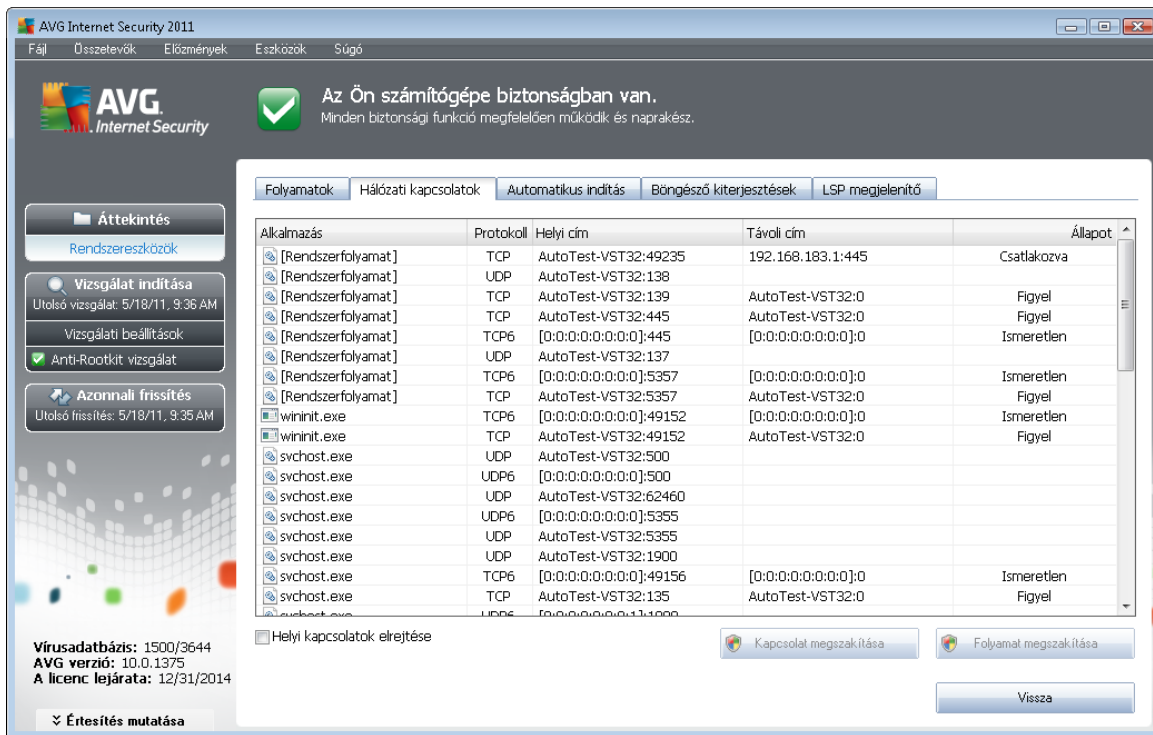
- **Súlyossági szint** - az adott folyamat kockázati szintjének grafikus értékelése egy négyzetszintű skálán a legkevésbé fontosabbtól (■□□□) a legfontosabbikig (■■■■)
- **Folyamat neve** - az aktív folyamat nevét jelzi
- **Folyamat elérési útvonala** - az aktív folyamat tényleges elérési útját jelzi
- **Ablak** - az alkalmazásablak nevét jelzi, ha van ilyen
- **PID** - a folyamatazonosító szám a Windows rendszerben használt belső folyamatazonosító, amely a folyamatok egyértelmű azonosítására szolgál

Vezérlogombok

A vezérlogombok a **Rendszerezszközők** felületen 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!**
- **Vissza** - ez a gomb átirányítja Önt az alapértelmezett [AVG felhasználói felületre](#) (összefoglaló áttekintése)

7.15.2. Hálózati kapcsolatok



AVG Internet Security 2011

Fájl | Összefoglaló | Előzmények | Eszközök | Súgó

AVG Internet Security

Az Ön számítógépe biztonságban van.
Minden biztonsági funkció megfelelően működik és naprakész.

Hálózati kapcsolatok

Alkalmazás	Protokoll	Helyi cím	Távoli cím	Állapot
[Rendszerfolyamat]	TCP	AutoTest-VST32:49235	192.168.183.1:445	Csatlakozva
[Rendszerfolyamat]	UDP	AutoTest-VST32:138		
[Rendszerfolyamat]	TCP	AutoTest-VST32:139	AutoTest-VST32:0	Figyel
[Rendszerfolyamat]	TCP	AutoTest-VST32:445	AutoTest-VST32:0	Figyel
[Rendszerfolyamat]	TCP6	[0:0:0:0:0:0:0:0]:445	[0:0:0:0:0:0:0:0]:0	Ismeretlen
[Rendszerfolyamat]	UDP	AutoTest-VST32:137		
[Rendszerfolyamat]	TCP6	[0:0:0:0:0:0:0:0]:5357	[0:0:0:0:0:0:0:0]:0	Ismeretlen
[Rendszerfolyamat]	TCP	AutoTest-VST32:5357	AutoTest-VST32:0	Figyel
wininit.exe	TCP6	[0:0:0:0:0:0:0:0]:49152	[0:0:0:0:0:0:0:0]:0	Ismeretlen
wininit.exe	TCP	AutoTest-VST32:49152	AutoTest-VST32:0	Figyel
svchost.exe	UDP	AutoTest-VST32:500		
svchost.exe	UDP6	[0:0:0:0:0:0:0:0]:500		
svchost.exe	UDP	AutoTest-VST32:62460		
svchost.exe	UDP6	[0:0:0:0:0:0:0:0]:5355		
svchost.exe	UDP	AutoTest-VST32:5355		
svchost.exe	UDP	AutoTest-VST32:1900		
svchost.exe	TCP6	[0:0:0:0:0:0:0:0]:49156	[0:0:0:0:0:0:0:0]:0	Ismeretlen
svchost.exe	TCP	AutoTest-VST32:135	AutoTest-VST32:0	Figyel

☐ Helyi kapcsolatok elrejtése

Kapcsolat megszakítása | Folyamat megszakítása

Vissza

Vírusadatbázis: 1500/3644
AVG verzió: 10.0.1375
A licenc lejárata: 12/31/2014

Értesítés mutatója

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:
 - o TCP – az internet protokollal (IP) együtt használatos protokoll, amely az adatok interneten történő továbbítására szolgál



o 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.

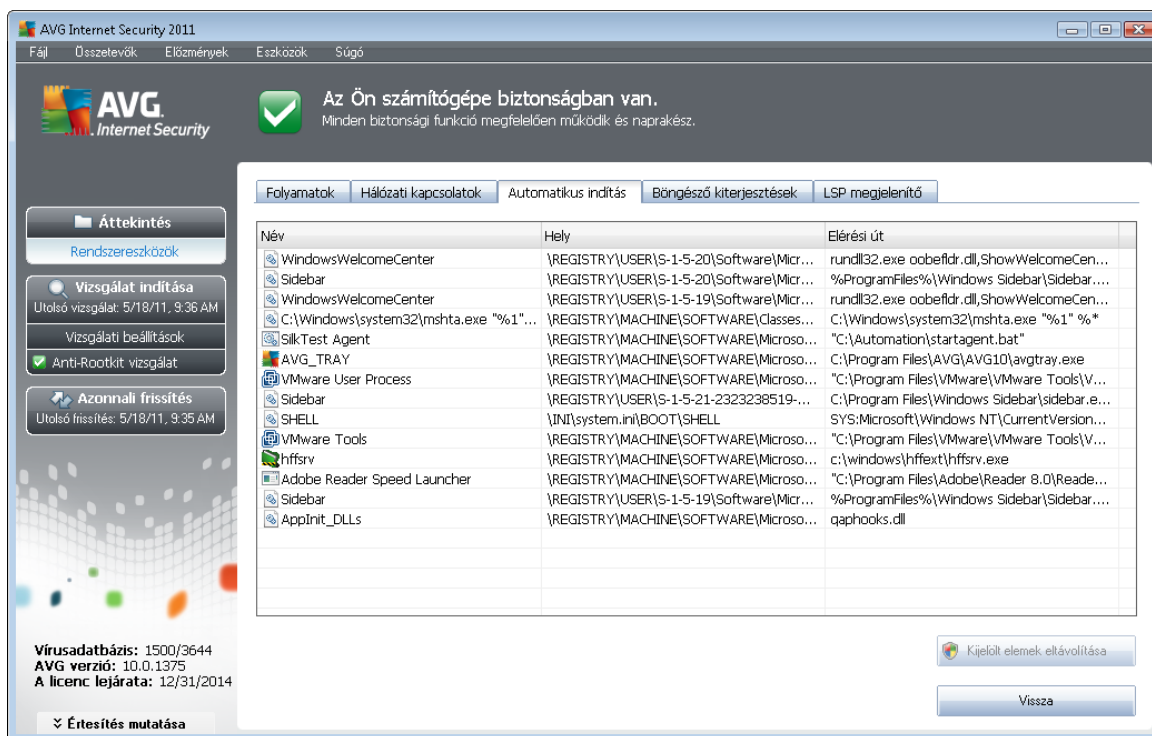
Vezérlogombok

A következő vezérlogombok érhetők el:

- **Kapcsolat megszakítása** - bezár egy vagy több kapcsolatot a listában
- **Folyamat megszakítása** - bezár egy vagy több kapcsolathoz tartozó alkalmazást a listában
- **Vissza** - visszaviszi Önt az alapértelmezett [AVG felhasználói felületre](#) (összetevők áttekintése).

Idonként 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!

7.15.3. Automatikus indítás

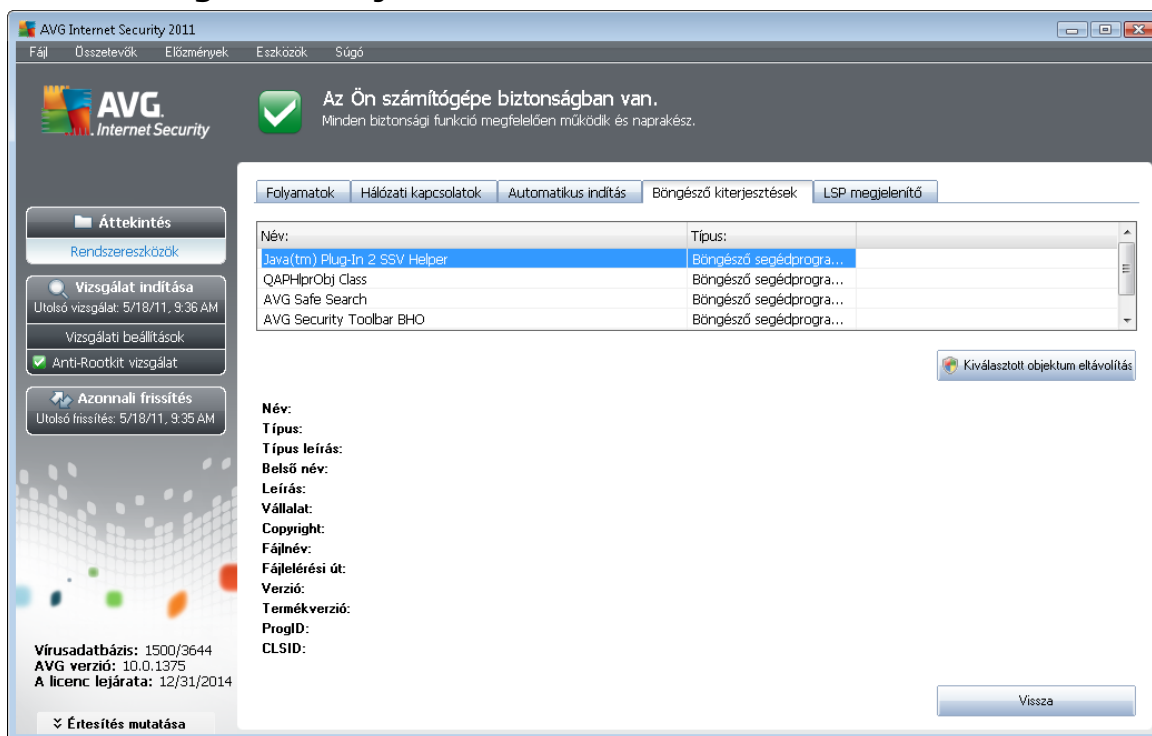


Az **Automatikus indítás**panel megjeleníti az összes olyan alkalmazást, mely a Windows rendszer indításakor elindul. Rendkívül gyakran előfordul, hogy a rosszindulatú szoftverek automatikusan hozzáadják magukat az indítási regisztrációs bejegyzéshez.

A bejegyzések úgy törölhetők, hogy kiválasztja azokat, majd a **Kijelölt elem(ek) törlése** gombra kattint. A **Vissza** gomb visszaviszi Önt a alapértelmezett [AVG felhasználói felületre](#) (összetevők áttekintése).

a listában szereplő alkalmazásokat csak akkor ajánlatos törölni, ha meg van győződve róla, hogy azok valódi veszélyeket rejteneek!

7.15.4. Böngésző kiterjesztések



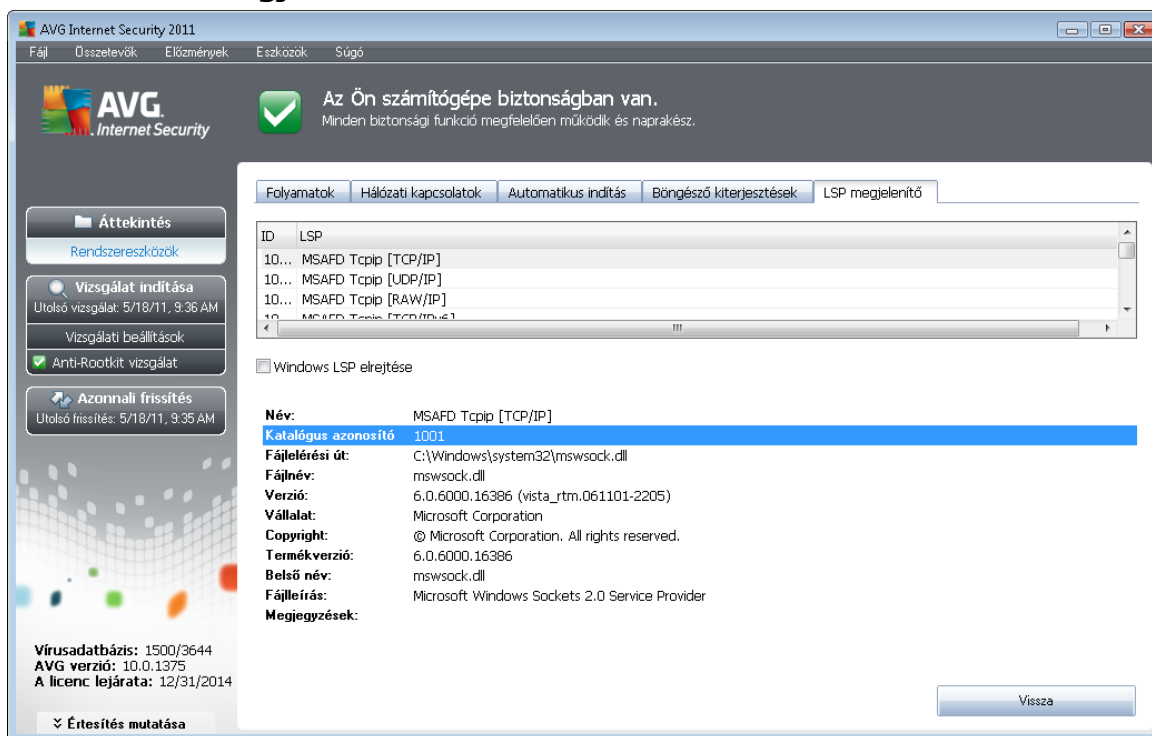
A **Böngésző kiterjesztések** panel az internetböngészőben telepített bővítmények (alkalmazások) listáját jeleníti meg. A listában a szabályos bővítmények és a lehetséges rosszindulatú programok egyaránt előfordulhatnak. Kattintson egy objektumra a listában a kiválasztott bővítménnyel kapcsolatos részletes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

Vezérlogombok

A vezérlogombok a **Böngészőkiterjesztés** lapon 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** - ez a gomb visszaviszi Önt az alapértelmezett [AVG felhasználói felületre](#) (összetevők áttekintése)

7.15.5. LSP megjelenítő



Az **LSP nézokepanel** megjeleníti a réteges szolgáltatók (LSP) listáját.

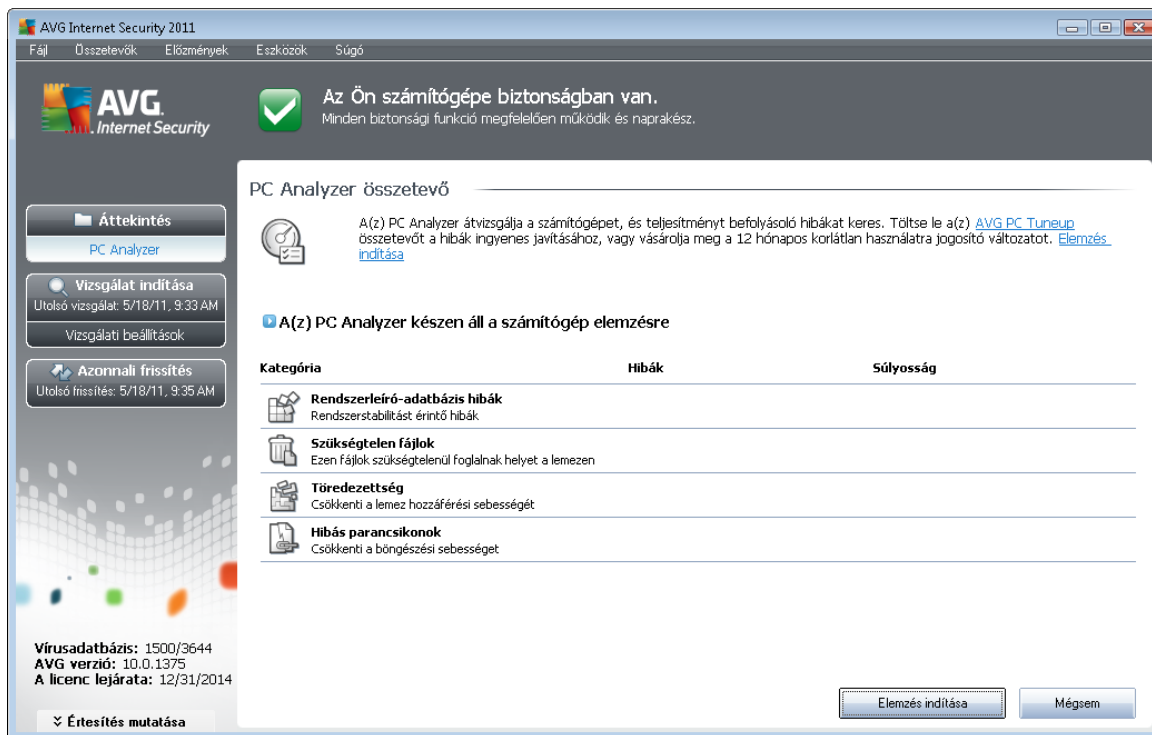
A **réteges szolgáltató** (LSP) a Windows operációs rendszer hálózati szolgáltatásaihoz kapcsolódó rendszerilleszto. A program hozzáfér a számítógép összes bejövő és kimenő adatához, és módosíthatja is ezeket. Bizonyos LSP programokra feltétlenül szükség van ahhoz, hogy a Windows kapcsolódni tudjon más 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.

A Windows LSP listában való megjelenítéséhez törölje a jelet a **Windows LSP elrejtése** jelölőnégyzetből. A **Vissza** gomb visszaviszi Önt a alapértelmezett **AVG felhasználói felületre** (összetevők áttekintése).

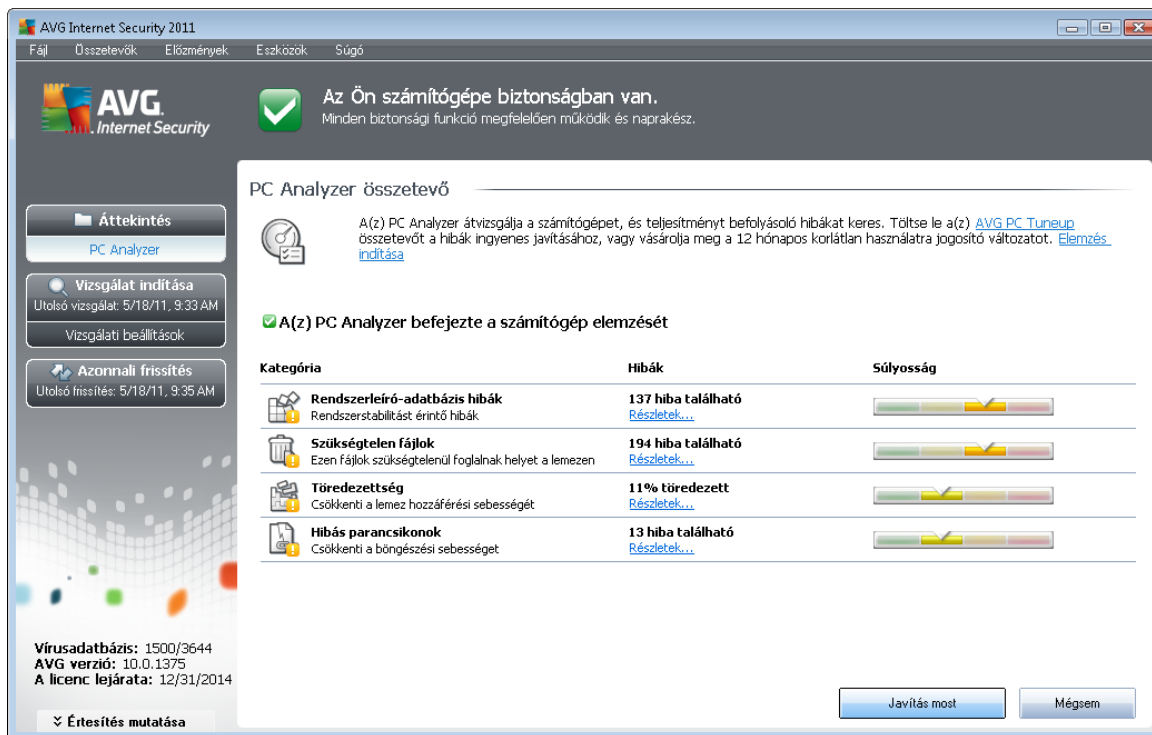
7.16. PC Analyzer

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** rész kiszámítja a merevlemez töredezettségének százalékos mértékét (a legtöbb fájl olyan régen volt használva, hogy azok a fizikailag a lemez több részén helyezkednek el töredékek formájában). 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.

Vezérlogombok

- **Elemzés** (az elemzés indítása előtt jelenik meg) – kattintson erre a gombra a számítógép azonnali elemzésének indításához
- **Javítás** (az elemzés befejezése előtt jelenik meg) - nyomja meg ezt a gombot az AVG weboldalára (<http://www.avg.hu/>) történő ugráshoz, ahol részletes és naprakész információkat tekinthet meg a **PC Analyzer** összetevőről
- **Mégsem** - nyomja meg ezt a gombot a folyamatban lévő elemzés leállításához és az alapértelmezett **AVG felhasználói felületre** (összetevők áttekintése) részre történő visszatéréshez az elemzés befejezése után

7.17. ID Protection

Az **AVG Identity Protection** olyan kártevők elleni összetevő, amely megakadályozza, hogy tolvajok jelszavakat, banki adatokat, hitelkártyaszámokat és egyéb személyes digitális adatokat lopjanak el különféle kártevők segítségével (*malware*). A program meggyőződik arról, hogy minden alkalmazás megfelelően működik a számítógépen. Az **AVG Identity Protection** folyamatosan észleli és letiltja a gyanús viselkedést, és védi az Ön számítógépét a legújabb kártevőktől.

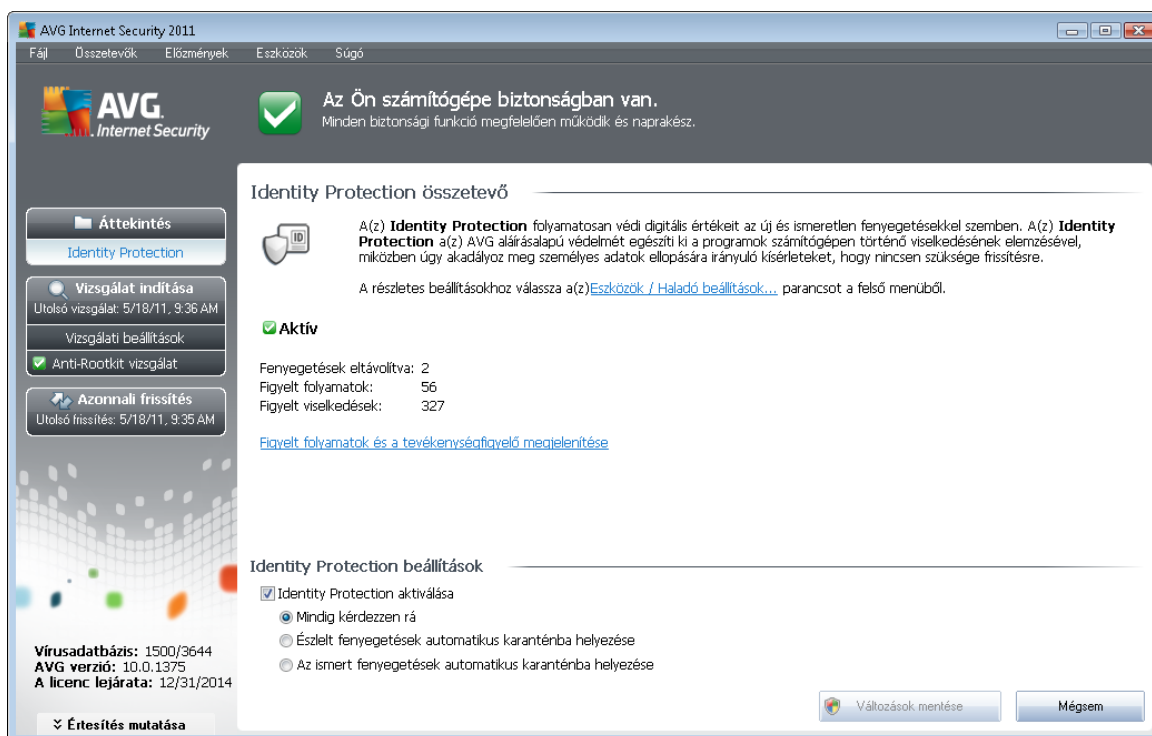


7.17.1. ID Protection alapelvek

Az **AVG Identity Protection** olyan kártevők elleni összetevő, amely mindenféle káros program ellen véd (kémprogram, bot, személyes adatok eltulajdonítása stb.), viselkedésalapú technológiát használ, és azonnali védelmet biztosít a legújabb vírusok ellen. A kártevők egyre kifinomultabbak, és olyan programokkal együtt érkezhettek, amelyek megnyitják a rendszert egy távoli támadó számára, az **AVG Identity Protection** mégis garantáltan képes megvédeni Önt ezen kártevőktől. A termék azt az **AVG Anti-Virus** terméket egészíti ki, amely fájlalapú védelemmel rendelkezik, és ismert vírusok ellen véd aláírásalapú mechanizmussal és vizsgálattal.

Különösen javasoljuk, hogy az **AVG Anti-Virus és az **AVG Identity Protection** terméket is telepítse a számítógép teljeskörű védelméhez.**

7.17.2. ID Protection felület



Az **Identity Protection** összetevő felületén megtalálja a működéssel, az állapottal kapcsolatos információkat, illetve néhány statisztikai adatot:

- **Eltávolított káros programok** - megjeleníti a káros 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 figyelo megjelenítése** linket, amely a **Rendszereszközök** összetevő felhasználói felületére irányítja Önt, ahol megtekintheti az összes figyelt folyamat részletes áttekintését.



Identity Protection beállítások

Az ablak alsó részén megtalálhatja az **Identity Protection beállításokat**, ahol megadhatja az összetevő alapszintű beállításait:

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

Bizonyos esetekben az **Identity Protection** egyes legitim fájlokat gyanúsak 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:

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

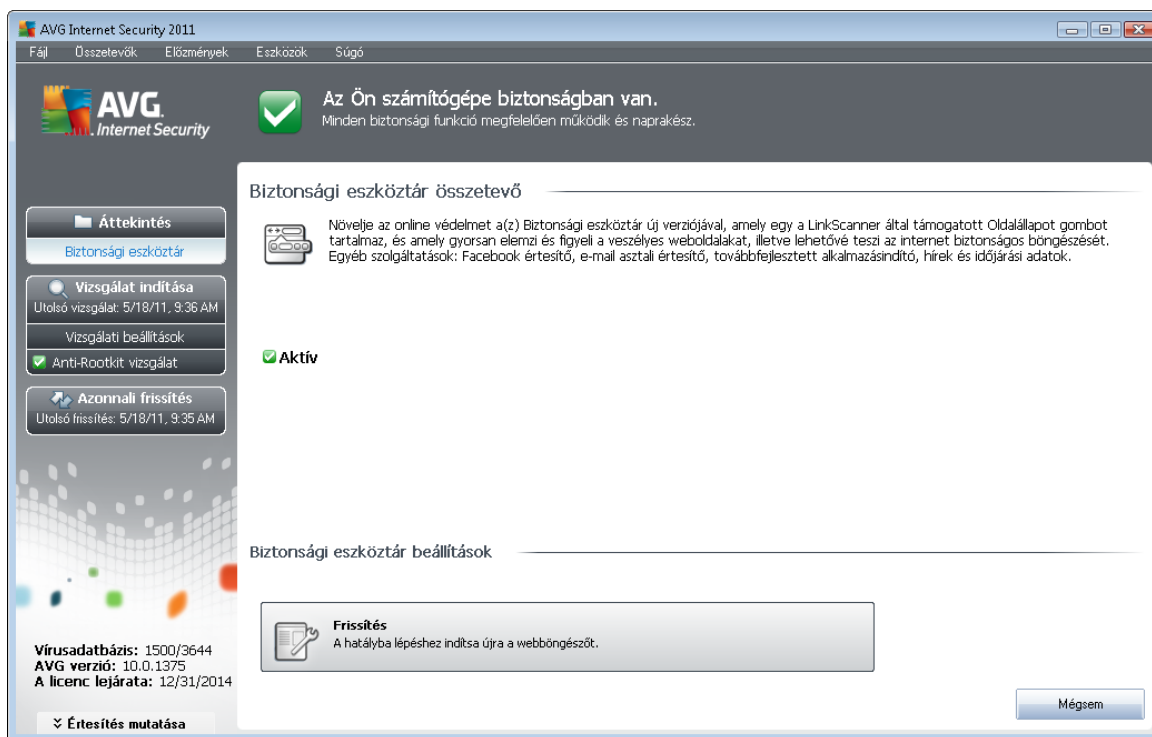
Vezérlogombok

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

- **Változások mentése** - nyomja meg ezt a gombot a mentéshez és a változtatások alkalmazásához
- **Mégsem** - nyomja meg ezt a gombot az alapértelmezett [AVG felhasználói felületre](#) történő visszatéréshez (összetevők áttekintése)

7.18. Biztonság eszköztár

A **Biztonsági eszköztár** egy választható böngészői eszköztár, amely továbbfejlesztett AVG védelmet és különböző hasznos szolgáltatásokat nyújt a webböngészés során. A **Biztonsági eszköztár** jelenleg kizárólag az Internet Explorer (6.0 vagy újabb) és a Mozilla Firefox (3.0 vagy újabb) böngészőket támogatja:



A **Biztonság eszköztár** összetevő beállításai közvetlenül a [Biztonság eszköztár](#) részen érhetők el a webböngészőben.



8. AVG Biztonság eszköztár

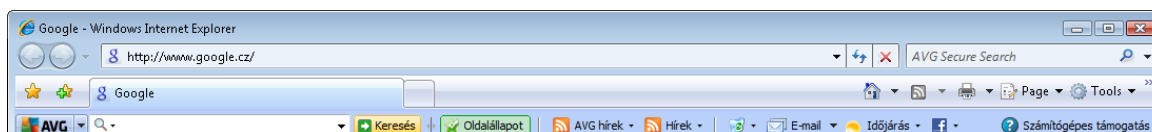
Az **AVG Biztonság eszköztár** egy olyan új eszköz, amely a [LinkScanner](#) összetevővel működik együtt. Az **AVG Biztonság eszköztár** használhatja a [LinkScanner](#) funkcióinak és viselkedésének szabályozásához.

Ha bekapcsolja az eszköztárat az **AVG Internet Security 2011** telepítése során, akkor az automatikusan beépül a webböngészőbe (*Internet Explorer 6.0 és Mozilla Firefox 3.0 vagy újabb*). Más internetböngészők jelenleg nem támogatottak.

Megjegyzés: Ha más böngészőt használ (pl. Avant Browser), akkor a program váratlanul viselkedhet.

8.1. AVG Biztonság eszköztár felület

Az **AVG Biztonság eszköztár** úgy terveztük, hogy együttműködjön az **MS Internet Explorerrel** (6.0 verzió vagy újabb) és a **Mozilla Firefox-szal** (3.0 verzió vagy újabb). Ha telepítette az **AVG Biztonság eszköztárat** (az [AVG telepítése során](#) a program rákérdez, hogy kívánja-e telepíteni az összetevőt), akkor az összetevő a webböngészőben a címsor alatt található:



Az **AVG Biztonság eszköztár** a következőket tartalmazza:

8.1.1. AVG logó gomb

Ez a gomb általános eszköztár elemekhez nyújt hozzáférést. Kattintson a logó gombra az [AVG weboldala](#) történő ugráshoz. Az AVG ikon melletti mutatóra való kattintás a következőket nyitja meg:

- **Eszköztár info** - hivatkozás az **AVG Biztonság eszköztár honlapra**, mely részletes információkat nyújt az eszköztár védelmével kapcsolatban
- **AVG indítása** - megnyitja az **AVG Internet Security 2011 felhasználói felületet**
- **AVG adatok** - megnyit egy helyi menüt a következő linkekkel, amelyek fontos biztonsági információkat tartalmaznak a következővel kapcsolatban **AVG Internet Security 2011**:
 - o **Információk a fenyegetésekről** - megnyitja az [AVG weboldalt](#), ahol megtalálhatja a legfontosabb adatokat a legveszélyesebb fenyegetésekről, a víruseltávolítási ajánlásokról, az AVG frissítési információkról, illetve megtekintheti a [Vírusadatbázist](#) és további kapcsolódó információkat
 - o **AVG hírek** - megnyitja az AVG aktuális hírekkel kapcsolatos weboldalt
 - o **Aktuális fenyegetettségi szint** - megnyitja a víruslabor weboldalt, ahol grafikus formában ellenőrizheti az aktuális fenyegetettségi szintet az interneten



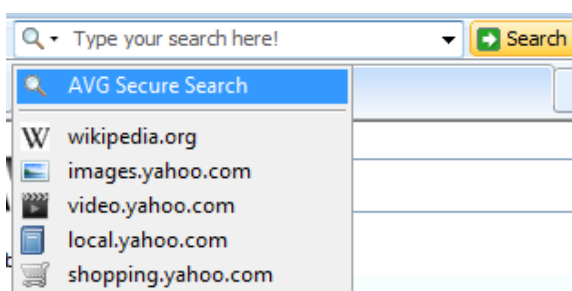
o *AVG Víruslabor* - megnyitja az [AVG webhelyjelentések](#) weboldalt, ahol név szerint kereshet az adott fenyegetések között, illetve részletes információkat kaphat róluk

- **Beállítások** - megnyit egy beállítási panelt, ahol módosíthatja az **AVG Biztonság eszköztár** beállításait saját igényeinek megfelelően - lásd a következő [AVG Biztonság eszköztár beállításai címu fejezetet](#)
- **Elozmények törlése** - lehetővé teszi az **AVG Biztonság eszköztárban** az összes elozmény törlését, vagy csak a keresési elozmények, a böngészési elozmények, a letöltési elozmények vagy a sütik törlését.
- **Frissítés** - frissítéseket keres az **AVG Biztonság eszköztárhoz**
- **Súgó** - lehetővé teszi a súgófájl megnyitását, a kapcsolatfelvételt az [AVG muszaki támogatással](#), termékviisszajelzések küldését, vagy részletek megtekintését az eszköztár aktuális verziójával kapcsolatban.

8.1.2. AVG Secure Search (powered by Google) keresotechnológia

A(z) **AVG Secure Search (powered by Google)** kereso egyszeru és biztonságos módja az internetes keresésnek a(z) **AVG Secure Search (powered by Google)** segítségével. Írjon be egy szót vagy egy mondatot a keresodobozba, majd kattintson a **Keresés** gombra, vagy nyomja meg az **Enter** billentyűt a(z) **AVG Secure Search (powered by Google)** oldalán történő keresés indításához a jelenleg megjelenített oldaltól függetlenül. A keresodoboz a keresési elozményeket is listázza. A keresodobozban indított kereséseket az [keresés védelem](#) védelem elemzi.

A keresomezoben átválthat a Wikipediára, vagy egyéb keresoszolgáltatásra is - lásd a képet:



8.1.3. Oldalállapot

Ez a rész az aktuálisan megjelenített weboldal értékelését jeleníti meg a [Böngészés védelem](#) összetevő alapján:

- - A hivatkozott oldal biztonságos
- - Az oldal gyanús.
- - Az oldal veszélyes weblapokra mutató linkeket tartalmaz.
- - A linkelt oldal aktív fenyegetést jelent! Saját biztonsága érdekében nem engedélyezett



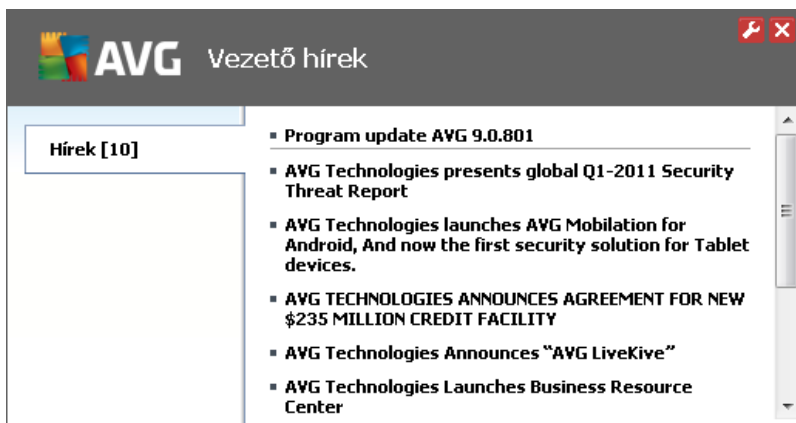
az oldal meglátogatása.

-  - A oldal nem elérhető, ezért nem lehet ellenőrizni.

Kattintson erre a gombra egy információs panel megnyitásához az adott weboldal részletes adataival kapcsolatban.

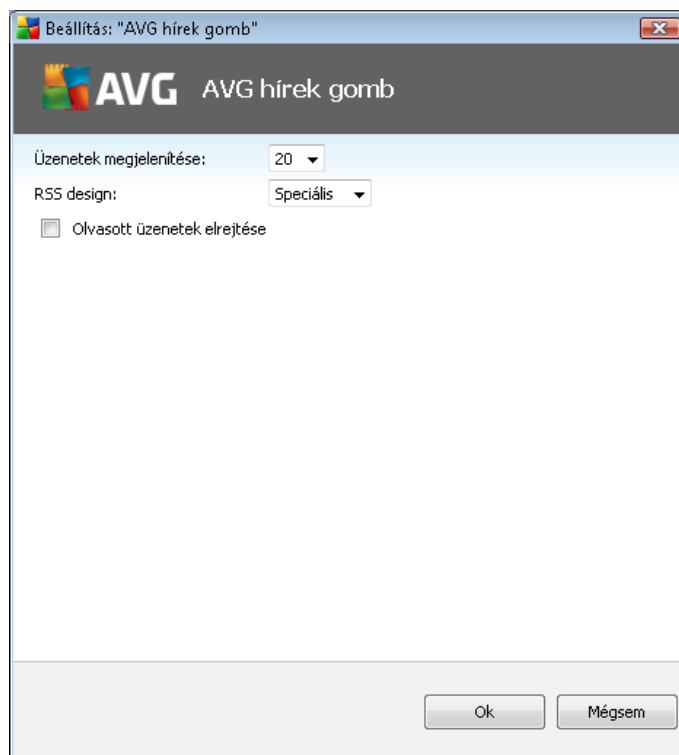
8.1.4. AVG hírek

A közvetlenül az **AVG Biztonság eszköztár**on található gomb megjeleníti az aktuális **AVG hírek** , beleértve a sajtóhíreket és a vállalati sajtóközleményeket:



A jobb felső sarokban két piros vezérlogombot láthat:

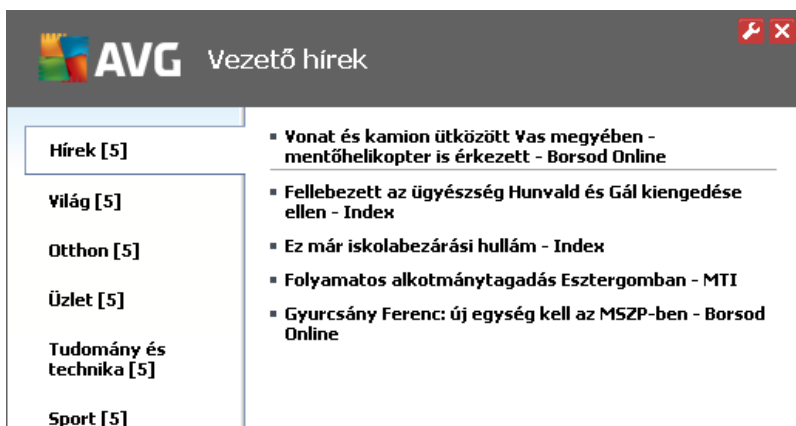
-  - ez a gomb a szerkesztőpanelt nyitja meg, ahol meghatározhatja az **AVG hírek** paramétereit (a gomb az **AVG Biztonság eszköztár**on jelenik meg):



- o **Üzenetek megjelenítése** - módosíthatja az egyszerre megjeleníthető üzenetek számát
- o **RSS design**- válassza ki a hírek haladó/alapszintű megjelenítési módját (*alapállapotban a Haladó mód van kiválasztva - lásd a fenti képet*)
- o **Olvasott üzenetek elrejtése** - ezen opcióval módosíthatja az olvasott üzenetek állapotát, így csak az új üzenetek lesznek megjelölve
-  - kattintson erre a gombra a jelenleg megnyitott hírek bezárásához

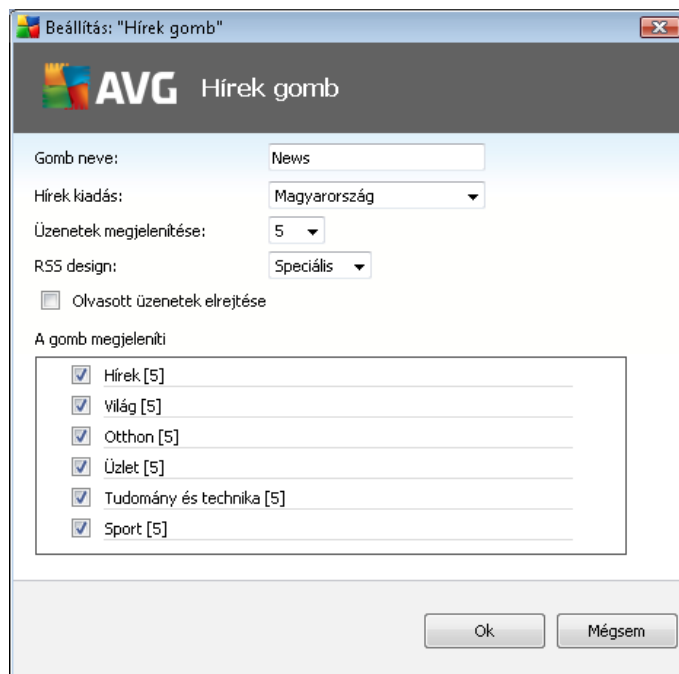
8.1.5. Hírek

Az **AVG Biztonság eszköztár**on található gombbal megnyithatja a különböző médiumok aktuális híreit különböző részekre csoportosítva:



A jobb felső sarokban két piros vezérlogobot láthat:

-  - ez a gomb egy olyan szerkesztőpanelt nyit meg, ahol meghatározhatja a **Hírek** paramétereit az **AVG Biztonság eszköztár**on:



- o **Gomb neve** - módosíthatja a gomb nevét, ahogyan az megjelenik az **AVG Biztonsági eszköztár**on
- o **Hírforrás** - válasszon egy országot a listáról az adott régióból történő hírek megjelenítéséhez
- o **Üzenetek megjelenítése** - adja meg az egyszerre megjeleníthető üzenetek kívánt számát
- o **RSS megjelenítés** - válthat az alapszintu/haladó híráttekintés között (**a haladó megjelenítés van**)

alapállapotban bekapcsolva, lásd a fenti képet)

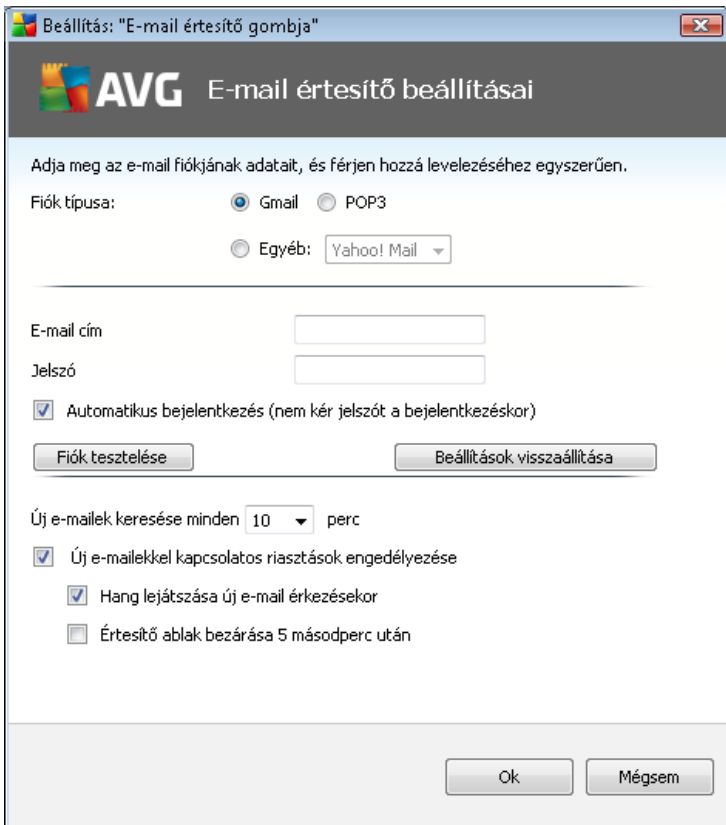
- o **Olvasott üzenetek elrejtése** - ezen opcióval módosíthatja az olvasott üzenetek állapotát, így csak az új üzenetek lesznek megjelölve
- o **Hírfajták** - ezen a részen megadhatja, hogy milyen híreket jelenítsen meg a rendszer a **AVG Biztonság eszköztár**
 -  - kattintson erre a gombra a jelenleg megnyitott hírek bezárásához

8.1.6. Elozmények törlése

Ezzel a gombbal törölheti a böngésző elozményeit az **AVG logó -> Elozmények törlése** opcióhoz hasonlóan.

8.1.7. E-mail értesítő

Az **E-mail értesítő** gomb lehetővé teszi, az újonnan kapott e-mail üzenetekről való értesítés bekapcsolását az [AVG Biztonság eszköztár](#) felületén. A gomb a következő szerkesztőablakot nyitja meg, ahol megadhatja az e-mail fiókjának adatait és a megjelenítési szabályokat. Kövesse a párbeszédpanelen megjelenő utasításokat:



- **Fiók típusa** - Adja meg az e-mail fiók által használt protokoll típusát. A következő lehetőségek közül választhat: *Gmail*, *POP3*, vagy válassza ki a szerver nevét a legördülő menüből az *Egyéb* részen (*jelenleg csak Yahoo! JP Mail vagy Hotmail*). Ha nem tudja, hogy a fiók milyen kiszolgáló típust használ, akkor vegye fel a kapcsolatot az e-mail szolgáltatóval vagy az internetszolgáltatóval.

- **Bejelentkezés** - Az alábbi részen adja meg az *e-mail címét* és az ahhoz tartozó *jelszót*. Jelölje be az *Automatikus bejelentkezés* opciót, ha nem akarja minden alkalommal megadni azt.
- **Fiók tesztelése** - Használja ezt gombot a megadott adatok ellenőrzéséhez.
- **Beállítások visszaállítása** - Eltávolítja a fent megadott e-mail címet.
- **Új e-mailek ellenőrzése ... percnként** - Meghatározhatja az új e-mail üzenetek ellenőrzéséhez tartozó idoközt (*5-120 perc között*), és megadhatja, hogy miként kíván értesülni új üzenetek érkezéséről.
- **Új e-mail értesítések engedélyezése** - Törölje ezt a jelölőnégyzetet az új e-mailekrol szóló értesítések letiltásához.
 - o **Hangjelzés új e-mailek érkezésekor** - Törölje ezt a jelölőnégyzetet a hangjelzések letiltásához új e-mailek érkezésekor.
 - o **Értesítési ablak bezárása 5 másodperc után** - Jelölje be az értesítési ablak 5 másodperc utáni bezárásához új e-mailek érkezésekor.

8.1.8. Időjárési adatok

Az **Időjárás** gomb (*információkat jelenít meg az aktuális hőmérsékletrol 3-6 óránként frissítve*) a kiválasztott helyen az **AVG Biztonság eszköztár** felületén. Kattintson erre a gombra egy új panel megnyitásához a részletes időjárési adatokkal:



Brno, CZ
[[hely módosítása](#)]

 **26° C**

Szél sebessége: 19,31 km/h
Napkelte: 05:04
Napnyugta: 20:34

 PÉN Magas: 24 °C Alacsony: 14 °C	 SZO Magas: 25 °C Alacsony: 14 °C
---	---

Frissítve 05/20/2011 14:42:38 **YAHOO! NEWS** [Teljes előrejelzés >](#)

Itt a következő lehetőségeket találja:

- **Hely módosítása** - kattintson a **Hely módosítása** részre a **Hely keresése** párbeszédpanel megnyitásához. Adja meg a kívánt helyet, vagy erősítse meg a **Keresés** gombra történő kattintással. Ezután az egyező helyek listája megjelenik, és Ön kiválaszthatja a kívánt helyet. Az információs panel ismét megjelenik, és immár a kiválasztott hely időjárási

adatait mutatja.

- **Fahrenheit / Celsius konvertálás** - az információs panel jobb felső részén választhat a Fahrenheit és a Celsius értékek között. Az időjárási adatok a kiválasztott hőmérsékleti skála alapján jelennek meg.
- **Teljes előrejelzés** - ha érdekli a teljes és részletes előrejelzés, akkor használja a **Teljes előrejelzés** linket, amely átirányítja Önt a megfelelő weboldalra.

8.1.9. Facebook

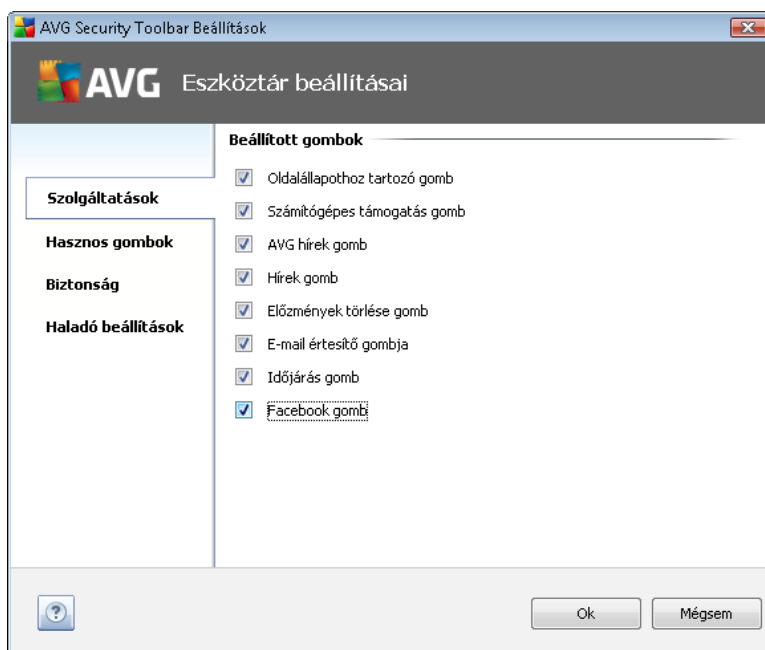
A **Facebook** gomb lehetővé teszi, hogy közvetlenül csatlakozzon a [Facebook](#) közösségi hálózathoz az **AVG Biztonság eszköztárról**. Kattintson a gombra, ekkor megjelenik a bejelentkezési értesítő. Kattintson ismét ide a **Facebook bejelentkezés** panel megnyitásához. Adja meg az adatokat, majd nyomja meg a **Csatlakozás** gombot. Ha még nincsen [Facebook](#) fiókja, akkor létrehozhat egyet közvetlenül a **Regisztráció a Facebook-on** linkre.

Miután végzett a [Facebook](#) regisztrációs folyamattal, engedélyezheti az **AVG közösségi bővítmény** alkalmazást. Ez az alkalmazás elengedhetetlen az eszköztár használatához - [Facebook](#) kapcsolathoz, ezért kapcsolja be, és engedélyezze azt. Ekkor a [Facebook](#) kapcsolat aktiválódik és a **Facebook** gomb az **AVG Biztonság eszköztáron** megjeleníti a szokásos [Facebook](#) menü lehetőségeket.

8.2. AVG Biztonság eszköztár beállítások

Az összes **AVG Biztonság eszköztár** paraméter közvetlenül elérhető az **AVG Biztonság eszköztár** panelen. A szerkesztőfelület az **AVG / Beállítások** menüelemen nyílik meg **Eszköztár beállításai** néven, és négy részből áll:

8.2.1. Általános fül

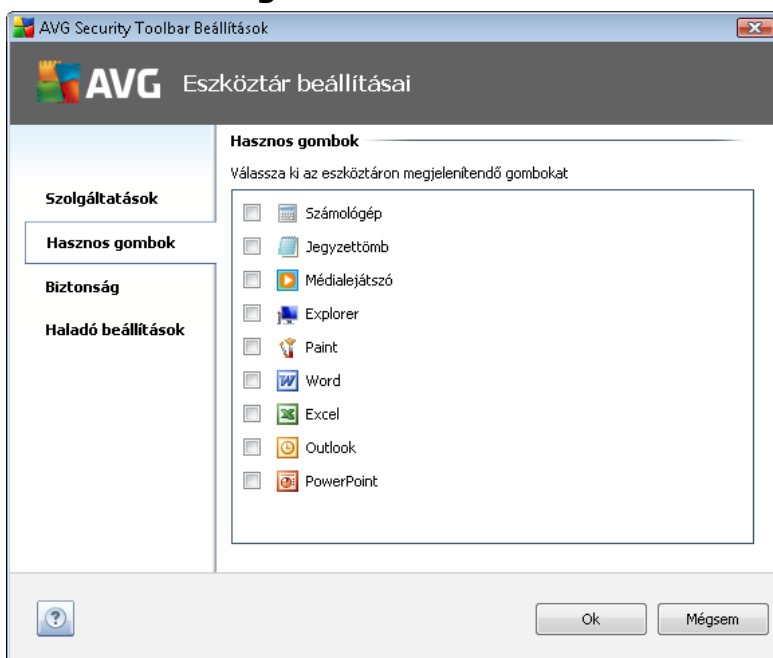




Ezen a lapon meghatározhatja, hogy mely gombok jelenjenek meg vagy legyenek elrejtve az **AVG Biztonság eszköztár** panelen. Jelölje be az adott gombot, ha megszeretné azt jeleníteni. Az alábbiakban az egyes gombok leírását találja:

- **Oldalállapot gomb** - ez a gomb lehetővé teszi információk megjelenítését a jelenleg megnyitott oldal biztonsági állapotáról az **AVG Biztonság eszköztáron**
- **AVG hírek** - megnyitja az AVG aktuális hírekkel kapcsolatos weboldalát
- **Hírek gomb** - aktuális hírek a napi sajtóból
- **Elozmények törlése gomb** - ez a gomb lehetővé teszi, hogy törölje az összes elozményt, vagy csak a keresési elozményt, böngészési elozményt, letöltési elozményt , sütiket közvetlenül az AVG Biztonság eszköztár panelen
- **E-mail értesítő gomb** - ezzel a gombbal megjeleníthető az újonnan érkezett e-mail üzeneteket az **AVG Biztonság eszköztár** felületén
- **Idojárás gomb** - ezzel a gombbal megjelenítheti az aktuális idojárást a kiválasztott helyen
- **Facebook gomb** - ez a gomb közvetlen kapcsolatot biztosít a [Facebook](#) közösségi hálózathoz

8.2.2. Hasznos gombok fül



A **Hasznos gombok** fül lehetővé teszi alkalmazások kiválasztását, valamint azok ikonjainak megjelenítését az eszköztáron. Ezen ikonok gyorsgomboként szolgálnak az adott alkalmazás azonnali indításához.

8.2.3. Biztonság fül

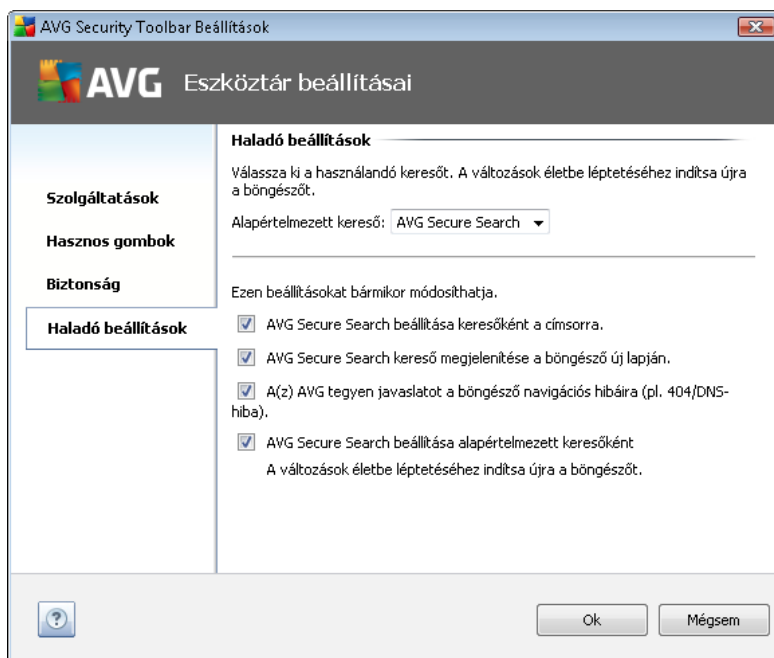


A **Biztonság** lap két részre van osztva: **AVG böngészővédelem** és **Értékelések**, ahol bejelölheti a megfelelő jelölőnyegzeteket az **AVG Biztonság eszköztár** használatához:

- **AVG Böngészés védelem** - jelölje be ezt az elemet az [AVG Keresővédelem](#) és/vagy [Böngészés védelem](#) szolgáltatás be- vagy kikapcsolásához
- **Értékelések** - válassza ki azon ikonokat, amelyet az [Keresővédelem](#) összetevő a keresési eredmények értékelésére fog használni:
 - o  az oldal biztonságos
 - o  az oldal gyanús
 - o  az oldal veszélyes weblapokra mutató linkeket tartalmaz
 - o  az oldal aktív fenyegetéseket tartalmaz
 - o  az oldal nem érhető el, ezért nem lehet ellenőrizni

Jelölje be a megfelelő opciót, ha értesülni szeretne az adott fenyegetési szintről. Az aktív és veszélyes fenyegetéseket tartalmazó oldalakra figyelmeztető piros színű jelzéseket nem lehet kikapcsolni. **Javasoljuk, hogy tartsa meg a program által felajánlott alapértelmezett beállításokat.**

8.2.4. Haladó beállítások fül



A **Haladó beállítások** fülön válassza ki az alapértelmezett keresomotort. A következők közül választhat: *AVG Secure Search (powered by Google)*, *Baidu*, *WebHledani*, *Yandex* és *Yahoo! JP*. Miután módosította az alapértelmezett keresomotort indítsa újra a böngészőt a változások életbe léptetéséhez.

Bekapcsolhatja, vagy kikapcsolhatja az adott **AVG Biztonság eszköztár** beállításait (a felsorolt lehetőségek az alapértelmezett *AVG Secure Search (powered by Google)* beállításokra vonatkoznak):

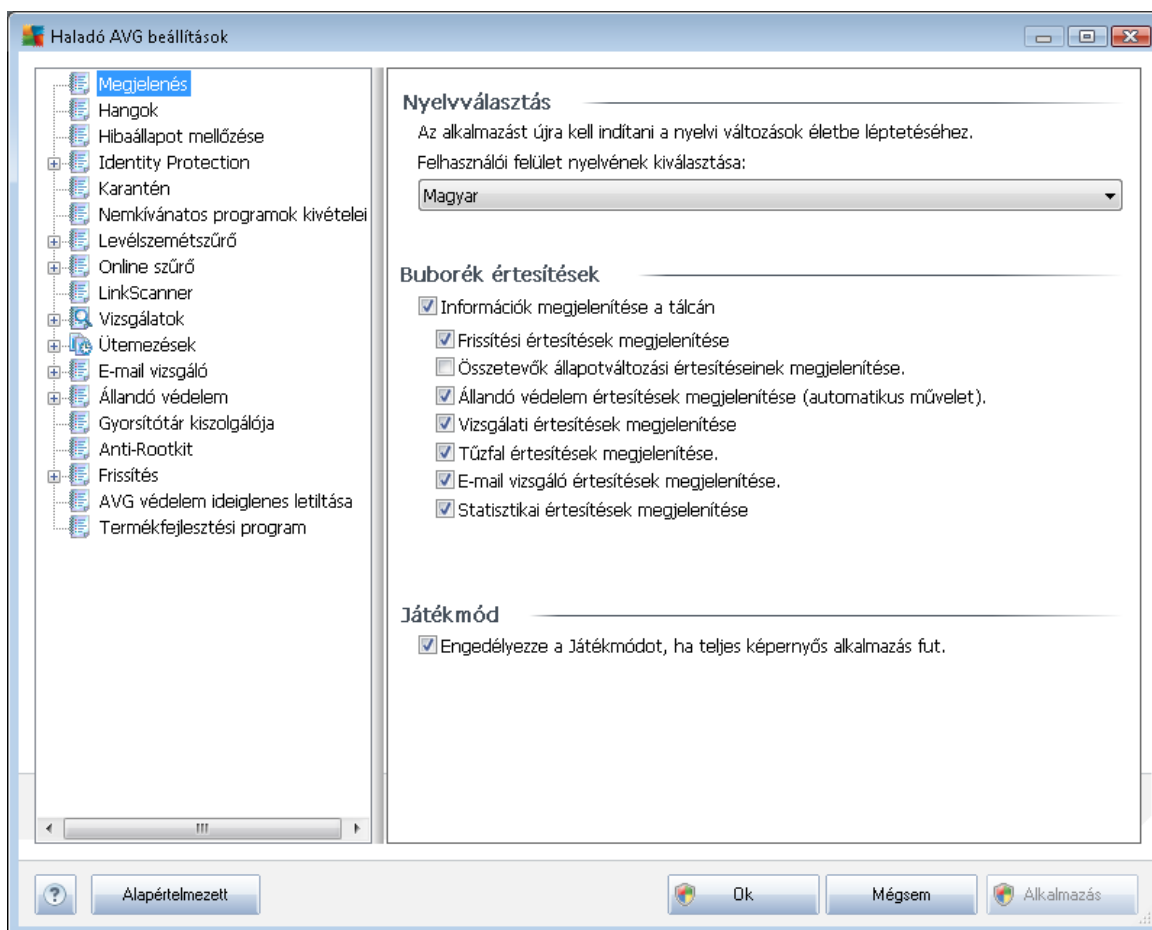
- **Legyen az AVG Secure Search (powered by Google) kereso a címsoron** - ha bejelöli, akkor a címsorba közvetlenül írhat be keresoszavakat, és a Google automatikusan átirányítja Önt a megfelelő weboldalak találataira.
- **Az AVG tegyen javaslatokat a navigálási hibákkal kapcsolatban (404/DNS)** - ha keres az interneten és egy nem működő weboldalra bukkan, vagy egy adott oldalt nem lehet megjeleníteni (404-es hiba), akkor a rendszer átirányítja Önt egy olyan weboldalra, ahol kapcsolódó oldalak közül választhat.
- **Legyen a(z) AVG Secure Search (powered by Google) az alapértelmezett keresomotor** - a Google az alapértelmezett keresomotor a webes keresésekhez az **AVG Biztonság eszköztáron**, ezen opció aktiválásával ez a szolgáltatás lesz a webböngésző alapértelmezett keresője is.

9. AVG Haladó beállítások

Az **AVG Internet Security 2011** 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 szerkesztoablak a jobb oldalon.

9.1. Megjelenés

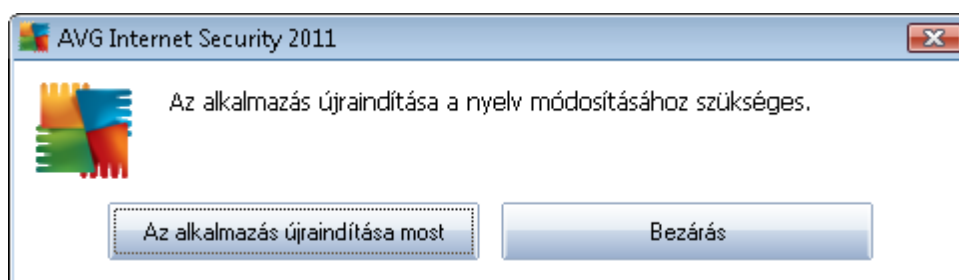
Az első elem, a **Megjelenés** az [AVG felhasználói felület](#) általános beállításaira illetve az alkalmazás viselkedésének néhány alapvető funkciójára vonatkozik:



Nyelvválasztás

A **Nyelvválasztás** részben kiválaszthatja a használni kívánt nyelvet a legördülő menübol. Ekkor az adott nyelv lesz használva a teljes [AVG felhasználói felületen](#). A legördülő menü csak azon nyelveket ajánlja fel, amelyet a [telepítési folyamat](#) során kiválasztott (lásd az [Egyéni beállítások](#) fejezetet), illetve az angol nyelvet (amely alapállapotban telepítve van). A felhasználói felület nyelvének megváltoztatásához újra kell indítani a programot. Ehhez kövesse az alábbi lépéseket:

- Válassza ki a program kívánt nyelvét, majd a megerosítéshez nyomja meg az **Alkalmaz** gombot (jobb alsó sarok)
- Nyomja meg az **OK** gombot a megerosítéshez
- Egy új párbeszédpanel jelenik meg, amely értesíti Önt, hogy az AVG felületének módosításához az alkalmazás újraindítása szükséges:



Buborék értesítések

Ebben a részben letilthatja a rendszerterületen megjelenő buborék értesítéseket az alkalmazás állapotával kapcsolatban. Alapértelmezés szerint a buborék értesítések megjelennek. A beállítás megtartása ajánlott! A buborék értesítések jellemzően az AVG összetevők állapotváltozásáról tájékoztatnak, és érdemes odafigyelni rájuk.

Ha valamilyen okból úgy dönt, hogy nem szeretné ezen értesítéseket megjeleníteni, vagy csak néhányat kapcsolna be közülük (bizonyos AVG összetevőnél), akkor ezeket a következő opciók be- és kikapcsolásával határozhatja meg:

- **Információk megjelenítése az értesítési területen** - alapértelmezés szerint ez az elem be van kapcsolva (*be van jelölve*), és az értesítések megjelennek. Ne jelölje be ezt az elemet, ha ki akarja kapcsolni az összes buborék értesítést. Ha be van kapcsolva, akkor kiválaszthatja, hogy milyen értesítések jelenjenek meg:
 - o **Értesítések megjelenítése a frissítésekkel kapcsolatban** - határozza meg, hogy az AVG frissítés indításával, magával a folyamattal illetve a befejezéssel kapcsolatban jelenjenek-e meg értesítések;
 - o **Összetevők állapotváltozásával kapcsolatos értesítések megjelenítése** - határozza meg, hogy az összetevők működésével/nem működésével vagy lehetséges problémákkal kapcsolatban jelenjenek-e meg értesítések. Egy AVG összetevő hibaállapotával kapcsolatos jelentés során ez az opció egyenértékű az értesítési terület ikonjának hibajelzésével (színváltozás);
 - o **Az Állandó védelemmel kapcsolatos értesítések megjelenítése (automatikus muvelet)** - azt határozza meg, 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).



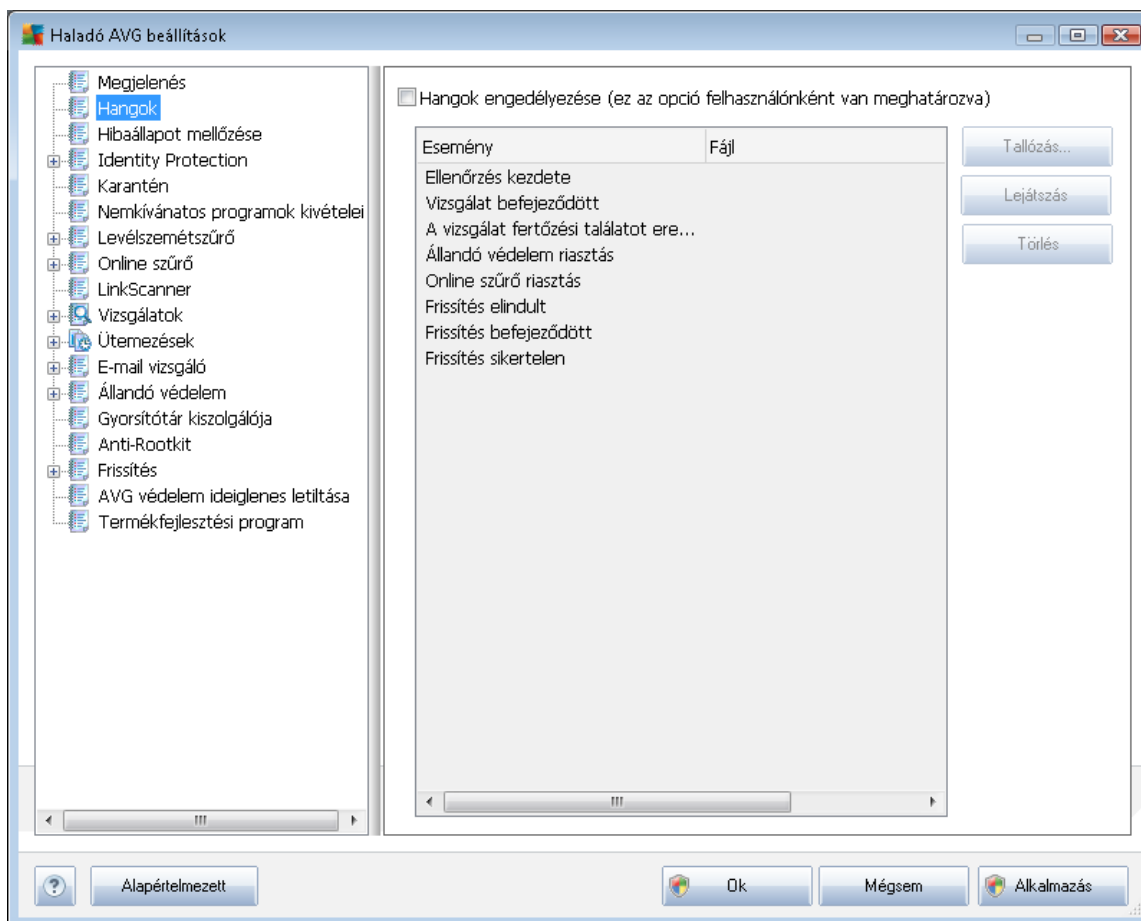
- o **Értesítések megjelenítése a vizsgálatokkal kapcsolatban** - az ütemezett vizsgálat indításával, magával a folyamattal, illetve az eredményekkel kapcsolatos értesítéseket jeleníti meg.
- o **Tuzfallal kapcsolatos értesítések megjelenítése** - határozza meg, hogy a tuzfal állapotával és folyamataival kapcsolatos értesítések, pl. az összetevő be- és kikapcsolásával kapcsolatos figyelmeztetések, adatforgalom esetleges blokkolása stb. megjelenjenek-e vagy sem;
- o **E-mail vizsgálóval kapcsolatos értesítések megjelenítése** - a bejövő és kimenő e-mailek vizsgálatakor megjelenő üzenetek megjelenítését határozza meg.
- o **Statistikai értesítések megjelenítése** - jelölje be rendszeres statisztikai értesítések megjelenítéséhez a tálcán.

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** panelen beállíthatja, hogy szeretne-e hangokat hozzárendelni bizonyos AVG műveletekhez. Ha igen, akkor jelölje be a **Hangos értesítések engedélyezése** opciót *(alapállapotban kikapcsolva)* egyes AVG műveletekhez:

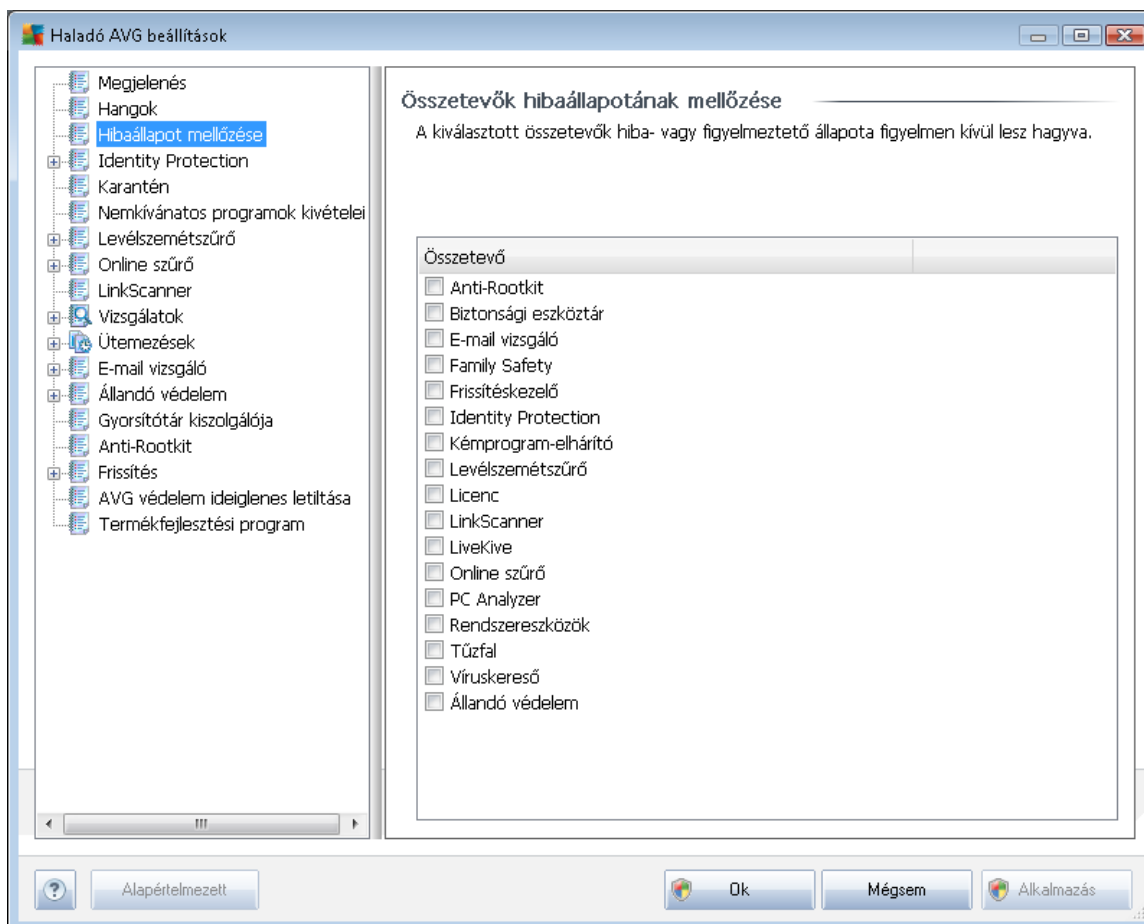


Válassza ki a kívánt eseményt a listából, majd keresse meg (**Tallózás**) a hozzárendelendő hangfájlt. A kiválasztott hang lejátszásához jelölje ki az adott eseményt a listában, majd nyomja meg a **Lejátszás** gombot. Használja a **Törlés** gombot a hang és az adott esemény társításának megszüntetéséhez.

Megjegyzés: Csak *.wav hangfájlok támogatottak!

9.3. Hibaállapot mellozése

Az **Összetevők hibaállapotának mellozése** panelen bejelölheti azokat az 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 foablakán

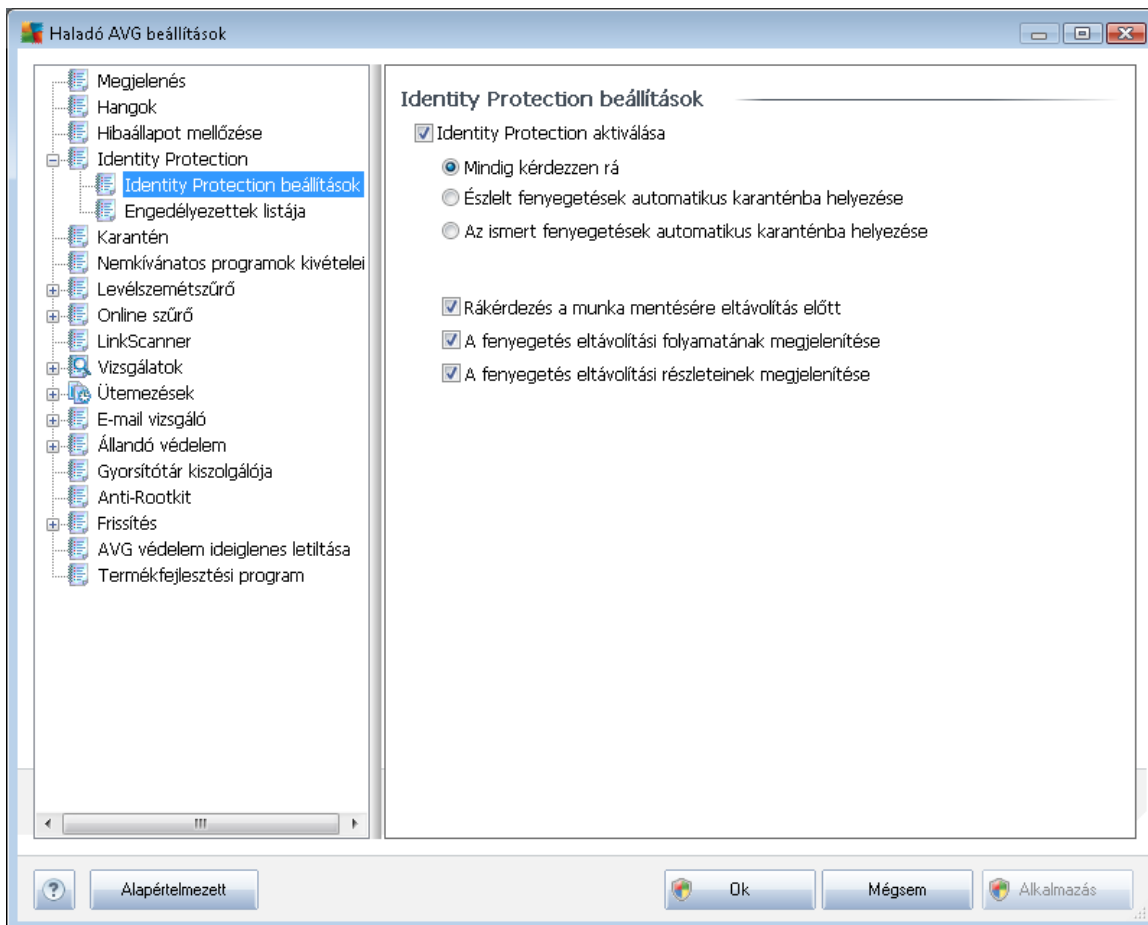
Elképzelhető olyan szituáció, hogy valamilyen okból átmenetileg ki kell kapcsolnia egy összetevőt (ez nem javasolt, az összes összetevőt bekapcsolva kell tartania, de átmenetileg előfordulhat ilyen helyzet). Ekkor a rendszerikon automatikusan jelzi az összetevő hibaállapotát. Ebben az esetben viszont 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 **Összetevő állapotának mellozése** opció közvetlenül is elérhető az [összetevők áttekintése](#) részen az **AVG** foablakában.

9.4. Azonosság védelem

9.4.1. 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.

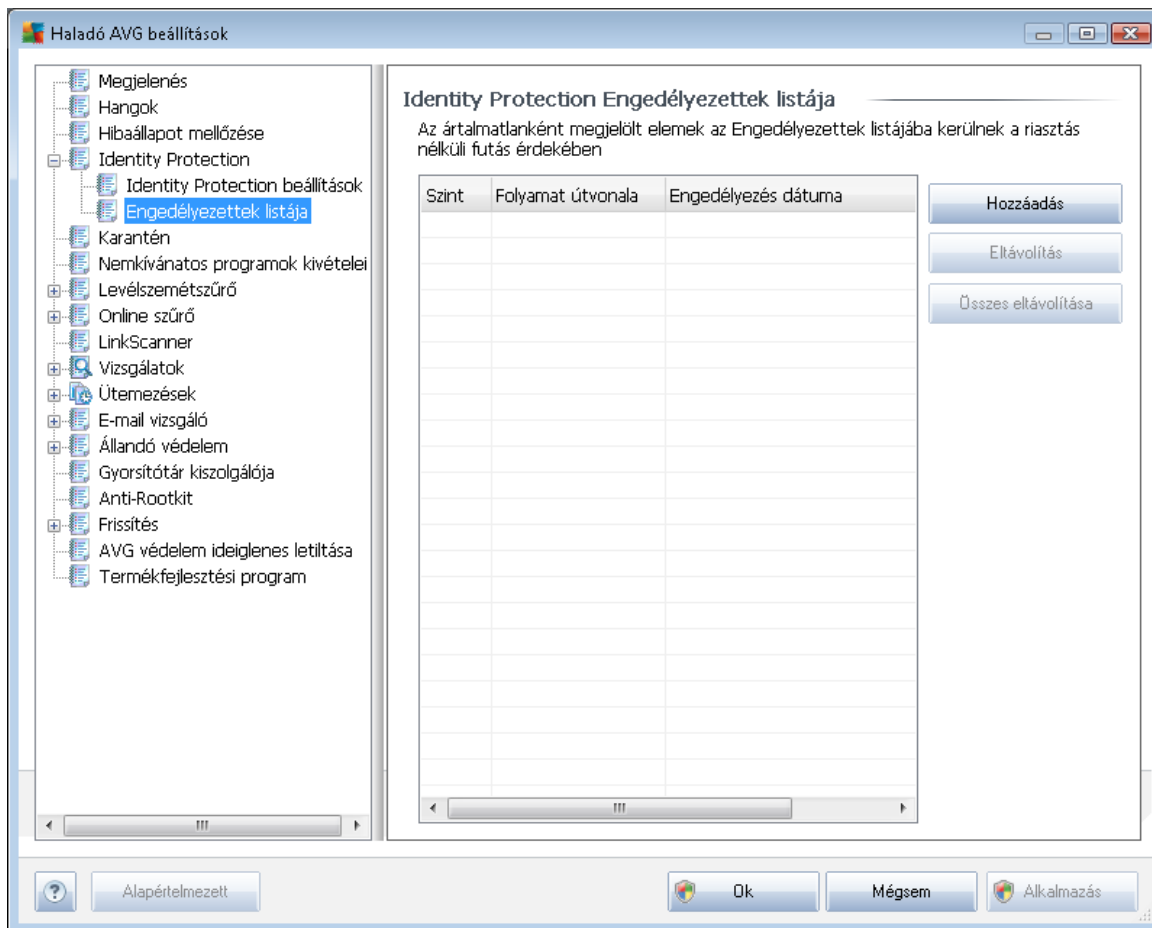
- **Észlelt fenyegetések automatikus karanténba helyezése** - jelölje be ezt a jelölőnégyzetet az összes észlelt fenyegetés automatikus és azonnali áthelyezéséhez az [AVG víruskaranténjába](#). Az alapértelmezett beállítások szerint egy új fenyegetés észlelésekor a program rákérdez, hogy karanténba helyezze-e azt (így csak azon alkalmazásokat távolítja el, amelyeket Ön nem kíván futtatni).
- **Ismert fenyegetések automatikus karanténba helyezése** - jelölje be a kártevok automatikus és azonnali áthelyezéséhez az [AVG 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 kártevoként észlelt alkalmazást áthelyezi a karanténba. Ha az alkalmazással dolgozik, akkor a munkája elveszhet, ezért eloször 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 kártevok észlelésekor egy új párbeszédpanel jelenik meg a kártevó 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.).

9.4.2. Engedélyezettek listája

Ha az **Identity Protection beállítások** párbeszédpanelen nem jelölte be az **észlelt fenyegetések automatikus karanténba helyezése** elemet, akkor az esetleges veszélyes kártevok 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:



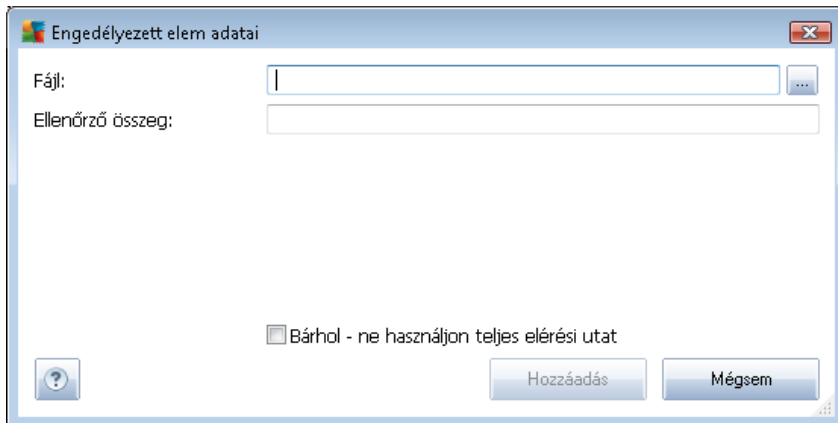
Az **Identity Protection engedélyezettek listája** a következő információkat tartalmazza az egyes alkalmazásokkal kapcsolatban:

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

Vezérlogombok

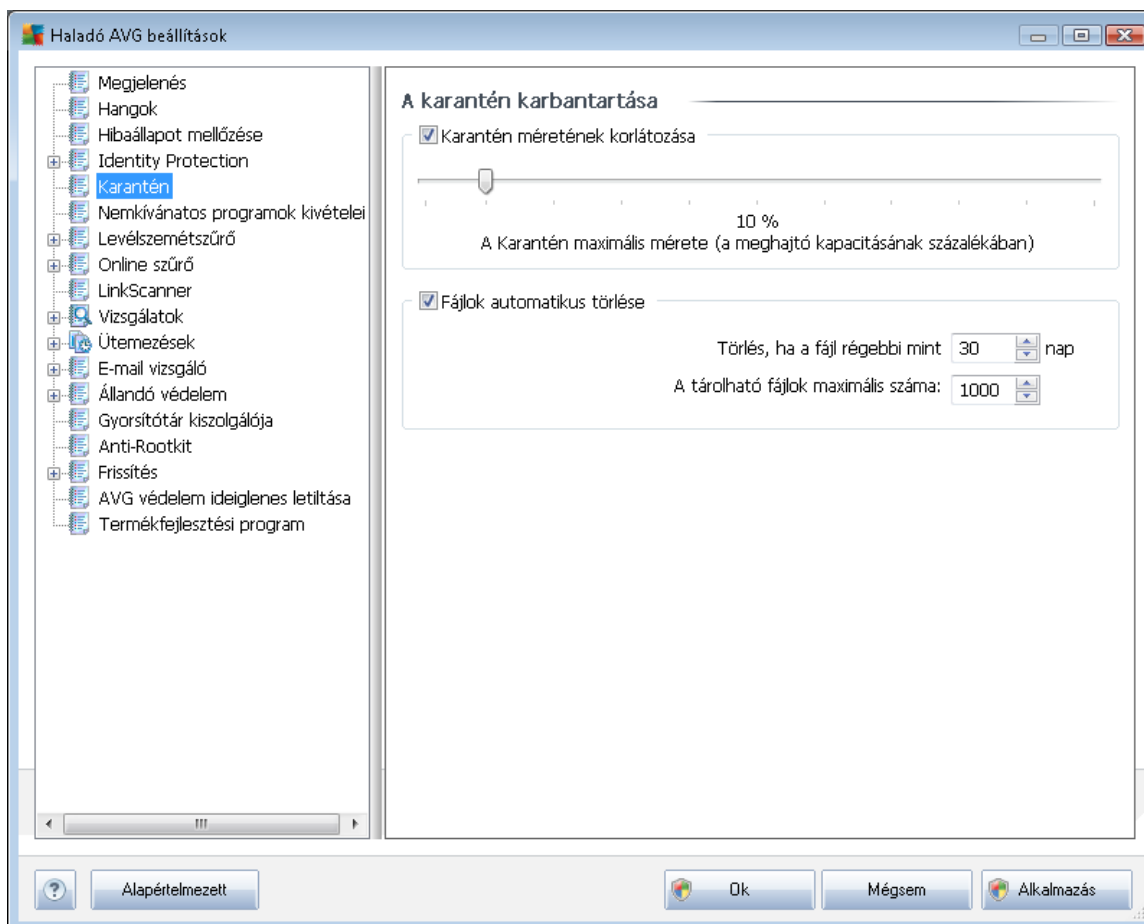
A vezérlogombok az **Identity Protection engedélyezettek listája** felületen a következők:

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



- o **Fájl** - írja be a teljes elérési útvonalat a fájlhoz (*alkalmazás*), amelyet kivételként kíván megadni
 - o **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.
 - o **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

9.5. Karantén



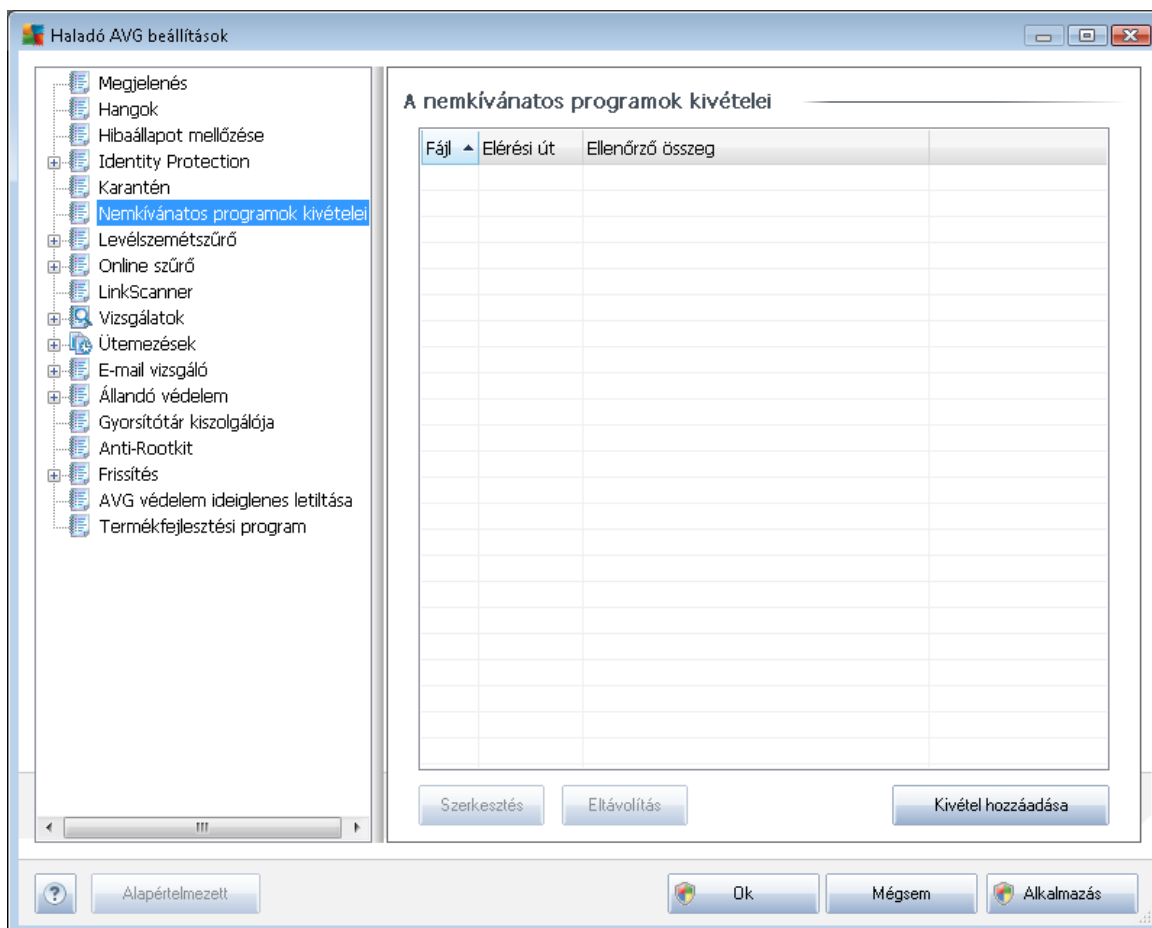
A **Víruskarantén karbantartása** ablak lehetővé teszi, hogy számos paramétert határozzon meg a **Karanténban** tárolt objektumok kezelésével kapcsolatban:

- **Karantén méretének korlátozása** - használja a csúszkát a **Karantén** maximális méretének meghatározásához. Az alapértelmezett méret helyi lemez kapacitásának függvényében, azzal arányosan lesz meghatározva.
- **Fájlok automatikus törlése** - ebben a részben meghatározhatja azt az időtartamot, ameddig az objektum a **Karanténban** marad (**Törlés, ha a fájl régebbi mint ... nap**), illetve a **Karanténban** tárolható fájlok maximális számát (**Tárolható fájlok maximális száma**)

9.6. Nemkívánatos programok kivételei

Az **AVG Internet Security 2011** képes a rendszer nemkívánatos végrehajtható alkalmazásainak és DLL könyvtárainak elemzésére és azonosítására. Eloffordulhat, 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 vírusirtó esetenként **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:

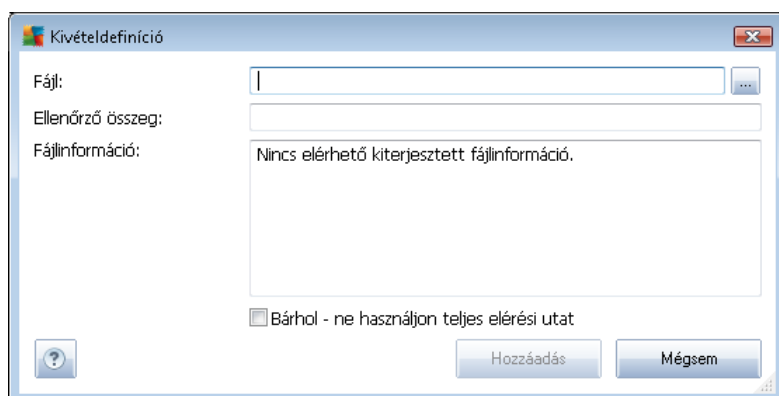
- **Fájl** - az adott alkalmazás nevét mutatja
- **Fájlútvonal** - az adott alkalmazás helyét mutatja meg
- **Ellenőrzőösszeg** - megmutatja a fájl egyéni "aláírását". Az ellenőrző összeg egy automatikusan létrehozott karakterlánc, amellyel az AVG vírusirtó egyértelműen meg tudja különböztetni a fájlt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

Vezérlogombok

- **Szerkesztés** - megnyitja a szerkesztőpanelt (megegyezik az új kivételek panellel, lásd lent

) a már létrehozott kivételekkel, ahol módosíthatja a kívánt paramétereket

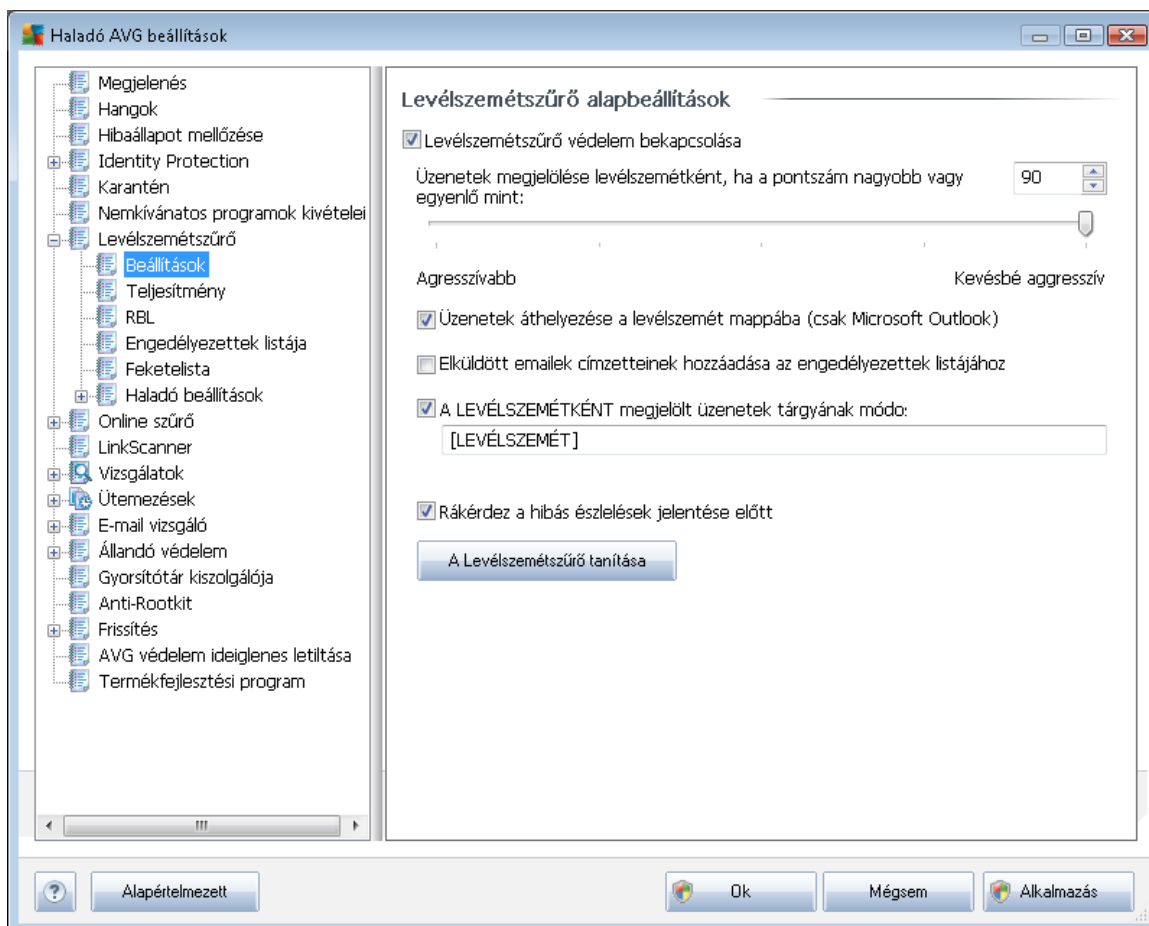
- **Eltávolítás** - törli a kiválasztott elemeket a kivételek listájából
- **Kivétel hozzáadása** - megnyit egy szerkesztőpanelt, ahol meghatározhatja egy új kivétel paramétereit:



- o **Fájl** - írja be a kivételként megadni kívánt fájl teljes elérési útját
- o **Ellenőrző összeg** - 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.
- o **Fájlinformációk** - megjelenít minden további információt a fájlról (*licenc/verzióinformációk stb.*)
- o **Bárhol – ne használjon teljes elérési utat** - ha az adott fájlt csak az adott helyen szeretné kivételként meghatározni, akkor ne jelölje be ezt az opciót. Ha a jelölőnégyzet be van jelölve, akkor a megadott fájl a helyétől függetlenül kivételként van meghatározva (*adja meg a fájl teljes elérési útvonalát arra az esetre, ha a rendszer két ugyanilyen nevű fájlt talál a számítógépen*).

9.7. Levélszemét-szuro

9.7.1. Beállítások



A **Levélszemétszűrő alapbeállításai** panelen használja a **Levélszemétszűrő védelem bekapcsolása** opciót a levélszemétszűrő engedélyezéséhez/kikapcsolásához. 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 [levélszemétszűrő](#) üzeneteket kiszuri 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 a nem levélszemét üzenetek is kiszűrésre kerülnek.

- **50-59 közötti érték** - Nagyon szigorú konfiguráció. A nem levélszemét üzenetek valószínűleg ugyanúgy kiszűrésre kerülnek, mint a valódi [levélszemét](#). Ez a tartomány nem javasolt az általános használatához.

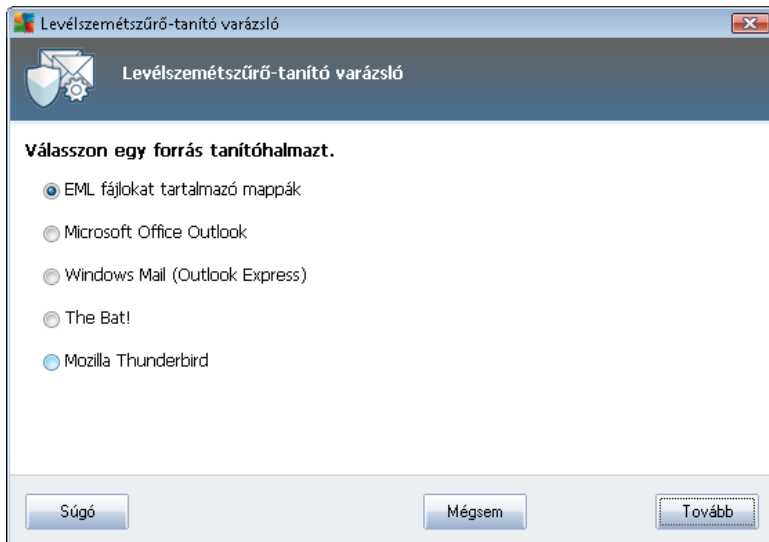
A **Levélszemétszuro alapbeállításai** ablakban meghatározhatja, hogyan legyenek kezelve a [levélszemétnek](#) minősülőüzenetek:

- **Üzenet áthelyezése a levélszemét mappába** - jelölje be, hogy a levélszemetek automatikusan átkerüljenek a levelezoprogram levélszemét mappájába.
- **Az elküldött emailek címzettjeinek hozzáadása az [engedélyezett 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 a szövegmezőben.
- **Kérdezzen rá a hibás észlelések jelentése előtt** - csak akkor, ha a [telepítési folyamat](#) során beleegyezett a [termékfejlesztési programban](#) való részvételbe. Ha igen, akkor Ön engedélyezte az észlelt fenyegetések jelentését az AVG-nek. 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).

Vezérlogombok

A **Levélszemétszuro tanítása** gomb megnyitja a [Levélszemétszuro-tanító varázslót](#), melyet részletesen a [következő fejezetben](#) ismerhet meg.

A **Levélszemétszuro-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:

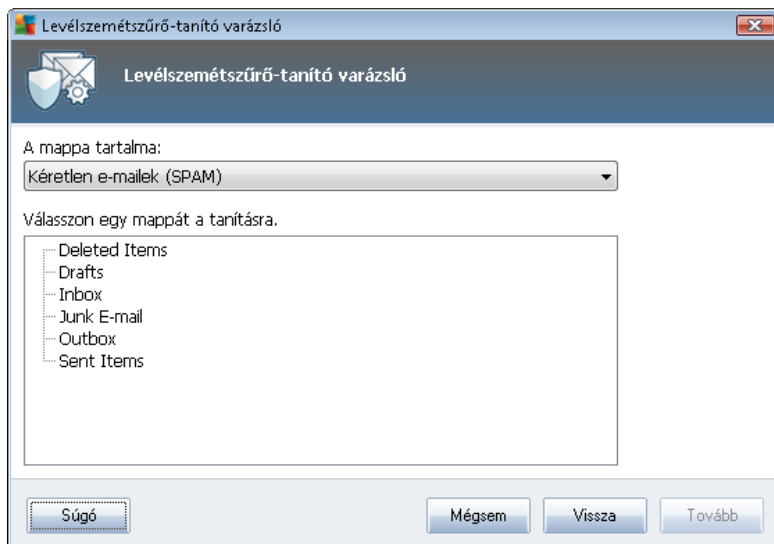
- **Bizonyos email kliens** - ha a felsoroltak közül valamelyik e-mail klienst használja (MS Outlook, Outlook Express, The Bat!), akkor egyszerűen válassza ki a megfelelő típust.
- **EML fájlokat tartalmazó mappa** - ha más email klienst használ, akkor először mentse az üzeneteket egy adott mappába (.eml 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



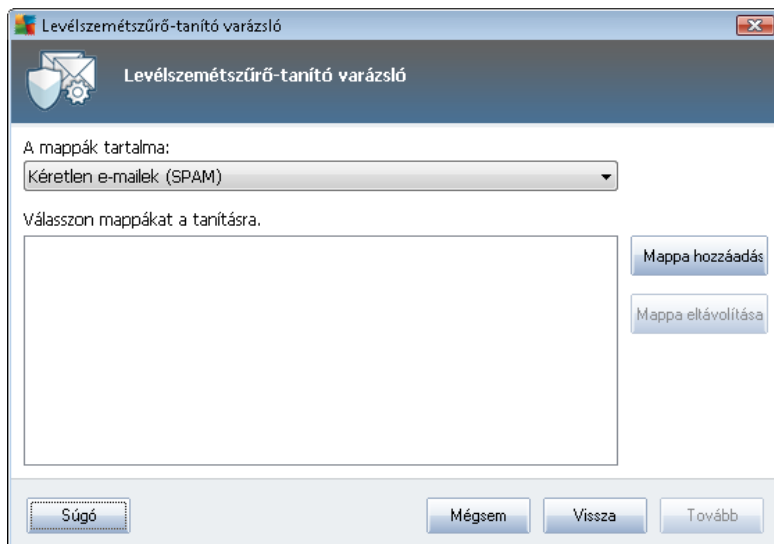
Ezen a panelen keresse meg a tanításhoz használandó mappát az üzenetekkel. Nyomja meg a **Mappa hozzáadása** gombot azon mappa megkereséséhez, mely tartalmazza az .eml fájlokat (*mentett emaileket*). A kiválasztott mappa megjelenik a panelen.

A **Mappa tartalma** legördülő menübol válassza ki az egyik opciót: hasznos üzenet (*NORMÁL*) vagy kéretlen üzenet (*LEVÉLSZEMÉT*). Vegye figyelembe, hogy az üzeneteket a következő lépésben szurni 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

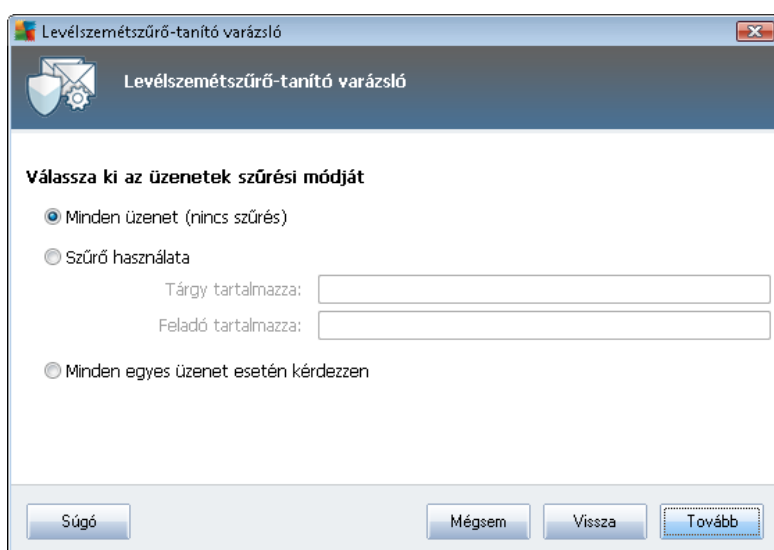
Miután megerősíti valamelyik opciót, egy új panel fog megjeleni.



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 könyvtárban. 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.

Ha biztos benne, hogy a kiválasztott mappa kizárólag tanításhoz használandó üzeneteket tartalmaz,

akkor válassza a **Minden üzenet (nincs szűrés)** opciót.

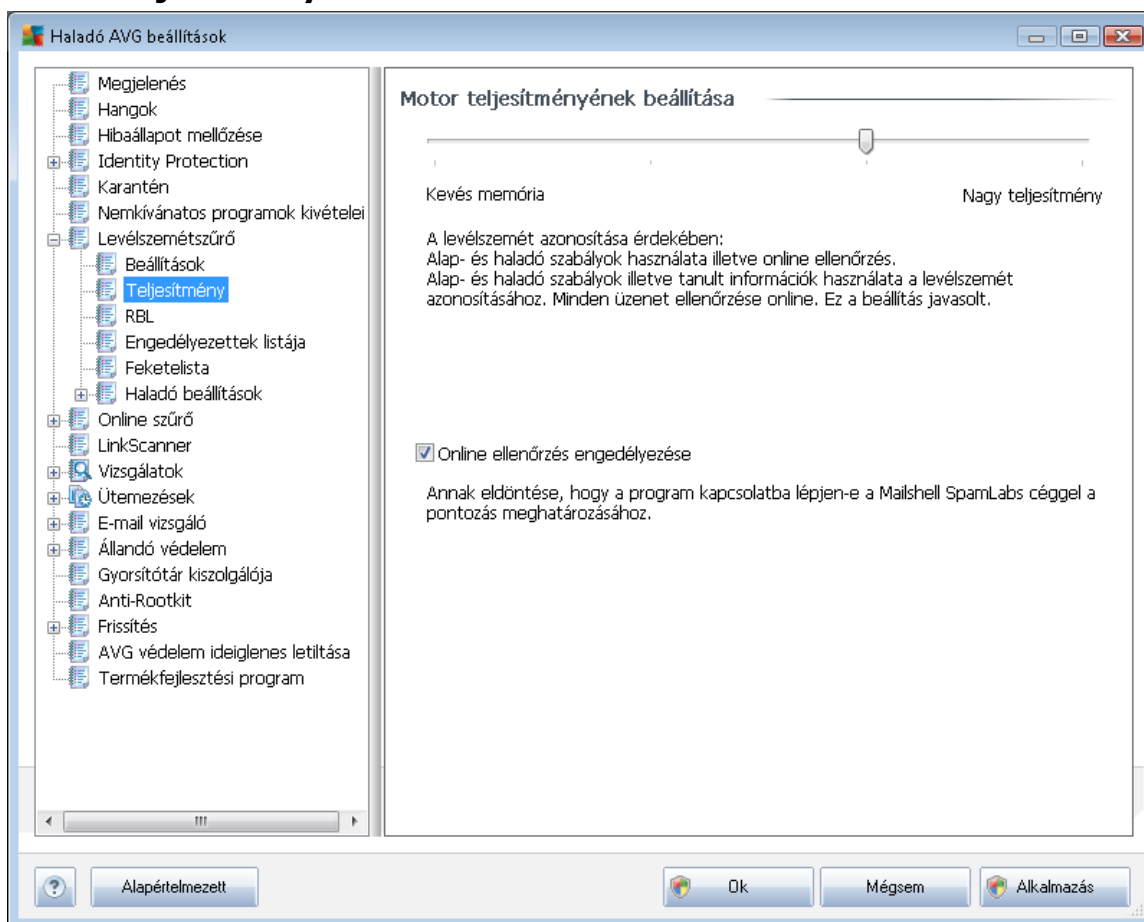
Ha nem biztos a mappában található üzenetekkel kapcsolatban, és azt szeretné, hogy a Varázsló minden egyes emailnél rákérdezzen az üzenet felhasználására, akkor válassza a **Kérdés minden üzenetnél** opciót.

A haladó szűréshez válassza a **Szuro használata** opciót. Beírhat egy a tárgy vagy feladó mezőben keresendő szót (*neve*), szótöredéket vagy mondatot. Minden beírt szöveggel egyező üzenet fel lesz használva a tanításhoz előzetes értesítés nélkül.

Figyelem! : Ha mindkét szövegmezőt kitölti, de csak az egyik feltétel egyezik, akkor azon üzenetek is fel lesznek használva!

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.

9.7.2. Teljesítmény



A **Motor teljesítményének beállítása** panelen (a **Teljesítmény** elemről a bal oldalon) megadhatja a **Levélszemétszuro** összetevő teljesítményének beállításait. Mozdassa a csúszkát a jobb oldalra a

teljesítmény szintjének módosításához a **Kevés memória** / **Nagy teljesítmény** módok között.

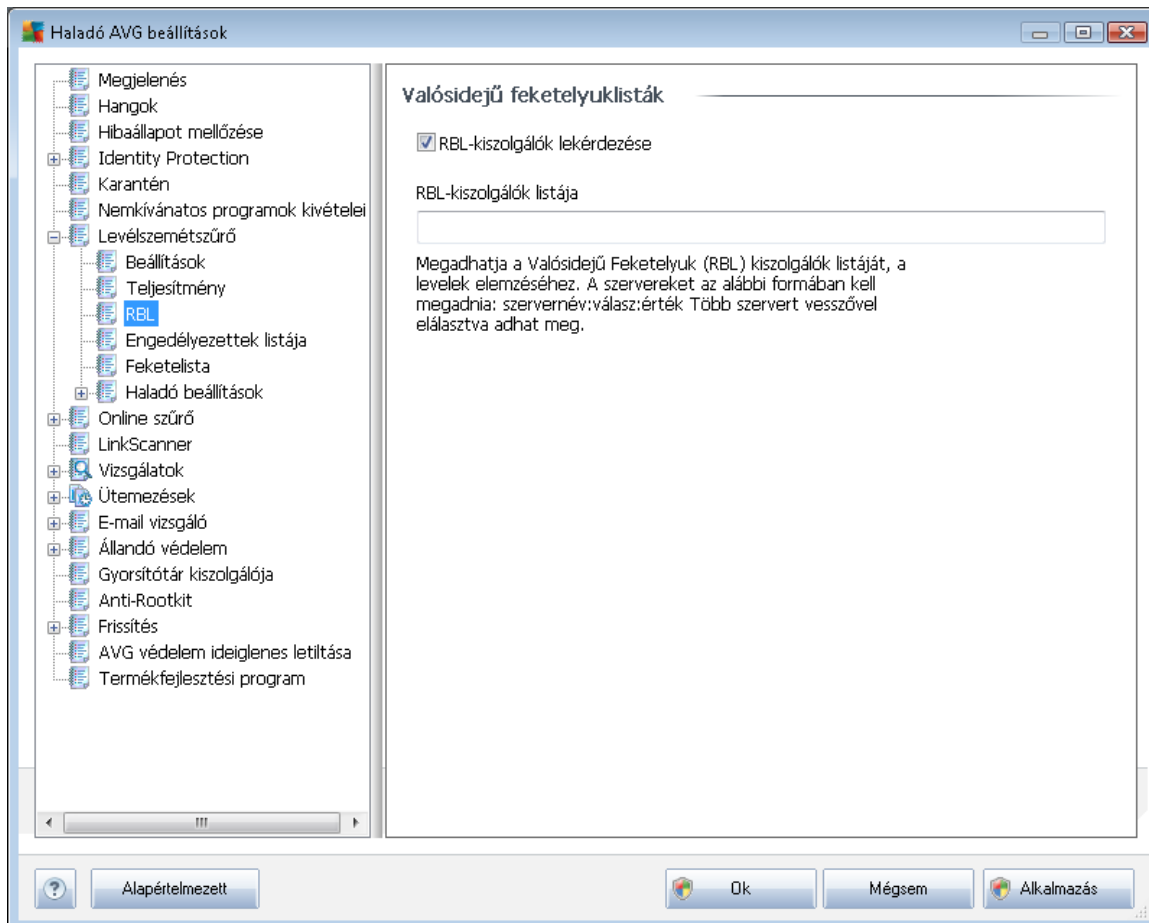
- **Kevés memória** - a vizsgálati folyamat alatt a [levélszemetek](#) meghatározásához semmilyen szabály nem lesz használva. Kizárólag a betanított adatok alapján történik az azonosítás. Ez a mód nem ajánlott általános használatra, hacsak nem nagyon elavult a számítógép hardvert használ.
- **Nagy teljesítmény** - ez a mód sok memóriát igényel. A vizsgálati folyamat során a [levélszemetek](#) azonosításához a következő funkciók lesznek használva: szabályok és [levélszemét](#) adatbázis gyorsítótár, alap és haladó szabályok, levélszemétküldők IP-címei és adatbázisai.

Az **Online ellenőrzés engedélyezése** elem alapállapotban be van kapcsolva. Még pontosabb [levélszemét](#) azonosítást tesz lehetővé a [Mailshell](#) kiszolgálókkal való kommunikáción keresztül, azaz a vizsgált adatok össze lesznek vetve a [Mailshell](#) online adatbázisaival.

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

9.7.3. RBL

Az **RBL** elem megnyit egy **Valósídejű feketelyuk-listák** new szerkesztoablakot:





Ezen a panelen be- és kikapcsolhatja az **RBL-kiszolgálók lekérdezése** funkciót.

Az RBL (*Real-time Blackhole List – valós idejű feketelyuk-lista*) kiszolgáló olyan tartománynév-kiszolgáló, amely egy nagy adatbázisban tárolja a világon ismertté vált ismert levélszemétküldöket. 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 ujjenyomatai, ezért ez a legjobb és legpontosabb [levélszemét-észlelési](#) módszer. Ez a szolgáltatás különösen hasznos azoknak a felhasználóknak, akik nagy mennyiségű levélszeméttel kapnak, és a [Levélszemétszűrő](#) motorja általában nem észleli azokat.

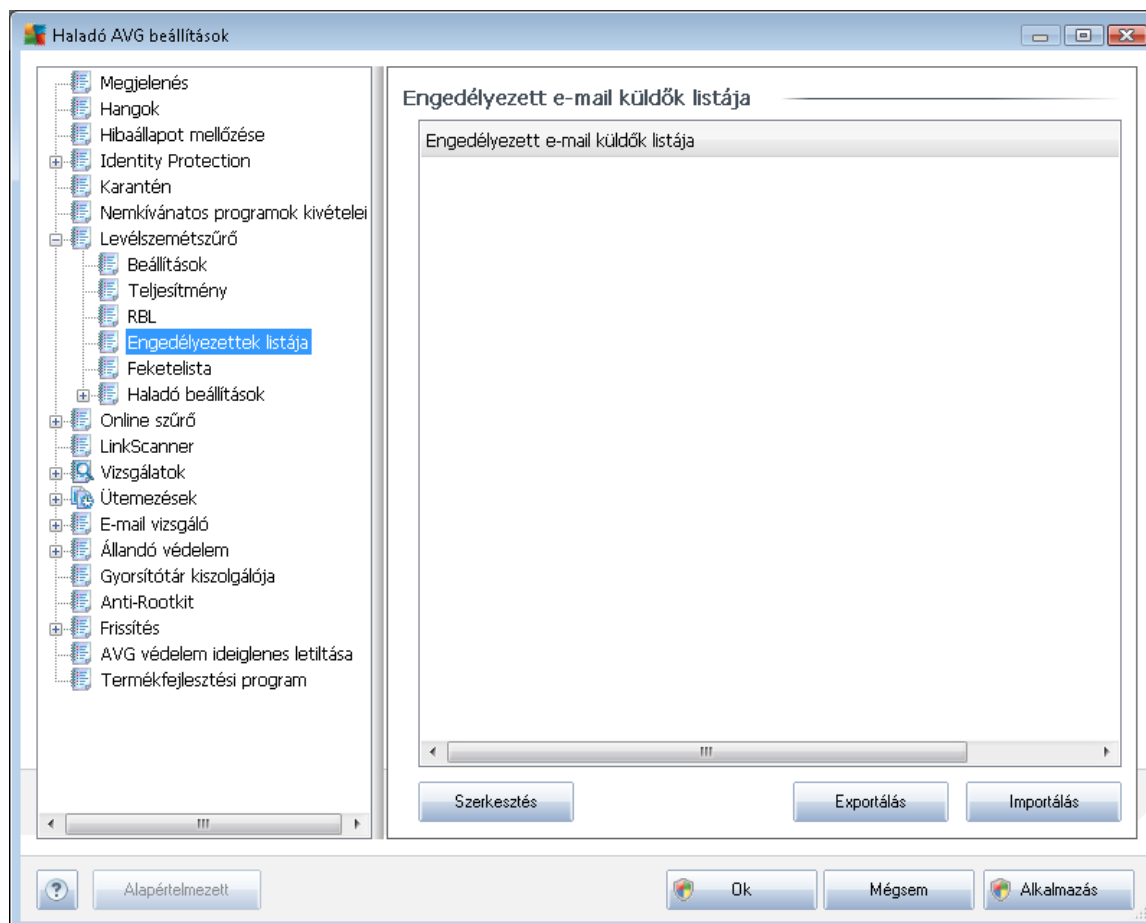
Az **RBL-kiszolgálók listája** segítségével megadhatja mely RBL kiszolgálókat kívánja használni.

Megjegyzés: 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!

9.7.4. Engedélyezettek listája

Az **Engedélyezettek listája** elem megnyitja az **Engedélyezett feladók listáját** azon feladók e-mail címeinek és tartományneveinek globális listájával, amelyek üzenetei soha nem számítanak [levélszemétnek](#).



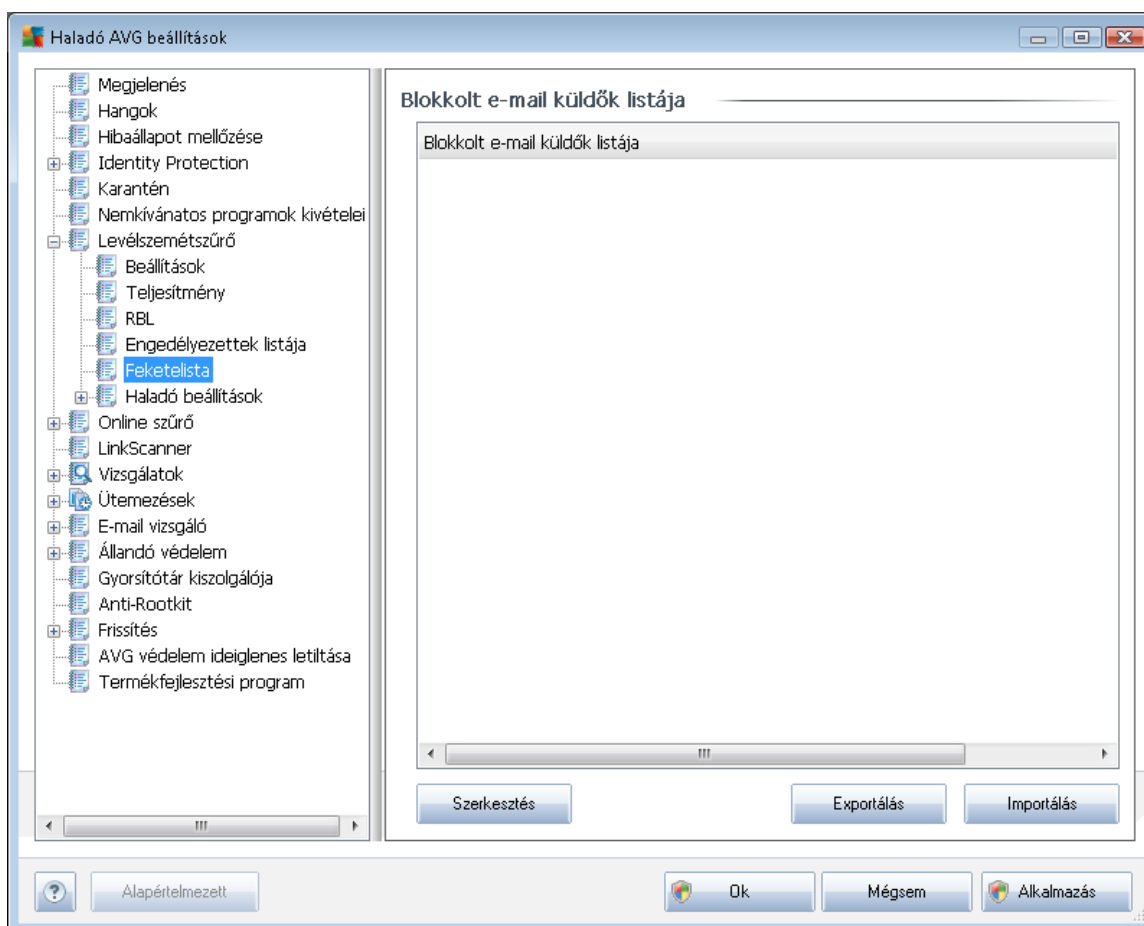
A szerkesztőfelületen összeállíthat egy listát azon feladókból, akikben megbízik, hogy soha nem küldenének Önnek nemkívánatos üzeneteket ([levélszemetet](#)). A listába olyan teljes tartományneveket is felvehet (pl. [avg.com](#)), amelyekről soha nem fog levélszemetet kapni.

Amint megvan a feladók és tartománynevek elokészített listája, megadhatja őket a következő módszerekkel: közvetlen bevitel, vagy a teljes címlista egyszerre történő importálása. Az alábbi vezérlogombok 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.

9.7.5. Feketelista

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, akikről nemkívánatos üzenetekre ([levélszemétre](#)) számíthat. A listába olyan teljes tartományneveket is felvehet (például a *levelszemetkuldovallalat.com* címet), amelyekről valószínűleg levélszemetet fog kapni. A felvett tartományba tartozó címekről érkező e-maileket mindig levélszemétként fogja azonosítani a program.

Amint megvan a feladók és tartománynevek elokészített listája, megadhatja őket a következő módszerekkel: közvetlen bevitel, vagy a teljes címlista egyszerre történő importálása. Az alábbi vezérlogombok 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.

9.7.6. Haladó beállítások

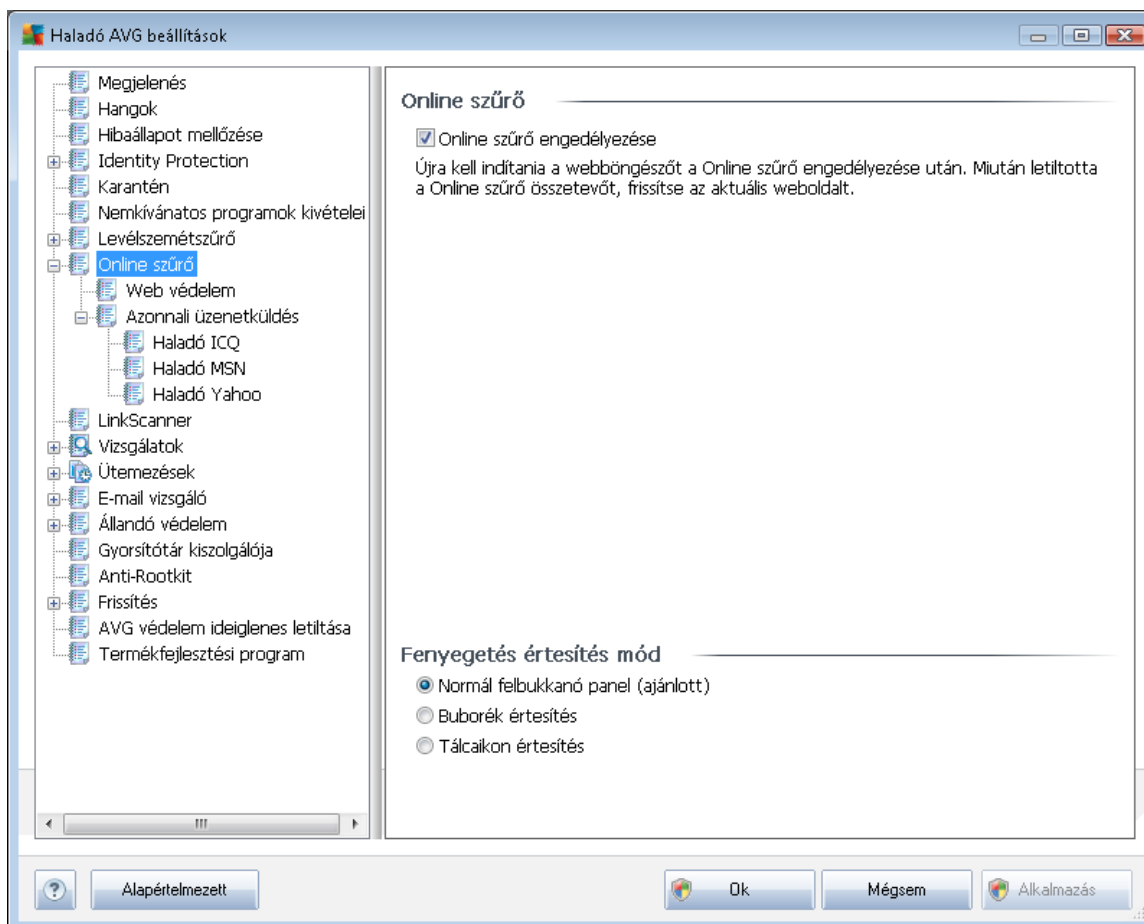
A Haladó beállítások rész részletes beállítási lehetőségeket tartalmaz a Levélszemétszuro összetevőhöz. Ezen beállítások módosítását csak haladó felhasználóknak ajánljuk. Jellemzően azon hálózati adminisztrátoroknak, akiknek részletesen meg kell adniuk a levélszemétszuro beállításait az email szerverek maximális védelmének érdekében. Ezért nincs külön súgó az egyes párbeszéd-ablakokhoz, bár egy rövid leírást találhat 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 [Levélszemétszuro](#) beállításait haladó szinten, akkor kövesse a felhasználói felületen megjelenő utasításokat. Általában mindegyik párbeszédablakban egy adott szerkeszthető funkciót találhat - a leírás mindig megtalálható ugyanitt:

- **Gyorsítótár** - lenyomat, tartomány hírnév, LegitRepute
- **Tanítás** - maximum bejegyzés, automatikus tanítási küszöb, súlyozás
- **Szurés** - nyelvi lista, országlista, engedélyezett IP-címek, blokkolt IP-címek, blokkolt országok, blokkolt karakterkészletek, hamisított feladók
- **RBL** - Valósídeju feketelyuk lista kiszolgálók, több találat, küszöb, időtűllépés, maximum IP-k
- **Internetkapcsolat** – időtűllépés, proxykiszolgáló, proxy hitelesítése

9.8. Online szuro



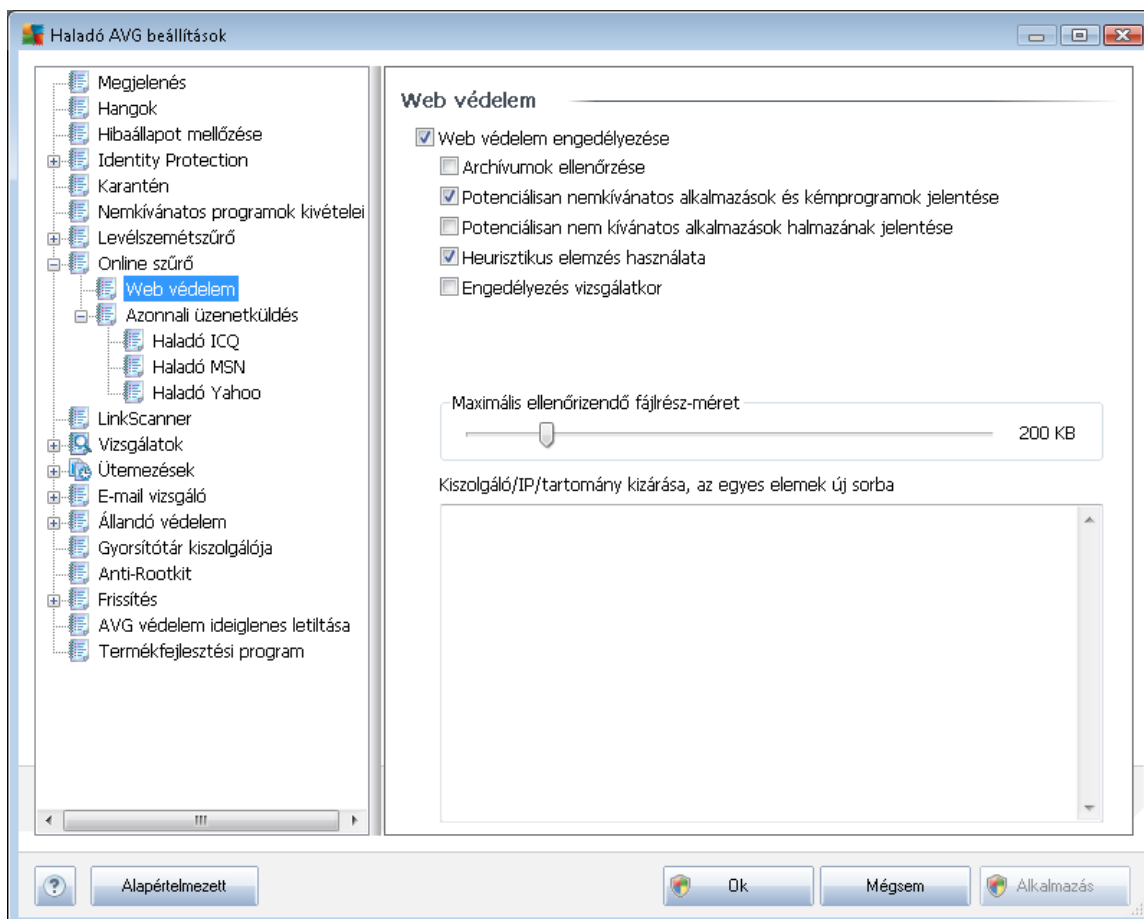
Az **Online szuro** panel lehetővé teszi, hogy be- és kikapcsolja az **Online szuro** összetevőt az **Online szuro engedélyezése** opció segítségével (*alapállapotban bekapcsolva*). Az összetevő haladó beállításaihoz menjen a navigációs részen a további panelekre:

- [Web védelem](#)
- [Azonnali üzenetküldés](#)

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.

9.8.1. Web védelem



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

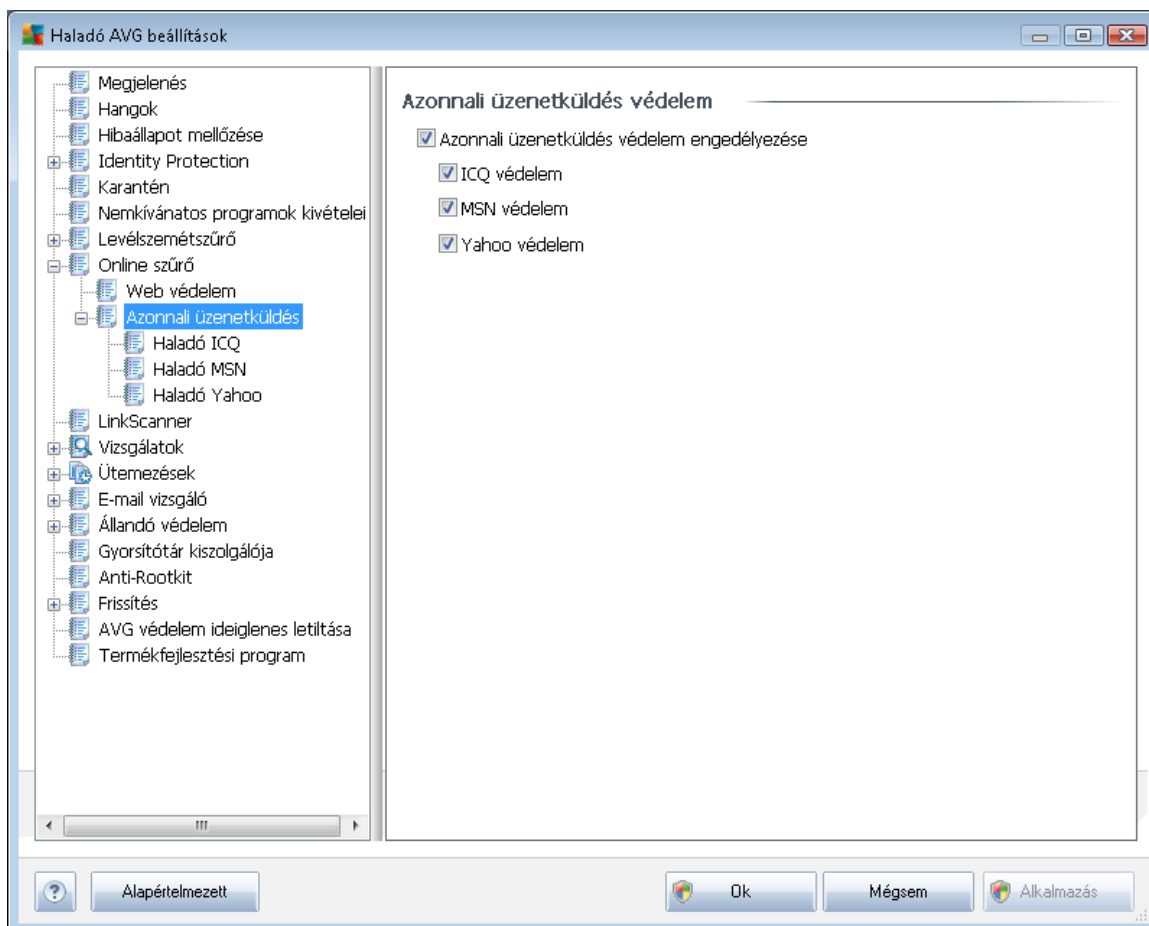
- **Web védelem engedélyezése** - ez az opció biztosítja, hogy az [Online szűrő](#) ellenőrizze a honlapok tartalmát. Ha az opció be van kapcsolva (*alapértelmezés szerint*), akkor a következő elemeket kapcsolhatja be és ki:
 - o **Archívumok ellenőrzése** - (*alapállapotban kikapcsolva*): ellenőrzi a megjelenítendő oldalba ágyazott esetleges archívumok, tömörített fájlok tartalmát.
 - o **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.
 - o **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.

- o **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).
- o **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.
- o **Maximális ellenőrzendő fájl méret** - ha beágyazott fájlok találhatók egy megjelenítendő weboldalon, 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 szurovel](#) vizsgálandó fájlok maximális méretének beállításához. Ha a letöltött fájl nagyobb a megadott méretnél, és az Online szuro nem ellenőrzi, de természetesen Ön ilyenkor is védve van: ugyanis az esetleges fertőzést az [Állandó védelem](#) azonnal észleli.
- o **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 szuronek](#) nem kell ellenőriznie. Csak olyan kiszolgálókat zárjon ki, amelyben teljesen biztos, hogy nem fognak veszélyes tartalmat nyújtani.

9.8.2. Azonnali üzenetküldés

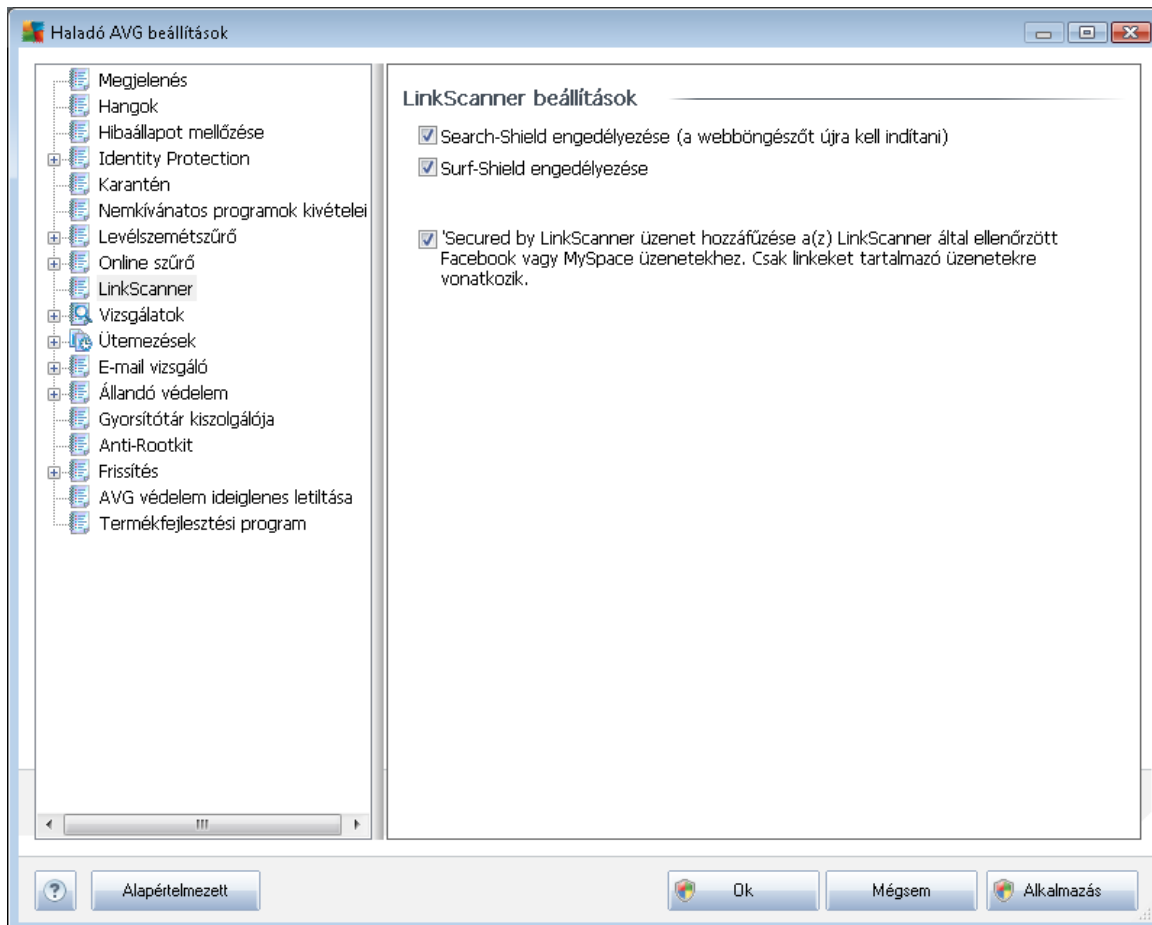


Az **Azonnali üzenetküldés védelem** panelben szerkesztheti az **Online szuro** összetevő azonnali üzenetküldésre vonatkozó beállításait. Jelenleg a következő három azonnali üzenetküldő program támogatott: **ICQ**, **MSN** és **Yahoo** - jelölje be a megfelelő opciót, ha szeretné, hogy az **Online szuro** ellenőrizze az online kommunikációt.

Az engedélyezett/letiltott felhasználókkal kapcsolatos további információkért lásd az adott panelt (**Speciális ICQ**, **Speciális MSN**, **Speciális Yahoo!**), és adja meg az **Engedélyezettek listáját** (azon felhasználók, akik kommunikálhatnak Önnel), illetve a **Letiltottak listáját** (azon felhasználók, akik le vannak tiltva).

9.9. Linkvizsgáló

A [Link Scanner](#) beállítások panel lehetővé teszi, hogy ki- és bekapcsolja a [Link Scanner](#) alapvető funkcióit:



- **Kereső védelem engedélyezése** – (alapállapotban bekapcsolva): értesítések a következő keresomotorok 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** - jelölje be ezt az elemet, ha tanúsítási megjegyzést szeretne hozzáfűzni a [Link Scanner](#) által ellenőrzött, linkeket tartalmazó azon üzenetekhez, amelyeket a Facebook és MySpace közösségi oldalakról küldött el.

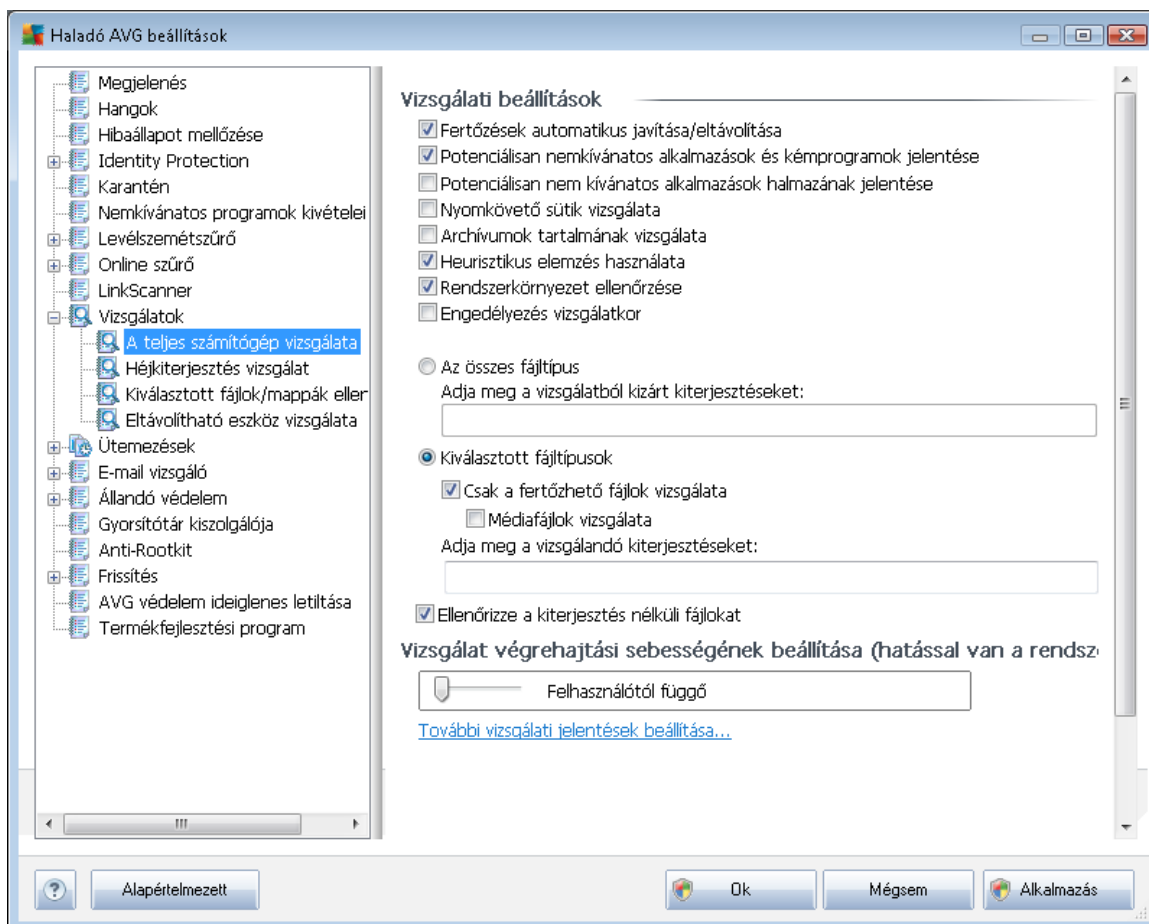
9.10. Vizsgálatok

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
- [Kiválasztott fájlok vagy mappák ellenőrzése](#) - a számítógép adott területeinek előre meghatározott normál vizsgálata
- [Cserélhető eszköz vizsgálata](#) - a számítógéphez csatlakoztatott cserélhető eszközök vizsgálata

9.10.1. A teljes számítógép vizsgálata

A **Számítógép teljes vizsgálata** opció lehetővé teszi, hogy szerkessze a szoftvergyártó által előre meghatározott paramétereket, [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 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.
- **Nyomkövető sütik vizsgálata** (alapállapotban kikapcsolva) - ez az opció a [Kémprogram-elhárító](#) összetevőben meghatározza, hogy a vizsgálat során felismert sütik törölve legyenek-e (a 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 fájl típus** - lehetséges megadnia kivételeket, amelyek kimaradnak a vizsgálatból (mentés után a vesszók pontosvesszőkre változnak).

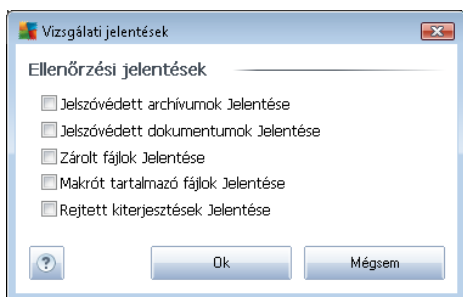
- **Kiválasztott fájl típusok** - megadhatja, hogy a program csak olyan fájlokat vizsgáljon, amelyek esetlegesen fertőzőek (a nem fertőzhető fájlok, mint pl. a sima szöveges fájlok vagy egyéb nem futtatható fájlok, nem lesznek ellenőrizve), pl. médiafájlok (video-, audiofájlok - ha nem jelöli be ezt 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.

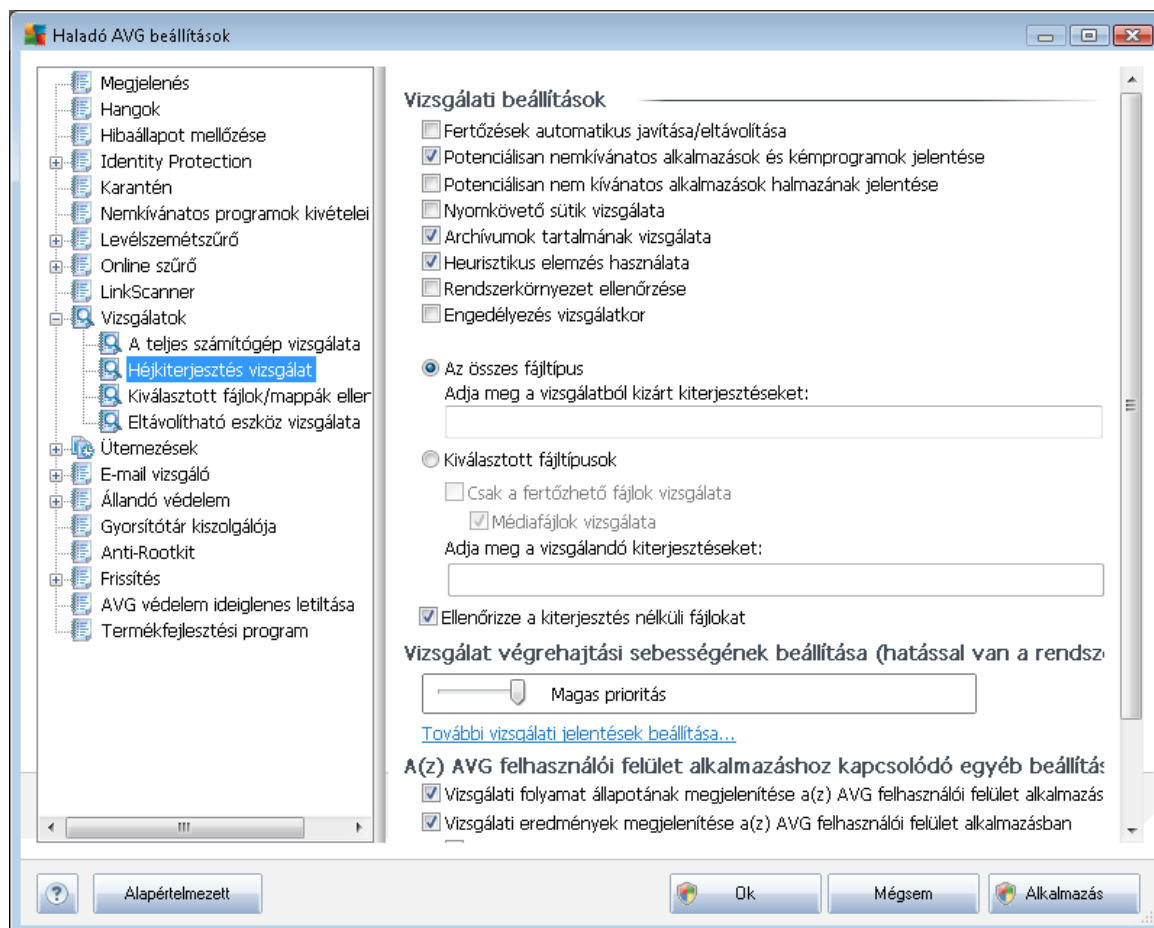
További vizsgálati jelentések beállítása...

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



9.10.2. Héjkiterjesztés vizsgálat

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



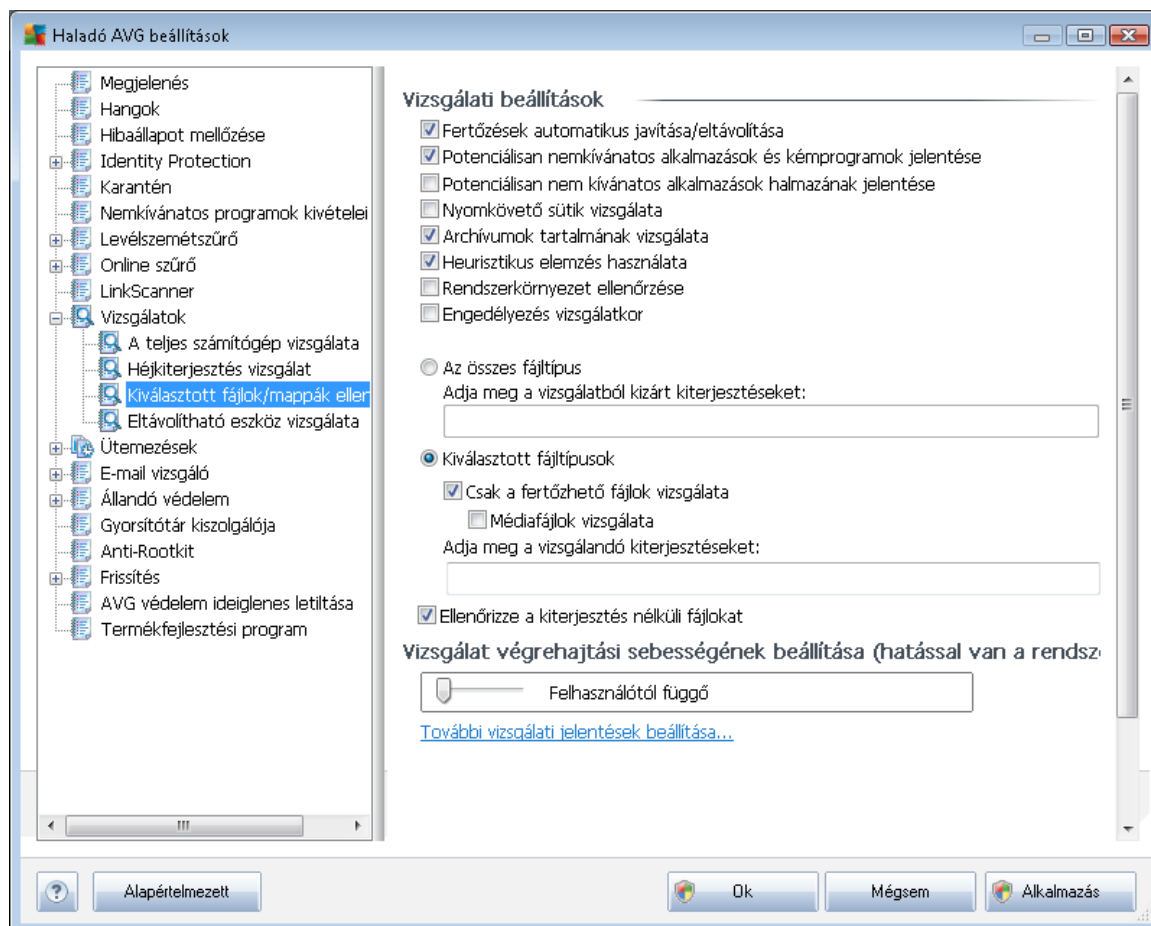
A paraméterek listája megegyezik a [Teljes számítógép vizsgálata](#) rész paramétereivel. Az alapértelmezett beállítások eltérnek (például a *Számítógép teljes vizsgálata* szolgáltatás nem vizsgálja a tömörített fájlokat, de ellenorzi a rendszerkörnyezetet, míg a *héjkiterjesztési vizsgálat* pont az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

Megjegyzés: Az adott paraméterek leírásával kapcsolatban lásd az [AVG Haladó beállítások / Vizsgálatok / Számítógép teljes vizsgálata](#) fejezetet.

A [Számítógép teljes vizsgálata](#) panelhez hasonlóan a *Héjkiterjesztési vizsgálat* panel 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 felületről. Meghatározhatja azt is, hogy a vizsgálati eredmények csak akkor jelenjenek-e meg, ha a rendszer fertőzést észlelt.

9.10.3. Kiválasztott fájlok vagy mappák ellenorzése

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:

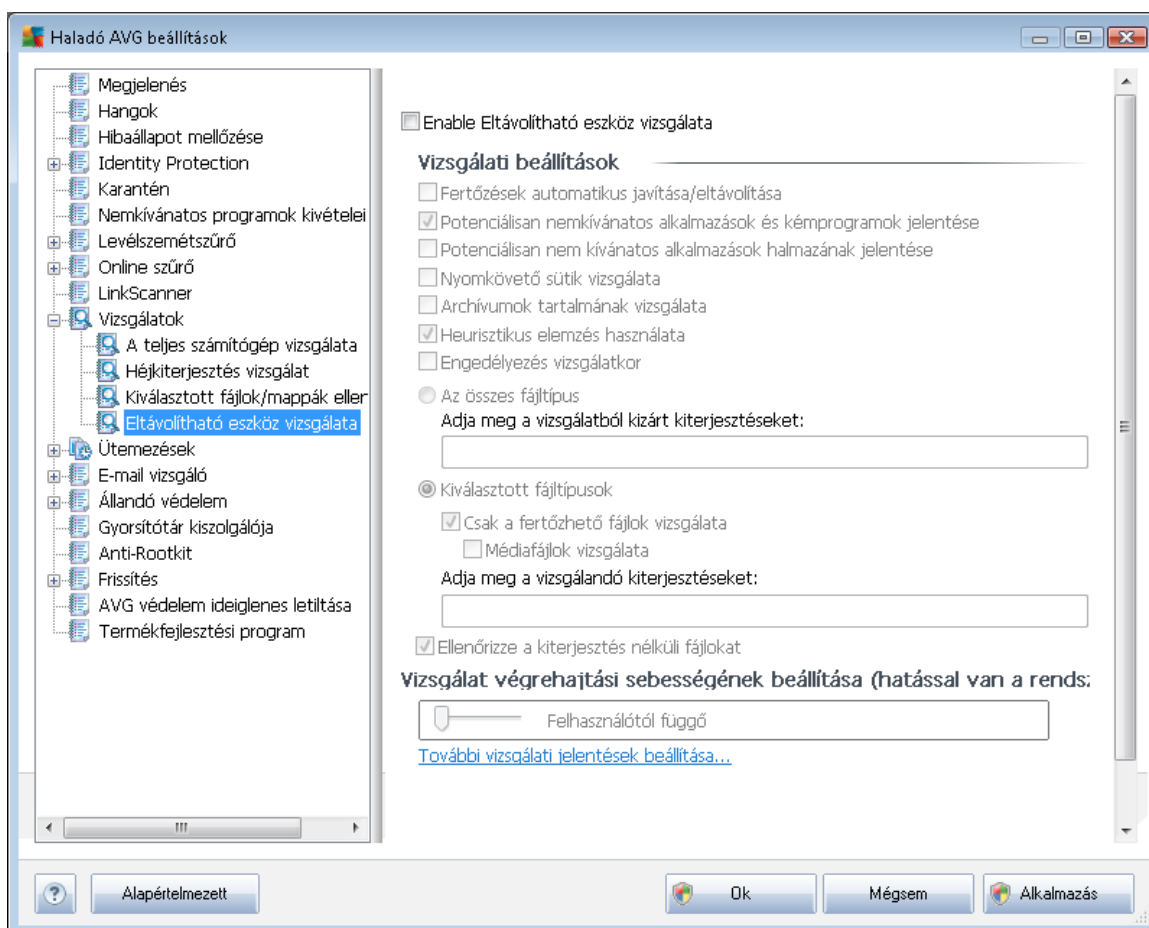


Az összes itt beállított paraméter csak a **Bizonyos fájlok vagy mappák vizsgálata** opcióra vonatkozik.

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

9.10.4. 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.

9.11. Ütemezések

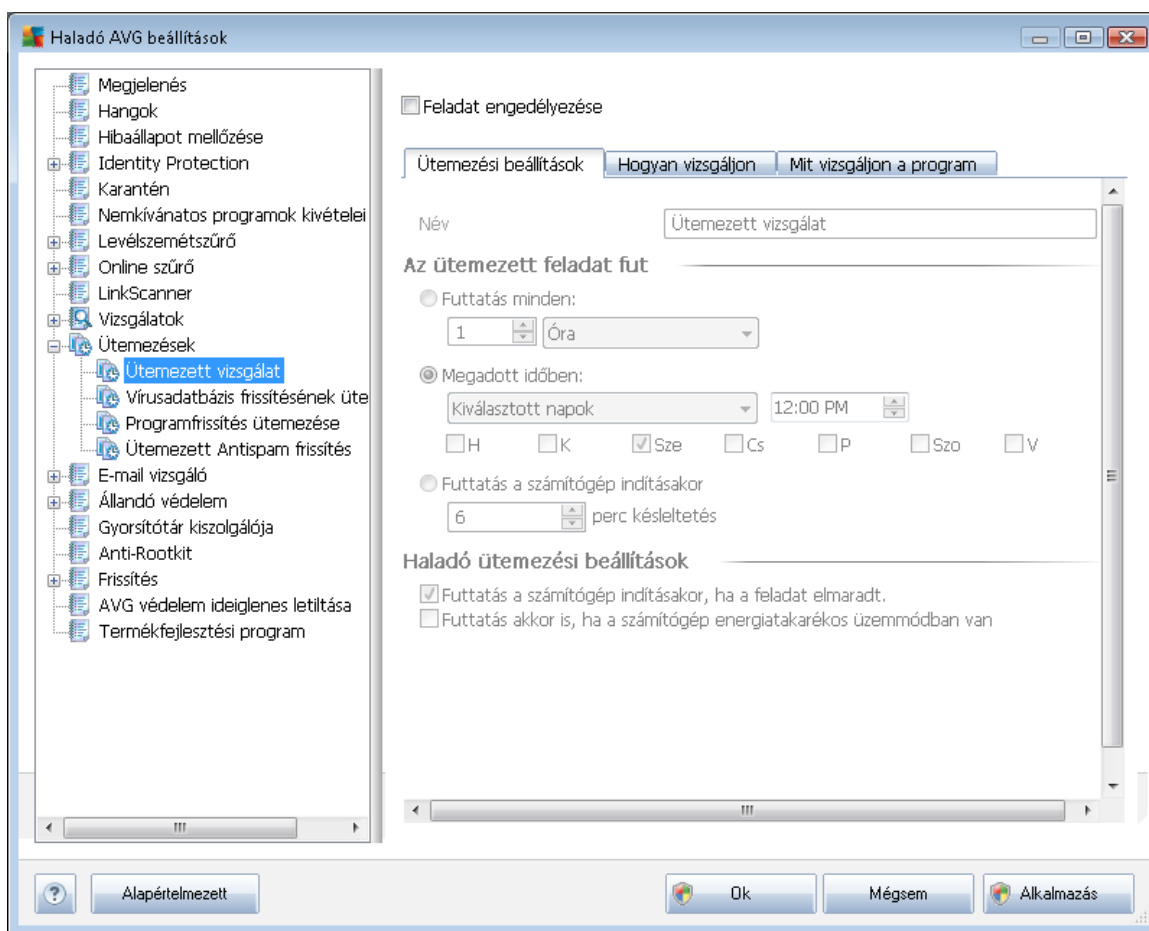
Az **Ütemezések** részben szerkesztheti a következők alapbeállításait:

- [Ütemezett vizsgálat](#)
- [Vírusadatbázis frissítésének ütemezése](#)

- [Programfrissítés ütemezése](#)
- [Levélszemétszuro frissítés ütemezése](#)

9.11.1. 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**(mezoben 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 minosülnek.

Ezen a panelen beállíthatja az adott keresés következő paramétereit:

Az ütemezett feladat fut

Itt megadhatja, hogy az ütemezett vizsgálatok milyen időközönként fussanak 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

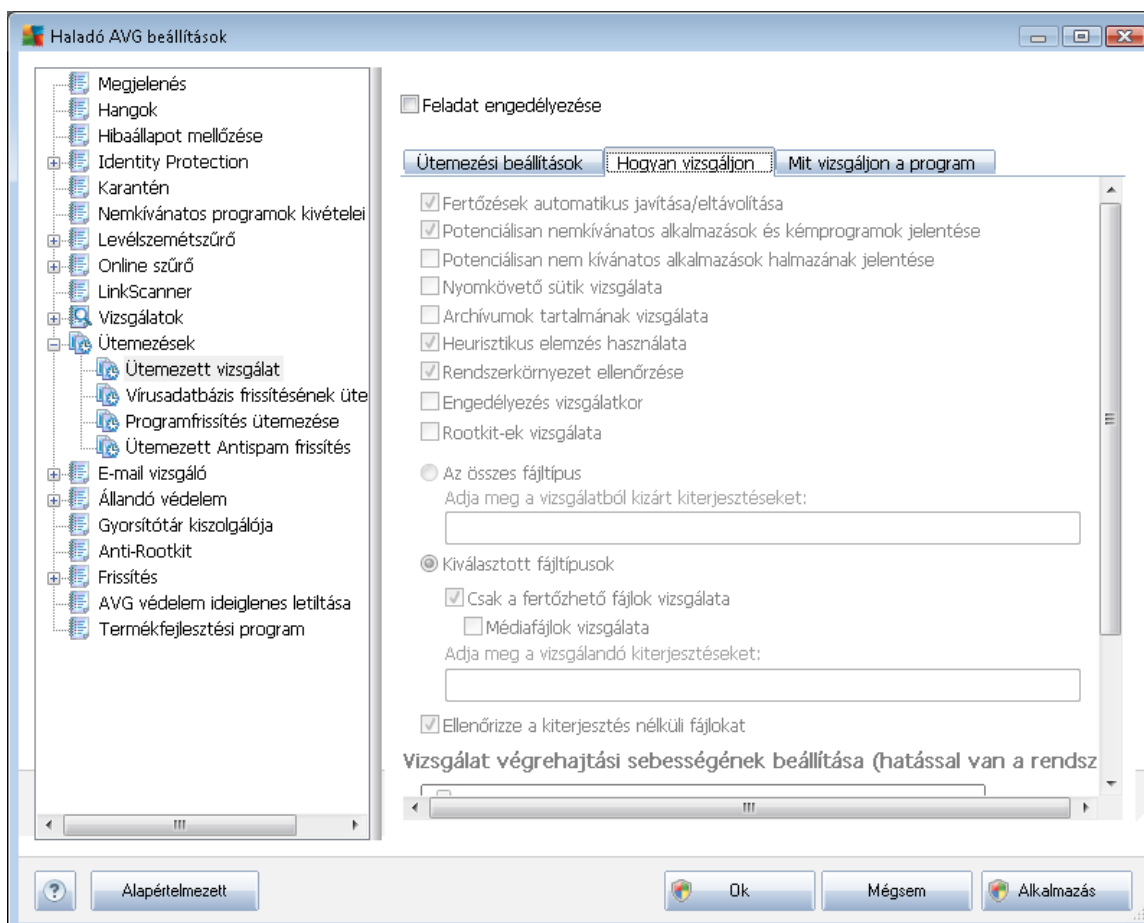
Ebben a részben meghatározhatja, hogy a vizsgálat mely körülmények között induljon/ne induljon, például ha a számítógép energiatakarékos módban van, vagy teljesen ki van kapcsolva.

Miután az ütemezett vizsgálat elindult a megadott időben, erről értesítést kap egy felbukkanó ablak formájában az [AVG ikonjánál](#) :



Egy új [AVG rendszerikon](#) jelenik meg (színes ikon), 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 vírusot 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 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.

- **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 fájl - köztük archív fájlokat 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 ellenőrizi.
- **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 ellenőrizi a biztonság kedvéért. Ne feledje, hogy ez a módszer meglehetősen időigényes.
- **Rootkitek vizsgálata** (alapállapotban kikapcsolva): jelölje be ezt az elemet, ha rootkitek 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 fájl típus** - lehetséges megadnia kivételeket, amelyek kimaradnak a vizsgálatból (mentés után a vesszók pontosvesszókra változnak).
- **Kiválasztott fájl típusok** - 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.

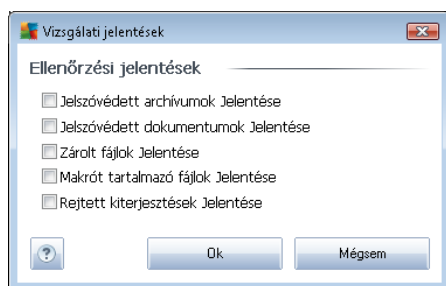
A vizsgálati sebesség beállítása

A **Vizsgálati sebesség beállítása** részben meghatározhatja a vizsgálat sebességét a rendszer erőforrásainak függvényében. Alapállapotban ez az érték *felhasználótól által függo* 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.

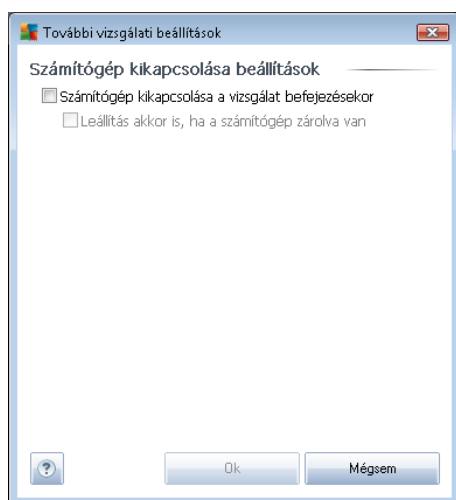
További vizsgálati jelentések beállítása

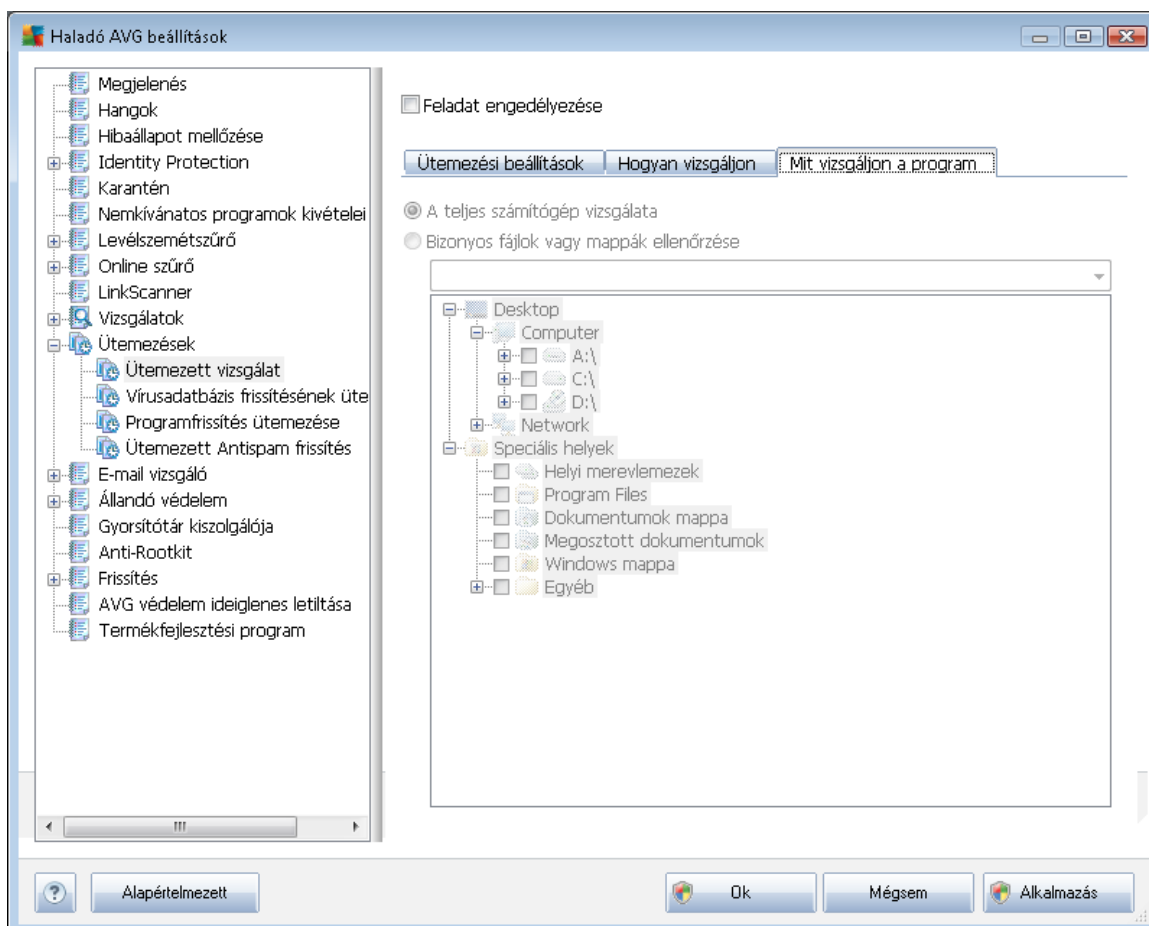
Kattintson a **További vizsgálati jelentések...** hivatkozásra a **Vizsgálati jelentések** panel megnyitásához, ahol számos opciót jelölhet be azzal kapcsolatban, hogy a programnak mit kell jelentenie:



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**).

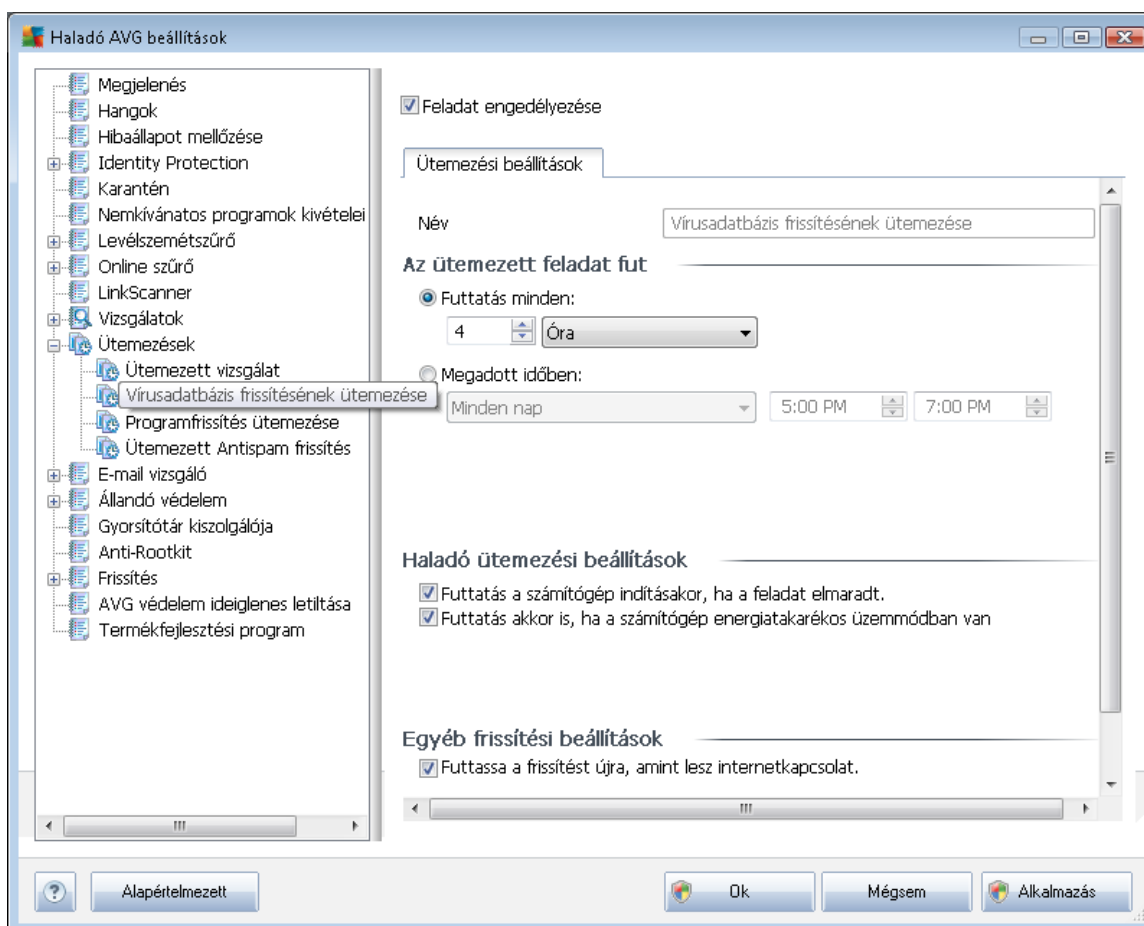




A **Mit vizsgáljon a program** fülön meghatározhatja, hogy a [számítógép teljes vizsgálatát](#) vagy csak [bizonyos fájlok és mappák vizsgálatát](#) szeretné ütemezni. Ha a bizonyos fájlok és mappák vizsgálatát választja, akkor a panel alsó részén a fastruktúra aktiválódik és bejelölheti az ellenőrzendő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

9.11.2. Vírusadatbázis frissítésének ütemezése

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



Az alapszintű adatbázis-frissítési ütemezés megtalálható a [Frissítéskezelő](#) összetevőben. Ebben az ablakban megadhatja a frissítési ütemezés részletes paramétereit. A **Név** mezőben (*kikapcsolva az alapértelmezett ütemezésekét*) találhat egy - a program gyártója által létrehozott - nevet ezen ütemezéshez.

Az ütemezett feladat fut

Ebben a részben adja meg, hogy a frissítés milyen gyakran fusson le. Az ütemezést meghatározhatja a rendszeresen történő futtatással (**Futtatás minden ...**), dátummal és időponttal (**Futtatás meghatározott időben ...**).

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.

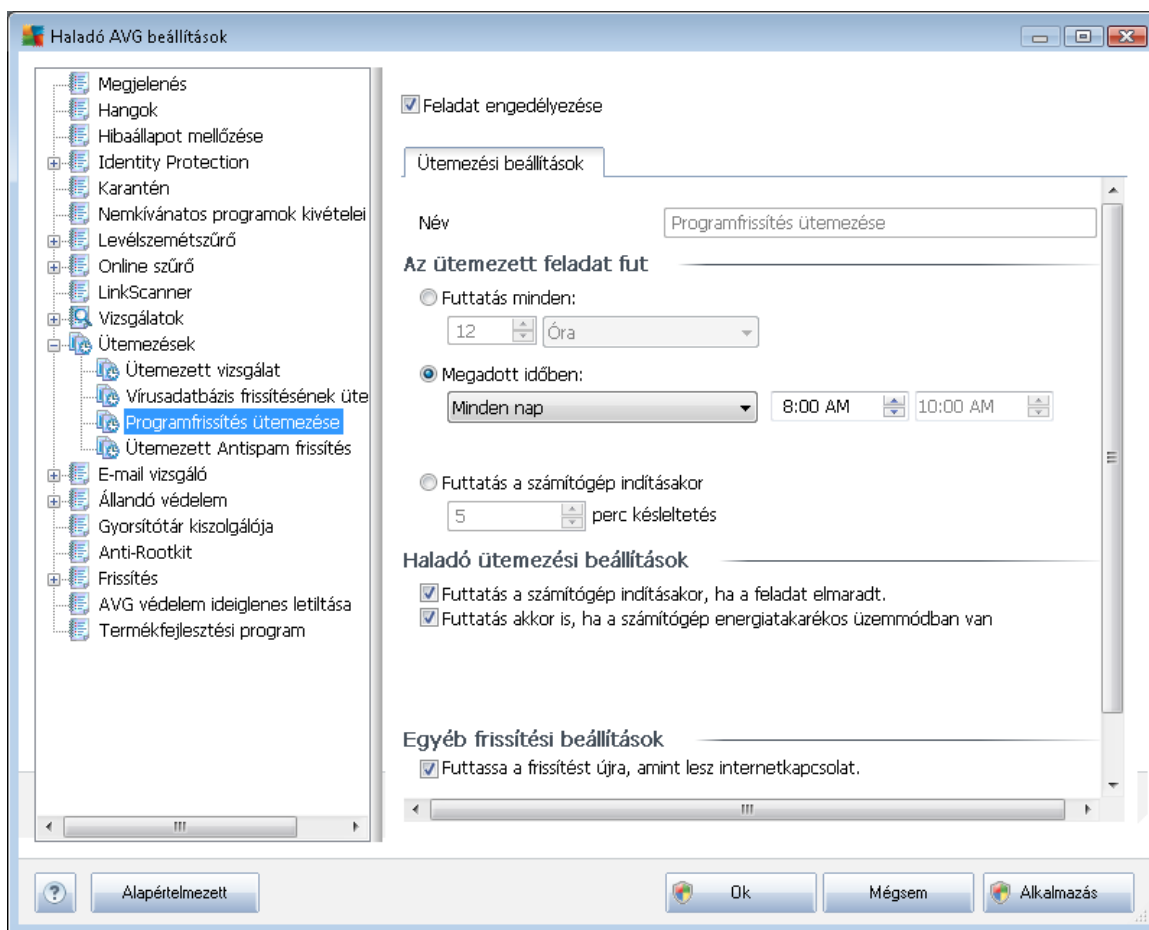
Egyéb frissítési beállítások

Jelölje be a **Frissítés futtatása ismét, amint az internetkapcsolat elérhető** opciót, hogyha 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 felbukkanó ablak formájában az [AVG ikonjánál](#) (feltéve, hogy megtartotta a [Haladó beállítások/Megjelenés](#) panel alapértelmezett beállításait).

9.11.3. 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

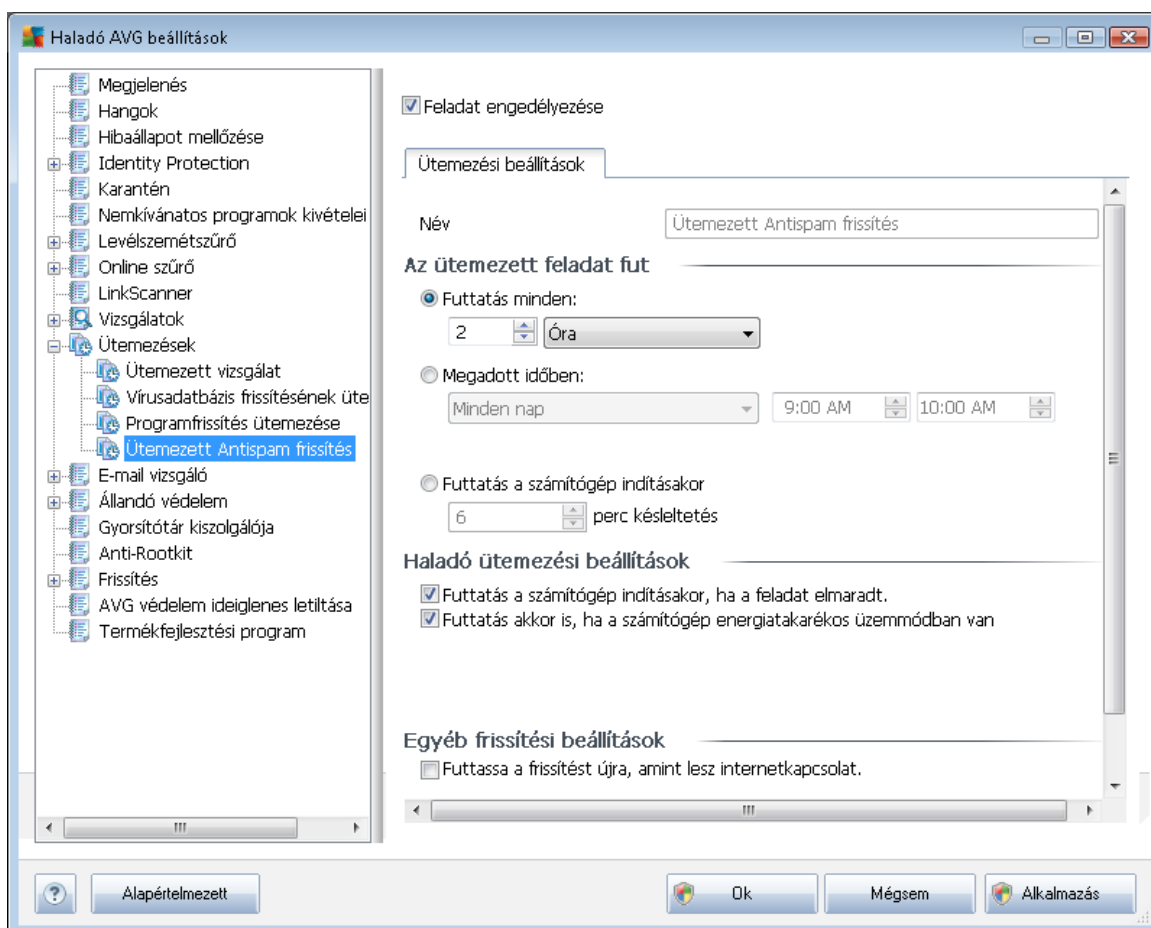
Jelölje be a **Frissítés futtatása ismét, amint az internetkapcsolat elérhető** opciót, hogyha az internetkapcsolat megszakad és a programfrissítés sikertelen, akkor az újra lefusson, miután az internetkapcsolat helyreállt.

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.

9.11.4. Levélszemétszuro frissítés ütemezése

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



Az alapszintű **levélszemétszuro** frissítési ütemezés megtalálható a **Frissítéskezelő** összetevőben. 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 időkört adhatja meg az újonnan létrehozott **Levélszemétszuro** frissítési ütemezésekhez. Az ütemezést meghatározhatja a **Levélszemétszuro** rendszeres időközönként történő futtatásával (**Futtatás minden ...**), pontos dátummal és időponttal (**Futtatás meghatározott időben ...**), vagy egy adott eseményhez kötheti (**Futtatás számítógép indításakor**).

Haladó ütemezési beállítások



Ebben a részben meghatározhatja, hogy a [Levélszemétszűrő](#) frissítése mely körülmények között ne induljon el (a számítógép energiatakarékos módban van vagy teljesen ki van kapcsolva).

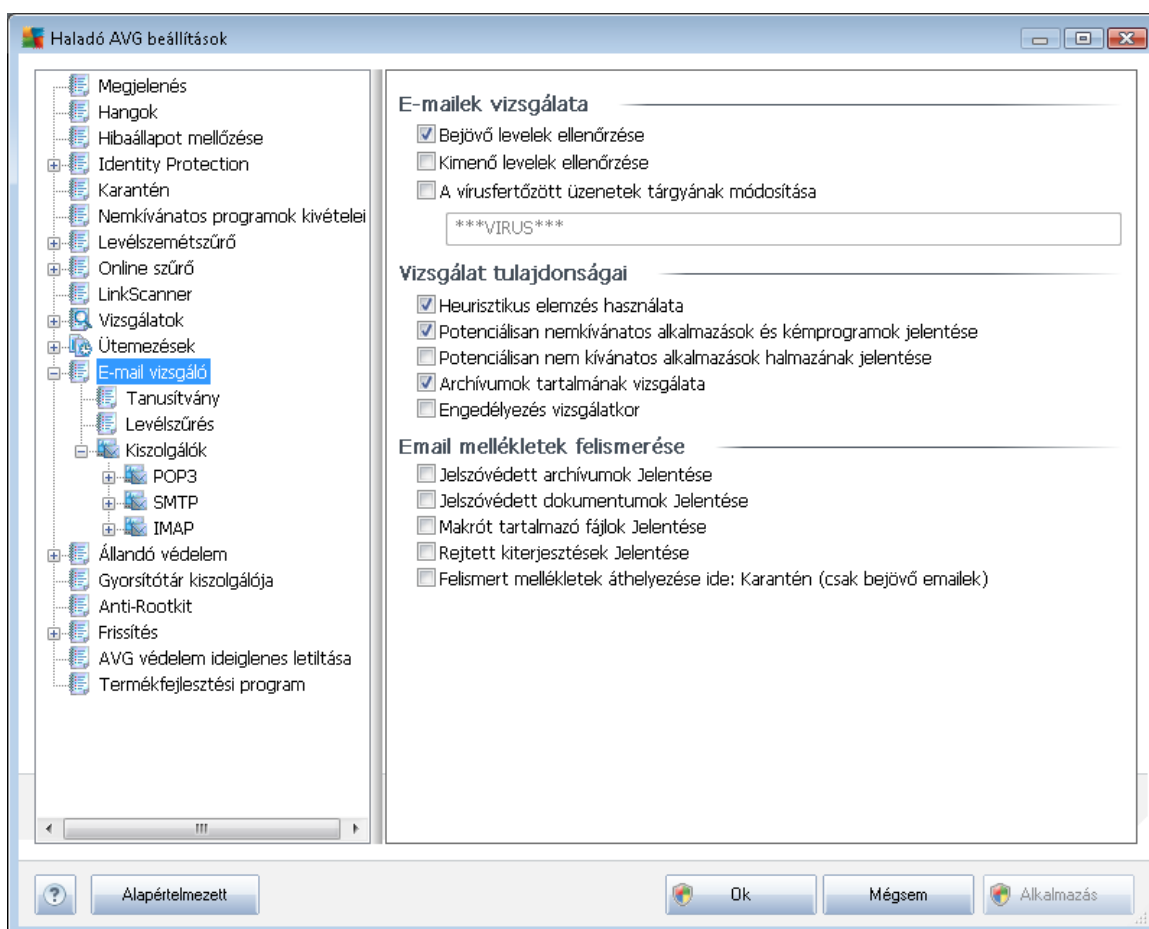
Egyéb frissítési beállítások

Jelölje be a **Frissítés futtatása ismét, amint az internetkapcsolat elérhető** opciót, hogy ha az internetkapcsolat megszakad és a [Levélszemétszűrő](#) frissítése sikertelen, akkor a frissítés újra lefusson, amint az internet kapcsolat helyreállt.

Miután az ütemezett vizsgálat elindult a megadott időben, erről értesítést kap egy felbukkanó ablak formájában az [AVG ikonjánál](#) (feltéve, hogy megtartotta a [Haladó beállítások/Megjelenés](#) panel alapértelmezett beállításait).

9.12. 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 tárgyhöz 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 megglehetősen 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

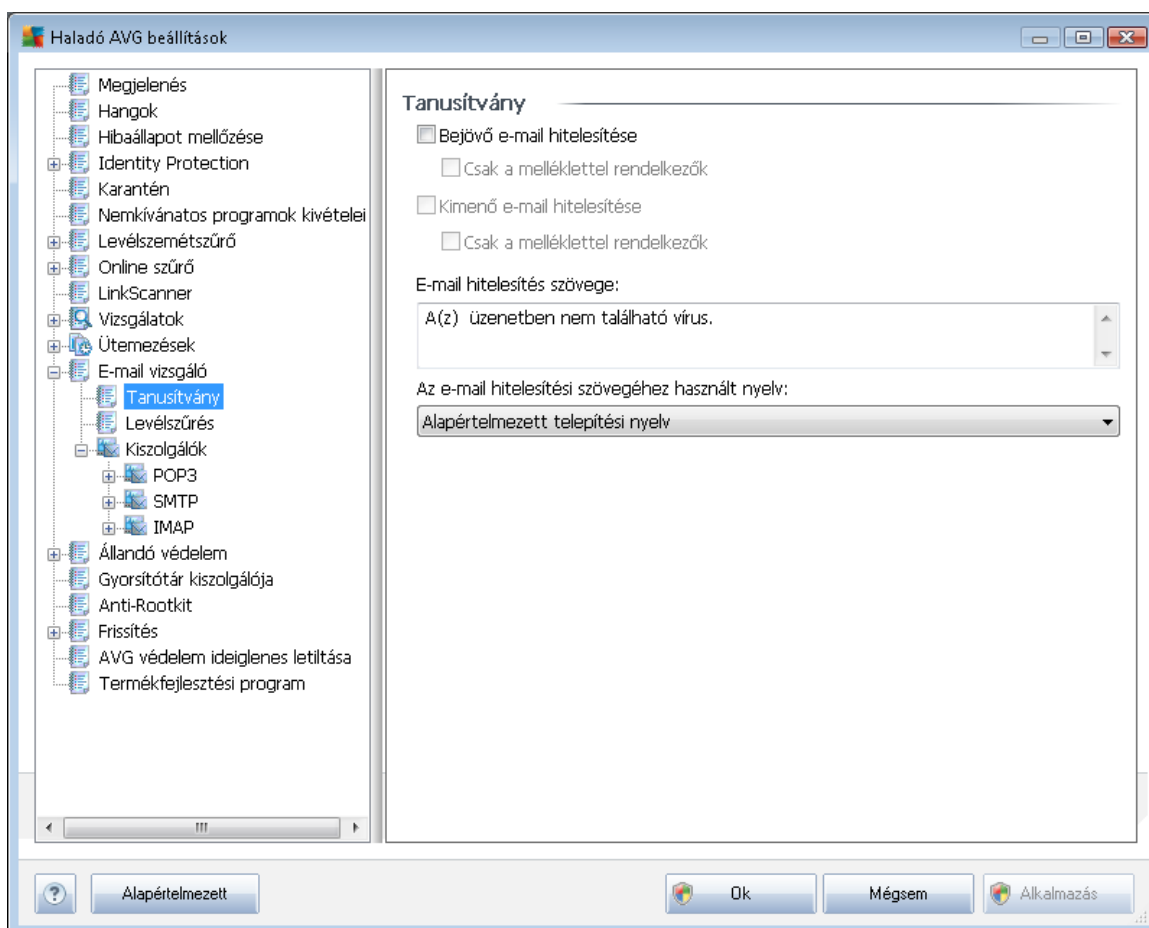


lesz megtalálható:

- **Jelszóval védett archívumok jelentése** – archívumok (ZIP, RAR stb.) melyek jelszóval védettek, nem lehet vizsgálni. Jelölje be az opciót ezen fájlok potenciálisan veszélyesnek minosítéséhez.
- **Jelszóval védett dokumentumok jelentése** - a jelszóval védett dokumentumokat nem lehet vizsgálni. Jelölje be az opciót ezen fájlok potenciálisan veszélyesnek minosítéséhez!
- **Makrókat tartalmazó fájlok jelentése** – a makró előre meghatározott muveleti 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 minosítéséhez!
- **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 minosítéséhez.
- **Mellékletek áthelyezése karanténba** - döntse el, hogy szeretne-e tájékoztatást kapni e-mailben a jelszóvédett archívumokról, jelszóvédett dokumentumokról, makrókat tartalmazó fájlokról és/vagy fájlokról rejtett kiterjesztéssel, melyek egy ellenorzött e-mailhez vannak csatolva. Ha ilyen üzenet lesz azonosítva a vizsgálat során, akkor döntse el, hogy az [Karanténba](#) kerüljön-e.

9.12.1. Tanúsítás

A **Tanúsítvány** panelen megadhatja a bejövő és a kimenő e-mailekhez tartozó tanúsítvány szövegét és nyelvét:



A tanúsítvány szövege két részből áll, egy felhasználói és egy rendszer általi részből - lásd a következő példát: az első sor a felhasználó általi, míg a többi a rendszer által automatikusan generált rész:

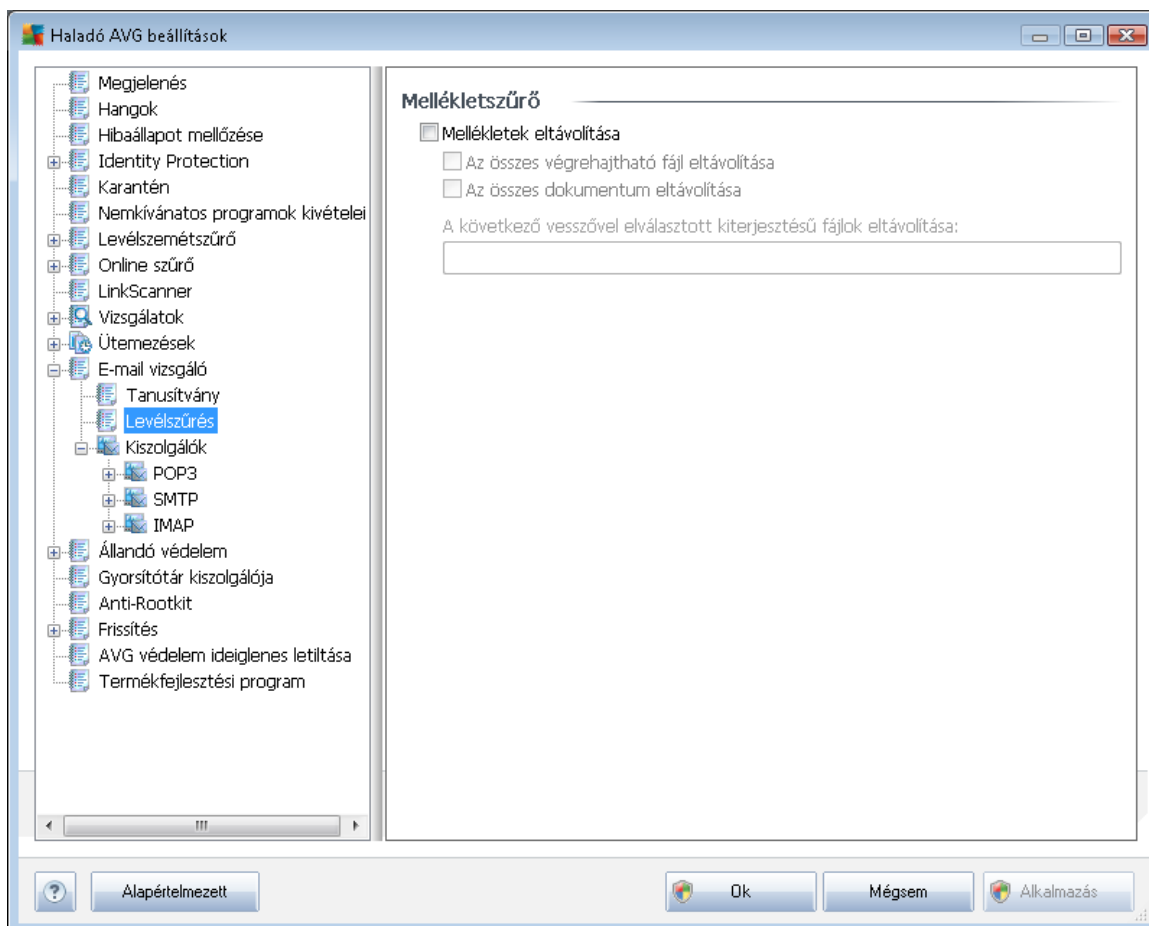
A(z) üzenetben nem található vírus.

Ellenőrizte az AVG.

Verzió: x.y.zz / Vírusadatbázis: xx.y.z - Kiadás dátuma: 12/9/2010

Ha tanúsítást használ a bejövő vagy kimenő e-mailekhez, akkor ezen a panelen megadhatja a tanúsítás pontos szövegét (**E-mail tanúsítási szövege**), és kiválaszthatja az automatikusan generált rész nyelvét (**Az e-mail tanúsítási szövegéhez használt nyelv**).

9.12.2. Levélszurás

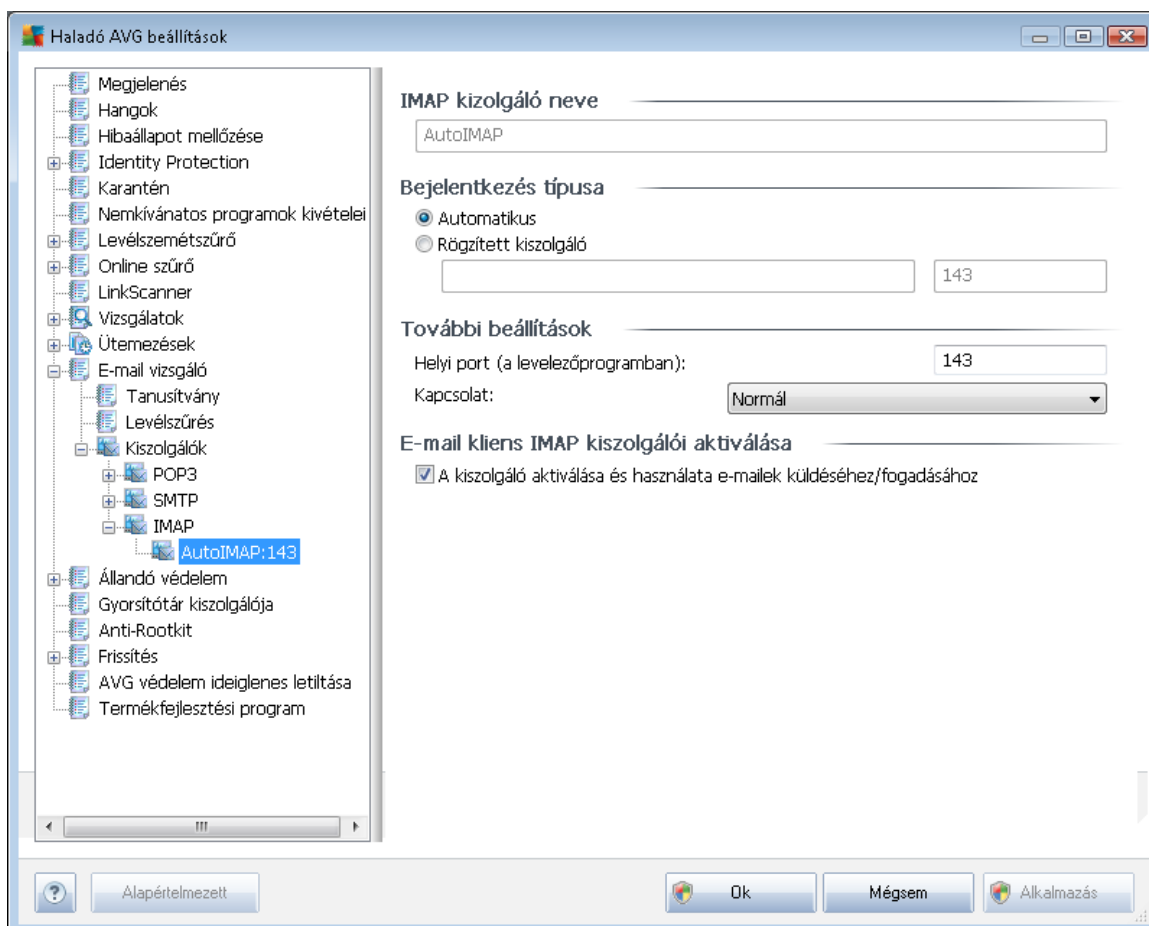


A **Mellékletszűrő** panel lehetővé teszi, hogy megadja az email csatolmányok vizsgálatának paramétereit. Alapállapotban a **Mellékletek eltávolítása** opció ki van kapcsolva. Ha úgy dönt, hogy bekapcsolja, akkor a fertőzött vagy potenciálisan veszélyesnek azonosított csatolmányok automatikusan el lesznek 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

9.12.3. Kiszolgálók

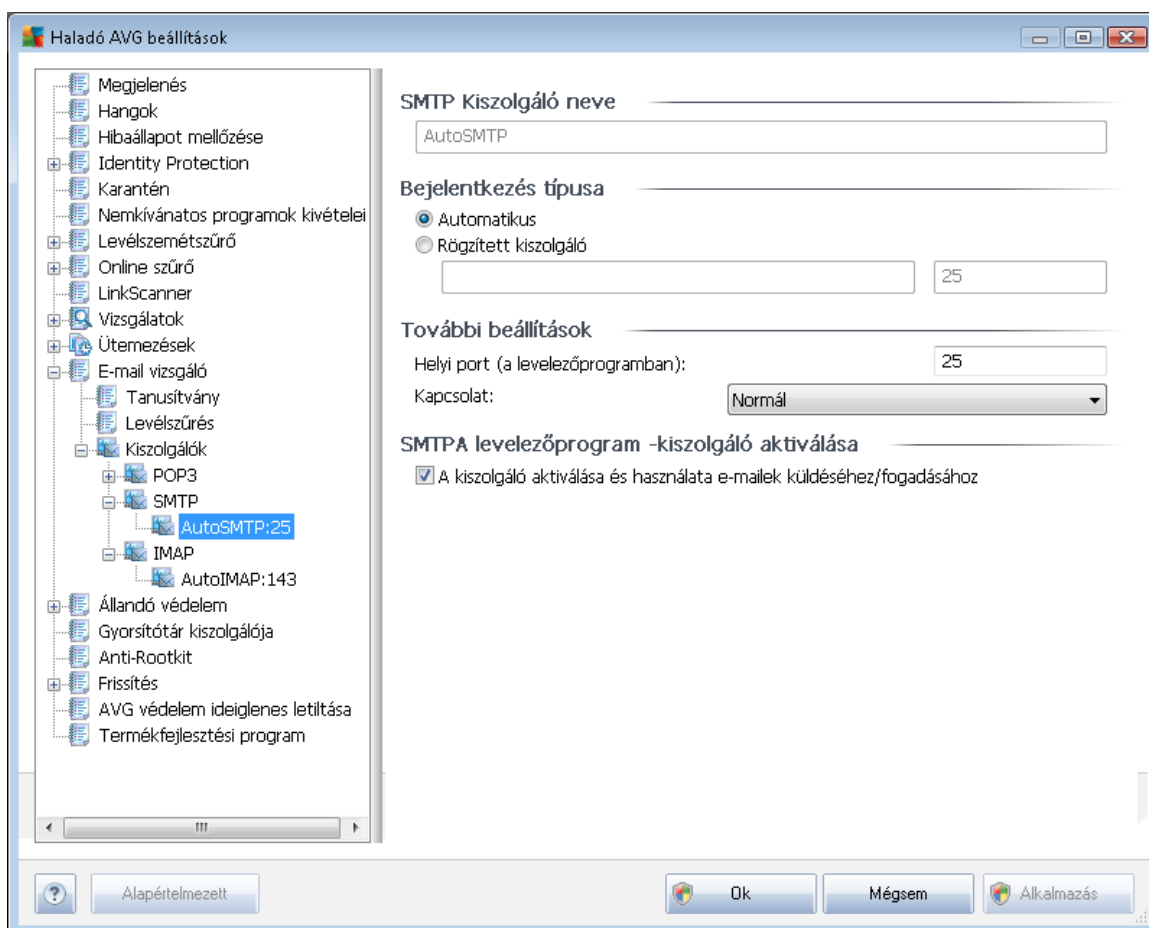
A **Kiszolgálók** részben szerkesztheti az **E-mail vizsgáló** összetevő szervereit, vagy megadhat egy újat az **Új kiszolgáló hozzáadása** gombbal.



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:
 - o **Automatikus** – a bejelentkezés az e-mail ügyfélprogram beállításainak megfelelően automatikusan megtörténik.
 - o **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 névél 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, kettosponttal elválasztva a kiszolgálónév után (például: *pop.acme.com:8200*). A POP3 kommunikáció szabványos portja 110.

- **További beállítások** - további paramétereket adhat meg:
 - o **Helyi port** - meghatározza azt a portszámot, amelyet a levelező program használni fog. Ezután a levelezőprogramban is ezt a portot kell beállítani a POP3 kommunikációhoz.
 - o **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 kívülről 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

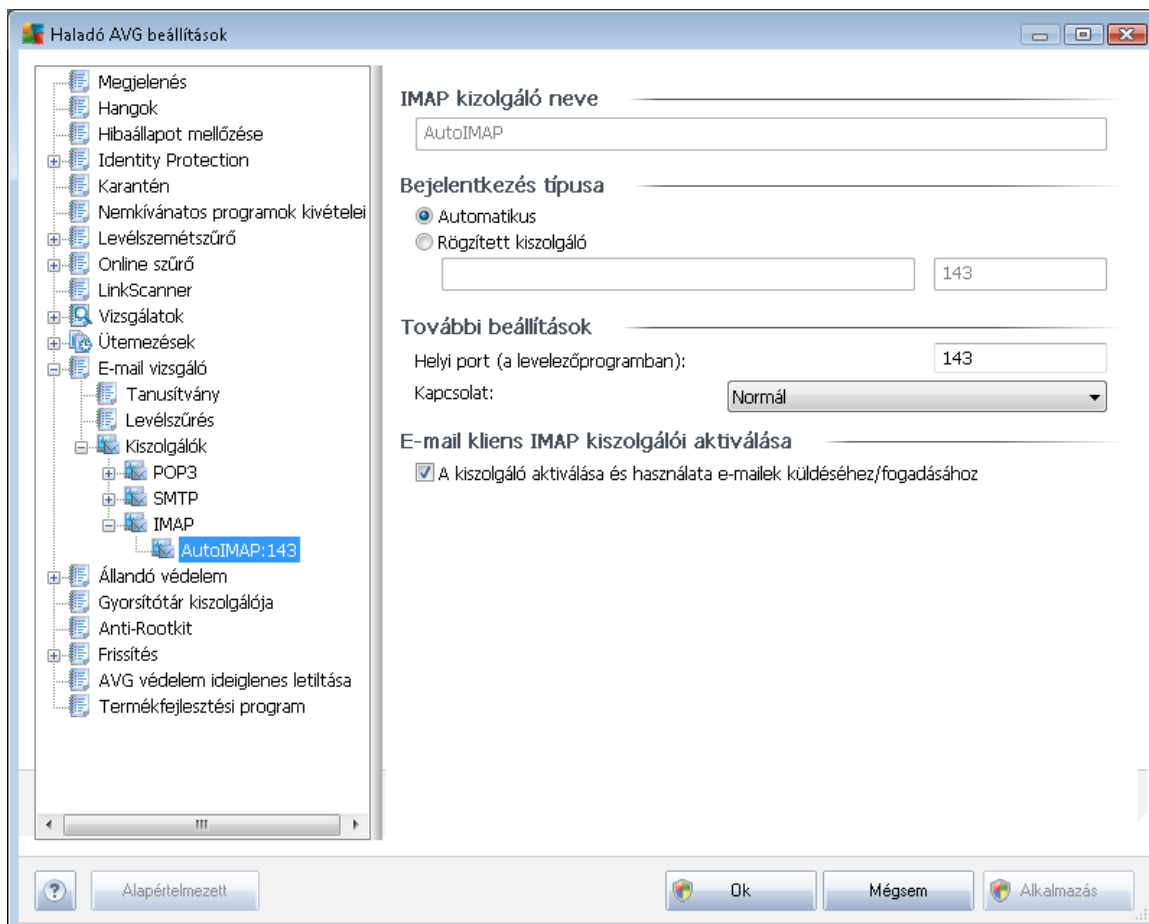


Ebben az ablakban (megnyitva innen: **Kiszolgálók / SMTP**) megadhat egy új **E-mail vizsgáló** kiszolgálót az SMTP protokoll használatával a kimenő levelekhez:

- **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:
 - o **Automatikus** – a bejelentkezés az e-mail ügyfélprogram beállításainak megfelelően automatikusan megtörténik
 - o **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, kettosponttal elválasztva a kiszolgálónév után (például: *smtp.acme.com:8200*). Az SMTP-kommunikáció szabványos portja a 25-ös.
- **További beállítások** - további paramétereket adhat meg:
 - o **Helyi port** - meghatározza azt a portszámot, amelyet a levelező program használni fog. Ezután a levelezőprogramban is ezt a portot kell beállítani az SMTP kommunikációhoz.
 - o **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 kívülről nyomon követhető vagy megfigyelhető 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:
 - o **Automatikus** – a bejelentkezés az e-mail ügyfélprogram beállításainak megfelelően automatikusan megtörténik
 - o **Fix kiszolgáló** - ebben az esetben a program mindig az itt megadott kiszolgálót fogja használni. Adja meg a levelezőkiszolgáló címét vagy nevét. A névél 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, kettosponttal elválasztva a kiszolgálónév után (például: *imap.acme.com:8200*). Az IMAP kommunikáció szabványos portja: 143.

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

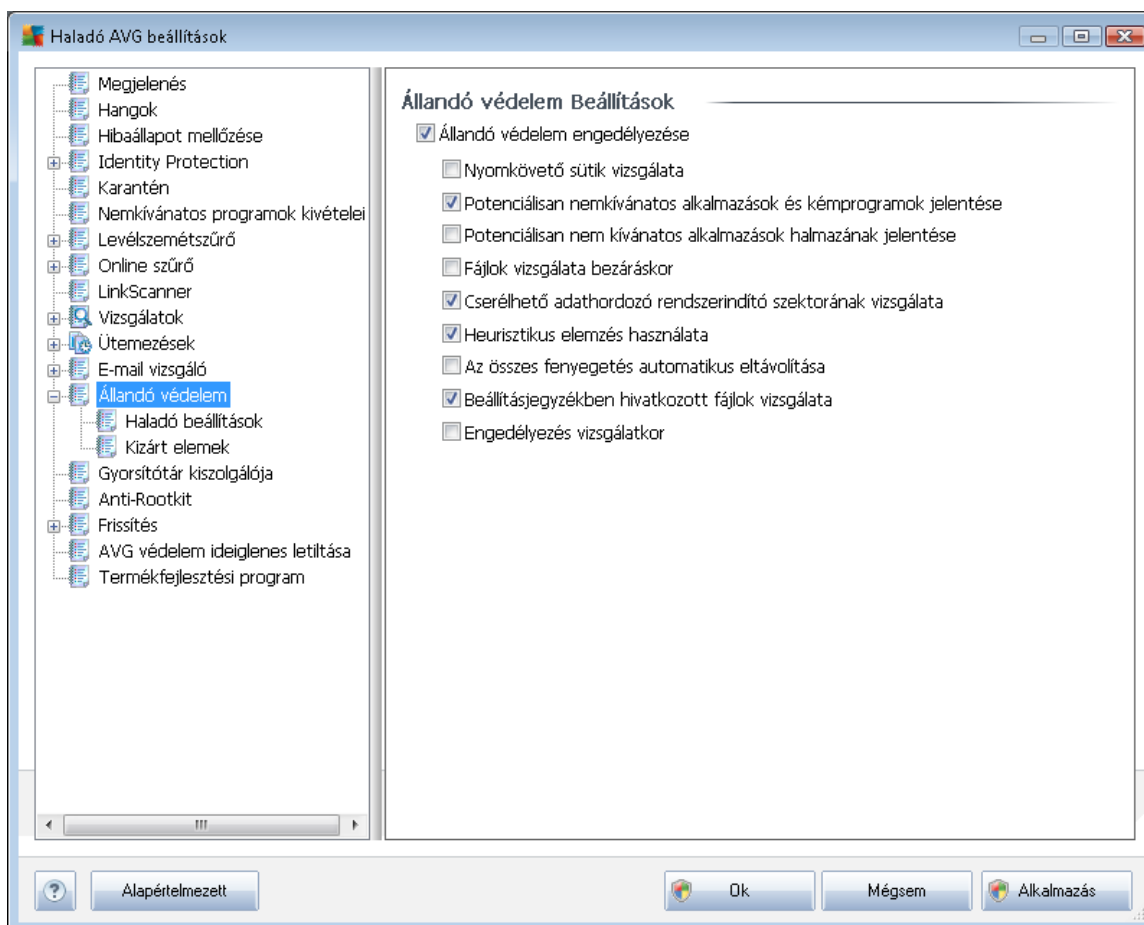
- o **Helyi port** - meghatározza azt a portszámot, amelyet a levelező program használni fog. Ezután a levelezőprogramban is ezt a portot kell beállítania az IMAP kommunikációhoz.

- o **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 kívülről 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

9.13. Állandó védelem

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



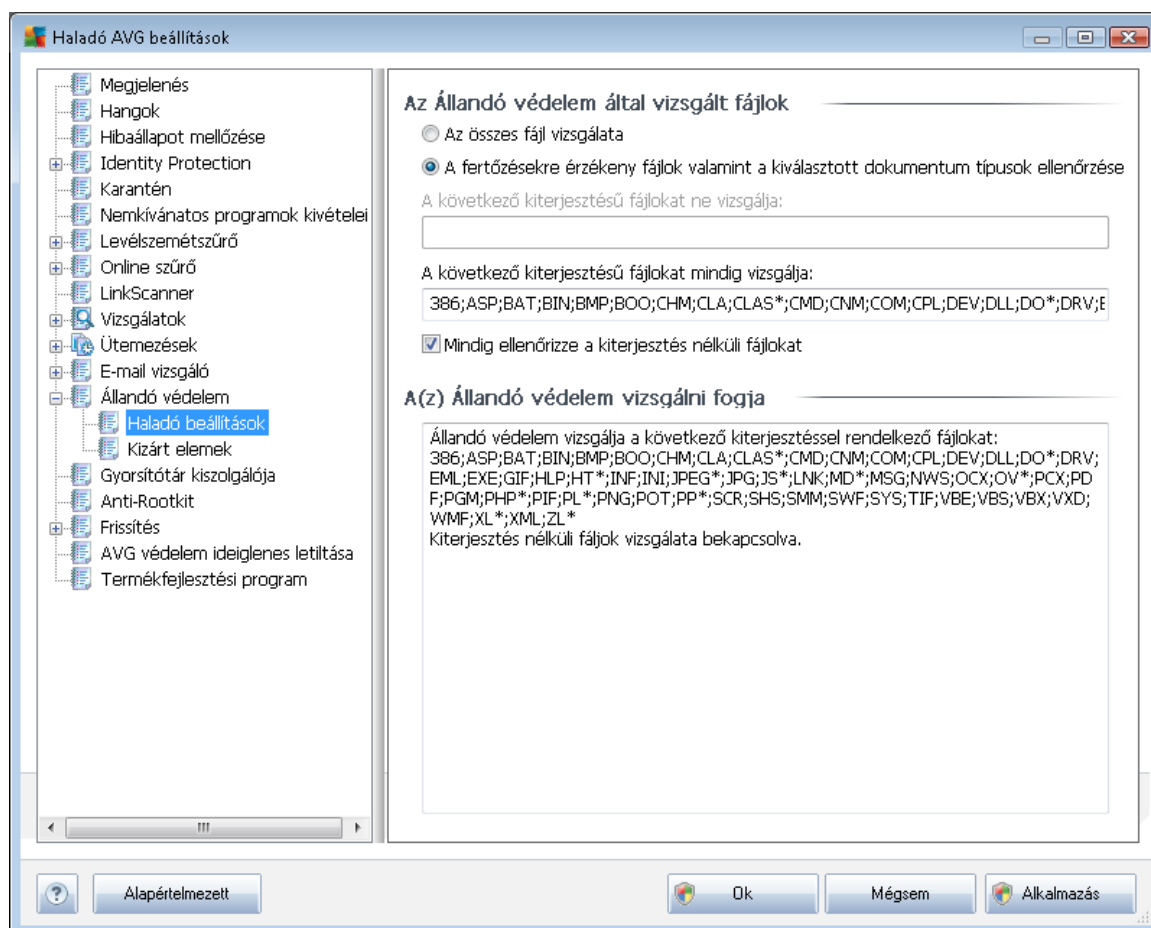
Az **Állandó védelem beállítások** panelen be- és kikapcsolhatja az **Állandó védelem** funkciót az

Állandó védelem engedélyezése elem segítségével (alapállapotban be van kapcsolva). Továbbá kiválaszthatja, hogy mely **Állandó védelem** funkciók legyenek aktiválva:

- **Nyomkövető sütik vizsgálata** (alapállapotban kikapcsolva) - ez a paraméter határozza meg, hogy a sütik fel legyenek-e ismerve a vizsgálat során. (a HTTP sütiket hitelesítéshez, nyomkövetéshez és bizonyos adatok gyűjtéséhez használják a felhasználókról, pl. honlap preferenciák vagy online vásárlás során a kosár tartalma)
- **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.
- **Fájlok vizsgálata bezáráskor** (alapállapotban kikapcsolva) - ez a funkció biztosítja, hogy az AVG vizsgálja az aktív objektumokat (pl. alkalmazásokat, dokumentumokat) megnyitáskor és bezáráskor, így segít megvédeni Önt néhány veszélyes vírustól.
- **Cserélhető adathordozó boot szektorának vizsgálata** (alapállapotban bekapcsolva)
- **Heurisztikus elemzés használata** - (alapállapotban bekapcsolva) [a heurisztikus elemzést](#) azonosításhoz használják (a vizsgált objektum utasításainak dinamikus emulálása' virtuális számítógépes környezetben)
- **Összes fertőzés eltávolítása automatikusan** (alapállapotban kikapcsolva) – az észlelt fertőzések automatikusan javítva lesznek, ha ez lehetséges. A nem javítható fertőzéseket a rendszer törli.
- **Beállításjegyzékben hivatkozott fájlok vizsgálata** (alapállapotban bekapcsolva) - ezzel a paraméterrel meghatározhatja, hogy az AVG vizsgálja a beállításjegyzékhez hozzáadott összes futtatható fájlt annak elkerülése érdekében, hogy egy ismert fertőzés elinduljon a számítógép következő indításakor.
- **Átfogó vizsgálat engedélyezése** (alapállapotban kikapcsolva) - bizonyos helyzetekben (pl. vészhelyzetben) ezen opció bejelölésével aktiválhatja a legátfogóbb vizsgálati algoritmust, amely a lehető legalaposabban vizsgálja át a fenyegető objektumokat. Ne feledje, hogy ez a módszer meglehetősen időigényes.

9.13.1. Haladó beállítások

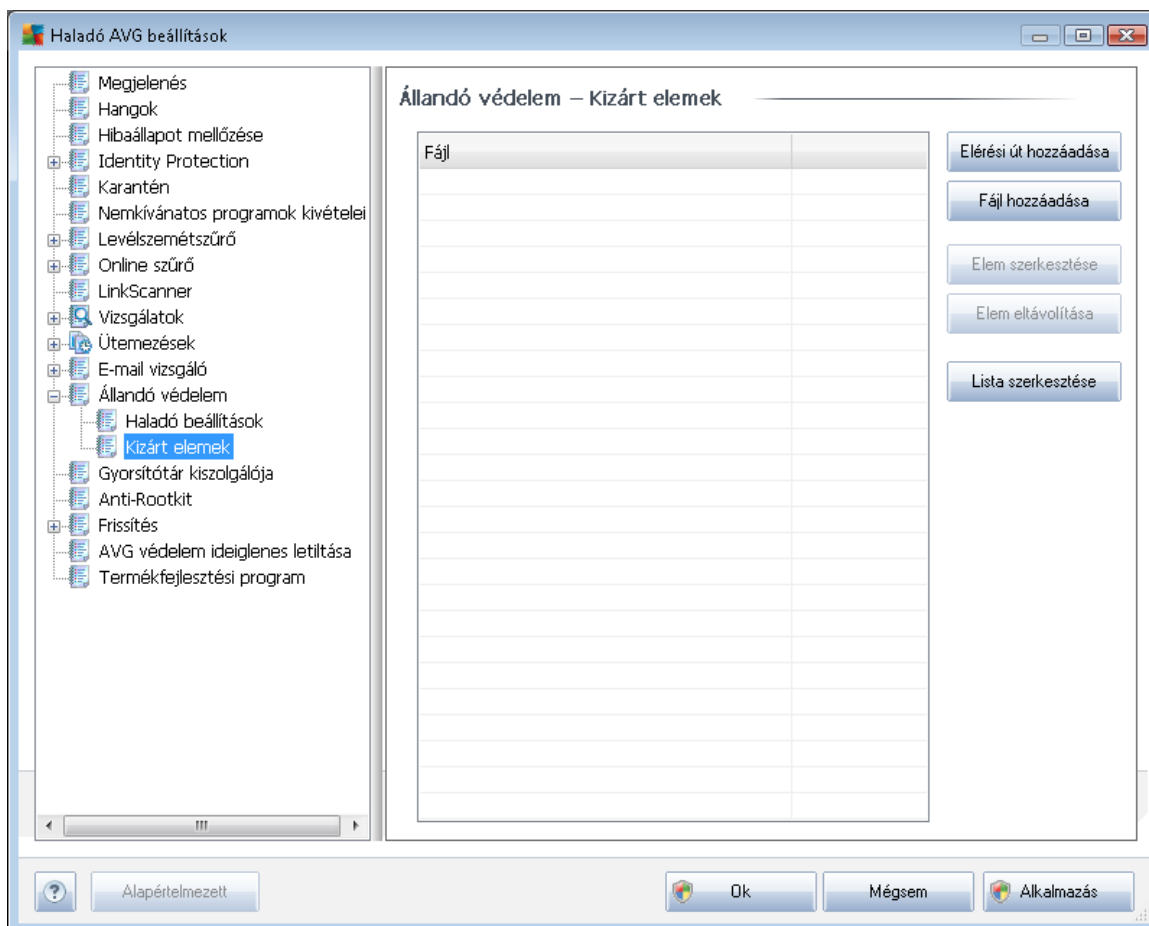
A **Az állandó védelem által vizsgált fájlok** ablakban beállíthatja, hogy mely fájlok legyenek vizsgálva (megadott kiterjesztések):



Megadhatja, hogy minden fájlt vagy csak a fertőzhető fájlokat ellenőrizze a program - továbbá meghatározhatja a kizárható fájlok, illetve a mindenképpen vizsgálandó fájlok kiterjesztéseit is.

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

9.13.2. Kizárt elemek



Az **Állandó védelem - Kizárt elemek** panel lehetővé teszi, hogy meghatározza az **Állandó védelem** vizsgálatból kizárandó fájlok és/vagy mappák listáját.

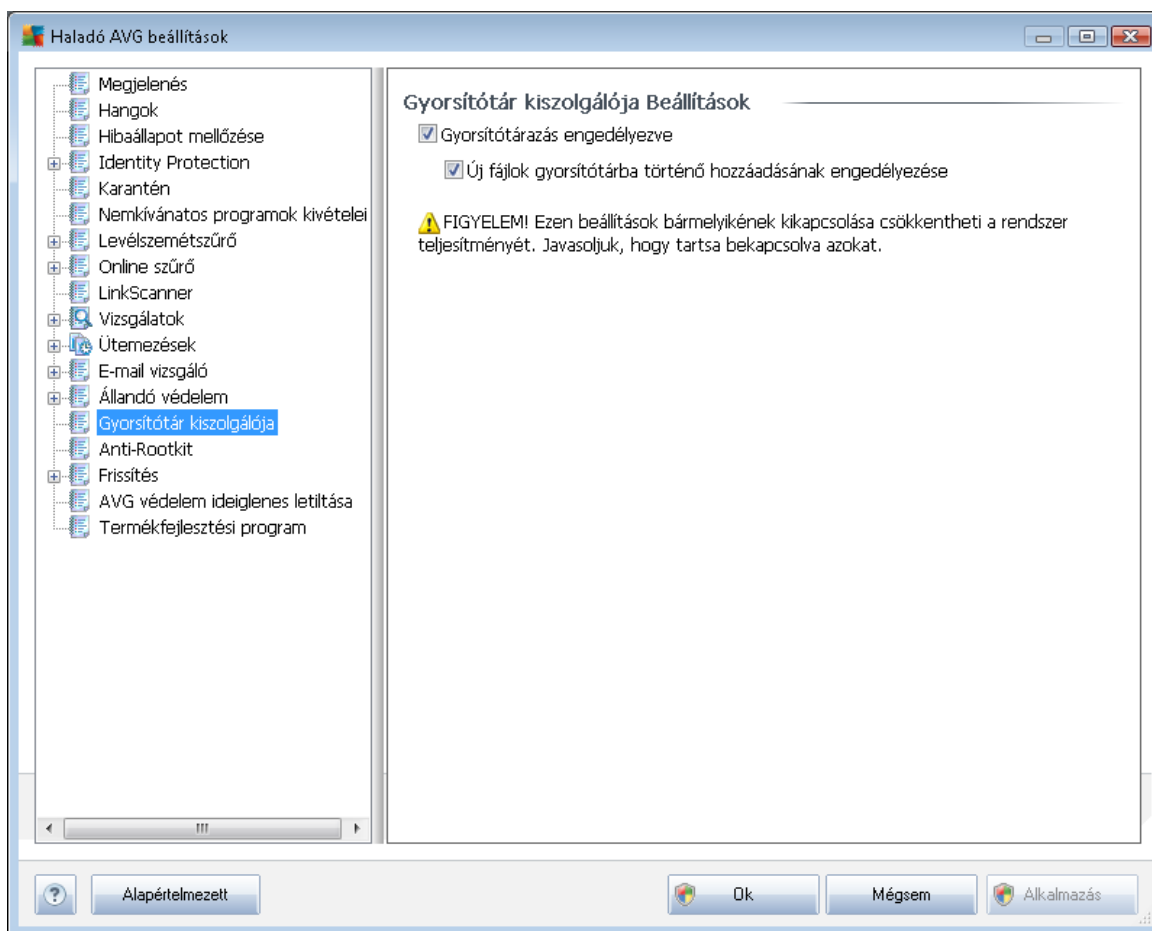
Ha nincs rá külön indoka, akkor nem ajánlott elemeket kihagyni a vizsgálatból!

A párbeszédpanel a következő vezérlogombokat tartalmazza:

- **Elérési út hozzáadása** – lehetőséget nyújt az ellenorzás alól mentesülő könyvtárak megadására. A könyvtárakat a helyi lemezről választhatja ki (egyesével)
- **Fájl hozzáadása** – lehetőséget nyújt az ellenorzás 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

9.14. Gyorsítótár kiszolgálója

A **Gyorsítótár-kiszolgáló** egy olyan folyamat, amely a vizsgálatok felgyorsítására szolgál (*manuális és tervezett vizsgálat, [Állandó védelem](#) vizsgálat*). Információkat tárol és gyűjt a megbízható fájlokról (pl. digitális aláírással rendelkező rendszerfájlokról): Ezen fájlok biztonságosnak tekinthetők és a vizsgálat során ki lesznek hagyva.

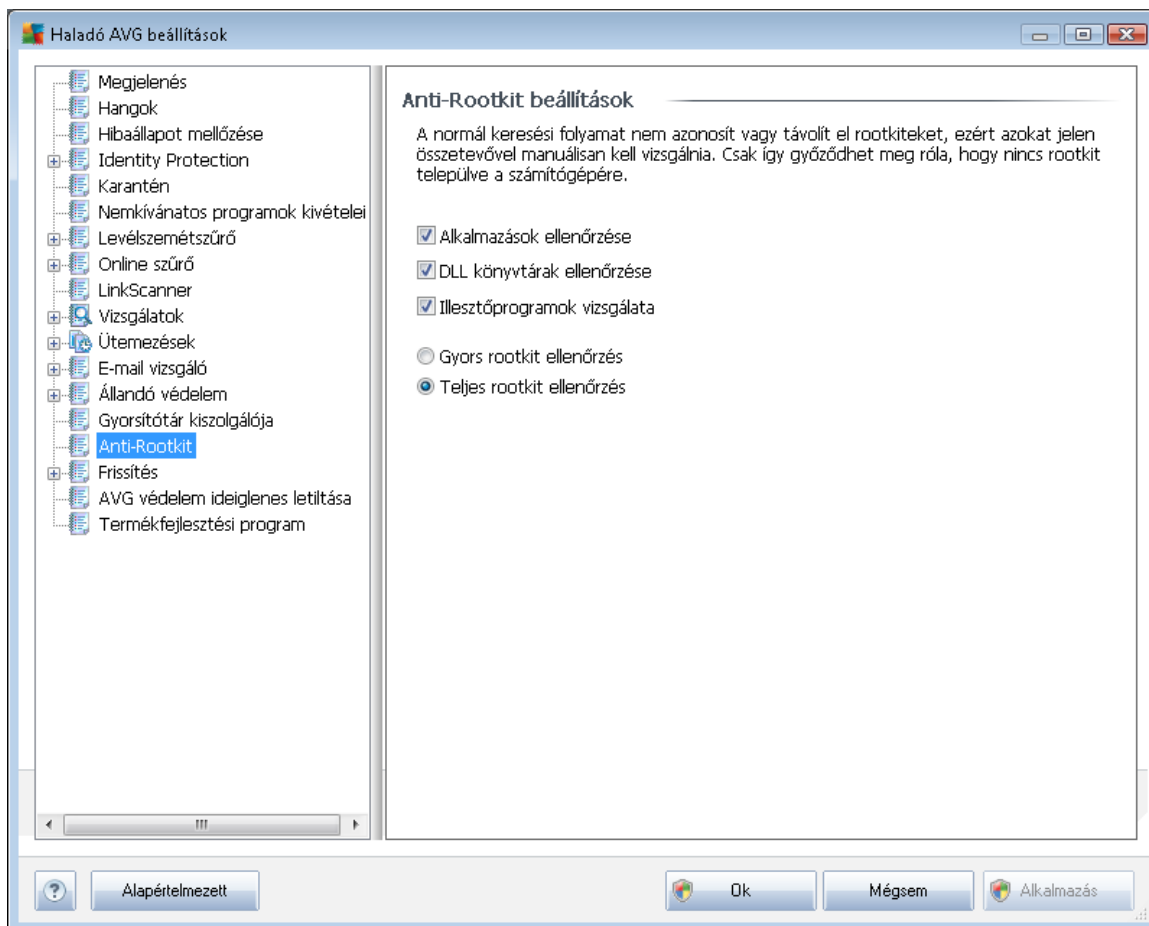


A panelen két beállítás áll rendelkezésre:

- **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.

9.15. Anti-Rootkit

Ezen a penelen szerkesztheti az [Anti-Rootkit](#) összetevő beállításait:



Az [Anti-Rootkit](#) összetevő összes funkciójának szerkesztése közvetlenül is elérhető az [Anti-Rootkit összetevő felületéről](#).

Jelölje be, hogy mely objektumokat kell ellenőrizni:

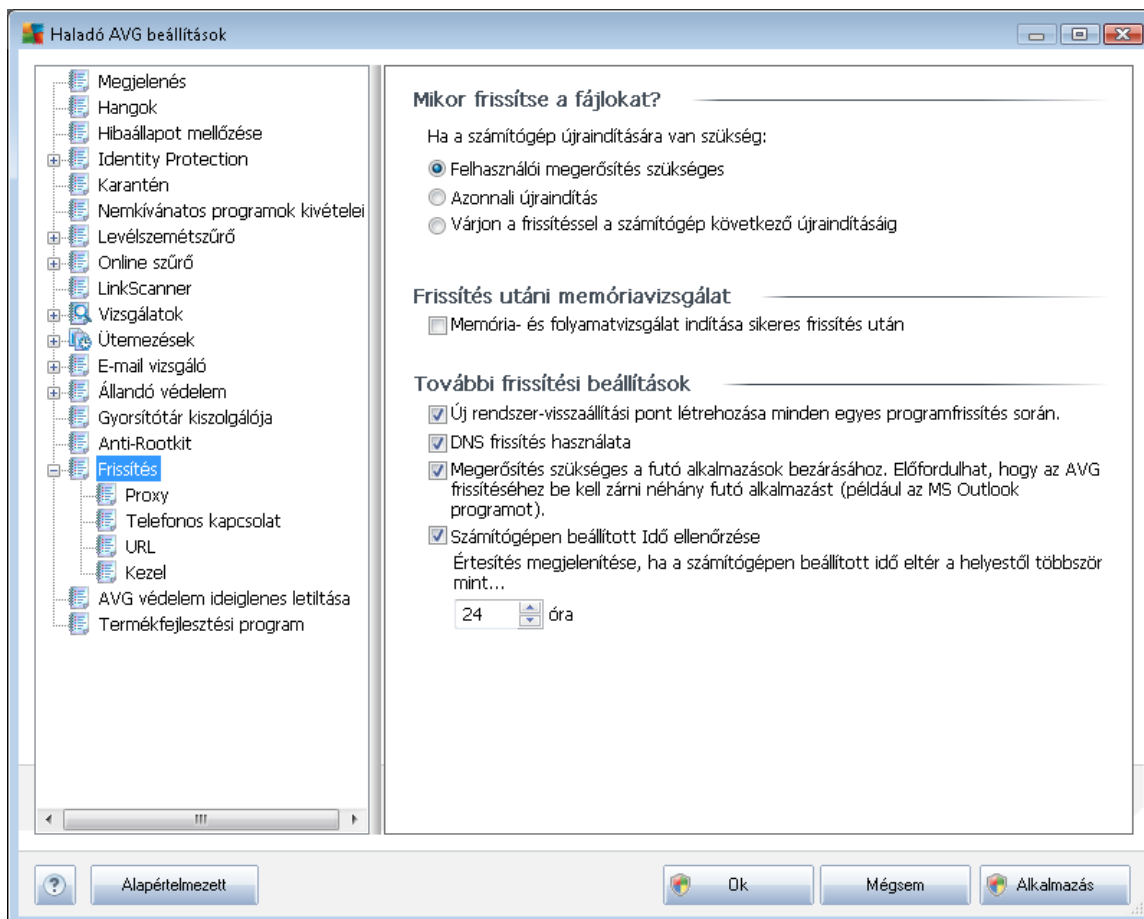
- **Alkalmazások ellenőrzése**
- **DLL könyvtárak ellenőrzése**
- **Illesztőprogramok keresése**

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

rendszerappát (általában c:\Windows), valamint az összes helyi lemezt (flash memóriával együtt, kivéve a floppy-/CD-meghajtókat) ellenorzi

9.16. Frissítés



A **Frissítés** navigációs elem egy új ablakot nyit meg, ahol általános paramétereket adhat meg az [AVG frissítésekkel](#) kapcsolatban:

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 rákérdez az újraindításra a [frissítési folyamat](#)
- **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).

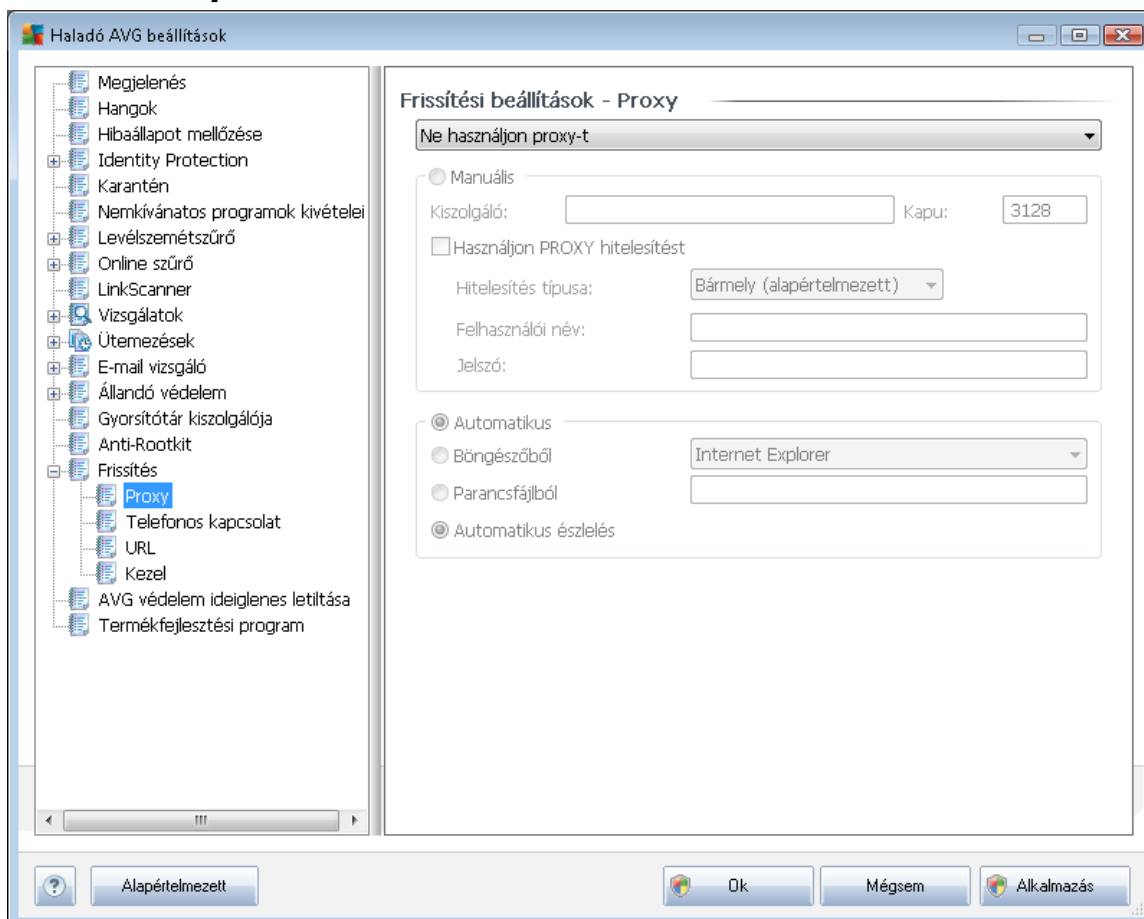
Frissítés utáni memóriavizsgálat

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 , menübol, 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 2011** 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 Megerosítés szükséges a futó alkalmazások bezárásához**(alapállapotban bekapcsolva) elem bejelölésével biztosíthatja, hogy egyetlen futó alkalmazás se legyen bezárva az Ön engedélye nélkül - ha ez szükséges a frissítési folyamat befejezéséhez;
- **Számítógépen beállított idő ellenőrzése** -jelölje be ezt az opciót, ha szeretne értesítést kapni arról, hogy a számítógépen beállított idő a megadottnál jobban eltér a tényleges időtől.

9.16.1. 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**
- **Proxykiszolgáló használatának mellozése**- 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)

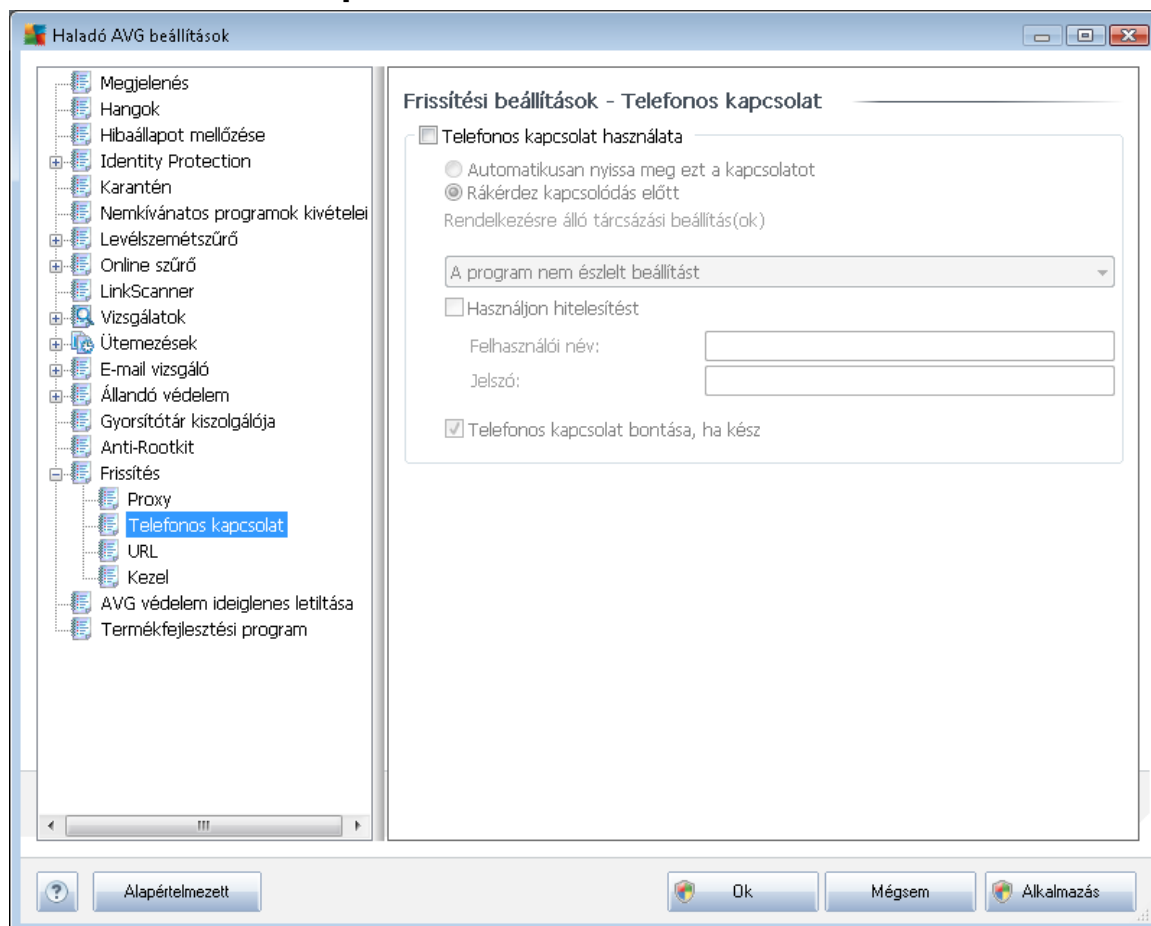
A proxykiszolgálónál az egyes felhasználókra különböző szabályok vonatkozhatnak. Ha így állítja be a proxy kiszolgálót, akkor jelölje be a **Használjon PROXY hitelesítést** opciót, hogy ellenőrizhesse, a kiszolgálón keresztüli internetcsatlakozáshoz megadott felhasználónév és jelszó megfelelő.

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

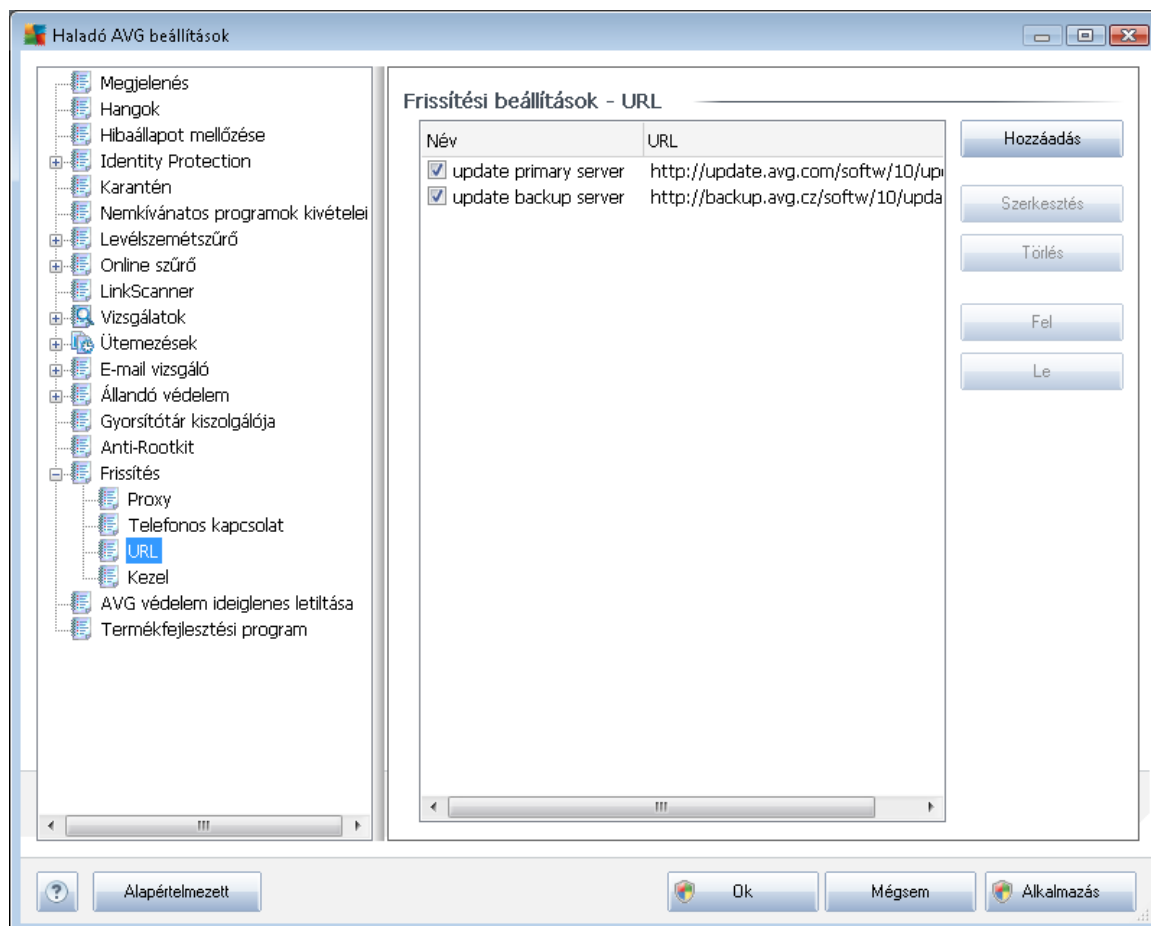
9.16.2. Telefonos kapcsolat



A tetszőlegesen meghatározható paraméterek a **Frissítési beállítások - Telefonos kapcsolat** panelen a betárcsázós internetkapcsolatra vonatkoznak. A panel mezői csak akkor válnak aktívá, 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**).

9.16.3. URL

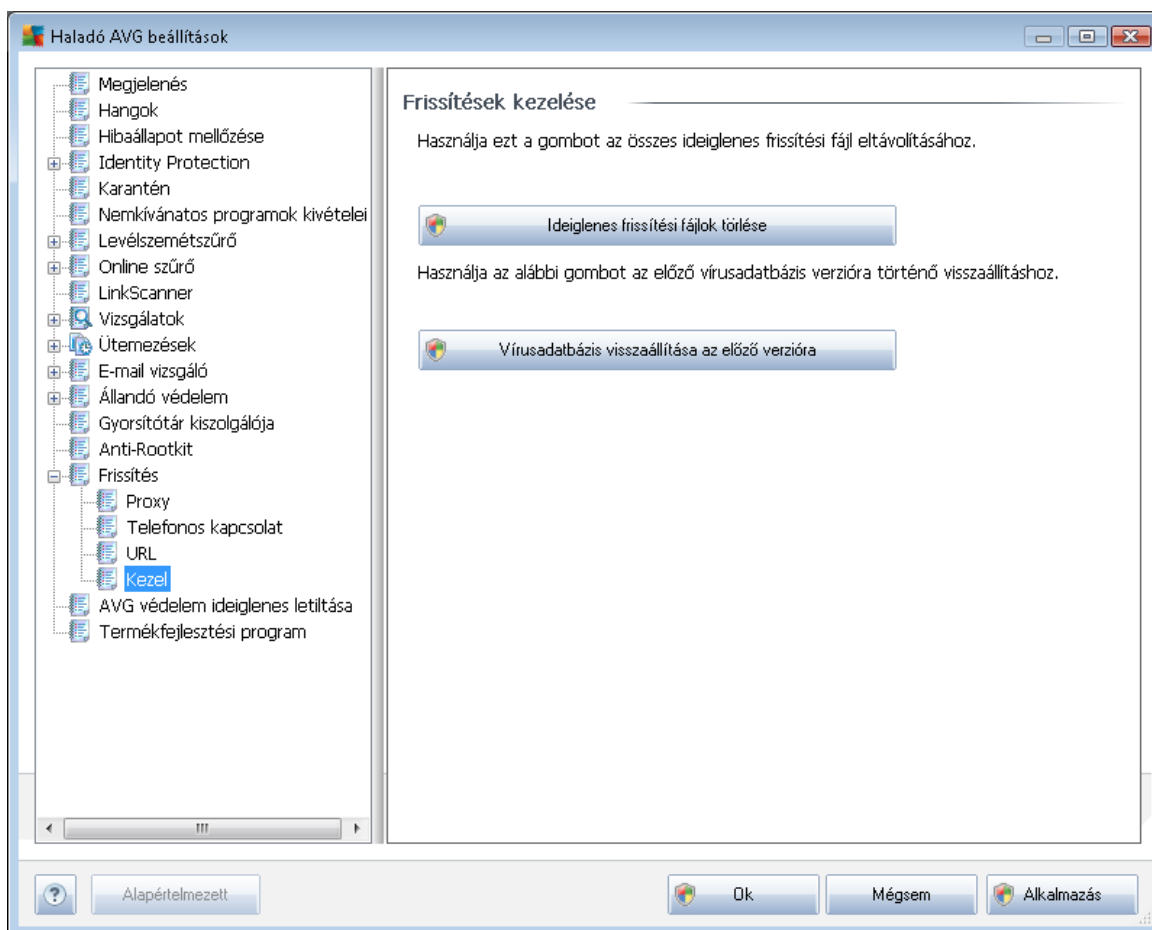


Az **URL** lapon a frissítési fájlok letöltésére használható internetes címek vannak felsorolva. A lista és a lista elemeinek megváltoztatása a következő kezelógombokkal történik:

- **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 előrebb mozdítása a listában egy hellyel
- **Le**- a kijelölt URL hátrébb mozdítása a listában egy hellyel

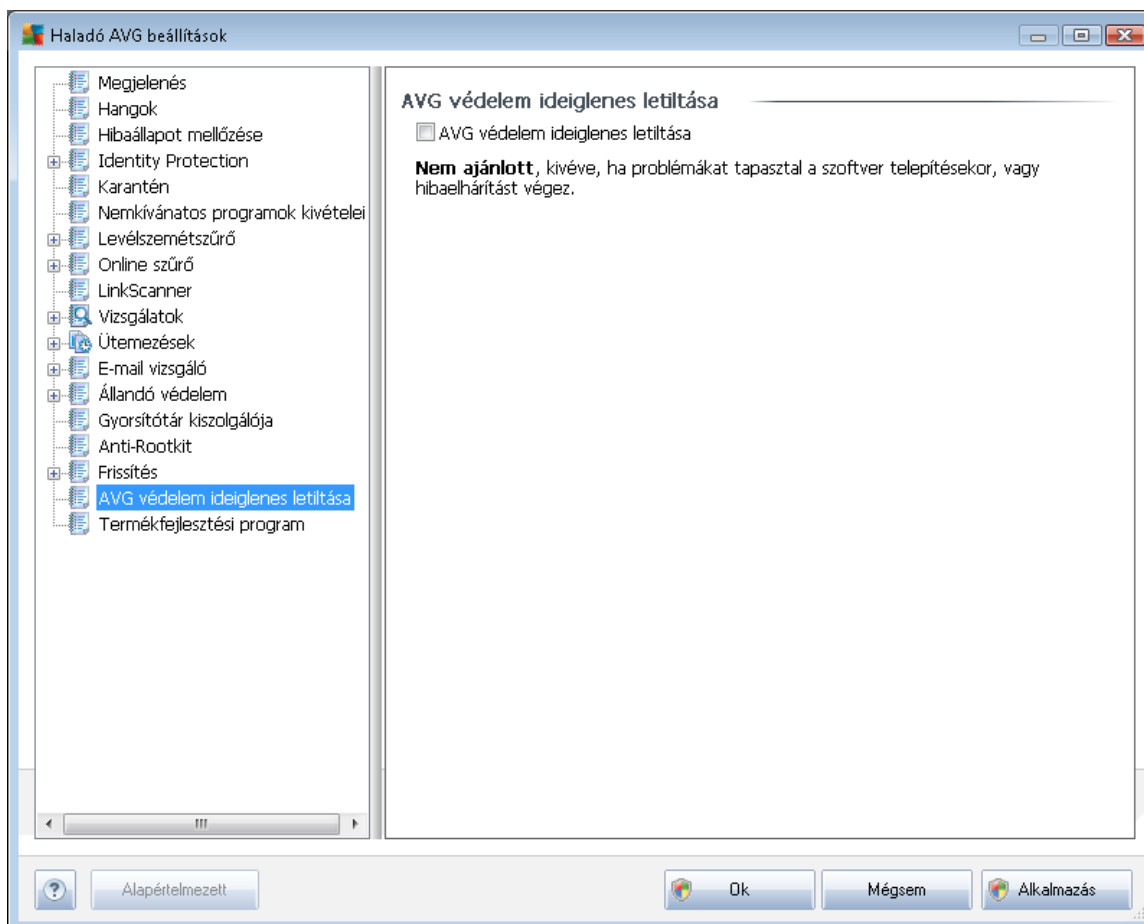
9.16.4. Kezel

A **Kezel** panel két opciót biztosít:



- **Ideiglenes frissítési fájlok törlése** - nyomja meg ezt a gombot az összes szükségtelen frissítési fájl törléséhez a merevlemezről (*alapállapotban ezek a fájlok 30 napig tárolódnak*)
- **Vírusadatbázis visszaállítása az elozo verzióra** - nyomja meg ezt a gombot az aktuális vírusadatbázis törléséhez, és az elozo mentett verzióhoz történő visszatéréshez (az új adatbázis verzió a következő frissítéskor fog települni)

9.17. Az AVG védelem ideiglenes letiltása



Az **AVG védelem ideiglenes letiltása** panel lehetővé teszi az **AVG Internet Security 2011** teljes védelmének kikapcsolását.

Ne feledje, hogy ezt az opciót csak akkor használja, ha feltétlenül szükséges.

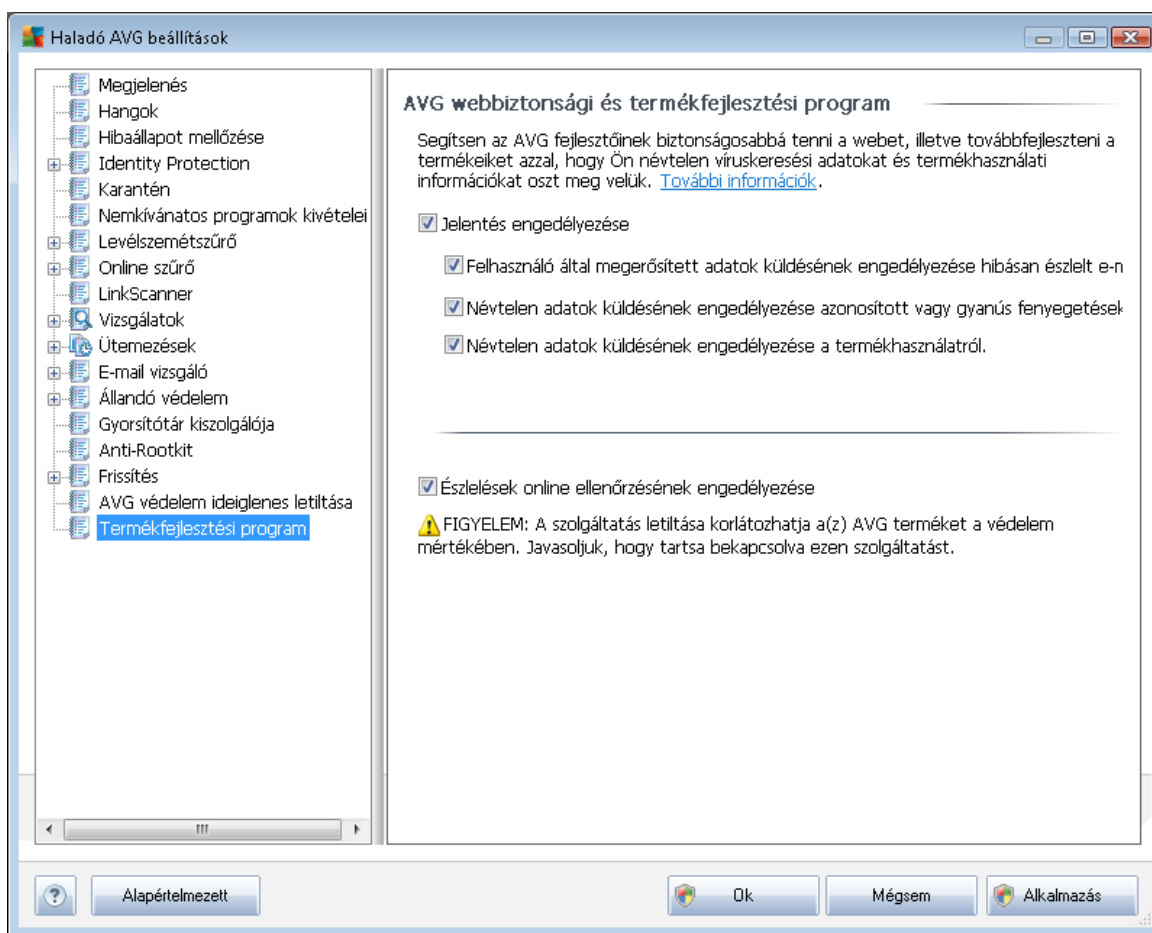
A legtöbb esetben **nem szükséges kikapcsolnia** az AVG védelmet az új szoftver vagy illesztőprogram telepítése előtt, még akkor sem, ha a telepítő vagy a varázsló azt javasolja, hogy zárja be a futó programokat és alkalmazásokat a telepítési folyamat zavartalanítása érdekében. Ha problémákat észlel a telepítések során, akkor kapcsolja ki az **Állandó védelem** összetevőt. Ha ideiglenes ki kell kapcsolnia az AVG védelmet, akkor mielőbb kapcsolja vissza azt, amint lehetséges. Ha kikapcsolt víruskereső szoftverrel kapcsolódik az internetre vagy egy hálózatra, akkor az Ön számítógépe támadásoknak van kitéve.

9.18. Termékfejlesztési program

Az **AVG webbiztonsági és termékfejlesztési program** panel meghívja Önt az AVG termékfejlesztésében való részvételre, így segíthet nekünk növelni az online biztonságot. Jelölje be a **Jelentés engedélyezése** opciót az észlelt fenyegetések AVG-nek történő jelentéséhez. Ez segít nekünk összegyűjteni a legfrissebb információkat a legújabb fenyegetésekről a világ számos

pontján, és cserébe továbbfejlesztjük az védelmet mindenki számára.

A jelentés teljesen automatikus, ezért nem okoz kényelmetlenséget, és semmilyen személyes azonosításra alkalmas adatot nem küld el. Az észlelt fenyegetések jelentése tetszoleges, de kérjük, hogy kapcsolja be ezt a funkciót, mivel ez segít nekünk továbbfejleszteni a védelmet Ön és más AVG felhasználók számára is.



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

- **A vírus olyan rosszindulatú kód, mely sokszorozítja 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 betölteni a számítógép memóriáját, és teljesen lebéníthatja azt.
- **A féreg** a vírusok egyik olyan kategóriájába tartozik, mely a vírustól eltérően semmilyen más hordozóhoz nem kapcsolódik, hanem egy az egyben küldi el saját magát más



számítógépekre (általában emailben), és ennek eredményeképpen gyakran túlterheli az email 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 elozmények 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 bújk. A potenciális áldozatokat általában csoportos emailben keresik meg, és arra kérik őket, hogy például frissítsék bankszámlájával 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 a következő különleges összetevőket alkalmazza:

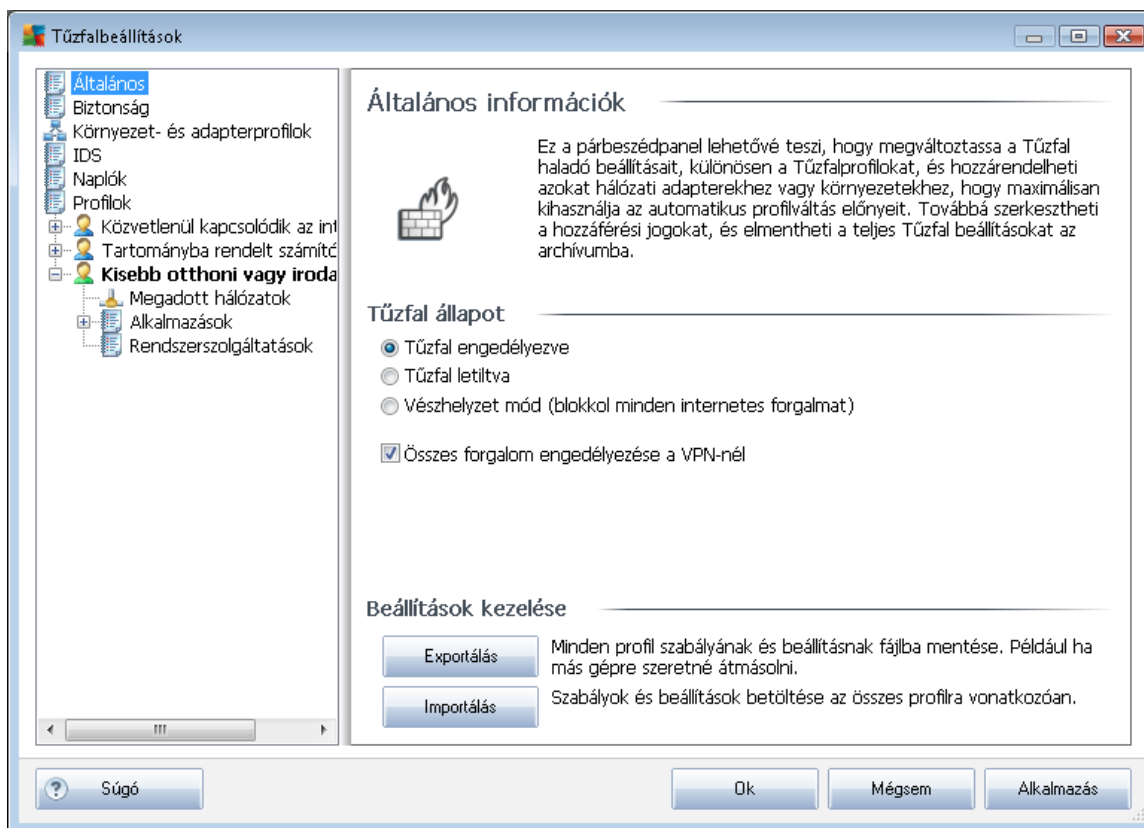
- [Víruskereso](#), mely megvédi a számítógépet a vírusoktól,
- [Víruskereso](#), mely megvédi a számítógépet a kémprogramoktól,
- Az [Online szuro](#) véd a vírusoktól és a kémprogramoktól az internet böngészése során,
- [míg a LinkScanner](#) ebben a fejezetben is említett egyéb online fenyegetésektől véd.

10. Tuzfalbeállítások

A **Tuzfal** beállítások új ablakban nyílnak meg, ahol megadhatja a haladó beállításokat. **A haladó beállítások szerkesztését csak szakérto és tapasztalt felhasználóknak javasoljuk.**

10.1. Általános

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



Tuzfal állapota

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

- **Tuzfal engedélyezve** - válassza ezt az opciót azon alkalmazások kommunikációjának engedélyezéséhez, melyek "engedélyezett" minősítést kaptak a **Tuzfal profilban**
- **Tuzfal letiltva** - ez az opció teljesen kikapcsolja a **Tuzfalat**, a rendszer minden hálózati forgalmat engedélyez, ellenőrzés nincs.
- **Vészhelyzet mód (minden internetes forgalom tiltása)** - válassza ezt az opciót az összes forgalom tiltásához minden porton. A **Tuzfal** fut, de a hálózati forgalom tiltva van
- **Összes forgalom engedélyezése a VPN-nél** – ha VPN kapcsolatot (virtuális



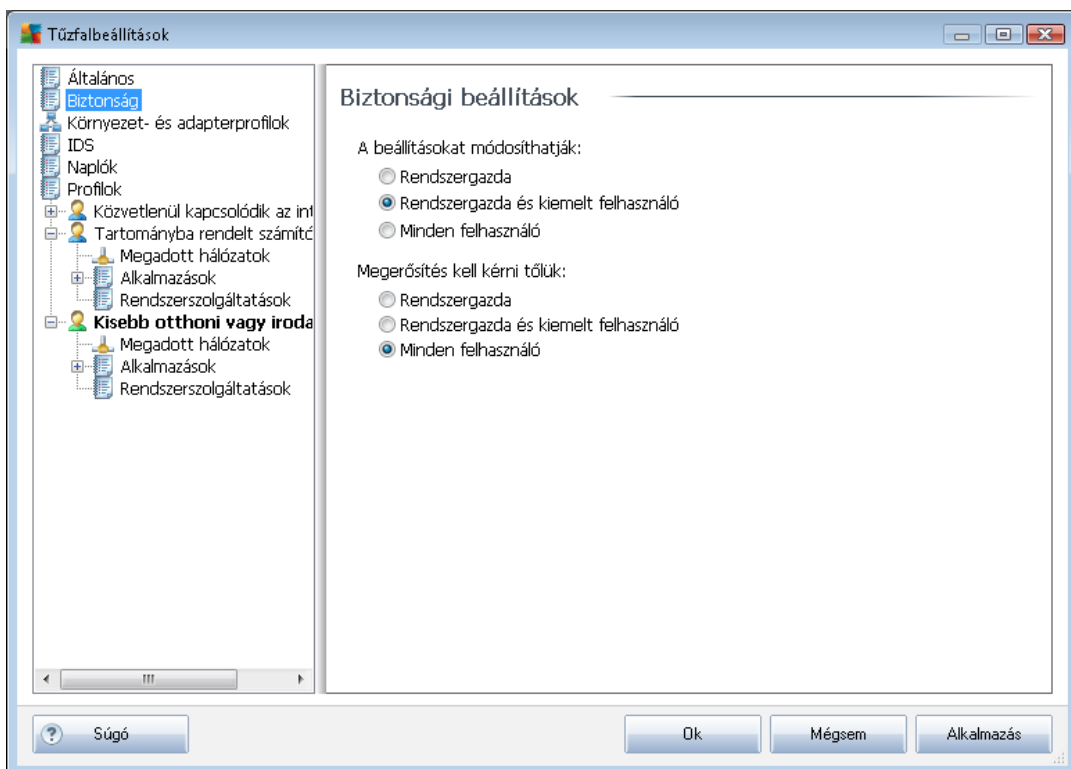
magánhálózatot) használ (például az irodájához kapcsolódik otthonról), akkor javasoljuk, hogy jelölje be ezt a jelölőnégyzetet. Az **AVG Tuzfal** automatikusan átnézi a hálózati adaptereket, és kiválasztja a VPN kapcsolathoz tartozókat, majd engedélyezi az összes alkalmazás kapcsolódását a célhálózathoz (*csak olyan alkalmazásoknál, amelyekhez nincs hozzárendelve külön Tuzfal 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 kezelé**sepanelen **exportálhatja** **importálhatja** a **Tuzfal** beállításait, pl. exportálhatja a meghatározott **Tuzfal** szabályokat és beállításokat az archívumba, vagy visszaállíthatja azokat az archívumból.

10.2. Biztonság



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

- **A beállításokat módosíthatják** - adja meg, hogy kinek engedélyezett a **Tuzfal** beállításainak módosítása

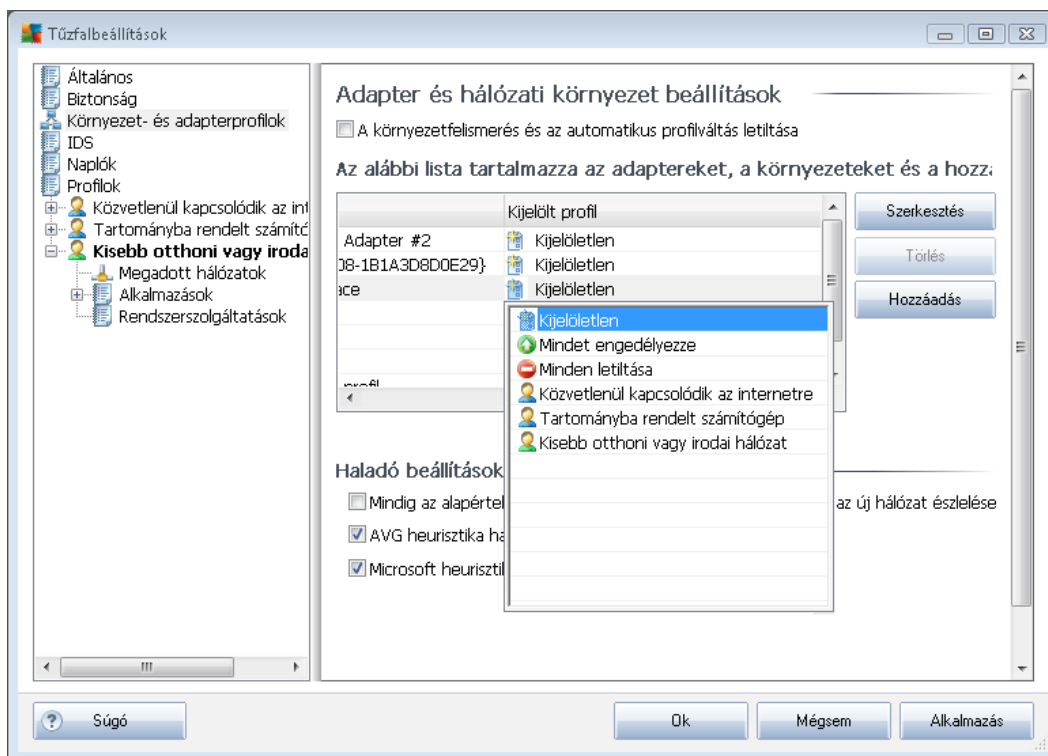
- **Megerősítést kell kérni tőlük** - adja meg, hogy kinek legyen megerősítő üzenet megjelenítve (olyan üzenetrol van szó, mely akkor kér megerősítést, ha az adott művelet nincs meghatározva a [Tuzfal](#) szabályokban)

Mindkét esetben a következő felhasználói csoporthoz rendelheti hozzá az adott jogokat:

- **Rendszergazda** – teljes hozzáféréssel bír a számítógépen, és joga van az egyes felhasználókat a megadott jogosultsággal meghatározott csoportokba sorolni
- **Rendszergazda és kiemelt felhasználók** – a rendszergazda bármely felhasználót a megadott csoportba (kiemelt felhasználók) sorolhat, és meghatározhatja a csoporttagok jogait
- **Minden felhasználó** – egyéb felhasználók, akik nem tartoznak egyik kijelölt 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** - egy adott profilt hozzá lehet rendelni egy adott hálózati interfész típushoz, 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.

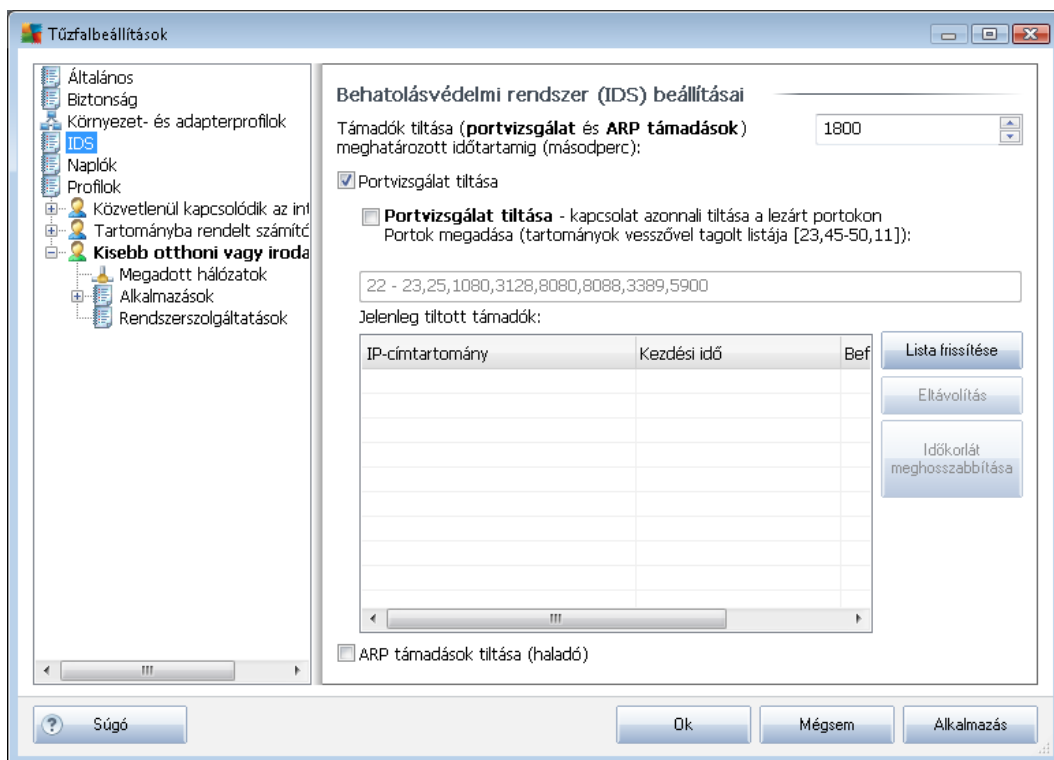
- **Adapterek, területek és kiosztott profilok listája** - itt egy áttekintést találhat az észlelt adapterekről és területekről. Mindegyikhez hozzá rendelhet egy külön profilt a meghatározott profilok menüjéből. A menü megnyitásához kattintson egy adott elemre a listában, és válasszon egy profilt.

Haladó beállítások

- o **Mindig az alapértelmezett profilt használja, és ne jelenítse meg az új hálózat észlelése párbeszédpanelét** - ha a számítógép új hálózatra csatlakozik, a [Tuzfal](#) értesíti Önt, és megjelenít egy olyan párbeszédpanelét, ahol kiválaszthatja a hálózat típusát, és egy [Tuzfal profilt](#) rendelhet hozzá. Ha nem szeretné megjeleníteni ezt a párbeszédpanelét, akkor jelölje be ezt a négyzetet.
- o **AVG heurisztika használata új hálózatok észlelésekor** - az újonnan észlelt hálózatokkal kapcsolatos adatokat a rendszer az AVG saját szolgáltatásától szerzi be (ez az opció kizárólag Windows Vista vagy újabb rendszerek esetén érhető el).
- o **Microsoft heurisztika használata új hálózatok észlelésekor** - az újonnan észlelt hálózatokkal kapcsolatos adatokat a rendszer a Windows szolgáltatástól szerzi be (ez az opció kizárólag Windows Vista vagy újabb rendszerek esetén érhető el).

10.4. IDS

A **Behatolásvédelmi rendszer** egy különleges viselkedéselemzési szolgáltatás, amely a számítógép bizonyos portjait használó gyanús adatforgalom észlelésére és letiltására szolgál. Az IDS paramétereit a következő felületen állíthatja be:



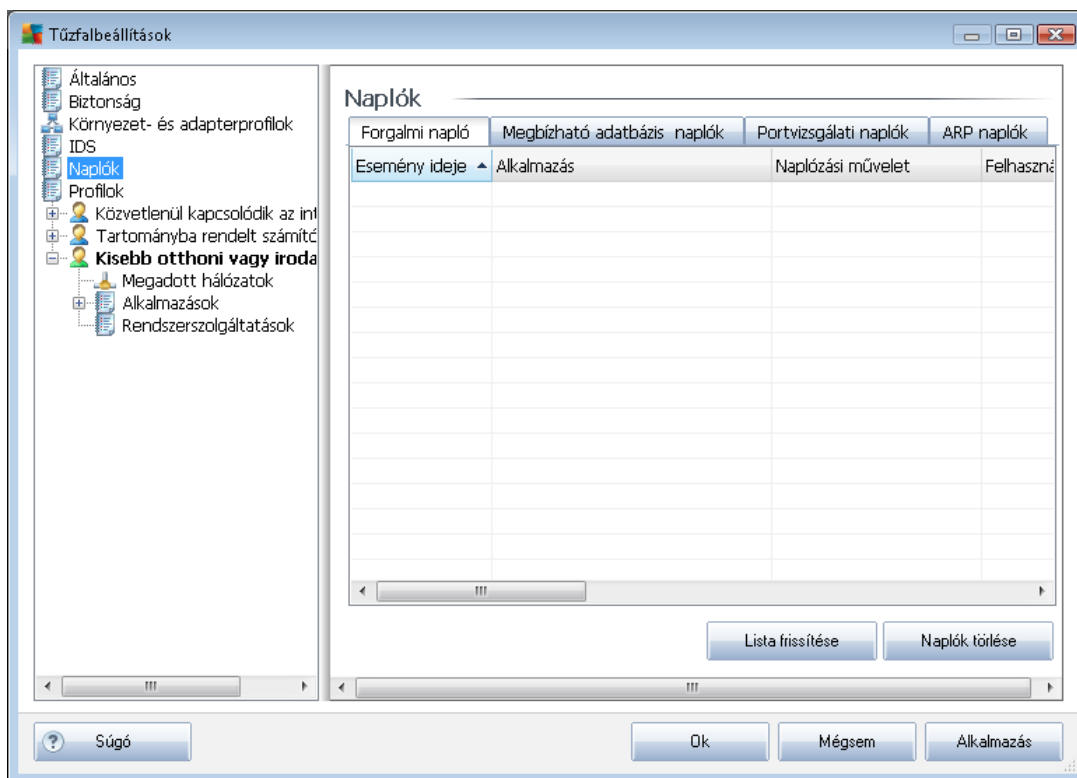
A **Behatolásvédelmi rendszer (IDS) beállításai** panel a következő lehetőségeket kínálja:

- **Támadók letiltása adott időtartamig** - lehetővé teszi annak meghatározását, hogy a rendszer hány másodpercig tiltson le egy portot, ha gyanús adatforgalmat észlel rajta. Alapállapotban az időtartam 1800 másodperc (30 perc).
- **Portvizsgálat tiltása** – jelölje be a jelölonégyzetet minden bejövő adatforgalom tiltásához az összes TCP és UDP porton. Az ilyen kapcsolatok esetén öt próbálkozás engedélyezett, a hatodik le lesz tiltva.
 - o **Portvizsgálat tiltása** – jelölje be a jelölonégyzetet az alábbi szövegmezőben meghatározott portokon áthaladó adatforgalomazonnali tiltásához. Az egyes portokat és porttartományokat vesszovel válassza el. Megtalálható itt az ajánlott portok listája, amennyiben használni kívánja ezt a szolgáltatást.
 - o **Jelenleg tiltott felhasználók**- listázza a [Tuzfal](#) által jelenleg tiltott összes adatforgalmat. A tiltott adatforgalmak teljes listája megtekinthető a [Naplók](#) panelen (a Portvizsgálati naplók fülön).
- A **ARP támadások tiltása** szolgáltatás az **IDS** által potenciálisan veszélyesként észlelt, a helyi hálózaton lévő adatforgalmak 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.

Vezérlogombok

- **Lista frissítése** - nyomja meg ezt a gombot a lista frissítéséhez (a legutóbb tiltott adatforgalmakkal együtt)
- **Eltávolítás** - nyomja meg ezt a gombot a 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



eldőntenie, hogy engedélyezi-e a hálózati kommunikációt az adott alkalmazás számára. Az AVG ellenorzi 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.

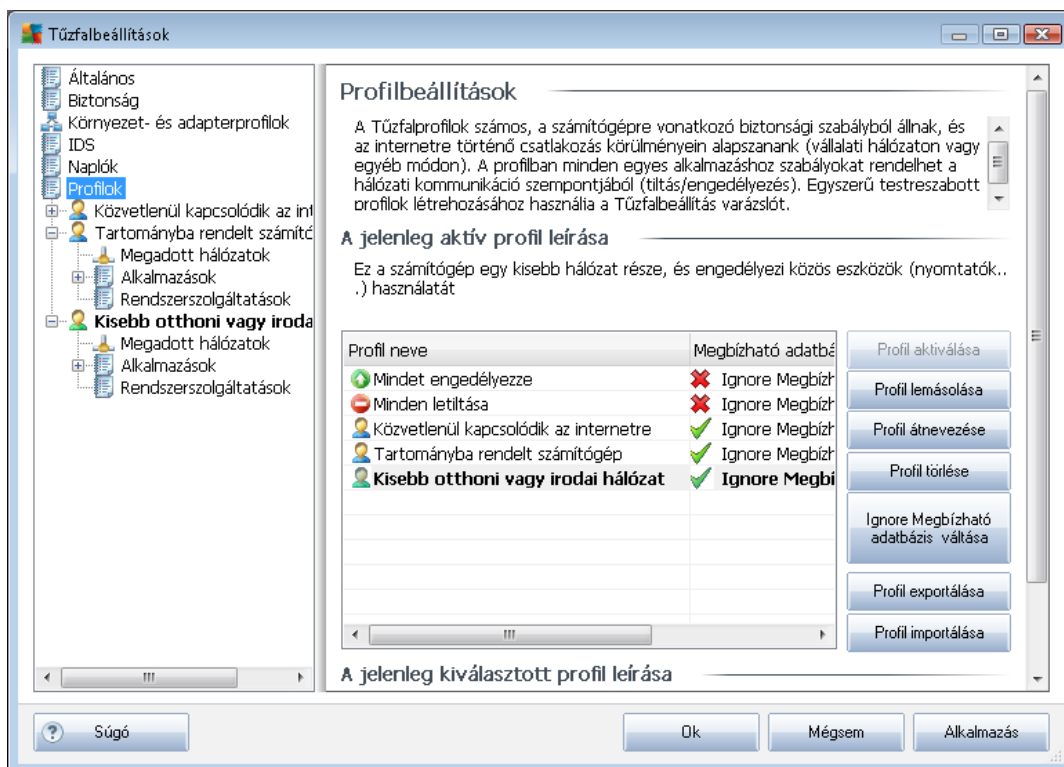
- **Portvizsgálati napló** - minden [behatolásvédelmi rendszerrel](#) kapcsolatos tevékenységet naplóz.
- **ARP napló** - naplózza a helyi hálózatok azon különleges kommunikációs kísérleteit ([ARP támadások tiltása](#) opció), amelyeket a [behatolásvédelmi rendszer](#) esetlegesen veszélyesnek minősített.

Vezérlogombok

- **Lista frissítése** - Az összes naplózott paramétert a következők alapján lehet rendezni: időrendben (dátum) vagy ABC sorrendben (egyéb oszlopok) - csak kattintson az adott oszlopra. Használja a **Lista frissítése** gombot a megjelenített információk frissítéséhez.
- **Lista ürítése** - törli az összes bejegyzést a listában.

10.6. Profilok

A **Profilbeállítások** panelen megtalálhatja az összes elérhető profilt.





Minden egyéb [profil](#)t szerkeszteni lehet ezen a panelen a következő vezérlogombokkal:

- **Profil aktiválása** - ez a gomb aktiválja az adott profilt, azaz a [Tuzfal](#) ezt fogja használni a hálózati forgalom szabályozásához
- **Profil duplázása** - 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** - a kijelölt profil törlése a listából
- **Megbízható adatbázis bekapcsolása** - a kiválasztott profilnál bekapcsolhatja a Megbízható adatbázis használatát (A Megbízható adatbázis olyan AVG belső adatbázis, amely adatokat gyűjt a hálózaton kommunikáló megbízható és tanúsított alkalmazásokról.)
- **Profil exportálása** - a profilbeállításokat egy fájlba menti későbbi használat céljából
- **Profil importálása** - a profilbeállításokat egy korábban elmentett konfigurációs fájlból tölti be

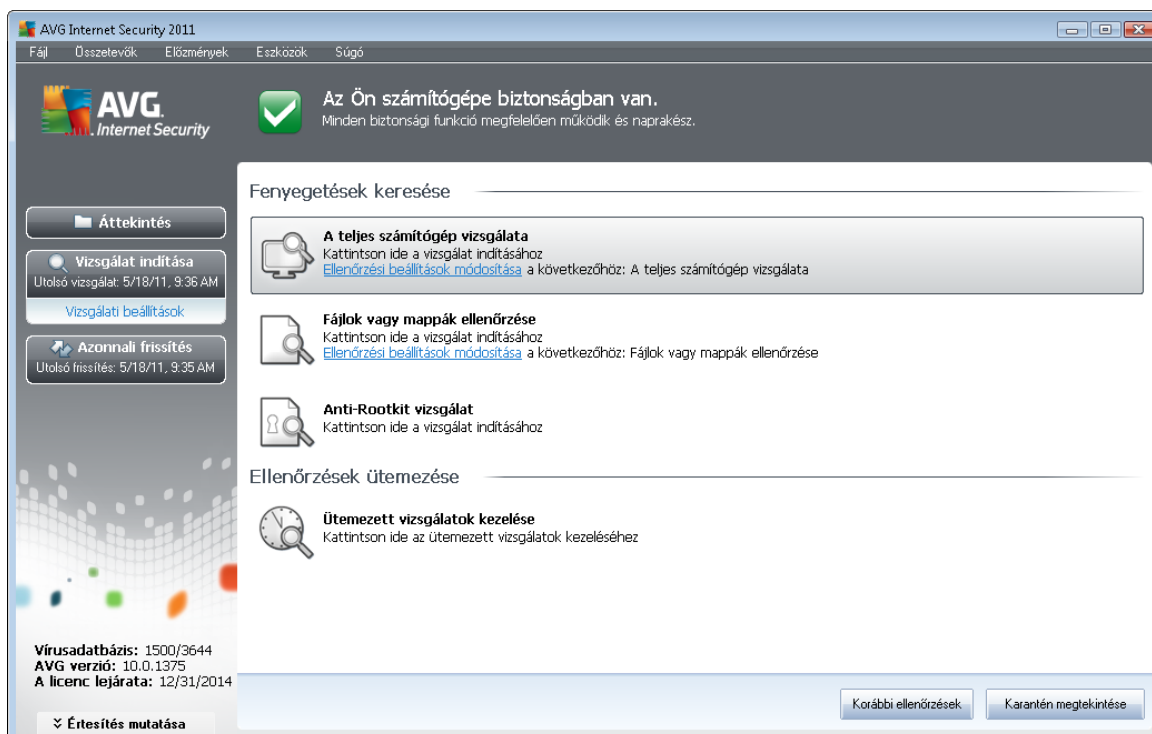
A panel alsó részén megtalálhatja az aktuálisan kiválasztott profil leírását.

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

11. AVG vizsgálat

A vizsgálat az **AVG Internet Security 2011** alapvető része. Lehetőség van a tesztek kézzel történő indítására, illetve azok előre meghatározott időpontokban történő [rendszeres indítását is be lehet állítani](#).

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:
 - o [Vizsgálat a teljes számítógépen](#)
 - o [Bizonyos fájlok vagy mappák ellenőrzése](#)
 - o [Anti-Rootkit vizsgálat](#)
- [vizsgálat ütemezése](#) rész - itt tetszőleges új vizsgálatokat és ütemezéseket (időzített vizsgálatok) hozhat létre.

Vezérlogombok

A vizsgálati felületen elérhető vezérlogombok a következők:



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

11.2. Elore meghatározott vizsgálatok

Az **AVG Internet Security 2011** 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.

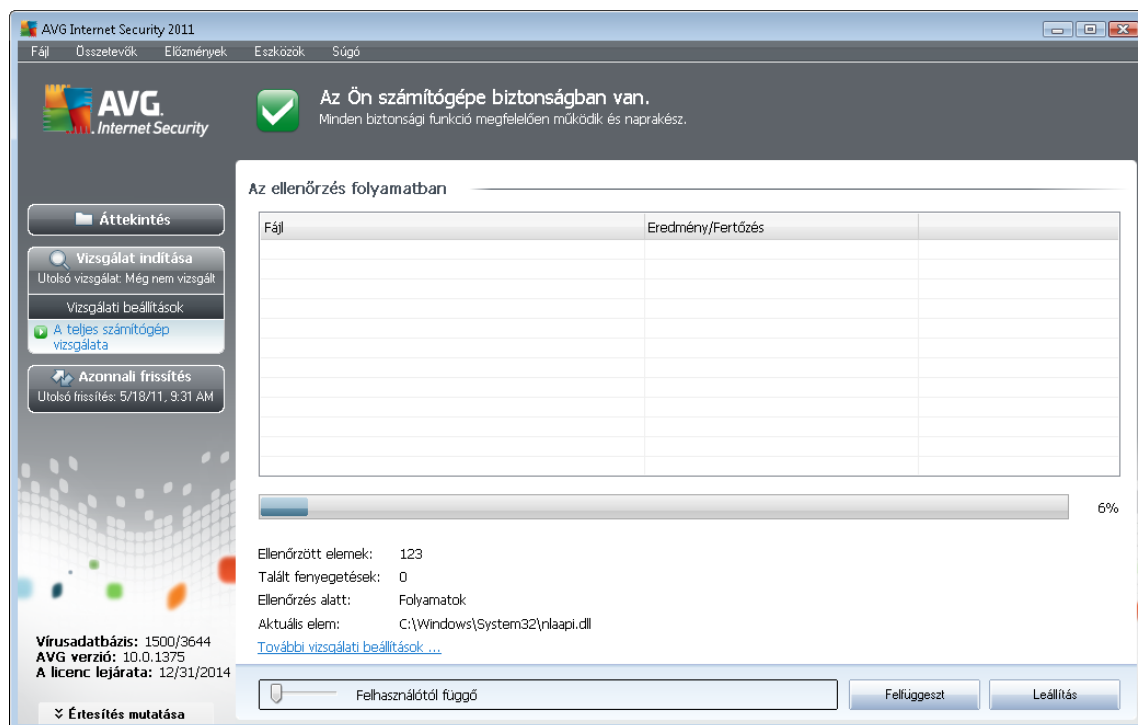
Az **AVG Internet Security 2011** programban a következő előre meghatározott vizsgálatokat találhatja, amelyeket a szoftver gyártója állított be:

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.

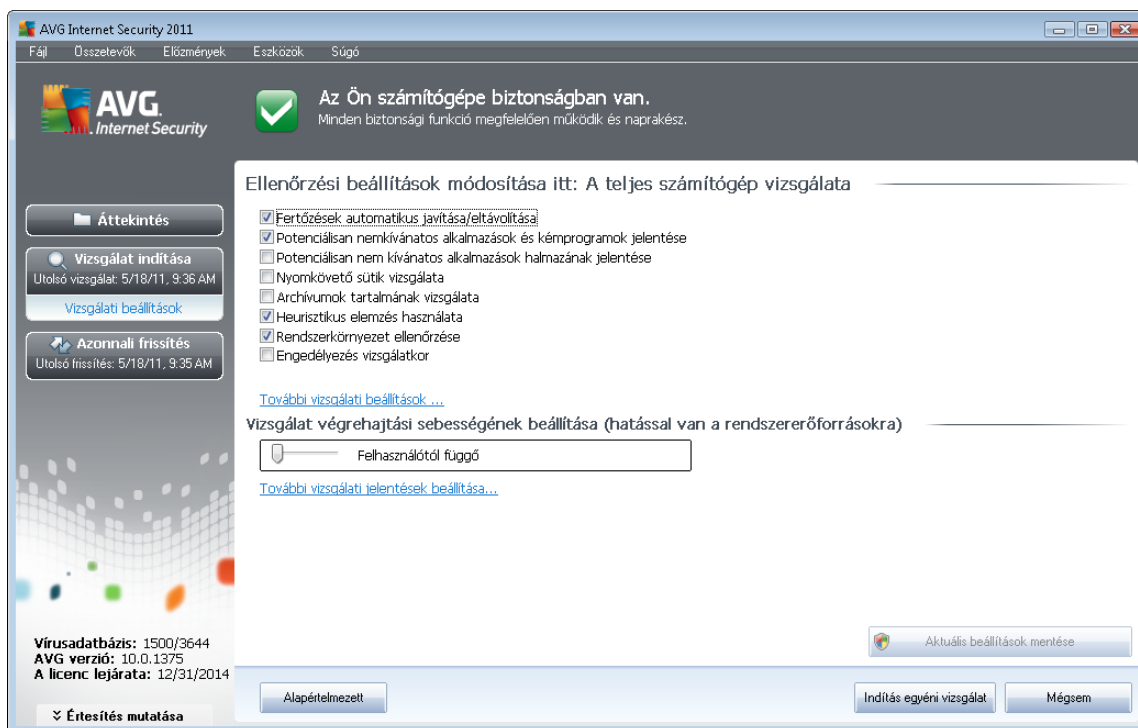
Vizsgálat indítása

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



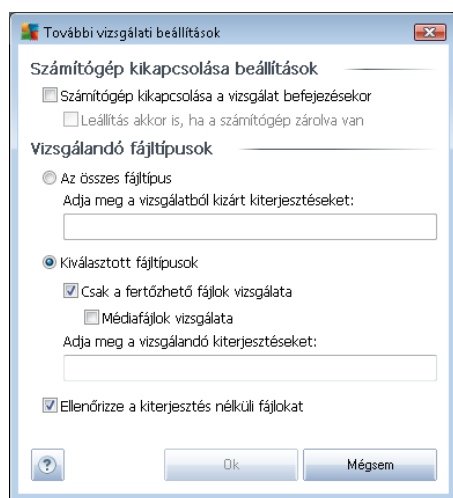
Vizsgálati beállítások szerkesztése

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

- o **Archívumok tartalmának vizsgálata** (alapállapotban kikapcsolva) - ez a paraméter meghatározza, hogy a vizsgálat ellenőrizze-e az archívumban tárolt fájlokat, pl. ZIP, RAR.
- o **Heurisztika használata** (alapállapotban bekapcsolva) - a heurisztikus elemzés (a vizsgált objektum utasításainak dinamikus emulációja egy virtuális környezetben) lesz az egyik víruskeresési módszer a vizsgálat során.
- o **Rendszerkörnyezet ellenőrzése** (alapállapotban bekapcsolva) - a vizsgálat a számítógép rendszerterületeit is ellenőrzi.
- o **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:

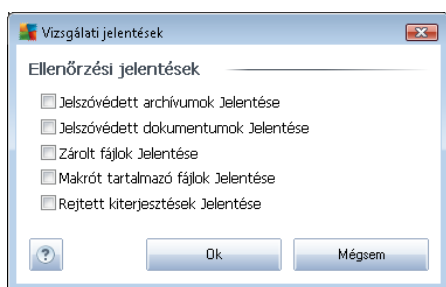


- o **A számítógép kikapcsolásának beállításai** - döntse el, hogy a számítógép automatikusan kikapcsoljon-e, miután a vizsgálati folyamat véget ért. Miután megerősítette ezt a beállítást (**Számítógép leállítása a vizsgálat után**), egy új opció aktiválódik, mely lehetővé teszi, hogy akkor is leállítsa a számítógépet, ha az éppen zárolt (**Számítógép leállítása zárolás esetén is**).
- o **A vizsgálandó fájltypusok megadása** - határozza meg a vizsgálandó fájlokat:
 - **Összes fájltypus** - lehetséges megadnia kivételeket, amelyek kimaradnak a vizsgálatból. Ezen fájlkiterjesztéseket vesszovel válassza el.
 - **Kiválasztott fájltypusok** - 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 fertőznék 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 beállításáival - 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

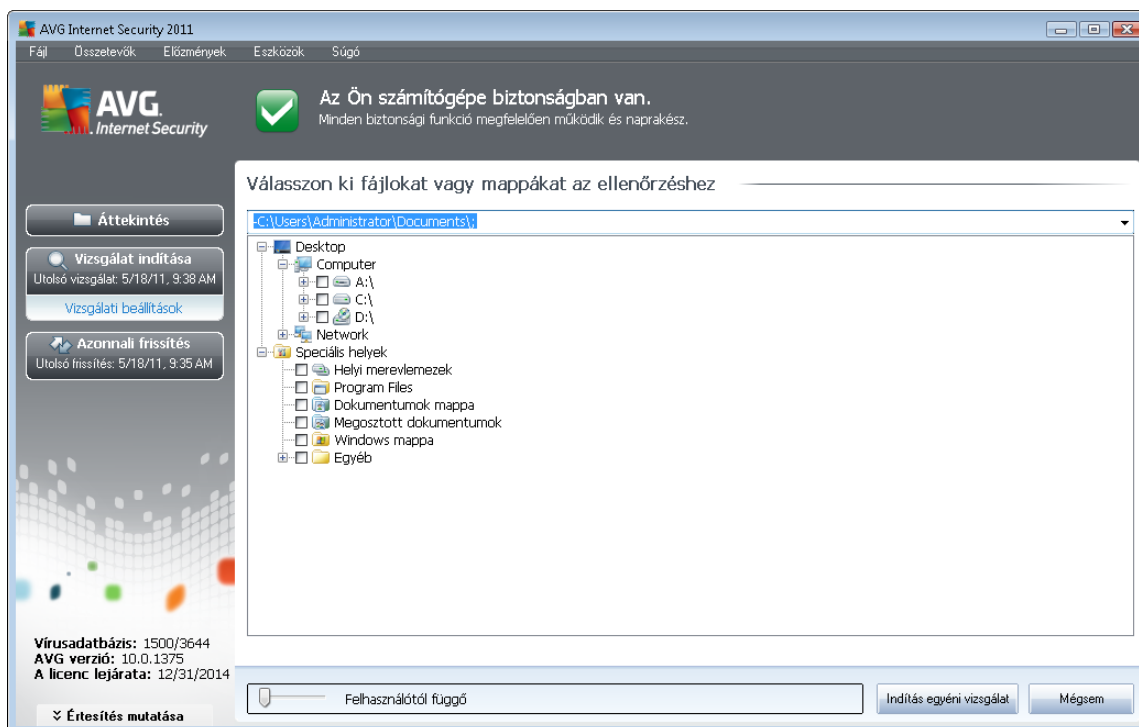
A **Bizonyos fájlok vagy mappák vizsgálatát** közvetlenül a **vizsgálati felületre** indíthatja a vizsgálat ikonjára történő kattintással. A **Válasszon ki bizonyos fájlokat vagy mappákat az ellenőrzéshez** panel megjelenik. Válassza ki a vizsgálandó mappákat a számítógépen. A kiválasztott mappák elérési útvonala automatikusan megjelenik a panel felső részén látható szövegdobozban.

Lehetősége van arra is, hogy egy bizonyos mappát almappák nélkül ellenőrizzen. Ehhez adjon egy



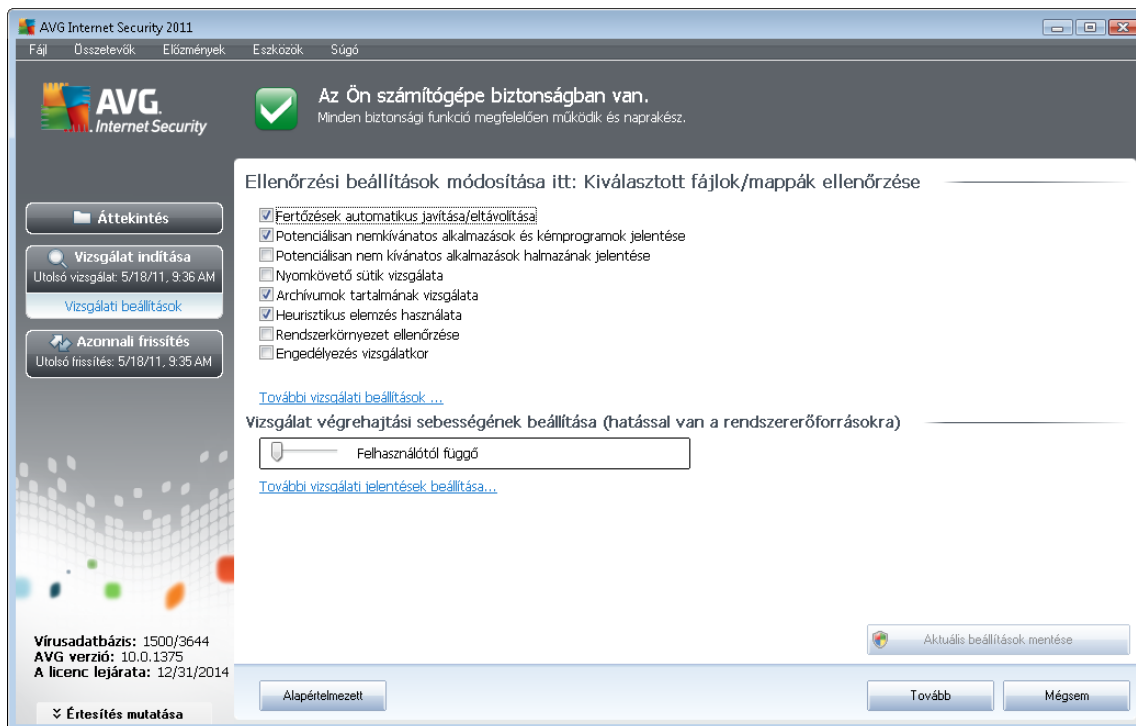
mínusz jelet "-" az automatikusan létrehozott elérési útvonal elé (lásd a képet). Egy teljes mappa vizsgálatból való kizárásához használja a "!" jelet paraméter.

Végül a vizsgálat indításához nyomja meg a **Vizsgálat indítása** gombot. A folyamat alapvetően megegyezik a [Számítógép teljes vizsgálata](#) funkcióval.



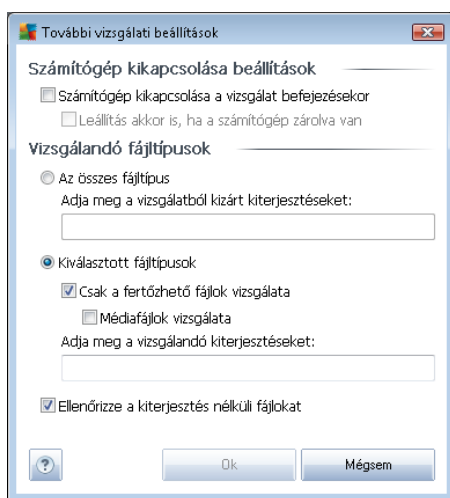
Vizsgálati beállítások szerkesztése

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

- o **Archívumok tartalmának vizsgálata** (alapállapotban bekapcsolva) - ez a paraméter meghatározza, hogy a vizsgálat ellenőrizze-e az archívumban tárolt fájlokat, pl. ZIP, RAR.
- o **Heurisztika használata** (alapállapotban kikapcsolva): a heurisztikus elemzés (a vizsgált objektum utasításainak dinamikus emulációja egy virtuális környezetben) lesz az egyik víruskeresési módszer a vizsgálat során.
- o **Rendszerkörnyezet ellenőrzése** (alapállapotban kikapcsolva) - a vizsgálat a számítógép rendszerterületeit is ellenőrzi.
- o **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:

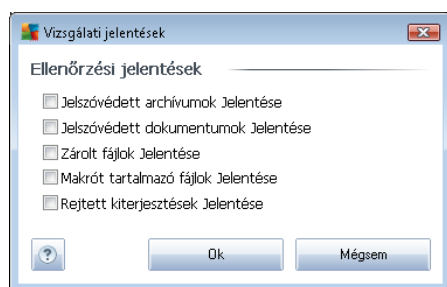


- o **A számítógép kikapcsolásának beállításai** - döntse el, hogy a számítógép automatikusan kikapcsoljon-e, miután a vizsgálati folyamat véget ért. Miután megerősítette ezt a beállítást (**Számítógép leállítása a vizsgálat után**), egy új opció aktiválódik, mely lehetővé teszi, hogy akkor is leállítsa a számítógépet, ha az éppen zárolt (**Számítógép leállítása zárolás esetén is**).
- o **A vizsgálandó fájl típusok megadása** - határozza meg a vizsgálandó fájlokat:
 - **Összes fájl típus** - lehetséges megadnia kivételeket, amelyek kimaradnak a vizsgálatból. Ezen fájl kiterjesztéseket vesszovel válassza el.
 - **Kiválasztott fájl típusok** - 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. média fájlok (video-, audio fájlok - 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 fertőznék 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 beállításáival - az [AVG Vizsgálat / Vizsgálat ütemezése/ Hogyan vizsgáljon](#) fejezetben leírtaknak megfelelően. Ha úgy dönt, hogy megváltoztatja az alapbeállításokat 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 vizsgálatához ([az egyéni keresések a Meghatározott fájlok vagy mappák vizsgálata rész aktuális beállításaitól függnék](#)).

11.2.3. Anti-Rootkit vizsgálat

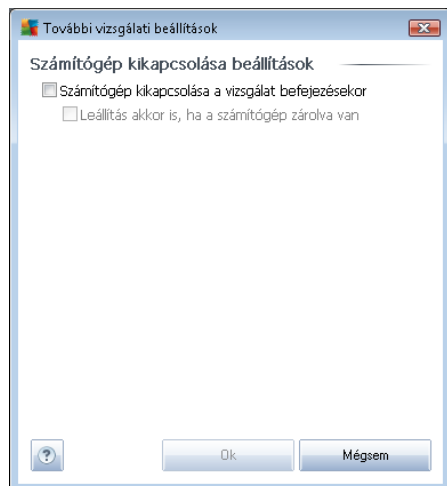
Az **Anti-Rootkit vizsgálat** esetleges rootkitek keres a számítógépen (olyan programokat és technológiákat, amelyek kártékony tevékenységet lepleznek a számítógépen). Ha a program rootkitet észlel, akkor az nem jelenti automatikusan azt, hogy a számítógép fertőzött. Bizonyos esetekben egyes eszközillesztők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

Vizsgálat indítása

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

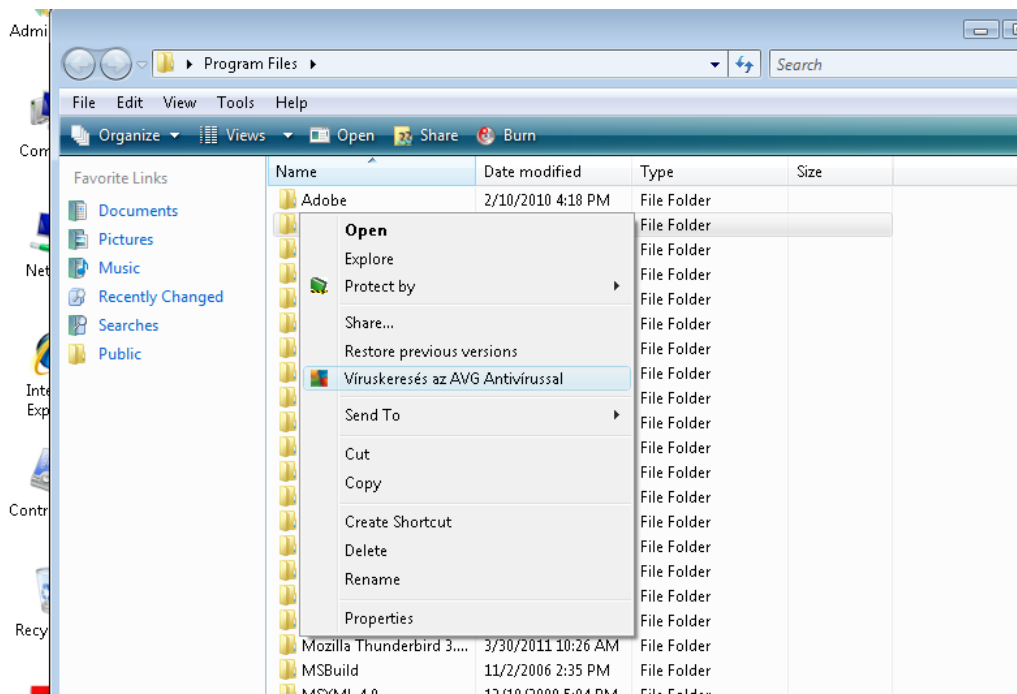


- **Automatikus vizsgálat** - használja a csúszkát a vizsgálati folyamat prioritásának módosításához. Alapállapotban ez az érték *felhasználótól függő* automatikus erőforráshasználatra van állítva. Alapállapotban a vizsgálati folyamatot lassabra állíthatja, ekkor a rendszer minimális erőforrást használ (*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 2011** 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 vizsgálandó fájlt (vagy mappát)
- Kattintson jobb gombbal az objektumra a helyi menü megnyitásához
- Válassza a **Vizsgálat AVG-vel** opciót az objektum ellenőrzéséhez



11.4. Parancssori vizsgálat

Az **AVG Internet Security 2011** 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 vizsgálatához szükséges összes paramétert:

- **/SCAN** [Bizonyos fájlok vagy mappák ellenőrzése](#) /SCAN=útvonal;útvonal (pl. /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** Zárt fájlok mellozése
- **/REPORT** Jelentéskészítés fájlba /fájlnév/
- **/REPAPPEND** Hozzáfűzés a jelentésfájlhoz
- **/REPOK** Nem fertőzött fájlok jelentése OK-ként
- **/NOBREAK** A CTRL+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 témakörrel



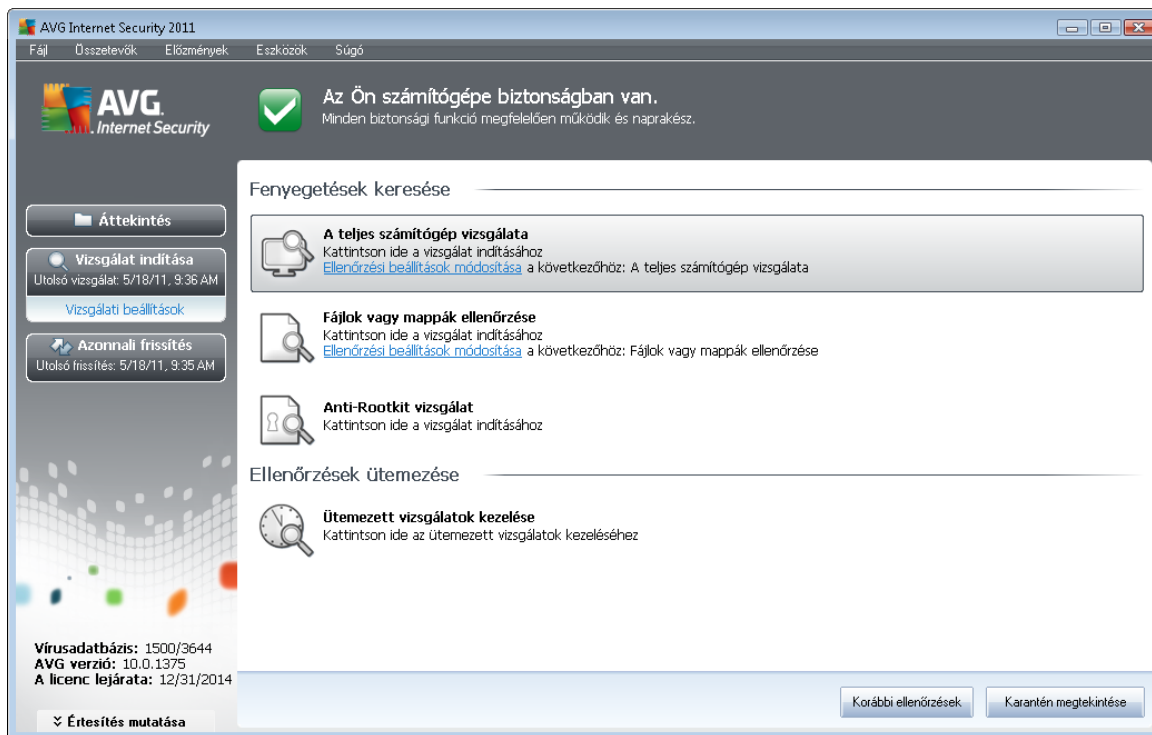
- **/HELP** Súlyos megjelenítése a témakörrel
- **/PRIORITY** Vizsgálati prioritás beállítása /Alacsony, Automatikus, Magas/ (lásd a [Haladó beállítások / Vizsgálatok részt](#))
- **/SHUTDOWN** A számítógép leállítása a vizsgálat befejezésekor
- **/FORCESHUTDOWN** A számítógép kényszerített leállítása a vizsgálat befejezésekor
- **/ADS** Alternatív adatfolyamok vizsgálata (csak NTFS)
- **/ARCBOMBSW** Újratömörített archívumfájlok jelentése

11.5. Vizsgálatok ütemezése

A **AVG Internet Security 2011** 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 aggodnia, hogy mikor és hogyan indítson el egy keresést.

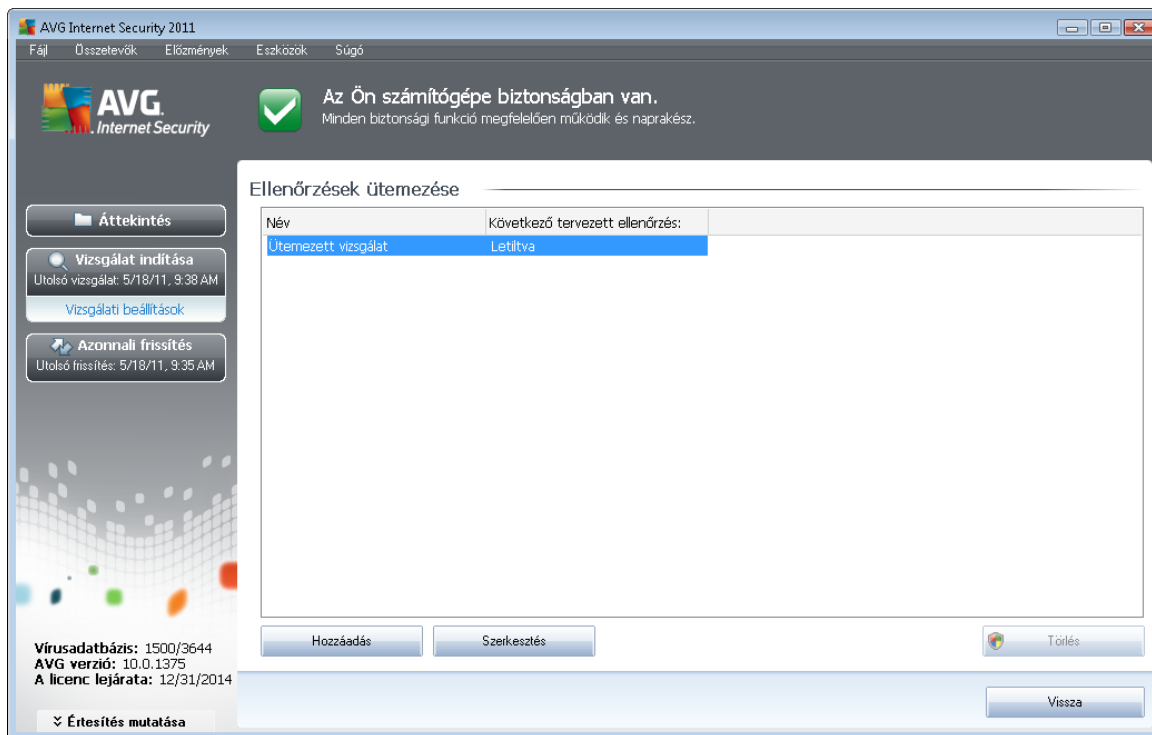
Rendszeresen, legalább hetente egyszer futtassa le a [Számítógép teljes vizsgálata](#) szolgáltatást. Azonban amennyiben lehetséges, a teljes számítógép vizsgálata napi szinten javasolt - az alapértelmezett vizsgálati ütemezésben is ez szerepel. Ha a számítógép mindig be van kapcsolva, akkor a munkaidő 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 az ikonra az **Ellenőrzések ütemezése** részben egy új **Ellenőrzések ütemezése** párbeszédpanel megnyitásához, ahol megtekintheti az összes ütemezett ellenőrzést:

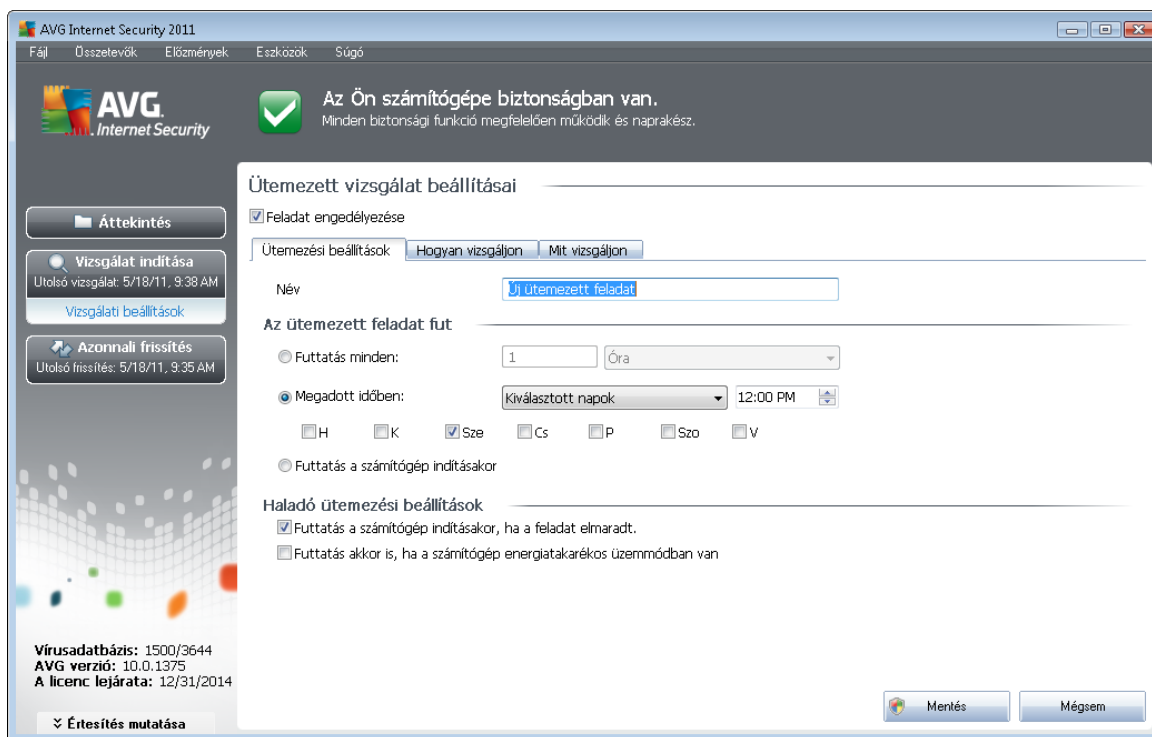


A vizsgálatokat szerkesztheti, illetve újakat vehet fel a következő vezérlogombok segítségével:

- **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 paramétereit itt van 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 vezérlogomra. 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). Az ablak három fülre van osztva: **Beállítások ütemezése** - lásd az alábbi képet (alapértelmezett fül, amelyre automatikusan átkerül), [Hogyan keressen a program](#) 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).

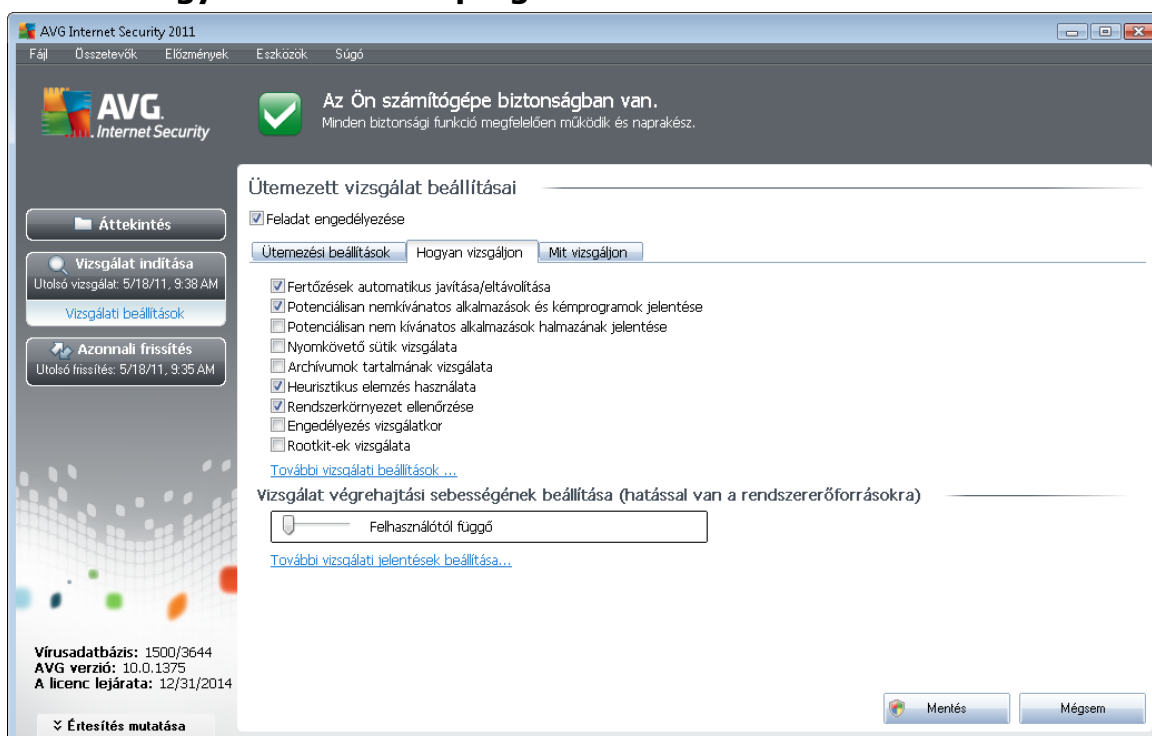
Vezérlogók az Ütemezett vizsgálat beállításai ablakban



Két vezérlogomb található az **Ütemezett vizsgálat beállításai** panel mindhárom fülén (**Ütemezési beállítások**, [Hogyan keressen a program](#) és [Mit vizsgáljon a program](#)) és ugyanazzal a funkcióval rendelkeznek, bármelyik fülön is legyenek:

- **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:

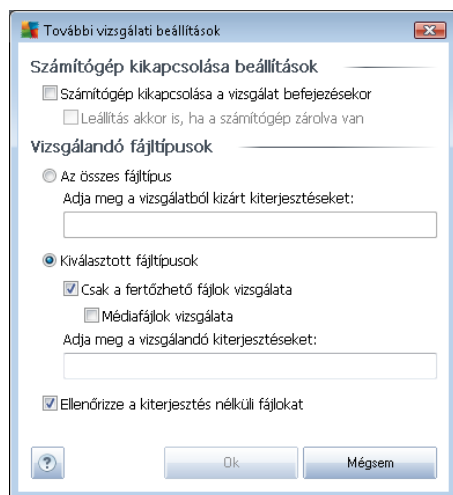
- **Fertőzés automatikus javítása/eltávolítása** (alapállapotban bekapcsolva): ha vírust talál a vizsgálat során, akkor automatikusan javítja, amennyiben ez lehetséges.. Ha a fertőzött fájlt nem lehet automatikusan javítani, vagy kikapcsolja ezt az opciót, akkor értesítést fog kapni a vírus azonosításáról,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

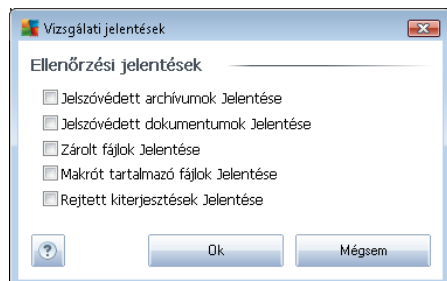
- **Potenciálisan nem kívánatos alkalmazások jelentése** (alapállapotban kikapcsolva): jelölje be ezt a jelölőnégyzetet a [kémprogramok](#) speciális változatainak észleléséhez: olyan programok kereséséhez, amelyek ártalmatlanok, de később kártékony célokra használhatók. Ezzel tovább növelheti a számítógép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

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:



- o **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**).
- o **A vizsgálandó fájl típusok megadása** - határozza meg a vizsgálandó fájlokat:
 - **Összes fájl típus** - lehetséges megadnia kivételeket, amelyek kimaradnak a vizsgálatból. Ezen fájl kiterjesztéseket vesszovel válassza el.
 - **Kiválasztott fájl típusok** - 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 fertőznék 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 lassabba állíthatja, ekkor a rendszer minimális erőforrást használ (*hasznos, ha a számítógépen kell dolgoznia, és nem számít a gyorsaság*); vagy gyorsabba 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:



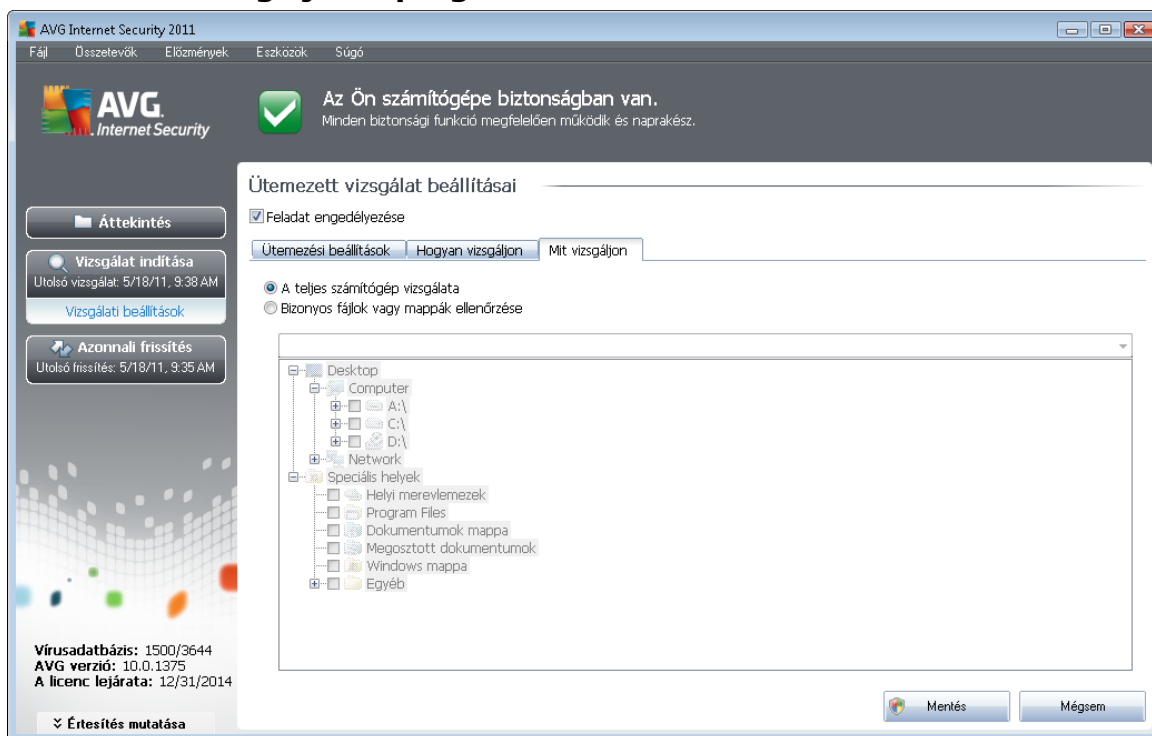
Megjegyzés: Alapértelmezés szerint a vizsgálati konfiguráció optimális teljesítményre van állítva. Javasoljuk, hogy tartsa meg az alapértelmezett vizsgálati beállításokat, és csak akkor módosítson rajtuk, ha feltétlenül szükséges. Bármely módosítást tapasztalt felhasználónak kell végeznie. További vizsgálati beállításokkal kapcsolatban nézze meg a [Haladó beállítások](#) ablakot a **Eszközök / Haladó beállítás** menüben.

Vezérlogombok

Két vezérlogomb található az **Ütemezett vizsgálat beállításai** panel mindhárom fülén ([Ütemezési beállítások](#), **Hogyan keressen a program** és [Mit vizsgáljon a program](#)) és ugyanazzal a funkcióval rendelkeznek, bármelyik fülön is legyenek:

- **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 elozményeket 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**
 - o C:\Program Files\
 - o a 64-bit verziónál: C:\Program Files (x86)
- **Dokumentumok mappája**
 - o Windows XP-nél: C:\Documents and Settings\Default User\My Documents\



o Windows Vista/7 rendszereknél: C:\Users\user\Documents\

- **Megosztott dokumentumok**

o Windows XP-nél: C:\Documents and Settings\All Users\Documents\

o Windows Vista/7 rendszereknél: C:\Users\Public\Documents\

- **Windows mappa** - C:\Windows\

- **Egyéb**

o Rendszermeghajtó - az a merevlemez, amelyen az operációs rendszer telepítve van (általában C:)

o Rendszermappa - C:\Windows\System32\

o Ideiglenes fájlok mappa - C:\Documents and Settings\User\Local\ (Windows XP); vagy C:\Users\user\AppData\Local\Temp\ (Windows Vista/7)

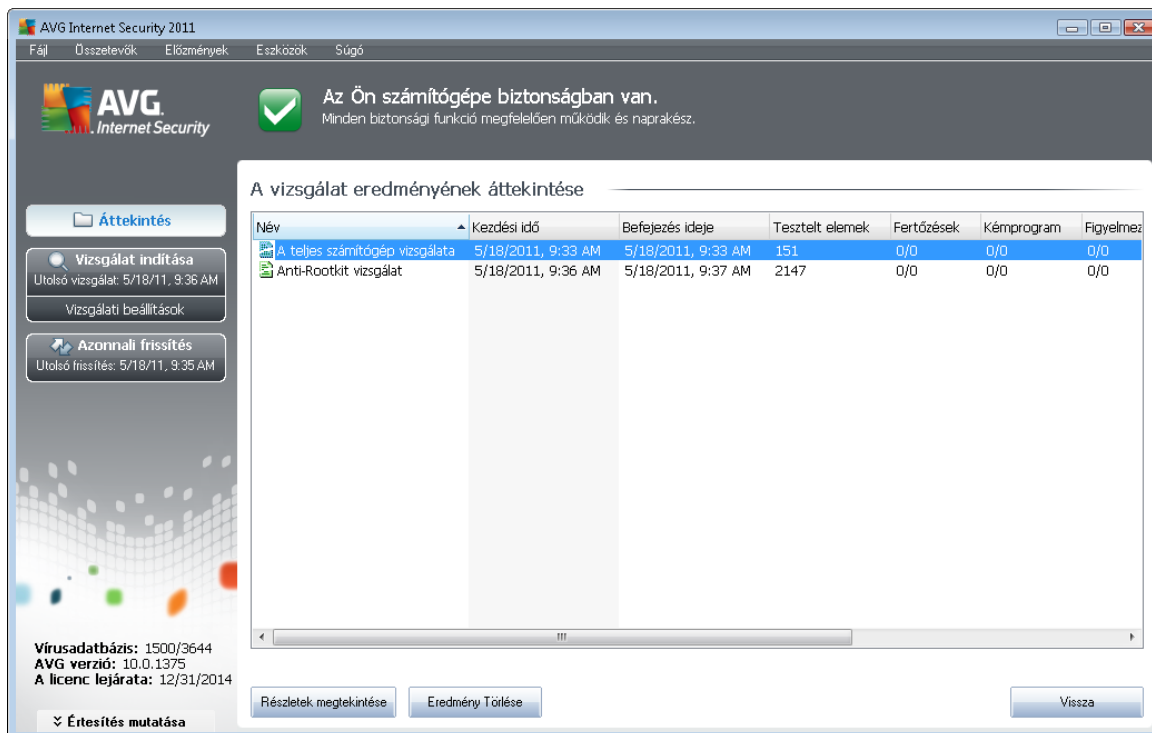
o Ideiglenes internetes fájlok - C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (Windows XP); vagy C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (Windows Vista/7)

Vezérlogombok az Ütemezett vizsgálat beállításai ablakban

Két vezérlogomb található az **Ütemezett vizsgálat beállításai** panel mindhárom fülén (**Ütemezési beállítások**, **Hogyan keressen a program** és **Mit vizsgáljon a program**) és ugyanazzal a funkcióval rendelkeznek, bármelyik fülön is legyenek:

- **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 **Vizsgálati eredményének áttekintése** ablak elérhető az [AVG vizsgálati felületről](#) a **Korábbi ellenőrzések** gombbal. Az ablak megmutatja az összes korábban indított vizsgálatot és azok eredményeit:

- **Név** - vizsgálatról 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 vizsgálatról kapcsolatos további információkért nézze meg a [Vizsgálati 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 megszakításakor)

Vezérlogombok

A vezérlogombok 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

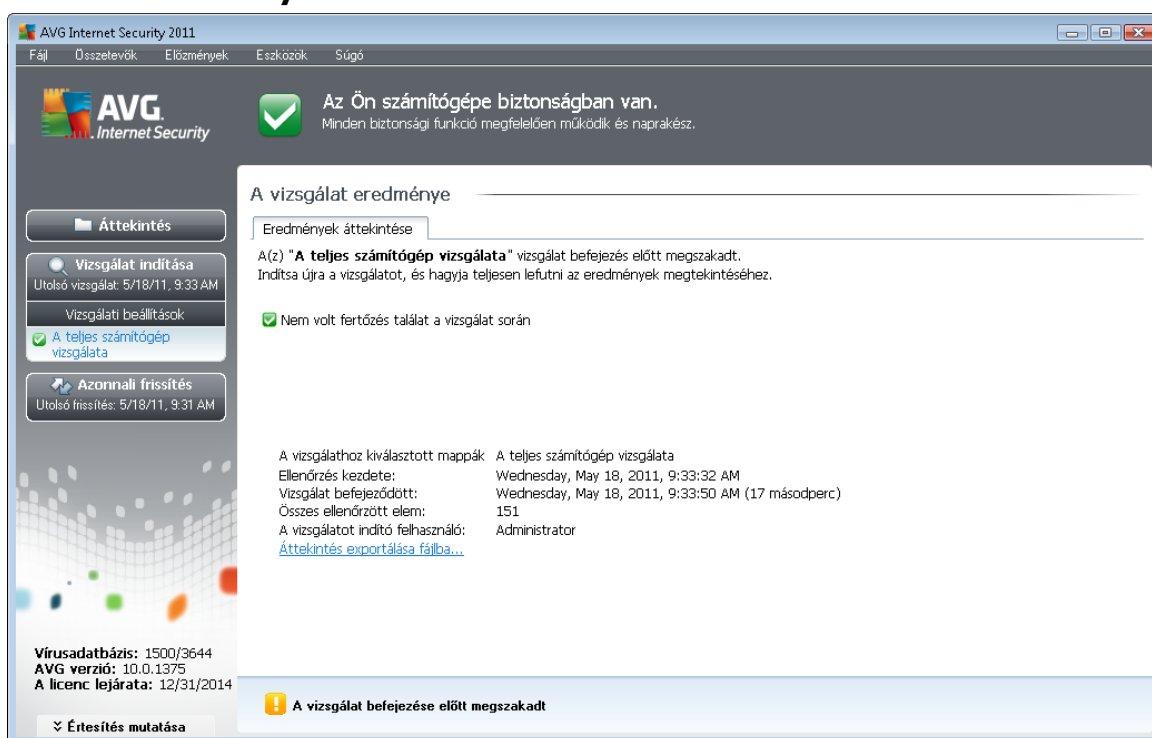
Ha a [Vizsgálati eredmények áttekintése](#) panelen egy adott vizsgálat ki van jelölve, akkor kattintson a **Részletek megtekintése** gombra a **Vizsgálati eredmények** ablak megnyitásához, mely részletes adatokat közöl a vizsgálat folyamatáról és eredményéről.

Az ablak több fülre 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 [vírusfertőzés](#) lett azonosítva a vizsgálat során
- **Kémprogramok** - ez a fül csak akkor jelenik meg, ha [kémprogramok](#) lettek azonosítva a vizsgálat során
- **Figyelmeztetések** - ez a fül csak akkor jelenik meg, ha például sütik lettek azonosítva a vizsgálat során
- **Rootkit-ek** - ez a fül csak akkor jelenik meg, ha [rootkit-ek](#) lettek azonosítva a vizsgálat során

- **Információk** - ez a fül csak akkor jelenik meg, ha potenciális fenyegetés lett azonosítva, de az nem sorolható be a fenti kategóriákba. Ezért a program figyelmeztető üzenetet jelenít meg a találattal kapcsolatban. Itt információkat találhat olyan objektumokról, amelyek nem vizsgálhatók (pl. jelszóval védett archívumok).

11.7.1. Eredmények áttekintése fül



A **A vizsgálat eredménye** fülön részletes statisztikákat találhat a következő információkkal:

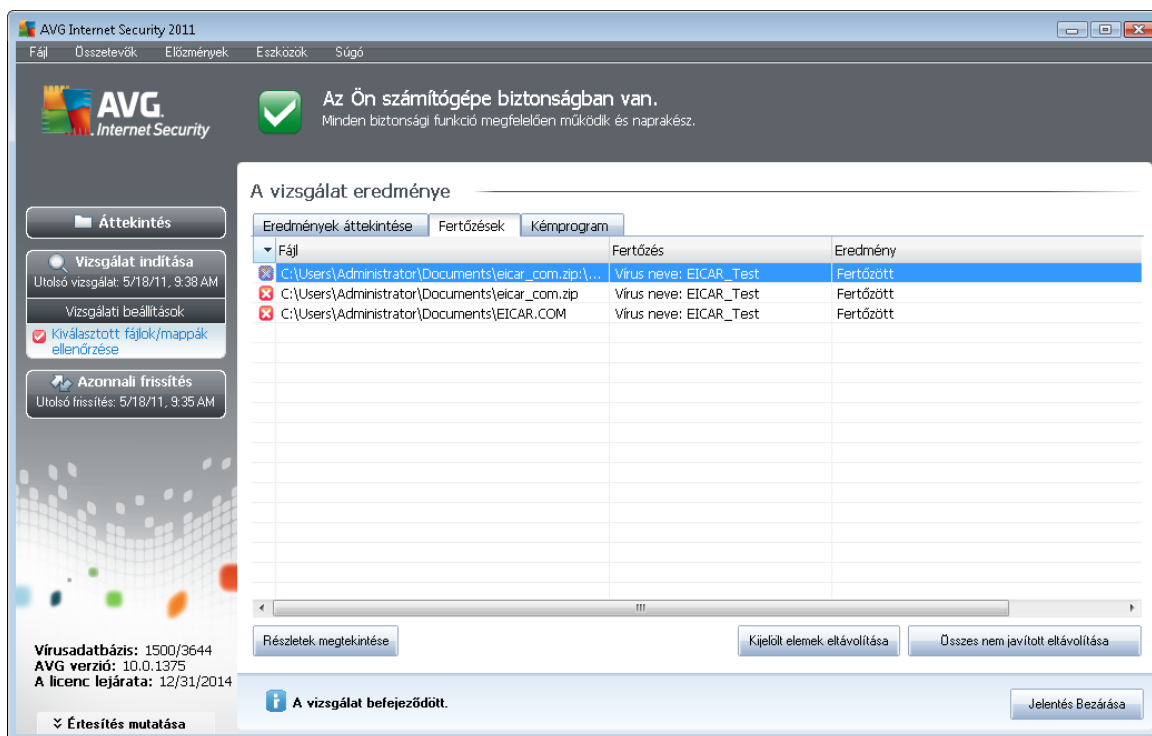
- felismert [vírusfertőzések](#) / [kémprogramok](#)
- eltávolított [vírusfertőzések](#) / [kémprogramok](#)
- a nem javítható vagy eltávolítható [vírusfertőzések](#) / [kémprogramok](#) száma

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.

Vezérlogombok

Csak egy vezérlogomb 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 információkkal:

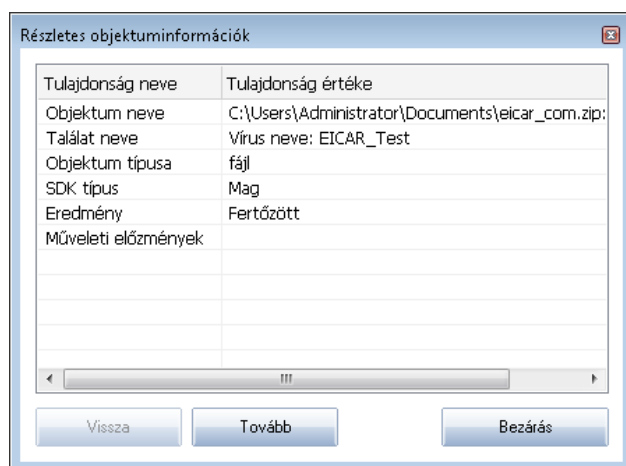
- **Fájl** - teljes elérési útvonal a fertőzött objektum eredeti helyéhez
- **Fertőzések** - a felismert [vírus](#) neve (adott vírussal kapcsolatos részletes információkért nézze meg a [Vírusenciklopédiát](#) online)
- **Eredmény** - megmutatja a fertőzött objektum vizsgálat során meghatározott állapotát:
 - o **Fertőzött** - a felismert és eredeti helyükön hagyott fertőzött objektumok (például ha az [automatikus javítás opció ki van kapcsolva](#) a vizsgálati beállításokban)
 - o **Javítva** - az automatikusan javított és eredeti helyükön hagyott fertőzött objektumok
 - o **Karanténba áthelyezve** - a [Karanténba](#) áthelyezett fertőzött objektumok
 - o **Törölve** - a törölt fertőzött objektumok
 - o **Hozzáadva a PUP kivételekhez** - kivételként értelmezett találat, mely hozzá lett adva a PUP kivételek listájához (meghatározva a [PUP kivételek](#) panelen a [haladó beállításokban](#))
 - o **Zárolt fájl - nem vizsgált** - az adott objektum zárolva van, ezért az AVG nem tudja megvizsgálni

- o **Potenciálisan veszélyes elem** - az objektum potenciálisan veszélyes de nem fertőzött (lehet például makró). Az információ csak figyelmeztetésnek számít
- o **Újraindítás szükséges a művelet befejezéséhez** - a fertőzött objektumot nem lehet eltávolítani, a teljes eltávolításhoz újra kell indítania a számítógépet

Vezérlogombok

Három vezérlogomb található az ablakban:

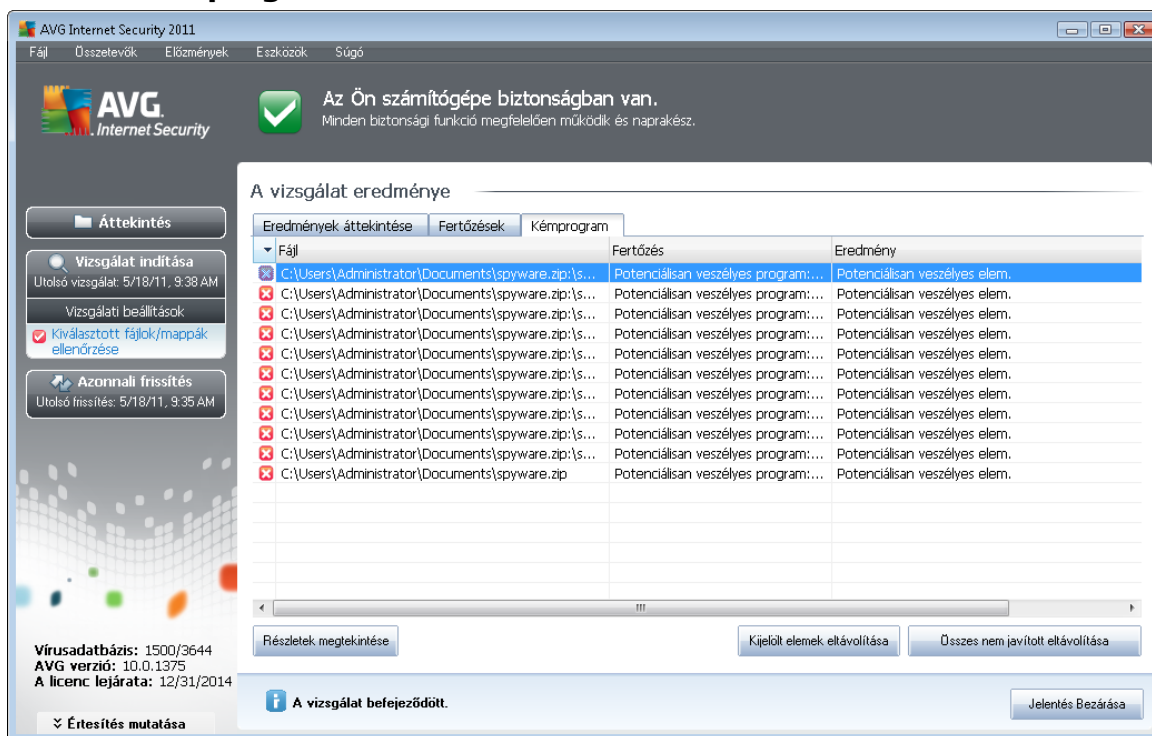
- **Részletek megtekintése** - ez a gomb egy újabb ablakot nyit meg **Részletes objektumadatok** néven:



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 elozményei*). 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. Kémprogramok fül



A **Kémprogram** fül a **Vizsgálat eredménye** ablakban csak akkor jelenik meg, ha a program [kémprogramokat](#) talált a vizsgálat során. A fül három részre van osztva a következő információkkal:

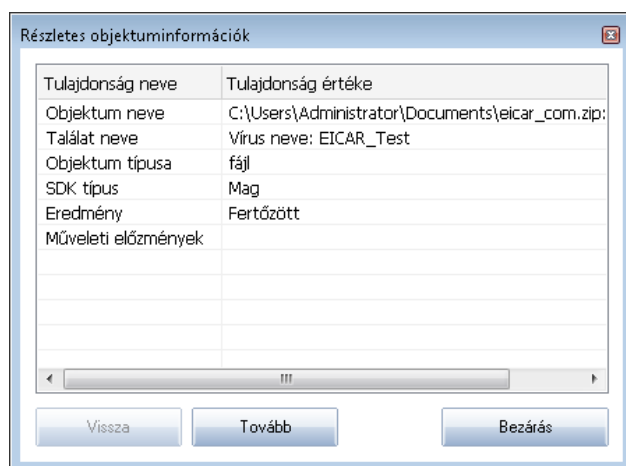
- **Fájl** - teljes elérési útvonal a fertőzött objektum eredeti helyéhez
- **Fertőzések** - a felismert [kémprogramok](#) neve (adott vírussal kapcsolatos részletes információkért nézze meg a [Vírusenciklopédiát](#) az interneten)
- **Eredmény** - megmutatja az objektum vizsgálat során meghatározott állapotát:
 - o **Fertőzött** - a felismert és eredeti helyükön hagyott fertőzött objektumok (például ha az [automatikus javítás opció ki van kapcsolva](#) a vizsgálati beállításokban)
 - o **Javítva** - az automatikusan javított és eredeti helyükön hagyott fertőzött objektumok
 - o **Karanténba áthelyezve** - a [Karanténba áthelyezett fertőzött objektumok](#)
 - o **Törölve** - a törölt fertőzött objektumok
 - o **Hozzáadva a PUP kivételekhez** - kivételként értelmezett találat, mely hozzá lett adva a PUP kivételek listájához (meghatározva a [PUP kivételekben](#) a haladó beállításokban)
 - o **Zárolt fájl - nem vizsgált** - az adott objektum zárolva van, ezért az AVG nem tudja megvizsgálni

- o **Potenciálisan veszélyes elem** - az objektum potenciálisan veszélyes de nem fertőzött (lehet makró például). Az információ csak figyelmeztetésnek számít
- o **Újraindítás szükséges a művelet befejezéséhez** - a fertőzött objektumot nem lehet eltávolítani, a teljes eltávolításhoz újra kell indítania a számítógépet

Vezérlogombok

Három vezérlogomb 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 muveletek elozményei*). 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](#) ablakba

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 csak figyelmeztetéseket szerepeltet az eredmények között, akkor nem szükséges további muvelet.

Az alábbiakban egy rövid leírást talál az ezen eredmények leggyakoribb előfordulásával kapcsolatban:

- **Rejtett fájlok** - A rejtett fájlok alapértelmezés szerint nem láthatóak a Windows-ban, és néhány vírus vagy egyéb fenyegetés úgy próbálja elkerülni az észlelést, hogy ezt a jellemzőt veszi fel. Ha az AVG rejtett fájlt talál, amelyet Ön is gyanúsnak vagy károsnak minősít, akkor helyezze azt át az [AVG 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 betölthessen, és hatással legyen a teljes operációs rendszerre.

11.7.5. Rootkit-ek fül

A **Rootkitek** fül információkat jelenít meg a vizsgálat során észlelt rootkitekrol, 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 olyan fájlokat is képes észlelni, amelyek nem fertőzöttek, de gyanúsak. Ezen fájlokhoz a program [figyelmeztetés](#) vagy [tájékoztató](#) megjegyzést fűz hozzá.

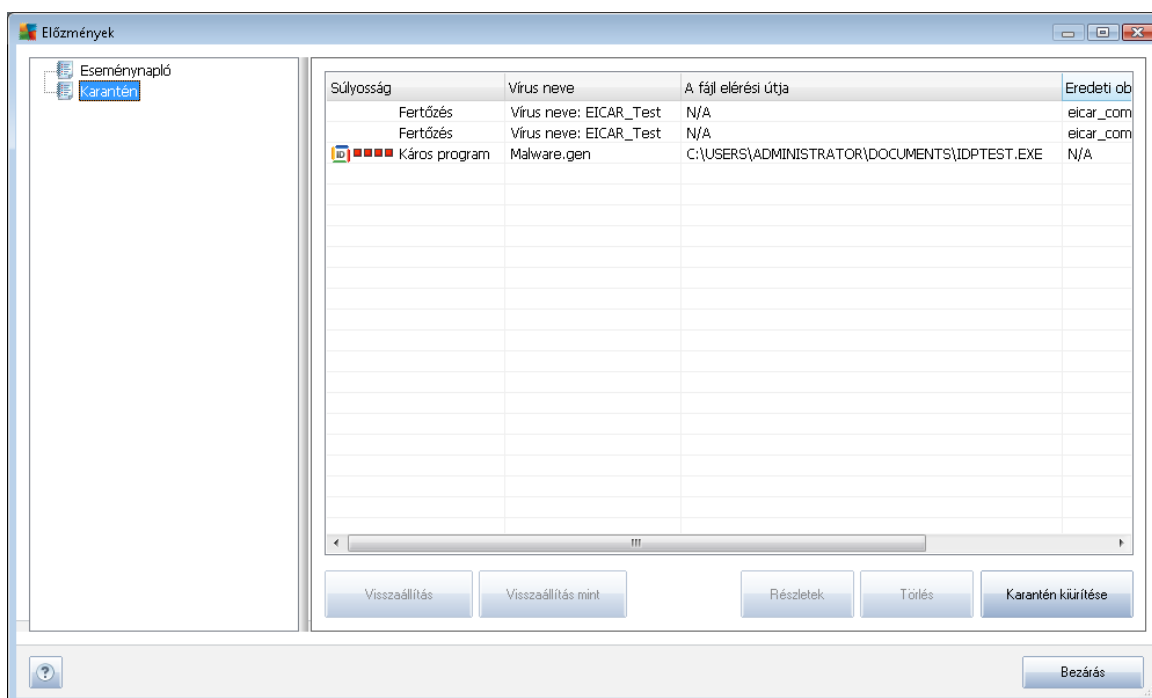
A **tájékoztató** megjegyzés a következő esetekben fordul elő:

- **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 nem tudja ellenőrizni (*más kártevők elleni 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 értesítést küld, hogy ezen fájlokat nem javasolt megnyitni.
- **Nem megfelelő fájlpálya** - Ha bizonyos fontos rendszerfájlok nem az alapértelmezett helyükről futnak (*pl. a winlogon.exe nem a Windows mappából*), akkor az AVG jelenti a normálistól eltérő viselkedést. Bizonyos esetekben a vírusok normál rendszerfolyamatok neveit használják, hogy kevésbé nyilvánvaló legyen jelenlétük a rendszerben.
- **Zárt fájl** - A fájl zárt, ezért az AVG nem tudja azt ellenőrizni. Ez azt jelenti, hogy bizonyos fájlokat folyamatosan használ a rendszer (*pl. lapozófájlok*).

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.



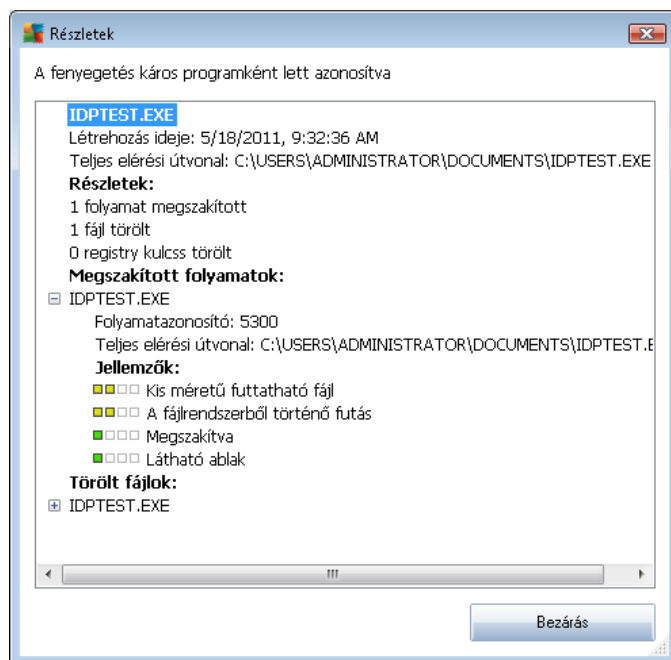
A **Karantén** felület külön ablakban nyílik meg, és áttekintést nyújt az elkülönített fertőzött objektumokról:

- **Kockázati szint** - ha telepítette az [Identity Protection](#) összetevőt, akkor **AVG Internet Security 2011** a kockázati szint grafikus formában jelenik meg egy négyszintű skálán a gyanútól (■□□□) 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**

Vezérlogombok

A következő vezérlogombok 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

Az AVG frissítése kulcsfontosságú az újonnan megjelenő vírusok elleni védelemhez.

Mivel az AVG frissítések nem előre meghatározott ütemezés szerint jelennek meg, hanem az új fenyegetések mértéke és súlyossága alapján, ezért javasolt, hogy naponta legalább egyszer ellenőrizze a frissítéseket. Csak így biztosíthatja, hogy az **AVG Internet Security 2011** állandóan naprakész legyen.

12.1. Frissítési szintek

Az AVG kétféle frissítési szintet kínál:

- **Az adatbázisfrissítés** a vírusok 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](#) meg lehet adni, hogy a program mely szintű frissítéseket töltsse le és alkalmazza.

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

12.2. A frissítés típusai

A frissítéseket két csoportba sorolhatjuk:

- **Az azonnali frissítés.** az AVG rögtön végrehajtott frissítése, amelyet bármikor el lehet indítani, amikor csak szükséges
- **Ütemezett frissítés** - Az AVG programban be lehet állítani egy [előre meghatározott frissítési tervet](#) is. A program a megadott beállítás alapján rendszeresen végrehajtja a tervezett frissítést. Valahányszor új frissítési fájlok jelennek meg a megadott helyen, azok akár közvetlenül az internetről, vagy a hálózati meghajtóról telepíthetőek a beállításoknak megfelelően. Ha nem érhető el az utoljára telepítettnél újabb frissítés, akkor semmi sem történik.

12.3. Frissítési folyamat

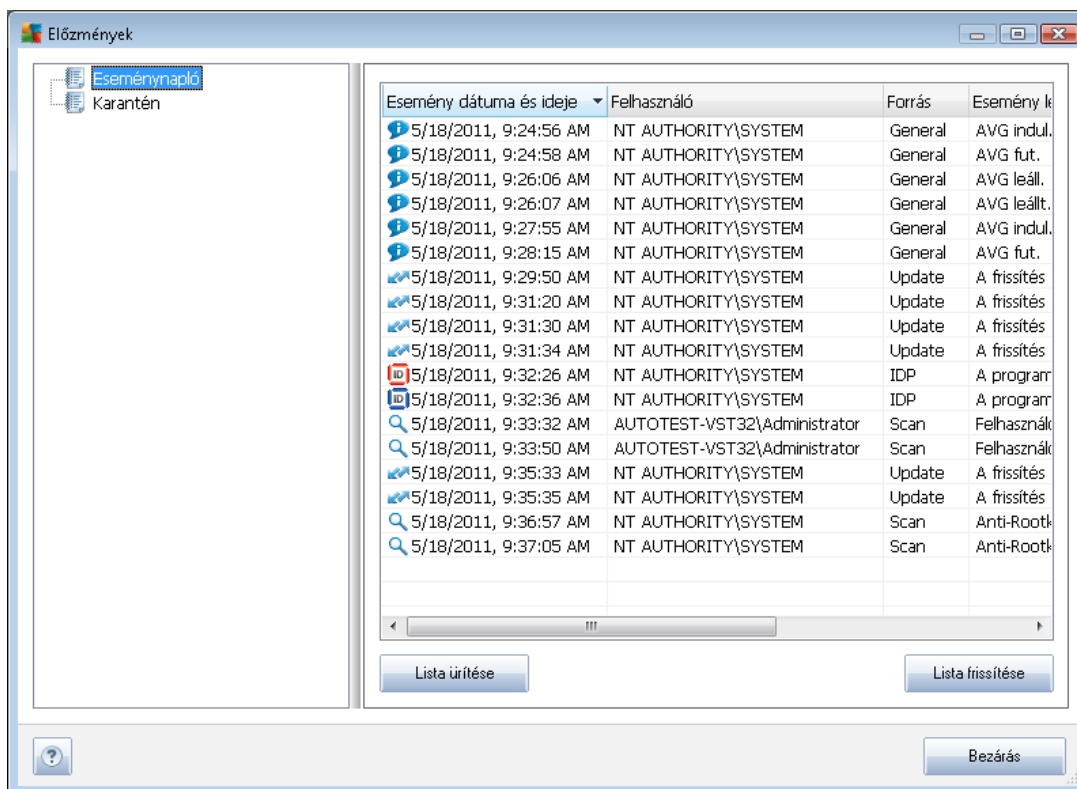
A frissítési folyamatot indíthatja azonnal manuálisan a **Frissítés mostgyorsgombbal**. A gomb mindig elérhető bármely [AVG felhasználói felület](#) ablakból. Azonban különösen ajánlott a rendszeres frissítések használata a [Frissítéskezelő](#) összetevő ütemezett frissítései segítségével.

Amikor elindítja a frissítést, az AVG eloszór ellenőrzi, hogy vannak-e új elérhető frissítési fájlok. Ha igen, az AVG elkezd letölteni őket és elindítja a frissítési folyamatot. A frissítési folyamat során a **Frissítés** felületre kerül, ahol ellenőrizheti a folyamat állapotát grafikus illetve statisztikai paraméterek formájában (a frissítési fájl mérete, fogadott adatok, letöltési sebesség, eltelt idő, ...).



Megjegyzés: Mielott az AVG programfrissítés elindul, egy rendszer-visszaállítási pont jön létre. 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. Csak tapasztalt felhasználók számára javasolt.

13. Esemény elozmények



Az **Elozmenyek** panel elérhető a [rendszermenü](#) az **Elozmenyek/Eseménynapló** elemen keresztül. Ezen a panelen az **AVG Internet Security 2011** 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 kezdete, vége és leállítása (az *automatikus vizsgálatokat is beleértve*)
- A vírusészleléshez kapcsolódó események és helyek (az [Állandó védelem](#) vagy [vizsgálat](#))
- Egyéb jelentős események.

Az egyes eseményeknél a következő adatok találhatóak:

- A **Dátum és idő** az esemény bekövetkezésének pontos dátumát és idejét mutatja
- A **Felhasználó** megmutatja, hogy ki kezdeményezte az eseményt
- A **Forrás** megmutatja a forrás összetevőt vagy az AVG rendszer azon részét, amely kiváltotta az eseményt



- **Az Esemény leírása** röviden leírja, hogy mit történt

Vezérlogombok

- **Lista ürítése** - törli az összes eseményt a listából
- **Lista frissítése** - frissíti az összes eseményt a listában



14. Gyakori kérdések és technikai támogatás

Ha az AVG termékkel üzleti vagy muszaki problémája adódik, akkor tájékozódjon a **GYIK** részben az AVG weboldalán (<http://www.avg.hu/>).

Ha ezen a módon nem talál megfelelő segítséget, lépjen kapcsolatba a technikai ügyfélszolgálattal emailben. Használja a rendszermenübol elérhető kapcsolatfelvételi urlapot (**Súgó / Online súgó**).